

**UNIVERSIDAD DON BOSCO  
FACULTAD DE INGENIERIA  
ESCUELA DE COMPUTACIÓN**



**“DISEÑO Y DESARROLLO DE UN SISTEMA DE INFORMACION  
DISTRIBUIDO PARA EL APOYO A LA AUDITORIA DE SISTEMAS”**

**TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE  
INGENIERO EN CIENCIAS DE LA COMPUTACIÓN**



**PRESENTADO POR:  
FREDY GERARDO BELTRAN SORTO  
WILLIAM BALMORE LOPEZ AMAYA**

**ABRIL DE 2008  
CIUDADELA DON BOSCO, EL SALVADOR, CENTROAMÉRICA**

**UNIVERSIDAD DON BOSCO  
FACULTAD DE INGENIERIA**



**ING. FEDERICO MIGUEL HUGUET RIVERA  
RECTOR**

**LIC. MARIO RAFAEL OLMOS  
SECRETARIO GENERAL**

**ING. ERNESTO GODOFREDO GIRÓN  
DECANO DE LA FACULTAD DE INGENIERÍA**



**ING. HERNÁN ARÉVALO**  
ASESOR

**ING. RAÚL MARTÍNEZ**  
TUTOR

**ING. MIGUEL BARAHONA**  
JURADO

**ING. JAIME ANAYA**  
JURADO

**ING. ALBERTO DAVILA**  
JURADO

## AGRADECIMIENTOS

En primer lugar a Dios Todopoderoso por darme la vida, la energía y la sabiduría necesaria para llegar al final de mi carrera Universitaria. Es una bendición que he recibido y que he logrado gracias a su bondad infinita.

Sin lugar a duda, a mis padres, William y Alba por haberme apoyado constantemente desde el inicio en todos los sentidos y dimensiones. Les agradezco grandemente y les dedico este triunfo.

A mi hermana Iris, por acompañarme en algunas noches de desvelo haciendo sus trabajos de universidad.

A mis abuelos, Natalia y Miguel, por tenerme siempre en sus oraciones en cada prueba y logro que he tenido en mi vida.

A mis tíos Daysi, Lilian, Nelson y Nohemí, por su cariño, disposición a ayudarme en todo momento, por confiar en mí y llevarme en sus oraciones, a quienes agradezco mucho.

A mis primos, Jese, Nereyda, Judith Nohemí, Eliseo e Isaac, por brindarme su apoyo incondicional y por sus buenos deseos en todas las metas que me he propuesto y he logrado.

A Judith, por su amor y paciencia que me tuvo durante el desarrollo de la tesis.

A mi compañero de tesis Fredy Gerardo por ser un excelente compañero y amigo, aunque tuvimos muchas dificultades pero pudimos salir adelante gracias a su tolerancia y comprensión.

Al comité evaluador, Ing. Raúl Martínez, Ing. Hernán Arévalo, Ing. Miguel Barahona, Ing. Jaime Anaya e Ing. Alberto Dávila, por confiar en nosotros y ser objetivos a la hora de la evaluación.

A todos los que estuvieron involucrados indirectamente en esta tesis y los que estuvieron pendientes de mis defensas. Muchísimas gracias por todo.

**William Balmore López Amaya.**

## **AGRADECIMIENTOS**

Mis más sinceros agradecimientos

A nuestro Señor y la Virgen María, por haberme guiado en este camino que hemos tenido que recorrer, iluminándonos en los momentos más difíciles y obsequiándonos paciencia, sabiduría y humildad para enfrentar todos los retos que se nos presentaron a lo largo de este trabajo de graduación.

A mis padres José Alfredo y María Alicia, por apoyarme y amarme en todos los momentos de mi vida y por no dejar de creer en mí en ningún momento, ayudándome de esta manera a nunca desistir de mis sueños.

A mi hermano José Luís, por su cariño, disposición a ayudarme en todo momento y por sus deseos en todas las metas que me he propuesto y he logrado.

A mis tías Carmela y Nena, porque siempre me han tenido en sus oraciones contantes, a quienes dedico este trabajo de graduación como muestra de mi amor por ellas.

A mis amigos y compañero de Tesis William López, por haber compartido sus conocimientos y de esta manera haber finalizado nuestro Trabajo de Graduación.

A Mayra por su apoyo constante en parte del proceso, su colaboración incondicional ha sido muy importante.

Al comité evaluador, Ing. Raúl Martínez, Ing. Hernán Arévalo, Ing. Miguel Barahona, Ing. Jaime Anaya e Ing. Alberto Dávila, por confiar en nosotros.

A todos los que estuvieron involucrados indirectamente en todo el proceso. Muchísimas gracias por todo.

**Fredy Gerardo Beltrán Sorto.**

# INDICE

Introducción.....	i
<b>Capítulo I. Marco Referencial</b>	
1. Antecedentes.....	1
2. Importancia de la investigación.....	4
2.1 Planteamiento del problema.....	4
2.2 Definición del tema.....	6
2.3 Justificación.....	7
3. Objetivos.....	8
3.1 General.....	8
3.2 Específicos.....	8
4. Alcances.....	9
5. Limitaciones.....	10
6. Marco Teórico.....	11
6.1 Situación Actual.....	11
6.1.1 Procedimientos de Auditoría.....	11
6.1.2 Proceso de Auditoría.....	12
6.1.3 Auditoría Asistida por Computadoras.....	13
7. Marco Conceptual.....	14
7.1 Generalidades Teóricas.....	14
7.1.1 Auditoría.....	14
7.1.2 Clases de Auditoría.....	14
7.1.2.1 Auditoría Informática.....	14
7.1.2.1.1 Tipos de Auditoría en Informática.....	15
a. Producción o Explotación.....	15
b. Desarrollo de Proyectos.....	15
c. Auditoría de Sistemas.....	15
d. Comunicación y Redes.....	17
e. Seguridad Informática.....	17
f. Aplicaciones en Internet.....	17
7.1.3 Tecnología de Información.....	18
7.1.4 Normas Generales de Auditoría de Sistemas.....	18
7.1.4.1 COBIT.....	18
7.1.4.2 ISACA.....	19
7.2 Generalidades Técnicas.....	19
7.2.1 Técnicas y Herramientas Utilizadas en Auditoría.....	19
7.2.1.1 Técnicas.....	19
7.2.1.2 Herramientas.....	19
7.2.1.2.1 Tipos de Software utilizados por Auditores.....	20
8. Marco Experimental.....	21
8.1 Software para el Apoyo de Auditoría a nivel Internacional.....	21
9. Plan de Solución.....	25
9.1 Desarrollo de la Investigación.....	25
9.2 Planificación del Proyecto.....	25
9.3 Definición de la Estructura del Sistema.....	25

9.4	Diseño de la Base de Datos.....	26
9.4.1	Análisis del Diseño.....	26
9.4.2	Selección del Sistema Gestor de Base de Datos.....	26
9.4.3	Diseño de la Base de Datos.....	26
9.5	Diseño del Sistema.....	26
9.6	Evaluación del Sistema.....	27
9.7	Depuración del Sistema.....	27
9.8	Documentación.....	27
9.8.1	Manual del Administrador.....	27
9.8.2	Manual del Usuario.....	27
10.	Presupuesto.....	28
10.1	Recursos de Desarrollo del Proyecto.....	28
10.2	Gastos Administrativos.....	29
10.3	Presupuesto sin Recurso de Hardware y Software.....	29
10.4	Presupuesto de Implementación.....	29

## Capítulo 2. Metodología de la Investigación

11.	Tipo de Investigación.....	30
11.1	Documental.....	30
11.2	Investigación Aplicada.....	30
11.3	Técnicas y Herramientas de Investigación.....	31
11.3.1	Recolección de la Información.....	31
11.3.2	Entrevistas.....	32
12.	Ciclo de Vida del Sistema.....	33
12.1	Investigación Preliminar.....	33
12.2	Análisis del Sistema.....	33
12.2.1	Determinación y Definición de Requerimientos.....	33
12.3	Diseño del Sistema.....	33
12.4	Desarrollo del Sistema.....	34
12.5	Evaluación y Seguimiento del Sistema.....	34
13.	Metodología de Desarrollo.....	34
13.1	Técnicas de Diseño de SI.....	34
13.1.1	Diagrama de Flujo de Datos(DFD).....	34
13.1.2	Diagrama Entidad Relación(ER).....	34
13.1.3	Diccionario de Datos.....	35

## Capítulo 3. Situación Actual

14.	Estudio de la Situación Actual.....	36
14.1	Valoración de la Situación Actual.....	36
14.1.1	Descripción de la Situación Actual.....	36
14.2	Sistemas de Información Existentes.....	38
14.2.1	Descripción de la Situación Actual.....	38
15.	Procedimientos.....	39
15.1	Metodología de Desarrollo en Auditoría de Sistemas.....	39
16.	Catálogo de Usuarios.....	43
16.1	Usuarios Involucrados en Auditoría de Sistemas.....	43
16.1.1	Auditor Informática General.....	43
16.1.2	Usuarios de los SI.....	43
16.1.3	Coordinadores Asignados.....	43

## Capítulo 4. Desarrollo del Sistema

17. Planificación del Sistema.....	44
17.1 Requerimientos o Requisitos Generales.....	45
17.2 Definición de la Arquitectura Tecnológica.....	45
17.2.1 Arquitectura Web.....	45
17.2.2 Arquitectura Cliente-Servidor.....	46
17.2.3 Selección de la Arquitectura Tecnológica.....	47
17.3 Entorno de Implementación del Sistema.....	47
17.4 Identificación de Subsistemas de Análisis.....	48
17.4.1 Parametrización del Sistema.....	48
17.4.1.1 Proceso de Conexión a la Base de Datos.....	49
17.4.2 Catálogo Maestros.....	50
17.4.3 Seguridad.....	50
17.4.4 Inicialización de Auditoría.....	50
17.4.5 Estudio Preliminar.....	51
17.4.6 Recursos.....	51
17.4.7 Planificación.....	52
17.4.8 Consultas o Seguimiento.....	52
17.5 Estructura de Seguridad del Sistema.....	53
17.5.1 Perfiles de usuario.....	53
17.5.2 Procedimiento de administración.....	54
18. Análisis del Sistema.....	55
18.1 Diagrama de Flujo de Datos.....	55
18.2 Descripción de los Diagramas de Flujo.....	56
18.2.1 Diagrama de Contexto.....	56
18.2.2 DFD Nivel 0.....	57
18.2.3 DFD Módulo de Configuración Auditoría.....	57
18.2.3.1 Tabla Descriptiva de Procedimientos.....	58
18.2.4 DFD Módulo de Inicio de Auditoría.....	59
18.2.4.1 Tabla Descriptiva de Procedimientos.....	60
18.2.5 DFD Módulo Recursos y Planificación.....	60
18.2.5.1 Tabla Descriptiva de Procedimientos.....	61
18.2.6 DFD Módulo Desarrollo e Informe.....	62
18.2.6.1 Tabla Descriptiva de Procedimientos.....	62
18.3 Modelo Conceptual de Datos.....	64
18.4 Modelo Lógico de Datos.....	65
19. Diseño del Sistema.....	74
19.1 Diseño de la Arquitectura del Sistema.....	74
19.1.1 Importancia de la Arquitectura.....	75
19.2 Descripción del Software a utilizar.....	77
19.2.1 Internet Information Server.....	77
19.2.2 Windows Server 2003.....	78
19.2.2.1 Características.....	79
19.2.3 Microsoft SQL Server 2005.....	80
19.2.3.1 Arquitectura Cliente-Servidor.....	81
19.2.3.2 RDBMS.....	82
19.2.3.3 Transact SQL.....	82
19.2.4 ASP .Net.....	83
19.3 Ventajas y Desventajas de Software utilizado.....	85
19.3.1 Internet Information Server.....	85
19.3.2 Principales Razones para ocupar Windows 2003.....	85
19.3.3 SQL Server 2005.....	87

19.3.3.1 Plataformas para SQL 2005.....	87
19.3.3.2 Integración de SQL con Microsoft Windows.....	87
20. Diseño de la Base de Datos.....	89
20.1 Entidad Relación.....	90
20.2 Descripción por Módulos de la Base de Datos.....	90
20.2.1 Módulo de Inicio y Parametrización de Catálogos.....	90
20.2.2 Módulo de Inicialización de Auditoría.....	92
20.2.3 Módulo de Estudio Preliminar y Recursos.....	93
20.2.4 Módulo de Planificación.....	94
20.2.5 Módulo de Desarrollo y Seguimiento.....	95
20.3 Diccionario de Datos.....	96
20.4 Diseño de la Interfase Web.....	119
20.4.1 Interfase Web.....	120
20.4.1.1 Panel Parametrización del Sistema.....	122
20.4.1.2 Panel Seguridad.....	123
20.4.1.3 Panel Inicialización Auditoría.....	129
20.4.1.4 Panel Catálogos Maestros.....	136
21. Conclusiones.....	155
22. Recomendaciones.....	156
Glosario.....	157
Fuentes de Información.....	163
Anexos	

# INTRODUCCION

La tesis que se presenta trata sobre el desarrollo de una herramienta de software que asiste al auditor de sistemas en el proceso de auditoría. El desarrollo de la misma se base en herramientas Microsoft como ASP .Net y Microsoft SQL Server 2005, siendo su acceso a través de un navegador web.

El trabajo tiene como objetivo fundamental el de brindar una herramienta software que asista al auditor de sistemas desde el punto de vista metodológico, en todas las fases de su trabajo.

El trabajo está dirigido fundamentalmente a ingenieros del software, auditores de sistemas, profesionales del área de sistemas, y cátedras universitarias vinculadas a la auditoría de sistemas y la ingeniería del software. Esta tesis puede tomarse como material de referencia para la adopción de buenas prácticas en la auditoría de sistemas.

El documento está organizado en 4 capítulos y anexos, cada capítulo está compuesto por temas específicos:

**Capítulo 1. Marco Referencial.** Presenta el tema de la tesis, los destinatarios de la misma y la manera en que está organizado el documento, incluye también un panorama de la actual situación relacionada con la auditoría de sistemas, se hace descripción del problema identificado, una exploración de los objetivos de la tesis, se justifica la realización, se trazan los alcances en los que se regirá la tesis y los procesos que no realizará el sistema.

**Capítulo 2. Metodología de Investigación.** Se aplican técnicas de investigación que son utilizadas según los requerimientos, condiciones y características del objeto de estudio.

**Capítulo 3. Situación Actual.** Incluye un panorama de la actual situación relacionada con la auditoría de sistemas, especificando el contexto en el que se desarrolla la tesis.

**Capítulo 4. Desarrollo del Sistema.** Comprende la planificación, análisis, diseño y desarrollo del sistema.

# CAPÍTULO I. MARCO REFERENCIAL

## 1. Antecedentes

Durante el tiempo se ha observado el interés y necesidad de implementar tecnología de información(TI) para agilizar los procesos en las organizaciones y empresas, convirtiéndose en una estrategia competitiva en general. Esto trajo como consecuencia que se destinara capital para obtener tecnología reciente y costosa.

La adquisición de una nueva tecnología implica un riesgo de inversión, ya sea porque son mal administradas ó no son las adecuadas para satisfacer los objetivos del negocio.

Las organizaciones y empresas necesitan gestionar de una forma óptima todos los recursos que poseen; para cumplir los objetivos propuestos se necesita una reingeniería de las operaciones empresariales que tiene como ingrediente clave las tecnologías de información, rescatando así un papel importante en el respaldo de cambios innovadores del diseño de flujo de trabajo en las operaciones.

La tecnología de información puede utilizarse para mejorar estratégicamente la calidad del desempeño empresarial.

Dos organizaciones internacionales ISACA<sup>1</sup> e ISACF<sup>2</sup> empezaron a observar la importancia que tiene el buen uso de las TI, concluyeron que son la base fundamental para el éxito de un negocio, dedicándose además a ampliar la conciencia acerca de la necesidad y beneficio de un manejo adecuado de la TI.

La ISACF desarrolló un conjunto común de conceptos sobre la materia, denominado COBIT; el cual es un sistema internacional aceptado para el control de TI que

---

<sup>1</sup> Asociación de auditoría y control de sistemas de información, creada en 1979 por la ISACF

<sup>2</sup> Fundación de auditoría y control de sistemas de información, fundada en 1976.

permite a las organizaciones implementar una estructura para su manejo. Este integra y concilia normas existentes tales como: ISO 9000-3<sup>3</sup> y COSO<sup>4</sup>.

A nivel internacional se han desarrollado herramientas para el gerenciamiento, el control, la auditoría y el aseguramiento de la calidad en la tecnología de información basadas en normas COBIT.

El desarrollo de tecnologías de información en los últimos años ha sido constante, considerada como una evolución tecnológica. Hoy en día, la mayoría de organizaciones consideran que la información y su tecnología asociada representan uno de sus activos más importantes<sup>5</sup>.

Para tener un mejor control sobre sus tecnologías de información específicamente sobre los sistemas de información, las organizaciones se apoyan de la auditoría en sistemas, siendo la auditoría en sistemas “el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación de los sistemas de información en la empresa”.

La auditoría en sistemas fundamentalmente garantiza el correcto funcionamiento de los sistemas proporcionando los controles necesarios que permitan garantizar la seguridad, integridad, disponibilidad y confiabilidad de los mismos. En este proceso se involucra a los auditores de sistemas que examinan y evalúan el desarrollo, implementación, mantenimiento y operación de los componentes que forman los sistemas. La opinión profesional, es un elemento esencial de la auditoría, se fundamenta y justifica por medio de procedimientos específicos tendentes a proporcionar una seguridad razonable de lo que se afirma.

---

<sup>3</sup> Normas de administración y garantía de calidad definidas por la ISO

<sup>4</sup> Comité de Organizaciones Patrocinantes de la Comisión Treadway

<sup>5</sup> Véase definición “Tecnologías de Información” en el glosario, página No. 161

Por otra parte las organizaciones requieren establecer en función de la auditoría en sistemas los siguientes factores<sup>6</sup> :

- Necesidad de control en un ambiente de constante aumento en el uso de la tecnología de información y abuso en la utilización de los recursos tecnológicos.
- Riesgo de enfrentar una pérdida de la capacidad de procesamiento informático y su correspondiente funcionalidad.
- Riesgo de tomar decisiones incorrectas si la información mantenida y proporcionada por las aplicaciones informáticas es incorrecta.
- Riesgo de enfrentar problemas operativos y hasta legales a consecuencia de procedimientos incorrectos en los sistemas informáticos.
- Necesidad de garantizar que se mantiene la seguridad y privacidad de la información.

A causa del impacto creciente de la información y la tecnología relacionada en las organizaciones, la auditoría en sistemas de información se hace cada vez más importante y solo puede ser vista y ejecutada como una disciplina independiente en las organizaciones y empresas de cualquier tamaño<sup>7</sup>.

---

<sup>6</sup> Taller de Auditoría de Sistemas, Corte de Cuentas de la República de el Salvador, C.A, 2005

<sup>7</sup> “Auditing Information System”, Mario Piattini, Editorial Idea Group Publishing, 2000

## **2. Importancia de la Investigación**

### **2.1 Planteamiento del Problema**

La auditoría de sistemas se puede definir como el proceso de revisión y evaluación, parcial o completo de los aspectos relacionados con el procesamiento automatizado de la información<sup>8</sup>. En este proceso se aplican métodos, técnicas y procedimientos para evaluar los recursos de la tecnología de la información.

La auditoría de sistemas comprende la evaluación formal y sistemática de todos los elementos relacionados con la tecnología de la información(TI), como: los datos, los sistemas de aplicación, la tecnología, las instalaciones, la gente; con el objetivo de garantizar el cumplimiento de las normas y procedimientos establecidos por la empresa en todo lo relacionado con la información y la tecnología de la información, de manera de minimizar los riesgos que amenacen la efectividad y eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información.

A la hora de realizar una auditoría de sistemas los profesionales responsables de esta actividad se encuentran con algunos de los siguientes problemas:

- Un importante porcentaje de profesionales que realizan esta tarea no son expertos en la misma, muchos de ellos realizan sus actividades en forma aislada, sin contacto con otros profesionales especialistas en la actividad.
- Desconocimiento de metodologías, técnicas y herramientas utilizadas para el proceso de auditoría de sistemas.
- Desconocimiento de estándares utilizados en el proceso de auditoría de sistemas.

---

<sup>8</sup> <http://www.isaca.org>

- La mayoría de auditorías de sistemas realizadas en la actualidad no utilizan herramientas software que asistan integralmente a los auditores de sistemas en su tarea.
- El proceso de adaptación de la planificación y ejecución de un proceso de auditoría de sistemas a organizaciones y empresas en particular se relaciona con la experiencia del auditor, sin que el mismo pueda utilizar herramientas que lo guíen en el proceso.

Los problemas antes descritos provocan en muchos casos auditorías de baja calidad que no cubren los objetivos previstos.

**¿Por qué es importante que al auditor de sistemas cuente con herramientas que le apoyen en el proceso de auditorías?**

Porque le permitirán mejorar la efectividad y eficiencia en los procedimientos de auditoría, además le pueden proporcionar pruebas de control efectivas y procedimientos sustantivos cuando no existan documentos de entrada o cuando la población y tamaños de muestra sean muy grandes.

**¿Por qué surge la necesidad por parte de las empresas e instituciones en El Salvador de controlar sus sistemas informáticos a través de una auditoría?**

Surge, ya que necesitan incrementar la satisfacción de los usuarios de los sistemas, asegurar una mayor integridad, confidencialidad y confiabilidad de la información, para alcanzar el logro de sus objetivos y metas.

## 2.2 Definición del Tema

El proyecto propuesto se denomina **“DISEÑO Y DESARROLLO DE UN SISTEMA DE INFORMACION DISTRIBUIDO PARA EL APOYO A LA AUDITORIA DE SISTEMAS”**, consiste en la elaboración de un sistema informático bajo ambiente web.

El objetivo fundamental de dicho sistema es el apoyo al proceso de auditoría en lo relacionado con la determinación de alcances y objetivos, estudio preliminar, determinación de recursos necesarios, ejecución de auditorías y redacción del informe final.

## 2.3 Justificación

La realización de auditorías en forma sistemática y organizada, significa que toda las auditorías principalmente la de sistemas de información, son en la actualidad un proceso manual que requiere la mayor cantidad de tiempo para su planificación. El auditor de sistemas antes de ejecutar un plan elabora pápeles de trabajo de forma manual con el objetivo de respaldar de manera detalla la descripción de las pruebas realizadas.

El sistema de información distribuido servirá de apoyo al auditor de sistemas en el proceso de planificación de auditorías, permitirá la elaboración de cuestionarios y listas de verificación. Desde el sistema se tendrá una clasificación por área de los cuestionarios y listas de verificación básicos que se encontraran previamente ingresados, servirán como guía de orientación metódica para la creación y modificación de cuestionarios de acuerdo al área de sistemas que se auditará.

Mediante el sistema, el cliente y el auditor de sistemas, tendrán la posibilidad de visualizar la información en reportes para dar seguimiento a las auditorías que están en proceso, se tendrá la ventaja de realizar la actualización de los cuestionarios y listas de verificación diseñados para las auditorías.

### **3. Objetivos**

#### **3.1 General**

Desarrollar un sistema de información que sirva de apoyo en el proceso de auditoría de sistemas, permitiendo la determinación de alcances, objetivos, estudio preliminar, planificación y desarrollo, considerando estándares existentes.

#### **3.2 Específicos**

- Automatizar una metodología que será aplicada al proceso de auditoría en sistemas.
- Asistir al auditor en las diferentes fases que conforman una auditoría en sistemas.
- Incorporar normas generales(COBIT) al proceso de auditoría en sistemas generado desde el sistema.
- Crear cuestionarios y listas de verificación personalizados, aplicados a auditorías en sistemas específicas.
- Brindar al auditor de sistemas dos alternativas para realizar una auditoría en sistemas, ya sea por áreas específicas o utilizando objetivos de control.
- Sugerir cuestionarios específicos de auditoría en sistemas que ayudarán a definir alcances, objetivos de una auditoría, la estructura o elementos de la auditoría, los recursos necesarios para la realización de la auditoría y un plan de trabajo tentativo.

#### 4. Alcances

- Deberá contemplar en forma completa la aplicación de una metodología que será utilizada y automatizada mediante el sistema para el desarrollo de auditorías en sistemas.
- Servirá como un asistente en el proceso de realización de auditorías en sistemas.
- En cada uno de los módulos que tendrá el sistema se podrá:
  - ✓ Definir el alcance y objetivos del proceso de auditoría.
  - ✓ Desarrollar el estudio preliminar en función del alcance de la auditoría planteada.
  - ✓ Definir los recursos necesarios para realizar la auditoría.
  - ✓ Desarrollar una planificación acorde con el alcance de la auditoría, las características de la empresa a auditar y el personal asignado a la tarea.
  - ✓ Desarrollar una auditoría considerando el alcance, las características de la empresa a auditar, los recursos asignados y la planificación realizada.
  - ✓ Realizar el informe final de la auditoría considerando las recomendaciones que surgen por parte del auditor a partir de las respuestas de los cuestionarios y listas de verificación realizados durante la auditoría.
- Tendrá un acceso selectivo para cada uno de los 34 procesos de COBIT, permitiendo incluirlos en la auditoría a ejecutar.
- Se tendrá a disposición una serie de cuestionarios y listas de verificación, pudiendo el auditor de sistemas modificarlos y adaptarlos a sus necesidades.
- Elección de realizar auditorías en sistemas ya sea por áreas o por objetivos de control(COBIT).

## **5. Limitaciones**

- Se desarrollará una primera versión del sistema, por lo tanto no se ha contemplado actividades relacionadas con el mantenimiento del sistema.
- La etapa de implementación solamente contemplará las pruebas del sistema, la configuración del hardware y software para su demostración.
- El sistema no se desarrollará para una empresa u organización en particular por lo tanto no se realizará un plan de sistemas de información aplicado a una empresa u organización en específica.
- El sistema no poseerá capacidades de decisión respecto al análisis de la información obtenida. Los datos, reportes y estadísticas que genere servirán como base para que el auditor en sistemas elabore el informe final de auditoría, y no será tarea del sistema.

## **6. Marco Teórico**

### **6.1 Situación actual**

#### **6.1.1 Procedimientos de Auditoría**

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias, la opinión profesional es el elemento esencial de la auditoría, se fundamenta y justifica por medio de unos procedimientos específicos tendentes a proporcionar una seguridad razonable de lo que se afirma.

Como es natural, cada una de las clases o tipos de auditoría poseen sus propios procedimientos para alcanzar el fin previsto aun cuando puedan en muchos casos coincidir. El alcance de la auditoría viene dado por los procedimientos, la amplitud y profundidad de los procedimientos que se apliquen nos definen su alcance. En las auditorías altamente reglamentadas como la financiera es perceptivo aplicar las normas y técnicas para decidir los procedimientos de auditoría. Cualquier limitación que impida la aplicación de lo dispuesto en las técnicas debe ser considerada en el informe de auditoría como una reserva al alcance.

Se pretende garantizar que se toman en consideración todos los aspectos, áreas, elementos, operaciones, circunstancias que sean significativas. Para ello se establecen normas y procedimientos que en cuanto a la ejecución de la auditoría se resumen en:

- El trabajo se planificará apropiadamente y se supervisará adecuadamente.
- Se estudiará y se evaluará el sistema de control interno.
- Se obtendrá evidencia suficiente y adecuada.

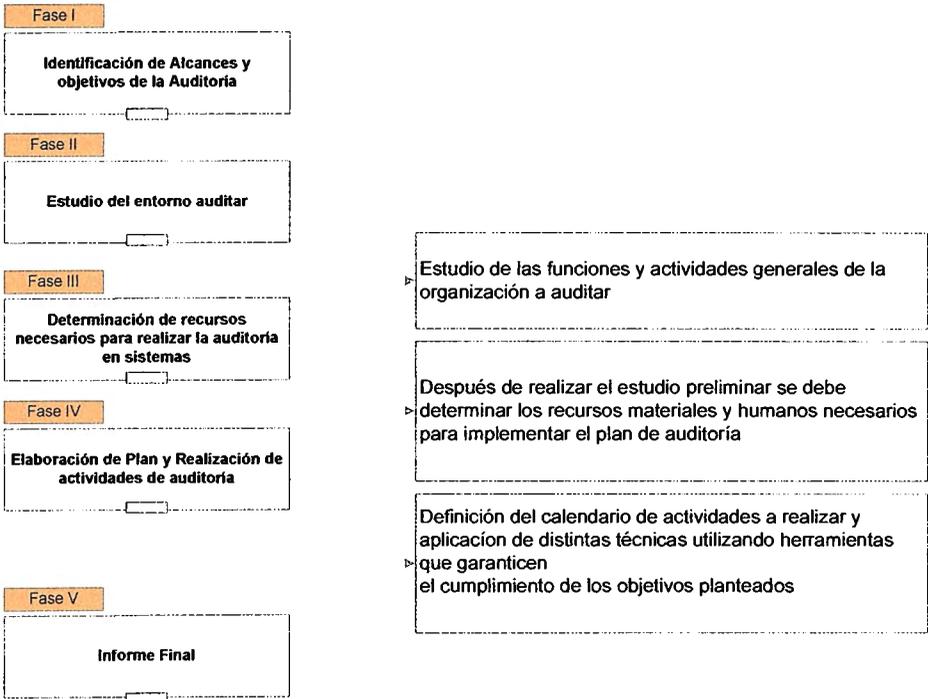
La evidencia obtenida deberá recogerse en los papeles de trabajo del auditor como justificación y soporte del trabajo efectuado y la opinión expresada. Con la introducción de la tecnología de la información en los sistemas, esto impone un

nuevo condicionamiento al auditor, el de trabajar con elementos de tecnología de la información dado que según las propias normas técnicas de auditoría el auditor ha de tener en cuenta todos los elementos de la entidad incluso los informáticos. Actualmente los libros o soporte de los documentos financieros objeto de la labor del auditor en un entorno informatizado están materializados hoy en día en archivos electrónicos.

El auditor financiero ve alterado el objeto de su actividad en el sentido que se ha introducido la TI, ha de cambiar sus procedimientos en función de las nuevas circunstancias y por tanto la expansión de su alcance. La propia TI que incide en los procedimientos que el auditor ha de aplicar proporciona paralelamente medios de ejecutarlos de forma eficiente y directa.

### 6.1.2 Proceso de Auditoría

El proceso de auditoría consiste en la obtención y evaluación de evidencias con la finalidad de proporcionar en forma detallada un informe de auditoría, el esquema 1 detalla las fases y etapas a seguir en el proceso de una auditoría.



**Esquema 1.** Fases a seguir en el proceso de una auditoría.

### 6.1.3 Auditoría Asistida por Computadoras

Las técnicas de auditoría asistida por computadora son importantes para el auditor de TI cuando se realiza una auditoría. Las CAATS ponen a disposición del auditor una amplia variedad de herramientas que no sólo posibilitan los nuevos procedimientos sino que mejoran sensiblemente su aplicación y amplían la gama disponible, por lo tanto la introducción de la TI en los sistemas de información afectan a los auditores de dos formas:

- Cambia el soporte del objeto de su actividad.
- Posibilitan la utilización de medios informatizados (CAATS) para la realización de sus procedimientos.

Las herramientas y técnicas que más se utilizan son software de auditorías generalizadas, software utilitario, los datos de prueba y sistemas expertos de auditoría. Las CAATS se pueden utilizar para realizar varios procedimientos de auditoría como los siguientes:

- Prueba de los detalles de operaciones y saldos.
- Procedimientos de revisión analíticos.
- Pruebas de cumplimiento de los controles generales de sistemas de información.
- Pruebas de cumplimiento de los controles de aplicación.

## 7. Marco Conceptual

### 7.1 Generalidades Teóricas

Para entender el entorno del proyecto, se definen los siguientes conceptos:

#### 7.1.1 Auditoría

Conceptualmente la auditoría, es la actividad consistente en proporcionar una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar cumple las condiciones que le han sido prescritas<sup>9</sup>.

#### 7.1.2 Clases de Auditoría

En el siguiente cuadro se definen los tipos de auditoría, el objeto y finalidad de estas:

Clase	Contenido	Objeto	Finalidad
Financiera	Opinión	Cuentas anuales	Presentan realidad
Informática	Opinión	Sistemas de aplicación, recursos informáticos, planes de contingencia, etc.	Operatividad eficiente y según normas establecidas.
Gestión	Opinión	Dirección	Eficiencia, eficacia, economicidad.
Cumplimiento	Opinión	Normas establecidas	Las operaciones se adecuan a estas normas

Tabla 1. Cuadro conceptual de clases de auditoría.

##### 7.1.2.1 Auditoría Informática

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

---

<sup>9</sup> “Auditoría Informática – Un enfoque práctico” Piattini Mario, Editorial RA-MA, Segunda Edición

### **7.1.2.1.1 Tipos de Auditoría en Informática**

En la actualidad se han establecido principales divisiones de la auditoría informática, las cuales son: Explotación u Operación, Desarrollo de Proyectos, de Sistemas, de Comunicaciones, Redes y de Seguridad. La función de cada tipo se menciona a continuación:

#### **a) Producción o Explotación**

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

#### **b) Desarrollo de Proyectos**

La función de desarrollo es una evolución del llamado análisis y programación de sistemas, y abarca muchas áreas: prerequisites del usuario y del entorno, análisis funcional, diseño, análisis orgánico, pruebas, entrega a explotación o producción y alta para el proceso.

#### **c) Auditoría de Sistemas**

La auditoría de sistemas es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación de los sistemas de información en las empresas.<sup>10</sup>

---

<sup>10</sup> “Auditoría Informática” Gonzalo Alonso Rivas, Ediciones Díaz de Santos, Segunda Edición 1989

Los auditores de sistemas de información examinan y evalúan el desarrollo, implementación, mantenimiento y operación de los componentes de sistemas automatizados y sus interfaces con sistemas externos y no automatizados.

Los objetivos y prácticas de auditoría varían considerablemente de organización en organización y existen muchos tipos de practicantes envueltos en actividades relacionadas a la auditoría, ejemplo de ello son los auditores externos, auditores internos, evaluadores, verificadores de la calidad y asesores técnicos.

Los objetivos de la auditoría en sistemas son los siguientes:

- Evaluar la organización y gestión del área de tecnología de información para verificar que estén acorde con los objetivos y políticas de la empresa.
- Fiscalizar que las actividades informáticas se realicen mediante procedimientos establecidos, bien definidos y documentados, de forma tal que procuren un adecuado desarrollo y operación de los sistemas.
- Evaluar la adquisición y utilización eficiente de los recursos tecnológicos.
- Verificar que el desarrollo de sistemas satisfaga las necesidades de información, haciendo un uso eficiente y eficaz de los recursos tecnológicos.
- Evaluar los sistemas automatizados para que guarden la debida confiabilidad, seguridad, integridad y oportunidad de la información.
- Evaluar el acceso a los sistemas y bases de datos.
- Brindar asesoría en aspectos técnicos.

Los bienes a proteger por toda empresa o institución según COBIT:

- Datos, que son todos los objetos de la información.
- Aplicaciones, son el conjunto de sistemas de información.
- Tecnología, es el conjunto de hardware y software de base.
- Instalaciones, son los recursos necesarios para alojar a los sistemas de información.
- Recursos humanos, es el personal relacionado directamente con el desarrollo y producción de los sistemas de información.

#### **d) Comunicaciones y Redes**

Este tipo de revisión se enfoca en las redes, líneas, concentradores, multiplexores. La auditoría informática ha de analizar situaciones y hechos algunas veces alejados entre sí, y está condicionada a la participación de la empresa telefónica que presta el soporte. Para este tipo de auditoría se requiere un equipo de especialistas y expertos en comunicaciones y redes.

#### **e) Seguridad Informática**

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

Por su parte, la seguridad lógica se refiere a la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

#### **f) Aplicaciones en Internet**

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

- Evaluación de los riesgos de internet (operativo, tecnológico y financiero) y así como su probabilidad de ocurrencia.
- Evaluación de vulnerabilidades y la arquitectura de seguridad implementada.
- Verificar la confidencialidad de las aplicaciones y la publicidad negativa como consecuencia de ataques exitosos por parte de hackers.

### 7.1.3 Tecnología de Información

Una forma de denominar al conjunto de herramientas, habitualmente de naturaleza electrónica, utilizadas para la recogida, almacenamiento, tratamiento, difusión y transmisión de la información.

#### 7.1.4 Normas Generales de Auditoría de Sistemas

##### 7.1.4.1 COBIT (Control Objectives for Information and related Technology)

La misión y objetivos de COBIT es investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de la información (TI) con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores.

La *Information Systems Audit and Control Foundation* y los patrocinadores de COBIT, han diseñado este producto principalmente como una fuente de instrucción para los auditores en sistemas. COBIT ha sido desarrollado como estándares para mejorar las prácticas de control y seguridad de las TI que provean un marco de referencia para la administración, usuarios y auditores. COBIT define los siguientes elementos:

**Dominios:** Agrupación natural de procesos, definen cuatro: planificación y organización, adquisición e implementación, prestación y soporte, monitoreo. (Ver anexo B)

**Procesos:** Conjuntos o series de actividades unidas con delimitación o cortes de control. En cada proceso se definen objetivos de control. (Ver anexo B)

**Actividades:** Acciones requeridas para lograr un resultado medible. (Ver anexo B)

Se definen 34 objetivos de control generales, uno para cada proceso de las TI. Estos procesos están agrupados en cuatro grandes dominios.

### 7.1.4.2 ISACA

La **Information Systems Audit and Control Association (ISACA)** estableció un conjunto de normas generales para los sistemas de auditoría de la información.

## 7.2 Generalidades Técnicas

### 7.2.1 Técnicas y herramientas utilizadas en auditoría

#### 7.2.1.1 Técnicas

**Revisión:** análisis de la información obtenida tanto en el estudio inicial como en la propia auditoría, en general esta información es obtenida a través de cuestionarios y entrevistas.

**Entrevistas:** se trata de una de las actividades personales más importantes que realiza el auditor, esta técnica se basa fundamentalmente en la elaboración de preguntas al entrevistado, las entrevistas pueden tener diferentes estructuras que dependerán de los objetivos de la entrevista y el perfil del entrevistado.

**Observación:** donde el auditor observa en forma pasiva como se realizan las tareas.

#### 7.2.1.2 Herramientas

**Listas de verificación:** se trata de un conjunto de preguntas cerradas muy utilizadas en el proceso de auditoría que permiten obtener información tanto cualitativa como cuantitativa, destinada a determinar las fortalezas y debilidades de los sistemas de control.

### 7.2.1.2.1 Tipos de Software utilizados por el Auditor en Auditorías

- a) **Paquete de auditoría:** son programas generalizados de computadora diseñados para desempeñar funciones de procesamiento de datos que incluyen leer bases de datos, seleccionar información, realizar cálculos, crear archivos de datos e imprimir informes en un formato especificado por el auditor.

Son usados para control de secuencias, búsquedas de registros, detección de duplicaciones, detección de gaps, selección de datos, revisión de operaciones lógicas y muestreo, algunos de ellos son el IDEA, ACL.

- a) **Software para un propósito específico o diseñado a la medida:** son programas de computadora diseñados para desempeñar tareas de auditoría en circunstancias específicas. Estos programas pueden ser desarrollados por el auditor, por la entidad, o por un programador externo contratado por el auditor.

Por ejemplo programas que permitan generar listas de verificación adaptados a las características de la empresa y de los objetivos de la auditoría.

- b) **Programas de utilería:** son usados por la organización auditada para desempeñar funciones comunes de procesamiento de datos, como clasificación, creación e impresión de archivos. Como por ejemplo planillas de cálculo, procesadores de texto.

## **8. Marco Experimental**

En el proceso de auditoría existe software de apoyo para el desarrollo de la auditoría de sistemas entre los cuales podemos mencionar:

### **8.1. Software para el apoyo de Auditoría a nivel Internacional**

#### **a) Auditoría Laboral de Legalidad**

Software desarrollado en España en la ciudad de Barcelona, por la empresa de nombre Creinsa, S.A(Creaciones informáticas) este ha desarrollado un proyecto llamado Auditoría Laboral de legalidad. El sistema de auditorías socio-laboral mediante su base de datos de preguntas, documentos, contratos de trabajo, el auditor podrá realizar una investigación exhaustiva y emitir un informe sobre los estados laborales de la empresa.

**Algunas tareas que realiza el sistema son:**

- Revisión de los estados laborales de empresa, administraciones públicas, sindicatos y otros.
- Petición de documentos a revisar (hasta 40 documentos).
- Cuestionario o listas de verificación (216 preguntas).
- Control contratos de trabajo y control de certificados.

#### **b) Cynthus**

Cynthus es una empresa mexicana dedicada a la prestación de servicios profesionales y al desarrollo y comercialización de productos de software en áreas de competencia específica. El software llamado Working Paper un paquete de auditoría y de generación de estados financieros, Working Paper permite automatizar la metodología de trabajo para el desarrollo de auditorías financieras, operacionales.

El software permite generar programas de trabajo, oficios, documentos, informes y en general, crear toda una metodología de auditoría automatizada. Inclusive, permite implementar un marcador balanceado de auditoría para tener una verdadera posición de análisis directivo del avance y logros de los proyectos de auditoría en su organización.

#### **c) Meycor COBIT CSA (Control Self-Assessment)**

Software desarrollado en Uruguay, esta herramienta automatiza la evaluación de una organización contra los objetivos de control del marco COBIT, generando un diagnóstico y recomendaciones que facilitan la implementación de esos objetivos de control.

El software está basado en la 3ra. Edición de los objetivos de control de COBIT. No incluye las guías de auditoría de COBIT; pero provee un módulo de auditoría que permite la verificación de la veracidad y fiabilidad de las respuestas a los cuestionarios incorporados respecto del grado de cumplimiento con cada uno de los objetivos de control de COBIT. Este puede ser utilizado como una herramienta de autoevaluación enfocado a la Gerencia de TI, y permite obtener un diagnóstico de su situación actual y una serie de recomendaciones a seguir a fin de alcanzar un nivel deseable en cuanto a seguridad, calidad, eficacia y eficiencia de sus sistemas de información.

#### **d) Gesia 2000**

Software desarrollado en España por Audinfor S.L. los objetivos del GESIA 2000 es poner al alcance de los profesionales de la auditoría, y de forma muy especial de los responsables de despachos y firmas de auditoría, una herramienta que, acorde con las nuevas tecnologías, facilite su labor de organizar y controlar los trabajos.

### **e) ACL Edición de Escritorio / Red**

Desarrollado por ACL Services Ltd. ACL es la herramienta de software de auditoría preferida por la comunidad de auditoría interna internacional, para la extracción y el análisis de datos, la detección de fraudes y el control continuo. Al proporcionar una exclusiva y eficiente combinación de acceso a los datos, análisis y elaboración integrada de reportes, ACL permite transformar los datos en información significativa y asistirlo en el logro de objetivos comerciales para agregar valor a su organización.

### **f) COBIT 3rd EDITION Management Advisor**

Desarrollado en Costa Rica por MethodWare este software soporta análisis de brecha multinivel, permitiendo realizar un benchmark<sup>11</sup> efectivo de los procesos de TI y analizar resultados de evaluaciones actuales versus anteriores en una base de datos única. Con su sofisticada función de alerta, provee un rastreo instantáneo de las áreas que requieren seguimiento, asegurando la disposición de la máxima cantidad de información con el toque de un botón. COBIT 3rd EDITION Management Advisor permite:

- Incorporar sólo aquellas partes de la estructura COBIT que son relevantes para la revisión actual.
- Aplicar en forma consistente las guías Gerenciales de TI en toda su organización, utilizando como modelo base la estructura COBIT.
- Determinar y monitorear el nivel apropiado de seguridad y control de TI de su organización mediante las guías gerenciales.
- Contar con una interfaz completa con Microsoft Word y Excel para informes y análisis, y la habilidad de vincular cualquier documento existente, COBIT 3RD EDITION Management Advisor es una herramienta completa para los profesionales de TI.

---

<sup>11</sup> Véase definición “benchmark” en el glosario, página No. 158

### **g) COBIT Advisor 3rd. EDITION (Audit)**

COBIT Advisor 3rd. EDITION(Audit) provee una aplicación consistente de la estructura COBIT; aplicable a todo tipo de empresas. Entre sus muchos beneficios se encuentran:

- Seguir guías de las mejores prácticas para una administración efectiva de TI en la organización; aplica estas Guías de Auditoría de COBIT en un proceso comprensivo y consistente. Y asegura que éstas tienen como objetivo los procesos, criterios de información y recursos de TI más relevantes.
- Permitir incorporar sólo aquellas partes de la estructura COBIT que son relevantes para la revisión actual.
- Gastar más tiempo auditando y menos tiempo registrando.
- Provee informes estándar y ad-hoc y facilidades de representar en con gráficos las etapas del proceso de auditoría.
- Administrar las observaciones y recomendaciones de auditoría de SI en una base de datos única.

## **9. Plan de Solución**

El plan de solución o metodología del desarrollo del sistema son conceptos que han adoptado como referencia para el desarrollo de proyectos.

Para lograr lo anterior con efectividad, habrá de seguir un plan de acción basado en el ciclo de vida para el desarrollo de sistemas, en el se detallan los lineamientos generales y específicos para facilitar el desarrollo de la solución del sistema. El plan de solución para el desarrollo del proyecto planteado en este documento constará de las siguientes etapas:

### **9.1 Desarrollo de la Investigación**

El propósito de esta fase es recopilar toda la información que sea útil para el desarrollo del sistema. Este proceso involucra aspectos, como investigación general del problema, identificación de necesidades y documentación de apoyo.

### **9.2 Planificación del Proyecto**

La planificación del proyecto consiste en el proceso de las etapas del ciclo de vida de desarrollo, de manera más eficiente, tomando en cuenta los siguientes puntos: el trabajo que se ha de realizar, los recursos para llevarlo a cabo y el costo.

### **9.3 Definición de la Estructura del Sistema**

Se define en esta etapa, los límites de la aplicación en cuanto a los módulos que poseerá el sistema para satisfacer las necesidades planteadas en este documento. También se debe determinar quiénes son los usuarios, las áreas de aplicación y el entorno tecnológico.

## **9.4 Diseño de la Base de Datos**

La etapa consiste construir la estructura de la base de datos que procesará la información, además es la fase donde se implementa la investigación y planificación, mencionadas anteriormente. El diseño se divide en las siguientes etapas:

### **9.4.1 Análisis del Diseño**

Se hará una descripción de la solución que se desarrollará, se desglosarán los módulos principales del sistema, las entidades que van a interactuar y la forma cómo van a interactuar.

### **9.4.2 Selección del Sistema Gestor de Base de Datos (SGBD)**

El sistema gestor de base de datos (SGBD)<sup>12</sup> que se seleccionará para el diseño, será Microsoft SQL Server 2005, para desarrollar el diseño lógico de los datos.

### **9.4.3 Creación de la Base de Datos**

La construcción de la base de datos constará de tres partes importantes: diseño conceptual, diseño lógico y diseño físico

## **9.5 Diseño del Sistema**

Para realizar el diseño lógico y físico del sistema de información, es necesario cubrir los requerimientos que son necesarios para el desarrollo de éste, para el diseño del sistema se han determinado tres fases principales:

---

<sup>12</sup> Véase definición “Sistema Gestor de Base de Datos” en glosario, página No. 161

## **9.6 Evaluación del Sistema**

Consiste en la realización de pruebas para determinar el funcionamiento correcto del sistema desarrollado, la evaluación es una de las fases del ciclo de vida de sistemas que tiene como objetivo obtener fallas e inconsistencias en el sistema de información.

## **9.7 Depuración del Sistema**

Después de la Evaluación del sistema y obtenidas las fallas, comienza el proceso de depuración que consiste en incorporar nuevos requerimientos, si es necesario o corregir los módulos del sistema que en la fase anterior fue sometido a prueba.

## **9.8 Documentación**

Como parte del proyecto, se documentará la investigación, los diagramas de diseño elaborados, el diccionario de datos del sistema y además, se elaborarán los manuales de usuario y administrador para que puedan referirse cuando se presenten dudas de realizar una operación dentro del sistema de información. Entre los documentos más importantes están:

### **9.8.1 Manual del Administrador**

Este manual será una guía para el administrador de sistema, para poder realizar tareas administrativas del sistema.

### **9.8.2 Manual del Usuario**

Este manual será una guía que le permitirá al usuario comprender el funcionamiento del sistema.

## 10. Presupuesto

Para el desarrollo del sistema los costos económicos en los que se incurriría en todo el proceso se definen en las siguientes tablas:

### 10.1 Recursos de Desarrollo del Proyecto

El desarrollo del proyecto incluye, los presupuestos para personal, el software y hardware a utilizar.

<b>Recurso de Personal</b>	<b>Sueldo Mensual(\$)</b>	<b>Sueldo Total(\$)</b>
Programadores (2)	\$700	\$ 9,800.00

**Tabla 2.** Recursos de personal.

<b>Recursos de Software</b>	<b>Precio U.</b>	<b>Sub Total</b>
Microsoft SQL Server 2005 licencia para un CPU incluye, opciones OLAP y Data Transformation Services	\$ 4,999.00	\$ 4,999.00
Licencia Windows XP Professional con Service Pack 2	\$ 149.77	\$ 149.77
Licencia Visual Studio Pro.Net 2003	\$ 429.99	\$ 429.99
<b>Total</b>		<b>\$ 5,479.76</b>

**Tabla 3.** Recursos de Software.

<b>Recursos de Hardware</b>	<b>Precio U.</b>	<b>Sub Total</b>
Dispositivo móvil	\$ 400.00	\$ 400.00
Dispositivos de red(Access Point)	\$ 115.00	\$ 115.00
Computadora de Desarrollo	\$ 579.00	\$ 579.00
Impresor	\$ 58.50	\$ 58.50
<b>Total</b>		<b>\$ 1,152.91</b>

**Tabla 4.** Recursos de Hardware.

## 10.2 Gastos Administrativo Estimados para Desarrollo del Proyecto

<b>Gastos Administrativos</b>	<b>Cantidad</b>
Servicios de energía eléctrica	\$ 150.00
Internet 256 kbps	\$ 200.00
Transporte	\$ 300.00
Tinta	\$ 100.00
Papelería	\$ 50.00
Otros	\$ 100.00
<b>Total</b>	<b>\$ 900.00</b>

Tabla 5. Gastos Administrativos.

<b>Descripción</b>	<b>Cantidad</b>
Recursos de Personal	\$ 9,800.00
Recursos de Software	\$ 5,479.76
Recursos de Hardware	\$ 1,152.91
Gastos Administrativos	\$ 900.00
<b>Total</b>	<b>\$ 17,332.67</b>

Tabla 6. Costo total del desarrollo del proyecto.

## 10.3 Presupuesto sin Recursos de Hardware y Software

Al contar con los recursos necesarios de hardware y software el costo se reduce en costo del personal y gastos administrativos como se indica en la siguiente tabla.

<b>Descripción</b>	<b>Cantidad</b>
Recursos de Personal	\$ 9,800.00
Gastos Administrativos	\$ 900.00
<b>Total</b>	<b>\$ 10,700.00</b>

Tabla 7. Costo del proyecto si se cuenta con hardware y software.

## 10.4 Presupuesto de Implementación

<b>Descripción</b>	<b>Item</b>	<b>Cantidad</b>
<b>Software</b>		<b>\$ 5,578.76</b>
Plataformas de desarrollo y licencias de software		
<b>Hardware</b>		<b>\$ 4,717.00</b>
Servidor	1	\$ 1,999.00
PC	1	\$ 579.00
Dispositivos de red	1	\$ 139.41
PDA	5	\$ 2,000.00
<b>Total</b>		<b>\$ 10,296.17</b>

Tabla 8. Presupuesto de Implementación.

# **CAPÍTULO 2. METODOLOGÍA DE LA INVESTIGACIÓN**

## **11. Tipo de Investigación**

Los tipos de investigación adoptados para el desarrollo del proyecto son los siguientes:

### **11.1 Documental**

La investigación documental es aquella que se realiza a través de la consulta de documentos, con el objetivo de identificar conceptos relacionados con el tema. Se consultaron trabajos de graduación sobre proyectos similares de sistemas de información diseñados en ambiente web, esta información sirvió de apoyo para aspectos de diseño y desarrollo del proyecto.

### **11.2 Investigación Aplicada**

Es la utilización de los conocimientos en la práctica, para aplicarlos, en la mayoría de los casos, en provecho de la sociedad, se caracteriza por su interés en la aplicación, utilización y consecuencias prácticas de los conocimientos. La investigación aplicada busca el conocer para hacer, actuar, construir y modificar.

La investigación aplicada conlleva a una solución y comprensión de los problemas, permitiendo así la obtención de toda la información necesaria para crear una solución eficiente, al problema relacionado con el proceso cuando se realiza una auditoría de sistemas, enfocándonos al desarrollo del sistema de información que se utilice como apoyo para las auditorías. La problemática que el auditor de sistemas se le presenta al desarrollar una auditoría son muchas, entre estas están, la inexperiencia o desconocimiento del proceso de auditoría y de las metodologías existentes, como también a las técnicas y herramientas aplicadas en el proceso de auditoría.

Además, la mayoría de las auditorías de sistemas, no cuentan con herramientas de software que asistan a los auditores en sus tareas, por lo cual dicha investigación aplicada, permitirá mejorar la efectividad y eficiencia en los procedimientos de auditoría, al desarrollar un software para apoyo en labores relacionadas con la auditoría en sistemas.

## **11.3 Técnicas y Herramientas de Investigación**

Existen diversas técnicas y herramientas para el desarrollo de una investigación que pueden ser aplicadas para el proyecto, de estas técnicas y herramientas se adoptaron según requerimientos, condiciones y características del proyecto las siguientes:

### **11.3.1 Recolección de la Información**

El proceso de obtención de información es la recolección, que permite la medición de las variables en las unidades de análisis, con la finalidad de dar solución al problema identificado mediante la obtención de datos necesarios para el estudio del problema.

Las fuentes utilizadas para recabar información son:

- Código de ética Profesional de la ISACA(Information Systems Audit and Control Association).
- Normas Generales de Auditoría de Sistemas de Información de la ISACA.
- Resumen ejecutivo de COBIT.
- Descripción de la estructura COBIT.
- Objetivos de Control COBIT.
- Guías de Auditoría COBIT.

### 11.3.2 Entrevistas

La entrevista es un método de investigación social, que se utiliza para recabar información en forma verbal, a través de preguntas que propone el analista sistemas. Quienes responden son usuarios actuales del sistema existente, usuarios potenciales del sistema propuesto o aquellos que proporcionarán datos o serán afectados por la aplicación propuesta.

Para el desarrollo del sistema, se optó por realizar un estudio, entre la mayoría de personas conocedoras de la situación, ya que son ellos quienes tienen mayor relación con los procesos y actividades que se manejan. Con la finalidad de obtener la información se entrevistaron personas involucradas directamente en el proceso de realización de las auditorías. Para el caso serán auditores de sistemas quienes proporcionaran información exacta del proceso de auditorías de sistemas.

En la etapa de entrevistas, la Dirección de Auditorías de la Corte de Cuentas de la República de el Salvador, proporcionó documentación sobre un taller de formación de Auditoría de Sistemas<sup>13</sup>, dicho documento complementa el caso del problema en estudio sobre las auditorías de sistemas, los temas contemplados en el taller abarcan todo el proceso que se debe realizar en una auditoría con sus métodos. También se proporcionó otros documentos sobre auditorías relacionadas en otras aéreas con el objetivo de profundizar más la problemática en análisis.

---

<sup>13</sup> Ver Anexo A

## **12. Ciclo de Vida del Sistema**

### **12.1 Investigación Preliminar**

Se inspeccionará de forma general la problemática, con el objetivo de recopilar toda la información que sea de utilidad para el establecimiento de las necesidades principales en el proceso de auditorías en sistemas. Se tomará como referencia información bibliográfica, opiniones de auditores de sistemas y proyectos de graduación desarrollados que estén relacionados.

### **12.2 Análisis del Sistema**

#### **12.2.1 Determinación y Definición de Requerimientos**

En esta fase se detallan los requisitos generales del sistema.

- El sistema deberá servirle al auditor como un asistente en el proceso de auditoría informática.
- Deberá contemplar la metodología que se utiliza en la auditoría de sistemas.
- Deberá considerar el estándar COBIT.
- Deberá considerar las auditorías por áreas.
- Deberá desarrollarse en un entorno web.

### **12.3 Diseño del Sistema**

Esta es la fase donde se implementa la investigación y los requerimientos identificados, en base a esto se desarrollará la base de datos. Además se detallarán los procedimientos de usuario que describirán cómo debe de usarse el sistema.

## **12.4 Construcción o Desarrollo del Sistema**

En esta etapa comienza la elaboración de los componentes individuales del sistema, se desarrollarán las interfaces de usuario para los módulos de inicialización, ejecución, consulta y administración del sistema los que serán probados por usuarios. Se inicializará con datos la base de datos para las pruebas de validación respectivas.

## **12.5 Evaluación y Seguimiento del Sistema**

Es en esta etapa donde se realizan las pruebas del sistema, el resultado de dichas pruebas se analizará con el equipo de desarrollo de la tesis con el fin de mejorar el sistema propuesto.

## **13. Metodología del Desarrollo**

### **13.1 Técnicas de Diseño de Sistemas de Información**

#### **13.1.1 Diagrama de Flujo de Datos(DFD)**

La técnica de diagrama de flujo de datos, es una representación gráfica que permite presentar soluciones a problemas reales en forma visual, donde el analista define las entradas, procedimientos y salidas de la información en la organización bajo estudio, permitiendo así, comprender los procedimientos existentes dentro de la organización con la finalidad de optimizarlos, reflejándolos en el sistema propuesto.

#### **13.1.2 Diagrama de Entidad Relación(E-R)**

Los diagramas de entidad relación (E-R), se parte de una situación real a partir de la cual se definen entidades y relaciones entre dichas entidades, representa la realidad a través de un esquema gráfico empleando las terminologías de entidades, que son objetos que existen y son elementos principales que se identifican en el problema a

resolver con el diagrama y se distinguen de otros por sus características particulares denominadas atributos, el enlace que rige la unión de las entidades está representada por la relación del modelo.

### **13.1.3 Diccionario de Datos**

Permite especificar el significado y composición de los datos, un diccionario de datos contiene las características lógicas de los datos a utilizar en el sistema que se está programando, incluyendo nombre, descripción, alias, contenido y organización, es un documento complementario al modelo de datos, se desarrollan durante el análisis de flujo de datos y auxilia a los analistas que participan en la determinación de los requerimientos del sistema, su contenido también se emplea durante el diseño del proyecto.

Las definiciones de todos los datos mencionados en el diagrama de flujo de datos (DFD) y el diagrama de entidad relación, son representadas en un diccionario de datos.

### 14. Estudio de la Situación Actual

#### 14.1 Valoración de la Situación Actual

##### 14.1.1 Descripción de la Situación Actual

**Contexto del sistema actual:** La situación actual se caracteriza por sistemas de información cada vez más complejos, integrados y con uso intensivo de las nuevas tecnologías de la Información y comunicación que implican riesgos relacionados con la seguridad y calidad de la información que se genera y administra.

**Descripción de los sistemas de información actuales:** Parte de esta actividad se desarrolló en el contenido 8 “Marco Experimental”.

A continuación se realiza una descripción funcional de sistemas relacionados con la auditoría de sistemas:

✓ **Software: Meycor COBIT CSA (Control Self-Assessment)**

Es una herramienta de software que automatiza la evaluación de una organización contra los objetivos de control del marco COBIT, generando un diagnóstico y recomendaciones que facilitan la implementación de esos objetivos de control.

✓ **Software: Meycor COBIT MG (MANAGEMENT GUIDELINES)**

COBIT en su tercera edición incorpora las guías de gerenciamiento (Management Guidelines), que incluyen un conjunto de herramientas formado por el modelo de maduración, los factores críticos de éxito (CSFs), los indicadores clave de meta (KGIs) y los indicadores clave de desempeño (KPIs).

✓ **Software: Gesia 2000**

Las directrices y objetivos del GESIA 2000 no han sido otros que el de poner al alcance de los profesionales de la auditoría, y de forma muy especial de los responsables de despachos y firmas de auditoría, una herramienta que, acorde con las nuevas tecnologías, facilite su labor de organizar y controlar los trabajos.

✓ **Software: ACL Edición de Escritorio / Red**

ACL es la herramienta de software de auditoría preferida por la comunidad de auditoría interna internacional, para la extracción y el análisis de datos, la detección de fraudes y el control continuo. Al proporcionar una exclusiva y eficiente combinación de acceso a los datos, análisis y elaboración integrada de reportes, ACL permite transformar los datos en información significativa y asistirlo en el logro de objetivos comerciales para agregar valor a su organización.

✓ **Software: 3rd. EDITION Management Advisor**

COBIT 3rd. EDITION Management Advisor soporta análisis de brecha multinivel, permitiendo realizar un "benchmark" efectivo de los procesos de TI y analizar resultados de evaluaciones actuales versus anteriores en una base de datos única. Con su sofisticada función de alerta, provee un rastreo instantáneo de las áreas que requieren seguimiento, asegurando la disposición de la máxima cantidad de información con el toque de un botón.

✓ **Software: COBIT Advisor 3rd. EDITION (Audit)**

COBIT Advisor 3 RD EDITION (Audit) provee una aplicación consistente de la estructura COBIT; aplicable a todo tipo de empresas, permitiendo seguir las mejores prácticas para una administración efectiva de TI en la organización.

✓ **Software: Idea Data Analysis Software**

CaseWare IDEA ([www.caseware-idea.com](http://www.caseware-idea.com)) es un software de PC bajo Windows en Español, muy fácil de usar, que permite que el analista de datos o

Auditor de Negocios acceda virtualmente a cualquier archivo de datos de cualquier entorno y analice el cien por ciento de miles o millones de transacciones en segundos detectando la totalidad de las excepciones y construyendo las propias bases de datos de Análisis de datos o Auditoría con datos completamente flexibles y de entornos diversos.

## **14.2 Sistemas de Información Existentes**

### **14.2.1 Descripción de la Situación Actual**

No se desarrolla un estudio detallado de los sistemas mencionados en el punto anterior por no considerarse necesario para realizar el estudio de viabilidad del sistema al no tener ninguno de ellos las características que se esperan del desarrollo que se propone realizar.

En lo relacionado al software, se observa que existe poco desarrollo de la auditoría en sistemas asistida por computadora, encontrando las siguientes limitaciones y dificultades:

- Todos los paquetes de software existentes son de tipo comercial, con un alto costo que en muchos casos es inaccesible para los auditores.
- No se detectan paquetes que aborden de manera integral todos los pasos necesarios para realizar una auditoría, en general abordan una o algunas de las actividades necesarias para realizar esta tarea.
- Los paquetes relevados tienen un bajo nivel de adaptabilidad, por lo tanto su utilización en general se relaciona con las grandes empresas, quedando las pequeñas y medianas fuera del alcance de los mismos.

## 15. Procedimientos

### 15.2 Metodología de Desarrollo en Auditoría de Sistemas

Diferentes autores proponen metodologías de desarrollo de auditorías en sistemas, en general la mayoría de ellos coinciden en las siguientes fases:

- ✓ **Fase 1. Identificar el Alcance y los Objetivos de la Auditoría Informática**  
En esta fase se determinan los límites y el entorno en que se realizará la auditoría, es el momento donde se determina hasta donde debe llegar la tarea, debe existir un acuerdo muy preciso entre autoridades y clientes sobre las funciones, las materias y los departamentos o áreas a auditar.
  
- ✓ **Fase 2. Realizar el Estudio Inicial del entorno a auditar**  
Para realizar dicho estudio es necesario examinar las funciones y actividades generales de la organización a auditar y en particular de las relacionadas con las tecnologías de la información, se deberá obtener información sobre:

#### **Organización**

- Se debe definir la estructura organizativa del departamento o área de Informática a auditar.
- Organigrama, se trata de la estructura formal de la organización a auditar.
- Departamentos, entendiendo como departamentos a las áreas que siguen a la dirección, en el estudio inicial se deberá definir la función de cada uno de ellos.
- Relaciones funcionales y jerárquicas entre las distintas áreas de la organización, el auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas, o por el contrario, detectará, cualquier anomalía como por ejemplo, si algún empleado tiene dos jefes.

- Flujo de información, la calidad de este flujo tiene un enorme impacto sobre la eficacia y eficiencia de la gestión, deberá investigar sobre posibles canales alternativos o no formales de comunicación.

### **Entorno Operativo**

El equipo de auditoría informático debe poseer antes de comenzar la tarea una información fiable del entorno en el que se va a desarrollar las actividades. Se debe considerar:

- Situación geográfica de las áreas de sistemas a auditar, verificando la existencia de los responsables y la estructura interna del área informática, así como el uso de estándares de trabajo formales o informales, los planes de capacitación y las políticas de ingreso de personal a las áreas de sistemas.
- Arquitectura y configuración Hardware y Software.
- Inventario completo del hardware y software, incluyendo CPUs, procesadores, periféricos, software de base y aplicación, legalidad del mismo.
- Telecomunicaciones, topología, proveedores, servicios que se brindan, seguridad.
- Aspectos relacionados con la seguridad y planes de contingencia.

### **Aplicaciones Informáticas, Bases de Datos y Archivos**

- Se deben determinar los sistemas informáticos implementados en la empresa.
- Volumen, Antigüedad y Complejidad de las aplicaciones.
- Metodología de desarrollo de aplicaciones.
- Metodología de mantenimiento de las aplicaciones.
- Documentación de aplicaciones.
- Cantidad y complejidad de bases de datos, tamaño y características de bases de datos, número de accesos a BD, frecuencia de actualización.
- Planes de desarrollo.

✓ **Fase 3. Determinación de los recursos necesarios para realizar la auditoría de sistemas.**

Después de realizar el estudio preliminar se debe determinar los recursos materiales y humanos necesarios para implementar el plan de auditoría.

**Recursos Materiales**

- Software: paquetes de auditoría del equipo auditor, compiladores.
- Hardware: PCs, impresoras, líneas de comunicación.
- Se debe establecer quien provee estos recursos.

**Recursos Humanos**

La Auditoría de sistemas en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria y en algunos casos se requiere que los profesionales estén certificados por ISACA.

✓ **Fase 4. Elaborar el Plan de Trabajo**

En esta fase se definen el calendario de actividades a realizar, formalizando el mismo para la aprobación por parte de las autoridades. El plan de la auditoría en muchos casos es guiado por las recomendaciones que brinda ISACA a través de sus guías y contempla:

- Conocimiento de la organización y de sus procesos, para identificar problemas potenciales, alcance.
- Programa de auditoría: Calendario de trabajo (tareas y recursos) y su seguimiento.
- Evaluación interna del control, mediante pruebas de cumplimiento de los controles.

✓ **Fase 5. Realizar las Actividades de Auditoría**

Es el momento donde se hacen efectivas las actividades planificadas en la fase anterior, aplicando distintas técnicas y utilizando herramientas que

garanticen el cumplimiento de los objetivos planteados, se documenta esta etapa, monitoreando las posibles desviaciones que se detecten en relación con la planificación original.

✓ **Fase 6. Realizar el Informe Final**

El objetivo final del auditor es entregar por escrito un informe, en donde constarán las conclusiones y recomendaciones. El auditor justifica personalmente su auditoría en forma documentada. La elaboración del informe final es la única referencia constatable de toda auditoría, y el exponente de su calidad. Por lo tanto es muy importante que su contenido sea claro y estructurado de tal manera que responda a las expectativas del cliente en cuanto al cumplimiento de los objetivos planteados.

En el informe final deben quedar claramente formalizados los siguientes puntos:

- Alcance
- Objetivos
- Período de cobertura
- Naturaleza y extensión del trabajo de auditoría
- Organización
- Destinatarios del informe
- Restricciones
- Hallazgos
- Conclusiones
- Recomendaciones

## **16. Catálogo de Usuarios**

Los posibles usuarios serán los auditores internos y externos de cualquier empresa u organismo, estatal o privado, en el caso de empresas que no realicen ningún tipo de auditoría de sistemas podrá utilizarse el asistente para realizar un autodiagnóstico relacionado con el ambiente de control de los sistemas de información, este autodiagnóstico no será una salida del asistente, sino que podrá ser sencillamente deducido a partir de los distintas listas de verificación que propondrá el sistema.

### **16.1 Usuarios Involucrados en Auditorias de Sistemas**

#### **16.1.1 Auditor Informático General**

Son las personas encargadas de realizar las auditorías en sistemas de información, con experiencia en informática y auditoría, formado profesionalmente con conocimientos en gestión del cambio y de gestión empresarial. Siendo exactos un profesional dedicado al análisis de sistemas de información e informáticos

#### **16.1.2 Usuarios de los Sistemas de Información**

Son las personas encargadas de los sistemas de información o usuarios, delegados por la organización para proporcionar toda aquella información que está siendo solicitada por el auditor de sistemas para el análisis de auditoría.

#### **16.1.3 Coordinadores Asignados**

Son las personas encargadas de coordinar el desarrollo de la auditoría, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas al igual que los usuarios del sistema estos son asignados por la organización cuando se realiza la planeación de la auditoría.

## **CAPÍTULO 4. DESARROLLO DEL SISTEMA**

### **17. Planificación del Sistema**

La planificación del sistema tiene el objetivo crear un sistema integral, desarrollado con herramientas web, que asistirá desde el punto de vista metodológico al auditor de sistemas y que incorpore el estándar COBIT(Control Objectives for Information and Related Technology).

Un elemento crítico para el éxito y la supervivencia de las organizaciones, en esta sociedad global es la administración efectiva de la información y de la tecnología de Información(TI) relacionada. Esta surge de:

- La creciente dependencia que tienen las organizaciones en la información que manejan y en los sistemas que proporcionan dicha información.
- La creciente vulnerabilidad y la gran cantidad de amenazas a las que se exponen los sistemas de información.
- El costo y la escala de las inversiones actuales y futuras en información y en tecnología de información.
- El enorme potencial que tienen las tecnologías de la Información y las comunicaciones para cambiar radicalmente las organizaciones y las prácticas de negocio.

Los objetivos estratégicos relacionados con el sistema son:

- Lograr aplicar una metodología en el proceso de auditoría de Sistemas, que posibilite obtener información para minimizar los riesgos relacionados con sistemas informáticos.
- Lograr que el proceso de auditoría de sistemas se adapte al entorno a auditar.

Los factores críticos que podrían intervenir en el desarrollo del sistema son:

- Conocer en profundidad el estándar COBIT.
- Conocer en profundidad la metodología de desarrollo de auditorías de sistemas.
- Tener contacto permanente con auditores para poder tener claro el proceso de auditoría de sistemas.

## **17.1 Requerimientos o Requisitos Generales**

En esta fase se detallan los requisitos generales del sistema.

- El sistema deberá servirle al auditor como un asistente en el proceso de auditoría informática.
- Deberá contemplar la metodología que se utiliza en la auditoría de sistemas.
- Deberá considerar el estándar COBIT.
- Deberá considerar las auditorías por áreas.
- Deberá desarrollarse en un entorno web.

## **17.2 Definición de la Arquitectura Tecnológica**

### **17.2.1 Alternativa 1: Arquitectura Web**

Una aplicación web es aquella en que los usuarios acceden a un servidor web a través de internet o de una intranet. Las aplicaciones web son populares debido a lo práctico que son los navegadores web como cliente ligero, la habilidad para actualizar y mantener aplicaciones web sin distribuir e instalar software en miles de potenciales clientes es otra razón de su potencialidad.

Una ventaja más importante a considerar para la construcción de aplicaciones web, es que los navegadores funcionan igual independientemente de la versión del sistema operativo instalado en el cliente.

Una aplicación web está comúnmente estructurada con una arquitectura en tres-capas. Donde el navegador web es la primer capa, un motor usando alguna tecnología web dinámica (CGI, PHP, Java Servlets o ASP .NET) es la capa de en medio, y una base de datos como última capa. El navegador web manda peticiones a la capa media, que la entrega valiéndose de consultas y actualizaciones a la base de datos generando una interfaz de usuario.

### **17.2.2 Alternativa 2: Arquitectura Cliente-Servidor**

Es un modelo para el desarrollo de sistemas de información en el que las transacciones se dividen en procesos independientes que cooperan entre sí para intercambiar información, servicios o recursos. En esta arquitectura interactúan los clientes realizando generalmente funciones como:

- Manejo de la interfaz de usuario.
- Captura y validación de los datos de entrada.
- Generación de consultas e informes sobre las bases de datos.

Entre las principales características de la arquitectura cliente-servidor se pueden destacar las siguientes:

- El servidor presenta a todos sus clientes una interfaz única y bien definida.
- El cliente no necesita conocer la lógica del servidor, sólo su interfaz externa.
- El cliente no depende de la ubicación física del servidor, ni del tipo de equipo físico en el que se encuentra, ni de su sistema operativo.
- Los cambios en el servidor implican pocos o ningún cambio en el cliente.

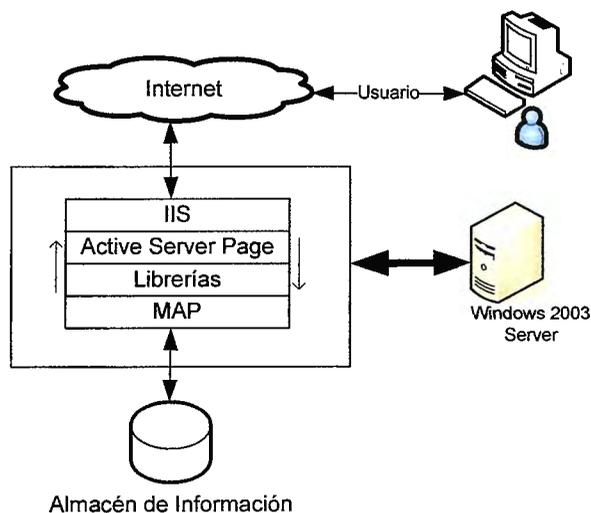
### 17.2.3 Selección de la Arquitectura Tecnológica

Analizadas las dos propuestas y evaluadas las necesidades y el entorno en el cual el sistema se utilizará se optó por la Arquitectura Web por las siguientes razones:

- Las características técnicas de esta arquitectura se adaptan a cualquier entorno donde se quiera aplicar el sistema.
- No requiere instalaciones en los clientes.
- No requiere en los clientes un sistema operativo en especial.
- Soporta la arquitectura en tres capas.
- Es más económica que la arquitectura cliente-servidor
- Su implementación es más sencilla.

### 17.3 Entorno de Implementación del Sistema

En la siguiente figura representa la manera en que interactúan todas las tecnologías de desarrollo y funcionamiento del sistema.



**Figura 1.** Tecnologías de desarrollo del sistema y funcionamiento del sistema.

## 17.4 Identificación de Subsistemas

El objetivo de esta actividad se relaciona con mostrar la estructura y relación de cada módulo y sub módulo.

### 17.4.1 Parametrización del Sistema

En este módulo se registrará el nombre físico ó dirección ip del servidor web, servidor de base de datos, la base de datos y la configuración por default que utilizará el sistema.

La configuración se almacenará en un archivo de texto (.ini) que se encontrará en el servidor web donde estará publicado el sistema. El archivo estará formado por tres secciones principales, cada sección contendrá los parámetros utilizados para la conexión al servidor y base de datos respectivamente. La estructura del archivo de configuración es la siguiente:

Nombre del Archivo **ConfigAudit.ini**

#### **[Servidor]**

ServidorActivo =

IpServidor=

#### **[Servidor BD]**

UsrConexionBD=

NombreSvrBD=

#### **[Base Datos]**

NombreBD=

Donde:

**ServidorActivo:** parámetro que indica que el servidor esta activo.

**IpServidor:** parámetro que indicara el nombre físico del servidor o dirección ip.

**UsrConexionBD:** parámetro que define el login de conexión a la base de datos.

**NombreSvrBD:** parámetro que define el nombre del servidor de base de datos.

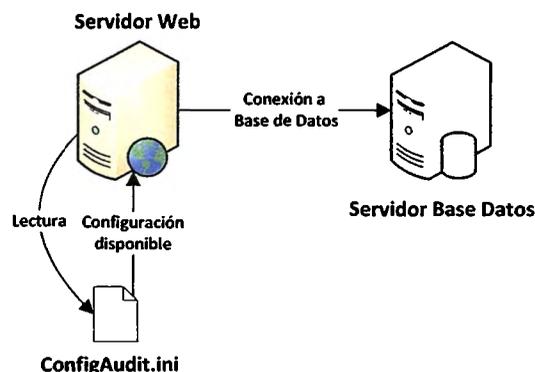
**NombreBD:** parámetro que define el nombre de la base de datos donde se conectará el sistema.

### 17.4.1.1 Proceso de Conexión a Base de Datos

Para establecer la conexión a la base de datos el sistema hace uso de un archivo de configuración que contiene los parámetros necesarios para su establecimiento, la secuencia lógica que utiliza este proceso se describe en los siguientes pasos:

- Verificación la existencia del archivo de configuración.
- Lectura de parámetros en archivo de configuración.
- Validación de parámetros.
- Establecimiento de conexión a Base de Datos con parámetros validados.

La siguiente figura describe la secuencia de conexión a la base de datos:



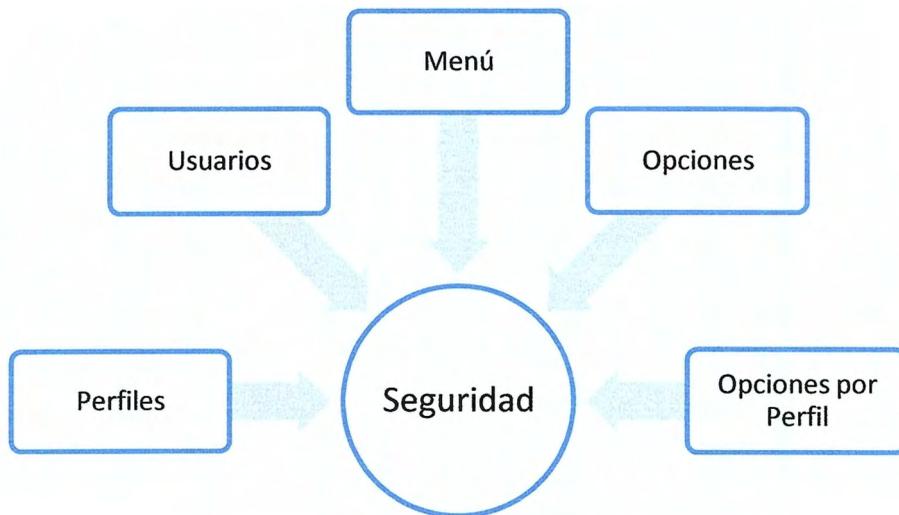
**Figura 2.** Lectura Archivo de Configuración.

## 17.4.2 Catalogo Maestros

En este módulo se realizará la alimentación de las tablas maestro que utilizará el sistema, para ello existirán una serie de mantenimientos que facilitarán dicha función.

## 17.4.3 Seguridad

Este módulo maneja la seguridad dentro del sistema, se podrá definir el nombre del sistema, menú del sistema, opciones por menú, perfiles dentro del sistema, usuarios del sistema, usuarios por perfil, acceso a opciones por perfil.



**Esquema 2.** Descomposición funcional del módulo de seguridad.

#### 17.4.4 Inicialización de Auditoría

En el módulo de inicialización de auditoría se especifica el tipo de auditoría a realizar, por áreas o COBIT, permite el ingreso de los datos de la empresa a auditar, los auditores y los datos del proyecto.



**Esquema 3.** Descomposición funcional del módulo de inicio de auditoría.

#### 17.4.5 Estudio Preliminar

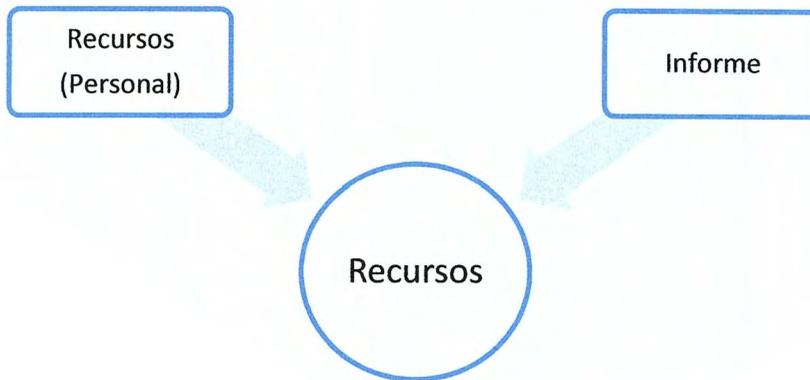
Este módulo tiene la función de asistir al auditor en el análisis preliminar, en función de los límites del proyecto propone cuestionarios que permitan definir, la estructura interna del área a auditar, las aplicaciones existentes, el personal relacionado con la tarea, el inventario y arquitectura del hardware y software, la documentación existente.



**Esquema 4.** Descomposición funcional del módulo Estudio Preliminar.

### 17.4.6 Recursos

Este módulo sugerirá los recursos necesarios, el recurso humano a sugerir serán los posibles auditores que llevarán el proceso de auditoría, una vez definido el o los auditores, se definirán tareas para cada auditor anteriormente elegido.



**Esquema 5.** Descomposición funcional del módulo Recursos.

### 17.4.7 Planificación

Asiste al proceso de planificación adaptando la misma a la organización específica donde se intenta realizar la tarea, proponiendo de acuerdo a los pasos anteriormente desarrollados un plan de trabajo tentativo.



**Esquema 6.** Descomposición funcional del módulo Planificación.

#### 17.4.8 Módulo de Consulta o Seguimiento

Da seguimiento a los avances de auditoría, obtención de resultados y redacción del informe final de auditoría a través de una plantilla establecida dentro del sistema.

### 17.5 Estructura de Seguridad del Sistema

El sistema tiene dos niveles de seguridad:

- El acceso a las páginas web
- El acceso a los datos almacenados en las bases de datos.

Por una cuestión de seguridad y simplicidad se solicitará el ingreso de una clave para el acceso a las páginas web y solo habrá un usuario para establecer la conexión a la base de datos

#### 17.5.1 Perfiles de usuario

El sistema prevé tres perfiles de usuario, administrador, supervisor y auditor. El perfil administrador, accede a todo el sistema incluyendo el módulo de administración que asigna roles de usuarios y permite la carga de lista de verificación. El perfil de auditor accede a todos los módulos menos el de administración.

A continuación se detalla los módulos a los que tendrá acceso cada perfil.

**Perfil administrador:** el módulo al que accede es el de configuración, donde realiza la carga de los parámetros básicos del sistema, como por ejemplo la carga de la estructura de COBIT, la carga de la estructura de áreas, la carga de preguntas del relevamiento inicial y el profundo, la administración de usuarios.

**Perfil de supervisor:** permite el acceso a los módulos de inicio, estudio preliminar, recursos, planificación, desarrollo e informe final. El perfil de jefe de proyecto se diferencia del de auditor ya que es la persona responsable de dar por iniciado un proyecto, administrará los recursos necesarios para cada proyecto y la planificación del mismo.

**Perfil auditor:** permite el acceso a los módulos estudio preliminar, desarrollo e informes, a los módulos de Inicio, recursos y planificación accede solo a modo de consulta y no accede al módulo de configuración. Es el responsable de realizar la auditoría, tanto el relevamiento inicial como el profundo.

### **17.5.2 Procedimientos de administración**

Las tareas de administración del sistema son:

- Administración de usuarios, carga y definición de perfiles.
- Administración de la base de datos, actualización de la estructura de la misma.

## 18. Análisis del Sistema

### 18.1 Diagramas de Flujos de Datos

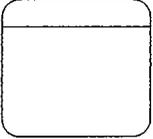
SIMBOLOGIA	DESCRIPCION
	<p><b><u>Proceso</u></b> Es un conjunto de tareas o acciones realizadas a partir del flujo de datos de entrada para producir flujos de datos de salida.</p>
	<p><b><u>Almacén de datos</u></b> Es un "inventario" de datos. Entre sus sinónimos se incluyen archivo y base de datos.</p>
	<p><b><u>Entidad</u></b> Define los límites de un sistema. Suministran entradas o salidas netas de un sistema.</p>
	<p><b><u>Flujo de datos</u></b> Representa la introducción de datos en un proceso o la obtención de datos de un proceso. Puede también representar la actualización de datos en un archivo, una base de datos u otro medio de almacenamiento de datos.</p>
	<p><b><u>Conector</u></b> Se usa para conectar diferentes flujos de datos.</p>

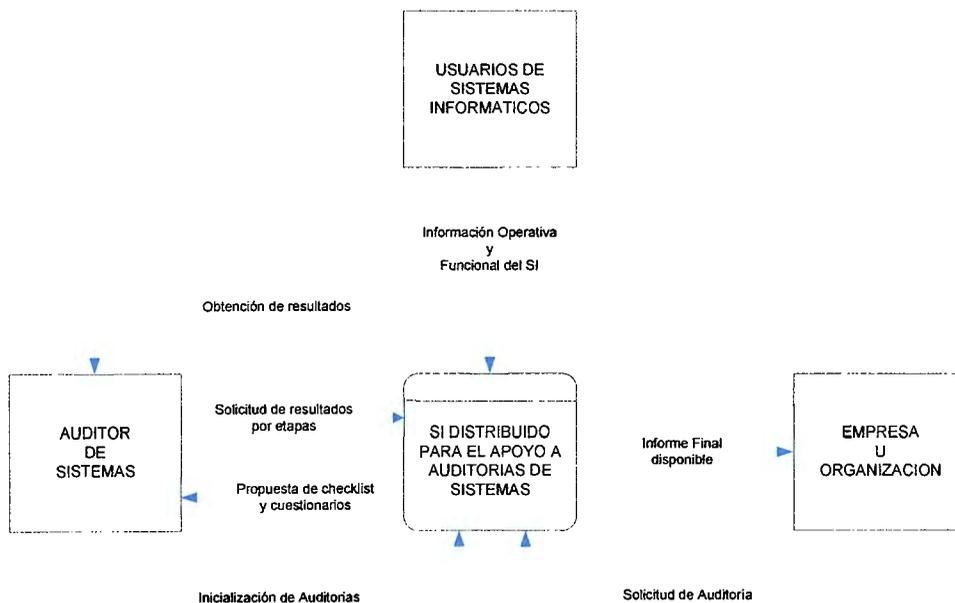
Tabla 9. Simbología de Gane y Sarson.

## 18.2 Descripción de los Diagramas de Flujo

### 18.2.1 Diagrama de Contexto

El siguiente diagrama presenta el contexto referente al Diseño y Desarrollo del Sistema de Información distribuido para el apoyo a la Auditoría de Sistemas.

En una auditoría de sistemas, al auditor se le presenta la necesidad de realizar dicha tarea una vez solicitada por la empresa u organización que demanda la revisión y evaluación de sus sistemas, en donde el sistema de información formará parte en la auditoría de sistemas como un apoyo para la actualización y envío de información a los usuarios del sistema y al auditor mismo.



**Diagrama 1.** Diagrama de Contexto.

## 18.2.2 DFD Nivel 0

En el siguiente diagrama se presentan las entidades y procesos del sistema con cada uno de los módulos interactuando entre ellos. Los módulos que se muestran en el diagrama de nivel 0 son los siguientes: Configuración de auditoría, definir recursos y planificación, inicio de auditoría, desarrollo e informe.

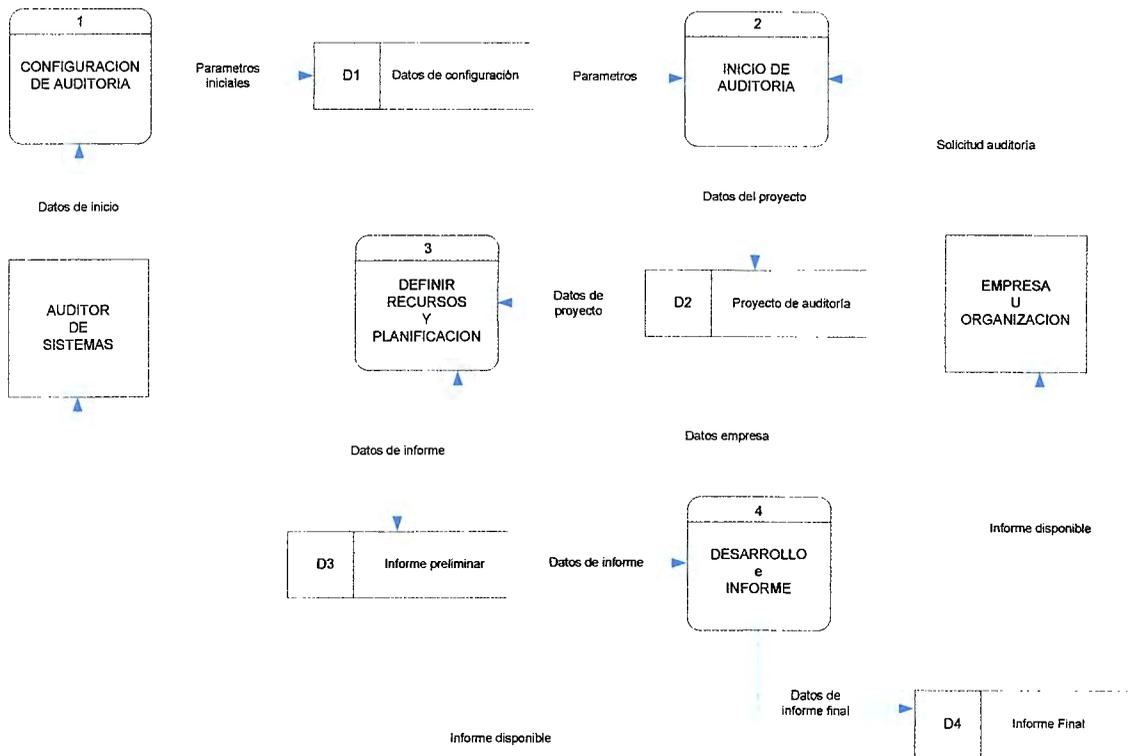
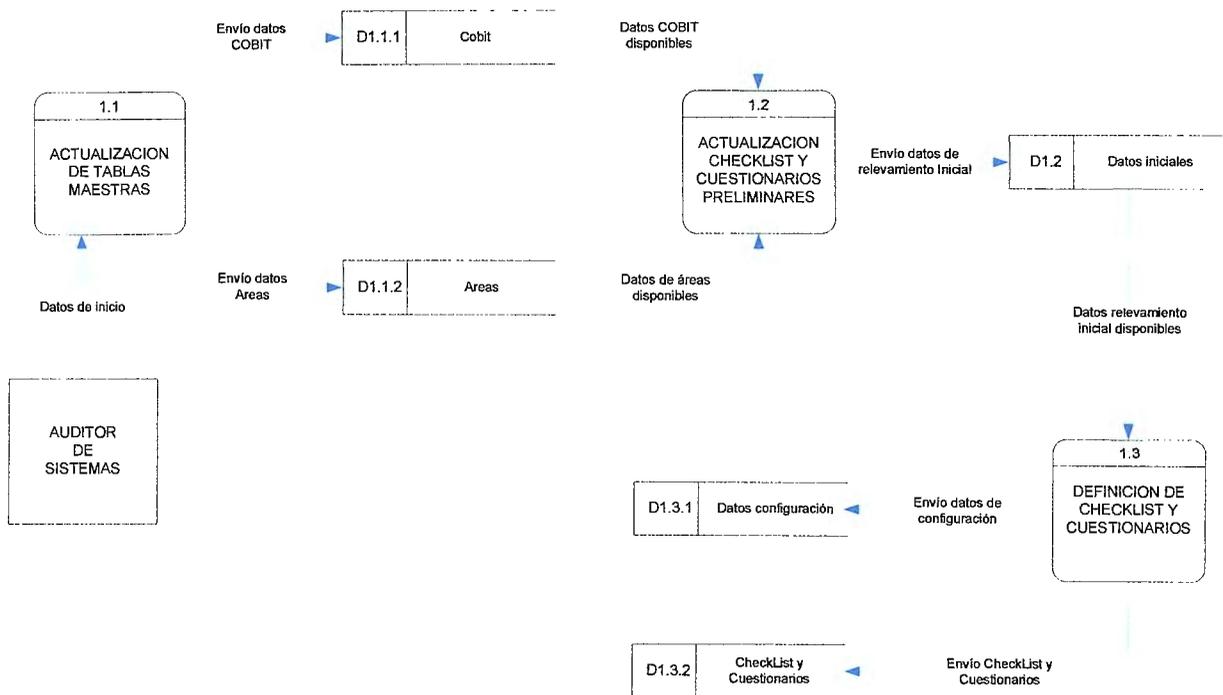


Diagrama 2. Nivel 0

## 18.2.3 DFD Módulo de Configuración de Auditoría

En el módulo de configuración de auditoría, las actividades o procesos principales que sobresalen en esta etapa de configuración son: la actualización de tablas maestras y la definición de listas de verificación y cuestionarios preliminares.



**Diagrama 3. Módulo de Configuración de Auditoría.**

### 18.2.3.1 Descripción de Procedimientos

MODULO DE CONFIGURACION DE AUDITORIA	
PROCESO	DESCRIPCION
Actualización de tablas maestras	<p>Éste proceso podrá ser realizado por el usuario administrador, a través de este proceso se podrán realizar ingresos y modificaciones de las tablas básicas necesarias para el funcionamiento del sistema.</p> <p>Se deberá mantener actualizadas las mismas de acuerdo a las normas dadas por COBIT, relacionándose las áreas y los dominios, con el perfil del auditor necesario para realizar la tare., y los procedimientos y técnicas necesarias en cada caso para realizar la auditoría.</p>
Actualización listas de verificación y cuestionarios preliminares	En este proceso se podrán ingresar, modificar, eliminar y listar las preguntas y las distintas alternativas de respuestas para cada área o dominio/proceso de COBIT preliminar.
Definición de listas de verificación y cuestionarios	En este proceso se podrán ingresar, modificar, eliminar y listar las preguntas, las distintas alternativas de respuestas para cada área o dominio/proceso/objetivo de control de COBIT importante en la definición, se deberá actualizar las distintas recomendaciones de acuerdo a las respuestas dadas en la definición.

**Tabla 10. Tabla Descriptiva de Procedimientos.**

## 18.2.4 DFD Módulo Inicio de Auditoría

Las actividades o procesos principales relevantes en esta etapa de inicio de auditoría son: Generar datos del proyecto, realizar lista de verificación inicial del proyecto y realizar informe de lista de verificación inicial.

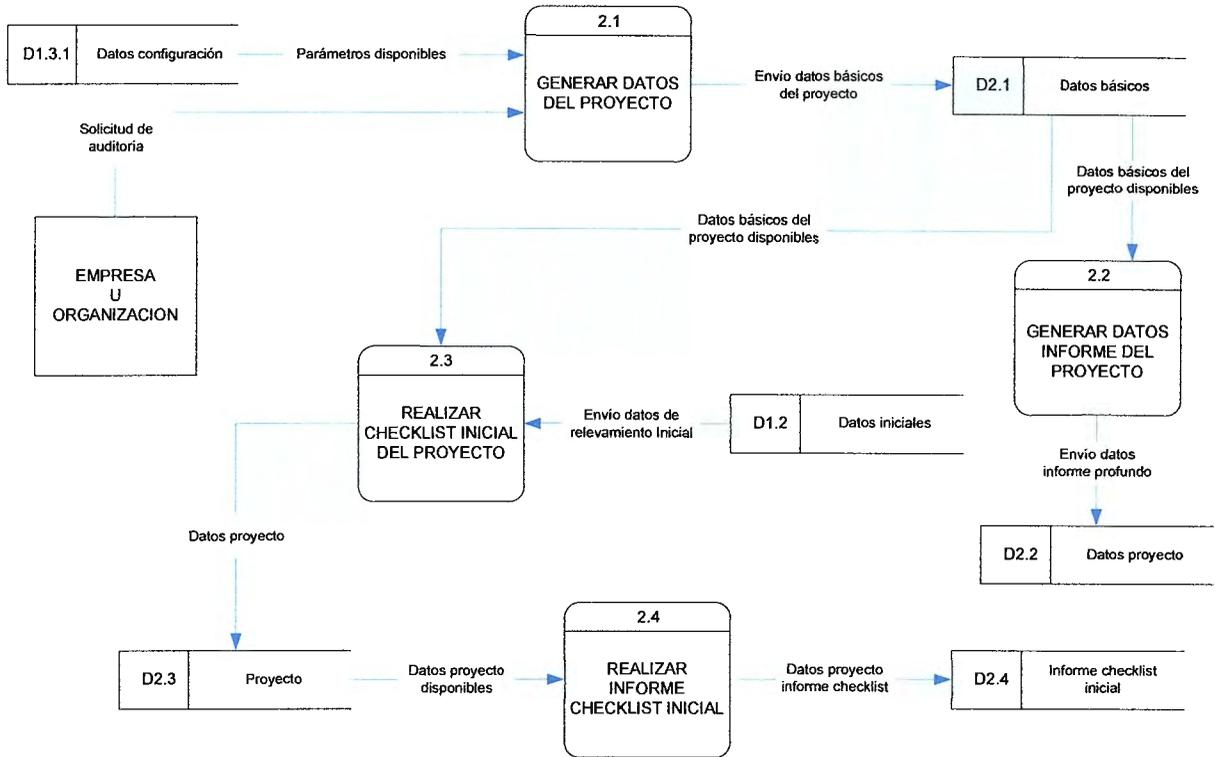


Diagrama 4. Módulo de Inicio de Auditoría.

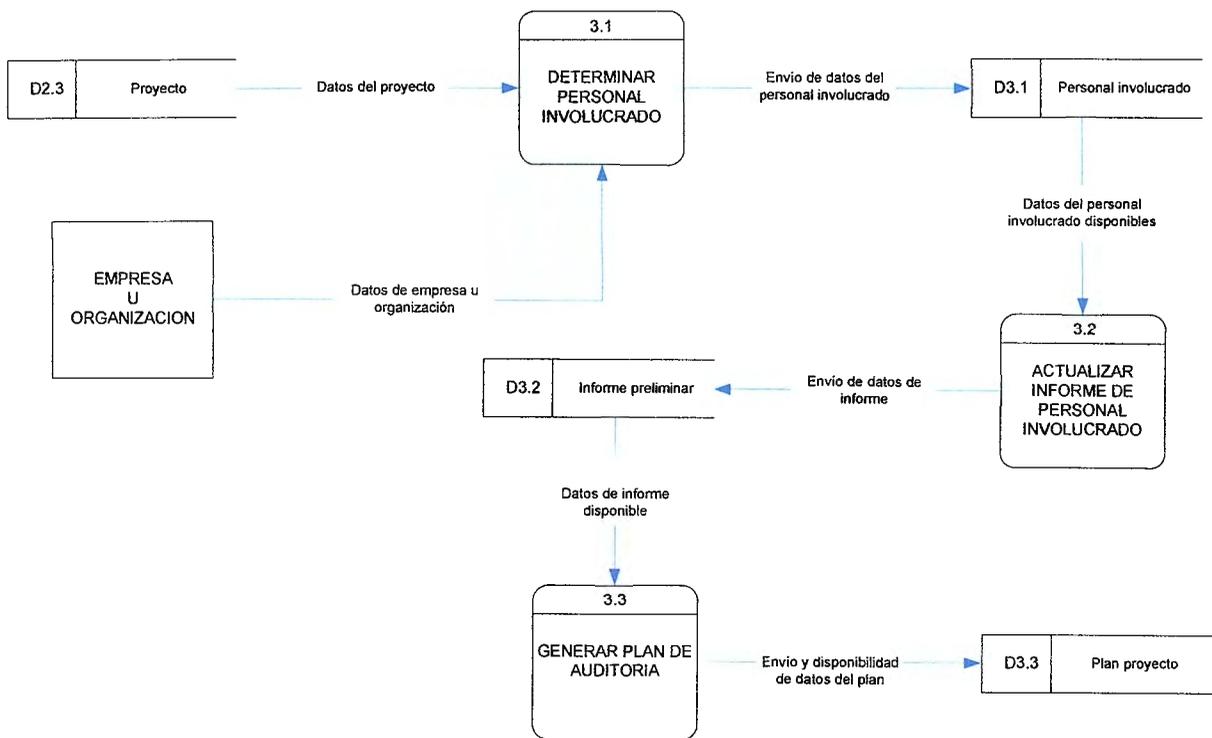
### 18.2.4.1 Descripción de Procedimientos

MODULO DE INICIO DE AUDITORIA	
PROCESO	DESCRIPCION
Generar datos del proyecto	<p>El proceso consiste en ingresar, modificar y listar los datos relacionados con el cliente del proyecto, los auditores asignados, los sectores o sucursales de la organización, a donde se realizará la auditoría.</p> <p>Parte del consistirá en definir desde el punto de vista metodológico si se trabaja por áreas o de acuerdo a COBIT por dominios y procesos, definiendo cual se abordará para establecer el alcance de la auditoría</p>
Generar Datos Informe del proyecto	En función de los datos del proyecto se generará un informe con los datos básicos y el alcance de la auditoría.
Realizar lista de verificación inicial del proyecto	<p>Se deberá generar en forma automática una lista de preguntas específicas para el proyecto, la misma se establecerá en función del alcance, es decir de las áreas o dominios/procesos que se establecieron para el proyecto, esta lista será un subconjunto del la matriz general de preguntas del proceso preliminar. Se repetirá esta lista de preguntas para cada sector a auditar.</p> <p>Se deberán poder ingresar las respuestas de cada pregunta, pudiendo modificarse las mismas.</p>
Realizar Informe de lista de verificación inicial del proyecto	En función de la definición inicial del proyecto se genera un informe del mismo. Este reporte se podrá filtrar para un sector determinado o para todos.

**Tabla 11.** Tabla Descriptiva de Procedimientos.

### 18.2.5 DFD Módulo Recursos y Planificación

El modulo de definición de recursos y planificación, las principales actividades o procesos que presenta esta etapa son: Determinación de personal involucrado, actualización de informe de personal involucrado y generación de plan de auditoría.



**Diagrama 5. Módulo Definir Recursos y Planificación.**

### 18.2.5.1 Descripción de Procedimientos

MODULO DEFINIR RECURSOS Y PLANIFICACION	
PROCESO	DESCRIPCION
Determinar Personal Involucrado	<p>Consiste en establecer el personal necesario para realizar la auditoría, así como también generar en forma automática los perfiles del personal necesarios para realizar auditorías, en base a, el alcance de la auditoría.</p> <p>El sistema en esta etapa permitirá la actualización y selección de los auditores, incorporando o eliminando alguno de ellos.</p>
Actualizar informe de personal involucrado	En función de los datos del proyecto se generará un informe con los datos del proyecto y el personal necesario para realizar la auditoría
Generar plan de auditoría	Consiste en generar la planificación de la auditoría del proyecto en función de las tareas propuestas cargando y modificando el plan de la auditoría según la necesidad del auditor

**Tabla 12. Tabla Descriptiva de Procedimientos.**

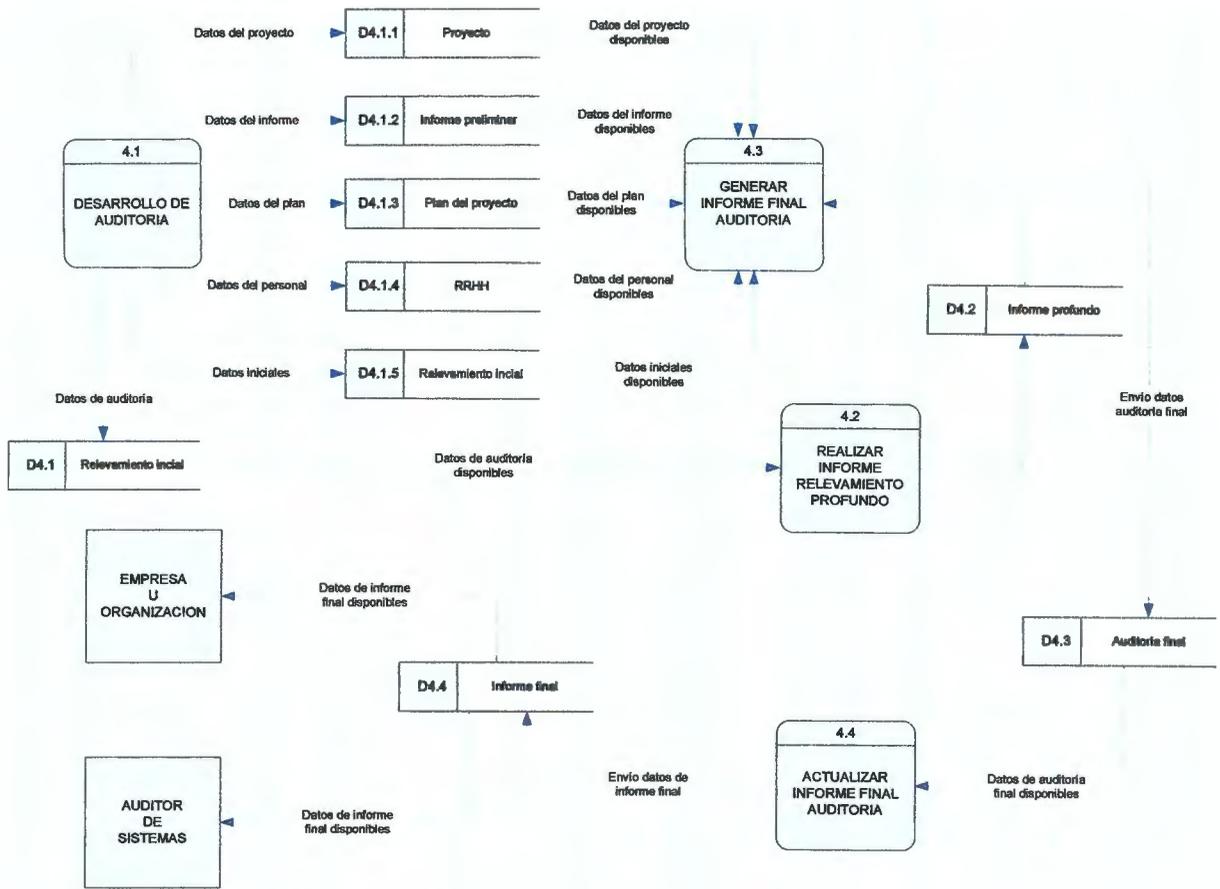
## 18.2.6 DFD Módulo Desarrollo e Informe

En el modulo Desarrollo e Informe, las actividades o procesos principales que sobresalen en esta son: Desarrollo de Auditoría, generar informe final de auditoría, realizar informe relevamiento profundo y actualización informe final de auditoría.

### 18.2.6.1 Descripción de Procedimientos

MODULO DE INICIO DE AUDITORIA	
PROCESO	DESCRIPCION
Desarrollo de Auditoría	<p>Este modulo permitirá generar en forma automática una serie de preguntas para el relevamiento profundo específico para el proyecto, estas se establecerán en función del alcance, ya sea por áreas o dominios que se establecieron anteriormente para el proyecto, esta lista de preguntas será un subconjunto de la lista general de preguntas del relevamiento profundo</p> <p>Se repetirá esta lista de preguntas para cada sector a auditar.</p> <p>Se deberán poder ingresar las respuestas de cada pregunta, pudiendo modificarse las mismas.</p> <p>Se deberá poder ingresar observaciones para cada pregunta</p>
Realizar Informe Relevamiento profundo	<p>En función del relevamiento profundo del proyecto se genera un informe del mismo. Este reporte se podrá filtrar para un sector determinado o para todos.</p>
Generar Informe Final de Auditoría	<p>Permitirá generar en forma automática en función del resultado del relevamiento profundo y de las recomendaciones estándares ingresadas para cada respuesta posible, las recomendaciones y propuestas a realizar.</p>
Actualizar Informe Final de Auditoría	<p>Permitirá ingresar, eliminar, modificar ítems del informe final y listar el informe final</p>

**Tabla 13.** Tabla Descriptiva de Procesos.



**Diagrama 6. Desarrollo e Informe.**

### 18.3 Modelo Conceptual de Datos

La figura # muestra el modelo conceptual de datos.

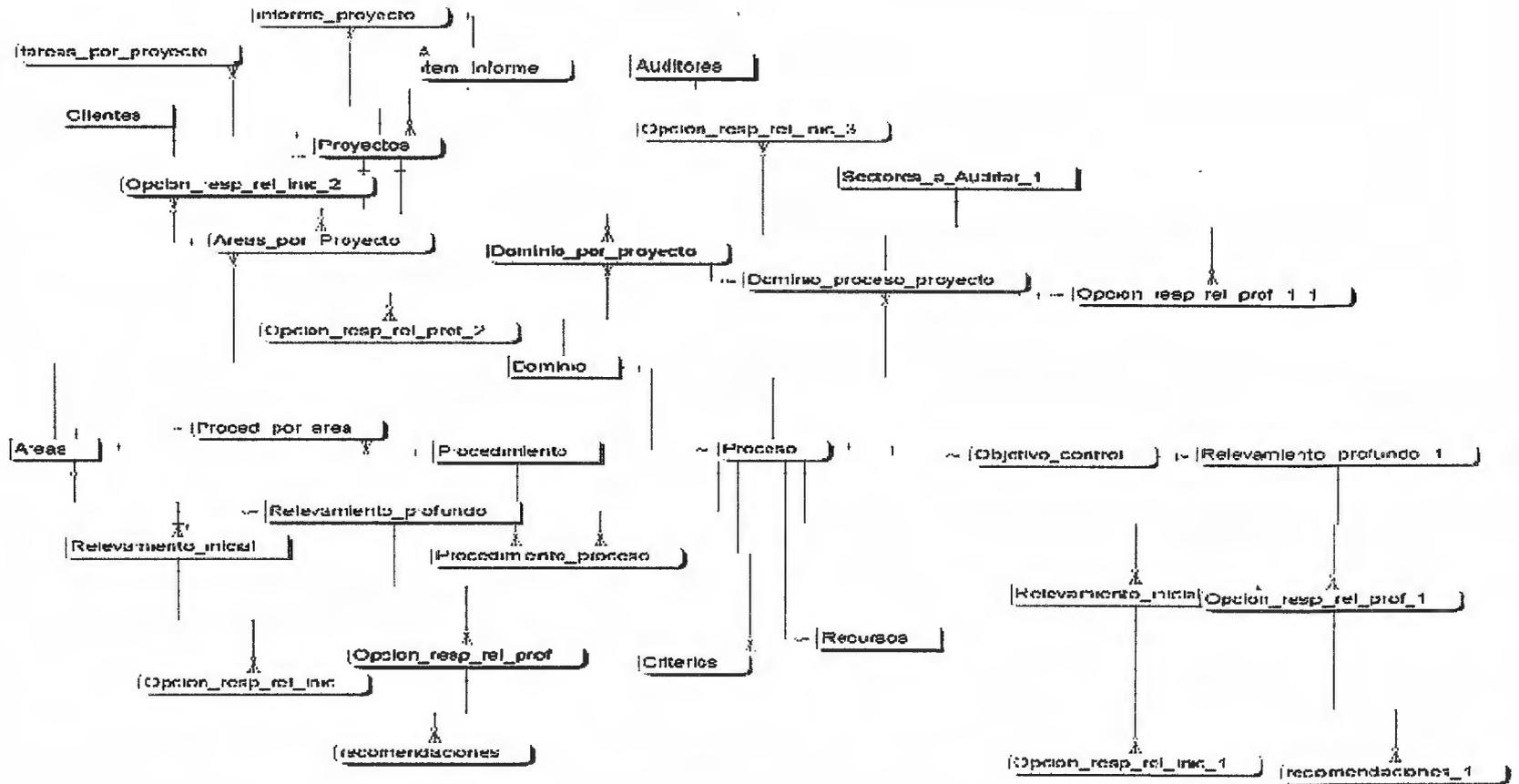


Figura 3. Modelo Conceptual de datos.

## 18.4 Modelo Lógico de Datos

Las siguientes tablas muestran las descripciones de entidades y atributos.

Entidad	Descripción	Atributo	Valor / Descripción
1. Areas	Representa las áreas donde se desarrolla la auditoría de sistemas.	Cod_area	Numérico Código del área donde se desarrollara la auditoría
		desc_area	Organización gestión y base jurídica Recursos Humanos Sistemas en desarrollo Operación y soporte Ambiente físico Hardware Software Seguridad lógica y física Parámetros de medición
			Nombre del área donde se desarrollara la auditoría
2. Areas_por_proyecto	Representa las áreas que abordará cada proyecto	Id_proyecto	(ver entidad PROYECTOS)
		Cod_area	(ver entidad AREAS)
		Cod_sector	(Ver entidad SECTORES_A_AUDITAR)

		Observaciones_area	<i>Alfanumérico</i> Observaciones del auditor relacionadas con la auditoría realizada en el área	
		Documentacion_adjunta_area	<i>Alfanumérico</i> Documentación adjunta del área auditada	
3. Auditores	Representa los auditores de sistemas	Cod_auditor	<i>Númérico</i> Código del auditor	
		Nombre	<i>Alfanumérico</i> Nombre del auditor de sistema	
		Apellido	<i>Alfanumérico</i> Apellido del auditor de sistemas	
		Teléfono	<i>Númérico</i> Teléfono del auditor de sistemas	
		Título	<i>Alfanumérico</i> Título universitario del auditor de sistemas	
		e-mail	<i>Alfanumérico</i> Correo electrónico del auditor de sistemas	
4. Auditores por proyecto	Representa los auditores que intervienen en cada proyecto	Id_proyecto	(ver entidad PROYECTO)	
		Cod_auditor	(ver entidad AUDITORES)	
5. Clientes	Representa los clientes que son auditados	Cod_cliente	<i>Númérico</i> Código del cliente	
		Apellido_cli	<i>Alfanumérico</i> Apellido del cliente	
		Nombre_cli	<i>Alfanumérico</i> Nombre del cliente	
		Direccion_cli	<i>Alfanumérico</i> Dirección del cliente	
		Localidad	<i>Alfanumérico</i> Localidad del cliente	
		Provincia	<i>Alfanumérico</i> Provincia del cliente	

		Pais	<i>Alfanumérico</i>
			País del cliente
		e-mail	<i>Alfanumérico</i>
			Correo electrónico del cliente
6. Criterios	Representa los criterios comunes para seguridad en tecnología de información	Cod_criterio	<i>Númérico</i>
			Código del criterio
		desc_criterio	<i>Calidad Fiduciarios Seguridad</i>
			Criterios comunes relacionados con la tecnología de la información
7.criterios_proceso	Representa los criterios a considerar en cada proceso	Cod_proceso	(ver entidad PROCESO)
		Cod_dominio	(ver entidad DOMINIO)
		Cod_criterio	(ver entidad CRITERIOS)
8.Dominio	Representa las áreas donde se realiza una auditoría	Cod_dominio	<i>Númérico</i>
			Código del dominio donde se desarrollará la auditoría
		Des_dominio	<b><i>Planeación y organización Adquisición e implementación Entrega y soporte Monitoreo</i></b>
			Nombre del dominio donde se desarrollará la auditoría
9.Dominio_por_proyecto	Representa los dominios que se abordan en un proyecto	Id_proyecto	(ver entidad PROYECTOS)
		Cod_dominio	(ver entidad DOMINIOS)
10.Dominio_proceso_proyecto	Representa los procesos dentro de un determinado dominio que se abordan en un proyecto	Id_proyecto	(ver entidad PROYECTOS)
		Cod_dominio	(ver entidad DOMINIOS)
		Cod_proceso	(ver entidad PROCESOS)
		Observaciones_proceso	<i>Alfanumérico</i>
			Observaciones del auditor relacionadas con la auditoría realizada en el dominio/proceso
		Documentacion_adjunta_proceso	<i>Alfanumérico</i>
			Documentación adjunta del dominio/proceso auditado
11.informe_proyecto	Representa el informe final de la auditoría.	cod_informe	Númérico

			Código del informe
		Id_proyecto	(ver entidad PROYECTOS)
		observa_info	Alfanumérico
			Observaciones del informe
		fecha_info	Fecha
			Fecha del informe
12.item_informe	Representa un ítem del informe final	Cod_item	Númérico
			Código del ítem
		cod_informe	Númérico
			Código del informe
		Id_proyecto	(ver entidad PROYECTOS)
		desc_item_info	Alfanumérico
			Descripción del ítem del informe
13.Objetivo_control	Representa una definición del resultado o propósito que se desea alcanzar	Cod_objetivo_control	Númérico
			Código objetivo de control
	implementando procedimientos de control en una actividad de TI particular	Cod_proceso	(Ver entidad PROCESO)
		Cod_dominio	(Ver entidad DOMINIO)
		Descripcion_objetivo_control	(ver tabla 16: relaciones)
			Descripción del objetivo de control
14. Opcion_resp_rel_inic	Representa las opciones de respuesta a una determinada pregunta de la matriz de preguntas del relevamiento inicial	Cod_resp	Númérico
			Código de la respuesta
		cod_pregunta	(ver entidad RELEVAMIENTO_INICIAL)
		opcion_respuesta	Alfanumérico
			Opción de la respuesta
		riesgo	1-2-3-4-5
			Riesgo que implica la respuesta donde 1 es el menor riesgo
15Opcion_resp_rel_inic_area	Representa la respuesta dada en un sector determinado a una pregunta en un área específica del relevamiento inicial.	Cod_resp	Ver entidad (OPCION_RESP_REL_INIC)
		cod_pregunta	(Ver entidad RELEVAMIENTO_INICIAL)

		Id_proyecto	(Ver entidad PROYECTOS)
		Cod_area	(ver entidad AREAS)
		Cod_sector	(ver entidad SECTOR)
		Riesgo_area	1 - 2-3-4 - 5
			Riesgo
		Respuesta_AREA	Alfanumérico
			Observaciones
16.Opcion_resp_rel_inic_dom_proc	Representa la respuesta dada en un sector determinado a una pregunta en un dominio/proceso específico del relevamiento inicial.	Cod_resp	Ver entidad (OPCION_RESP_REL_INIC)
		cod_pregunta	(Ver entidad RELEVAMIENTO INICIAL))
		Id_proyecto	(Ver entidad PROYECTOS)
		Cod_dominio	(ver entidad DOMINIO)
		Cod_proceso	(ver entidad PROCESO)
		Cod_sector	(ver entidad SECTOR)
		respuesta_proceso	Alfanumérico
			Observaciones
		riesgo_proceso	1 - 2 - 3-4 -5
			Riesgo
17.Opcion_resp_rel_prof	Representa las opciones de respuesta de una determinada pregunta del relevamiento profundo para una determinada pregunta de un área o dominio/proceso	Cod_preg_prof	(ver entidad RELEVAMIENTO PROFUNDO)
		Cod_resp_resp_prof	Numérico
			Código de alternativa de respuesta del relevamiento profundo
		Riesgo_rel_prof	Alfanumérico
			Riesgo que implica la respuesta
		respuesta_rel_prof	1 - 2-3 - 4 -5
18.Opcion_resp_rel_prof_area	Representa la respuesta dada en un sector determinado a una pregunta en un área específica del relevamiento profundo.	Cod_preg_prof	(ver entidad RELEVAMIENTO PROFUNDO)
		Cod_resp_reñ_prof	(ver entidad OPCION_RESP_REL_PROF)
		Id_proyecto	(ver entidad PROYECTOS)
		Cod_area	(ver entidad AREAS)
		Resp_rel_prof	(ver entidad OPCION_RESP_REL_PROF)

		Cod_sector	(ver entidad SECTORES:A_AUDITAR)
		Riesgo_resp_rel_prof	1 - 2 - 3 - 4-5 Riesgo respuesta relevamiento profundo
		Resp_rel_prof	Alfanumérico Observación
19.Opcion_resp_rel_prof_dom_proc	Representa la respuesta dada en un sector determinado a una pregunta en un dominio/proceso especifica del relevamiento profundo.	Cod_resp_reñ_prof	(ver entidad OPCION_RESP_REL_PROF)
		Cod_preg_prof	(ver entidad RELEVAMIENTO PROFUNDO)
		Cod_objetivo_control	(ver entidad OBJETIVO_CONTROL)
		Cod_proceso	(ver entidad PROCESO)
		Cod_dominio	(ver entidad DOMINIO)
		Id_proyecto	(ver entidad PROYECTOS)
		Cod_sector	(ver entidad SECTORES:A_AUDITAR)
		Riesgo_resp-rel_prof	1 - 2 -3 -4 -5 Riesgo respuesta relevamiento profundo
		Resp_rel_prof	Alfanumérico Observación
20.Perfil	Representa perfiles de auditores	Cod_perfil	Numérico Código del perfil del auditor
		Desc_perfil	Alfanumérico Descripción del perfil del auditor
21.Perfil_area	Representa los perfiles de auditores necesarios para realizar una auditoría en un área determinada	Cod_perfil	(ver entidad PERFIL)
		Cod_area	(ver entidad AREA)
22.Perfil_por_auditor	Representa los perfiles de cada auditor	Cod_perfil	(ver entidad PERFIL)
		Cod_auditor	(ver entidad AUDITORES)
23.Perfiles_por_proceso	Representa los perfiles necesarios para realizar un auditoría en un determinado proceso/dominio	Cod_perfil	(ver entidad PERFIL)
		Cod_proceso	(ver entidad PROCESO)
		Cod_dominio	(ver entidad DOMINIO)

24.Proced_por_area	Representa los procedimientos necesarios para realizar una auditoría en un determinado AREA	Cod_area	(ver entidad AREA)
		Cod_procedimiento	(Ver entidad PROCEDIMIENTOS)
25.Procedimientos	Representa las distintas acciones necesarias para realizar una auditoría por ejemplo entrevista, observación, revisión, etc.	Cod_procedimiento	Numérico
			Código de procedimiento
		Desc_procedimiento	alfanumérico
			Descripción del procedimiento
26.Procedimiento_proceso	Representa los procedimientos necesarios para realizar una auditoría en un determinado proceso	Cod_procedimiento	(Ver entidad PROCEDIMIENTOS)
		Cod_proceso	(ver entidad PROCESO)
		Cod_dominio	(ver entidad DOMINIO)
27.Proceso	Representa el Conjunto de actividades que se desarrollan en un determinado	Cod_proceso	Numérico
			Código del proceso
		Cod_dominio	(Ver entidad DOMINIO)
		Desc_proceso	(Ver tabla 16: relaciones)
			Descripción del proceso
28.Proyectos	Representa cada proyecto de auditoría de sistemas	Id_proyecto	Numérico
			Identificación del proyecto
		Cod_cliente	(ver entidad CLIENTES)
		fecha_fin_proyecto	Fecha
			Fecha de fin del proyecto
		fecha_inicio_proyecto	Fecha
	Fecha de inicio del proyecto		
	observaciones_proyecto	Alfanumérico	
			Observaciones relacionadas con el proyecto
29.Recomendaciones	Representa la recomendación genérica que corresponde realizar a la respuesta dada. Esta recomendación es utilizada en el informe final	Cod_preg_prof	(ver entidad OPCION_RESP_REL_PRO)
		Cod_recomendacion	Numérico
			Código de recomendación
		Cod_resp_resp_prof	(ver entidad OPCION_RESP_REL_PRO)
	observa_recomendacion	alfanumérico	
			Recomendación
30.Recursos	Representa los recursos de la tecnología de la información	Cod_recurso	Numérico
			Código del recurso

		Desc_recurso	Gente Sistemas de aplicación Tecnología Instalaciones Datos
			Descripción de los recursos

31.Recurso_proceso	Representa los recursos intervinientes en cada proceso	Cod_proceso	(ver entidad PROCESOS)
		Cod_dominio	(ver entidad DOMINIO)
		Cod_recurso	(ver entidad RECURSOS)
32. Relevamiento_inicial	Representa la matriz completa de preguntas que se pueden realizar en un relevamiento inicial para un determinado área o un dominio/proceso	cod_pregunta	Numérico Código de la pregunta
		Cod_area	(ver entidad AREAS)
		Cod_proceso	(ver entidad PROCESOS)
		Cod_dominio	(ver entidad DOMINIOS)
		preg_rel_inicial	alfanumérico Pregunta del relevamiento inicial
33.Relevamiento_profundo	Representa las preguntas a realizar en el relevamiento profundo en un área o dominio/proceso determinado	Cod_preg_prof	numérico Código de pregunta del relevamiento profundo
		Cod_objetivo_control	(ver entidad OBJETIVO_CONTROL)
		Cod_proceso	(Ver entidad PROCESO)
		Cod_dominio	(Ver entidad DOMINIO)
		Cod_area	(Ver entidad AREA)
		preg_rel_prof	alfanumérico Pregunta del relevamiento profundo
34. Sectores_a_Auditar	Representa los sectores de una empresa que se auditan, estos sectores podrán ser sucursales, centros de costos, etc.	Cod_sector	(ver entidad SECTORES)
		Id_proyecto	(ver entidad PROYECTOS)
		observa_sector	alfanumérico Observaciones relacionadas con el sector a auditor.

	plan de trabajo	Id_proyecto	(ver entidad PROYECTOS)
		desc_tarea	<i>alfanumérico</i>
			Descripción de la tarea
		fecha_inicio_tarea	<i>fecha</i>
			Fecha inicio de la tarea
		fecha_fin_tarea	<i>fecha</i>
			Fecha fin de la tarea
observa_tarea	<i>alfanumérico</i>		
	observación		

## **19. Diseño del Sistema**

### **19.1. Diseño de la Arquitectura del Sistema**

El Sistema es básicamente una aplicación web dinámica y está basado en la comunicación entre los siguientes elementos:

- Lenguaje de programación HTML.
- Lenguaje de programación ASP .Net.
- La comunicación con un web server (IIS).
- Motor de base de datos relacional SQL Server 2005.

La aplicación se construye con los lenguajes HTML y ASP .Net, donde el primero resuelve la interfaz con el usuario final y el segundo las reglas de negocios, y se accede al motor de base de datos SQL 2005 donde están almacenados los datos.

El servidor web IIS permite el acceso remoto a la aplicación, para esto tiene acceso al directorio donde se encuentran las páginas web del sistema.

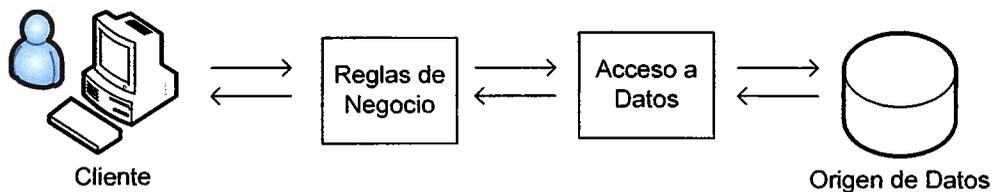
La base de datos puede estar en el mismo servidor web o en otro equipo, siendo lo optimo contar con un servidor web y un servidor de base de datos, aunque también pueden estar en el mismo equipo físico.

Se va a aplicar el modelo de tres capas, cuyos componentes principales son:

- La interfaz del usuario.
- Las reglas de negocios.
- Los datos.
- Origen de datos.

En la actualidad se pretenden desarrollar aplicaciones n capas, la que más comúnmente se utiliza es la de cuatro capas, la capa que se agrega es la que surge de separar definitivamente las reglas de negocio de la de “Acceso a datos”.

Esta arquitectura brinda la ventaja de aislar definitivamente nuestra lógica de negocios de todo lo que tenga que ver con el origen de datos, ya que desde el manejo de la conexión, hasta la ejecución de una consulta, la manejará la capa de acceso de datos. De este modo, ante cualquier cambio eventual, solo se deberá tocar un modulo específico, así como al momento de plantear la escalabilidad de nuestro sistema, si respetamos las reglas básicas de diseño no deberíamos afrontar grandes modificaciones.



**Esquema 7.** Modelo de diseño en cuatro capas.

### 19.1.1 Importancia de la Arquitectura

Existen muchas razones por las que usar el desarrollo de aplicaciones bajo la arquitectura de n capas. A continuación se mencionan:

#### a) Abstracción total acerca del Origen de Datos

Las distintas capas se especializan absolutamente en la funcionalidad que deben brindar (procesamiento en las reglas de negocio o presentación de datos en la capa cliente) sin importar cuál es el origen de los datos procesados.

## **b) Bajo Costo de Desarrollo y Mantenimiento de las Aplicaciones**

Al momento del diseño podemos observar una mayor carga de complejidad, la utilización de esta arquitectura brinda un control más cercano de cada componente, así como también la posibilidad de una verdadera reutilización del código.

## **c) Estandarización de las Reglas de Negocio**

Las reglas de negocio se encuentran encapsuladas en un set de rutinas comunes y pueden ser llamadas desde diversas aplicaciones sin necesidad de saber cómo esta funciona o ha sido diseñada.

## **d) Mejor Calidad en las Aplicaciones**

Como las aplicaciones son construidas en unidades separadas, estas pueden ser evaluadas independientemente y con mucho más detalle, esto conduce a obtener un producto mucho más sólido.

## **e) Reutilización de Código**

La concepción natural de un sistema desarrollado con esta arquitectura, promueve la reutilización de sus componentes en varias partes del propio desarrollo y de futuros sistemas.

## **c) Escalabilidad**

Utilizando servicios como MTS muchos objetos pueden escalar y ser distribuidos en un ambiente transaccional de alta seguridad.

## 19.2 Descripción del Software a Utilizar

### 19.2.1 Internet Information Server

Servicios de Internet Information Server(IIS<sup>14</sup>), es un componente para los ordenadores que funcionan con plataforma Windows. Los servicios IIS engloban un conjunto de herramientas destinadas al control de servicios de Internet como la administración de sitios Web. Entre las características que destacan los IIS, se encuentra una rica dotación de instrumentos satélite al servidor Web, así como características de arquitectura.

Unas de las características más importantes es la presencia del protocolo HTTP1.1<sup>15</sup>, el cual permite la transmisión de más de una solicitud sin tener que esperar su elaboración, por lo que disminuye el tiempo de respuesta en una transmisión. El protocolo HTTP1.1 reside en algunos de los elementos que lo componen, tales como el Pipeling<sup>16</sup>, las conexiones persistentes, las transferencias por bloques CHUNKED y el soporte Proxy<sup>17</sup>.

Los servicios IIS simplifican la creación de una plataforma eficiente para las comunicaciones y las aplicaciones de red. Incluye el soporte necesario para la creación de páginas dinámicas en el servidor mediante el lenguaje ASP<sup>18</sup>.

Los servicios IIS con Windows Server proporcionan capacidades de servidor Web Integrado, confiable, escalable, seguro, y administrable en una intranet<sup>19</sup>, una extranet<sup>20</sup> o en internet.

Los servicios IIS con Windows Server poseen características para la administración, disponibilidad, confiabilidad, seguridad, rendimiento y escalabilidad de los servidores

---

<sup>14</sup> En Inglés, Internet Information Server (IIS)

<sup>15</sup> Véase “Protocolo HTTP1.1”, en el Glosario, página N° 160

<sup>16</sup> Véase “Pipelining” en el Glosario, página N° 160

<sup>17</sup> Véase “Proxy” en el Glosario, página N° 160

<sup>18</sup> En Inglés, Active Server Page (ASP)

<sup>19</sup> Véase “Intranet” en el Glosario, página N° 159

<sup>20</sup> Véase “Extranet” en el Glosario, página N° 159

de aplicaciones web. Los servicios IIS 6.0 también mejoran el desarrollo de aplicaciones Web y la compatibilidad internacional. Juntos, los Servicios IIS y Windows Server proporcionan una solución para servidores Web más confiables, productivos, conectada e integrada<sup>21</sup>.

### 19.2.2 Windows 2003 Server

La elección de un sistema operativo de red es una decisión estratégica. Aunque los servicios de red, datos e impresión compartida aún son requerimientos vitales, las organizaciones actualmente se apoyan en el sistema operativo de servidores para proporcionar muchos servicios adicionales tales como:

- Tener aplicaciones de negocios y proporcionar una infraestructura para la siguiente generación de aplicaciones distribuidas.
- Tener sitios de internet e intranet.
- Proporcionar una infraestructura de comunicaciones completa para facilitar servicios como acceso remoto a través de redes privadas virtual y conexiones telefónicas.
- Proporcionar servicios completos de administración de directorios y de escritorio.

Windows Server 2003 ha incorporado innumerables ventajas, mejoras y nuevas tecnologías, orientadas a descubrir las necesidades actuales de las organizaciones de cualquier tamaño. En el entorno actual se demanda más seguridad, robustez, facilidad de administración e integración con nuevos dispositivos. En la medida en que la tecnología informática avanza, Microsoft Windows Server 2003 la integra y la hace a hacer asequible a los usuarios y organizaciones.

---

<sup>21</sup> Página de la Empresa Microsoft [www.microsoft.com/library](http://www.microsoft.com/library). Internet Information Server

### 19.2.2.1 Características

#### a) Servicios de archivos e impresión compartidos.

Al mejorar la infraestructura del sistema de archivos, destacando las tecnologías DFS, ahora es más fácil utilizar, asegurar y almacenar tanto archivos como otros recursos esenciales, y acceder a la información con herramientas de indexación de contenidos más rápidas.

Con el ASR<sup>22</sup> es más sencillo recuperar el sistema, hacer copias de seguridad de los ficheros y mantener la máxima disponibilidad. La conectividad se ve beneficiada con las características mejoradas de compartición de documentos a lo largo de toda la organización gracias al redirector WebDav<sup>23</sup>.

En lo que respecta a la impresión, además de contar con soporte a más de 3,800 periféricos, los servicios disponen de tecnología tolerante a fallos en clúster, aceptando tareas de otras plataformas como Macintosh, Unix, Linux o Novell, así como Wireless LAN<sup>24</sup> y Bluetooth.

#### b) Servicios de redes y comunicaciones.

Con ayuda de la Resultant Set of Policy se puede analizar el impacto de la implementación de políticas de red y comunicaciones, simplificando así la resolución de problemas.

Mediante los servicios de instalación remota, las herramientas para la migración de configuraciones de usuarios, el nuevo Windows Installer (con soporte de aplicaciones de 64 BI, así como de firmas digitales y CLR), los SUS<sup>25</sup> para testear las actualizaciones de Windows Update antes de ser aplicadas en la organización y

---

<sup>22</sup> En inglés, Automated System Recovery (ASR)

<sup>23</sup> En inglés, Web Digital Authoring & Versioning (WebDav)

<sup>24</sup> Véase “Wireless” en el Glosario, página N° 162

<sup>25</sup> En inglés, Software Update Services (SUS)

muchas otras nuevas características de Microsoft Windows Server 2003, se logra una mejor gestión centralizada de recursos de recursos servicios, contribuyendo así a la reducción de TCO y el aumento de la productividad de los usuarios.

### **c) Servicios de Internet**

IIS 6.0 es un potente servidor Web que ofrece una infraestructura de gran fiabilidad, capacidad de manejo y escalabilidad para aplicaciones Web sobre todas las versiones de Windows Server 2003. IIS hace posible el aumento en la disponibilidad de sitios y aplicaciones Web y a la vez reduce los costes administrativos. IIS 6.0, soporta la DSI<sup>26</sup> con monitorización de estado de salud automático, aislamiento de procesos y capacidades de gestión mejoradas.

#### **19.2.3 Microsoft SQL Server 2005**

SQL Server es un sistema de bases de datos completo y potente, resulta ideal para los programadores especializados en productos Microsoft: ASP, Visual Basic, modelos de objetos, componentes. Además es un sistema de base de datos perfectamente adecuado para aplicaciones críticas y con cualquier grado de complejidad. Es disponible solamente con sistema operativo Windows.

SQL Server utiliza una parte del espacio de la base de datos para guardar el log de transacciones con los comandos pendientes, lo que asegura que, independientemente de si el programador usa o no transacciones en su código, en ningún caso la base de datos quedaría en un estado inconsistente debido a una ejecución parcial de comandos. También ofrece otras características avanzadas orientadas a mantener integridad de la base de datos, como lo son los triggers<sup>27</sup>, y ofrece soporte completo ACID<sup>28</sup>

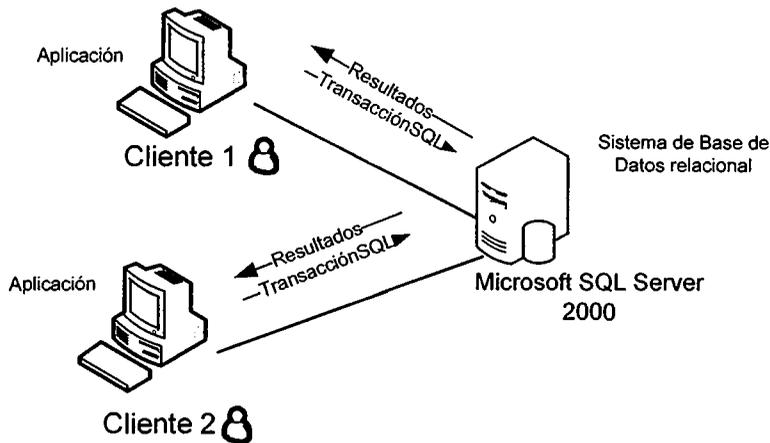
---

<sup>26</sup> Iniciativa de Sistemas Dinámicos de Microsoft (DSI)

<sup>27</sup> Véase “Triggers” en el Glosario, página N° 161

<sup>28</sup> Véase “ACID” en el Glosario, página N° 157

SQL Server es un sistema administrador de Bases de Datos relacionales basadas en la arquitectura Cliente/Servidor (RDBMS) que usa Transact-SQL para mandar peticiones entre un cliente y el SQL Server.



**Esquema 8.** Arquitectura Cliente Servidor

### 19.2.3.1 Arquitectura Cliente/Servidor

SQL Server utiliza la arquitectura Cliente/Servidor para separar la carga de trabajo en tareas que corran en computadoras tipo servidor y tareas que corran en computadoras tipo cliente.

SQL Server es un sistema de dos niveles, ya que, normalmente, un sistema de dos niveles implica que la aplicación del cliente se ejecute en un equipo y sean enviadas las peticiones a un servidor ubicado en otro equipo. Pero en SQL Server, Cliente/Servidor significa que una parte de SQL Server, la parte API<sup>29</sup> del cliente, reside en algún lugar remoto de la estructura de procesamiento, independiente del propio componente servidor.

<sup>29</sup> Interfaces de programación de aplicación (API). Véase “API” en el Glosario, página N° 157

### 19.2.3.2 Sistema Administrador para Base de Datos Relacionales (RDBMS)

El RDBMS es responsable de:

- Mantener las relaciones entre la información y la Base de Datos.
- Asegurarse que toda la información es almacenada correctamente, es decir, que las reglas que define las relaciones entre los datos no sean violadas.
- Recuperar toda la información en un puto conocido en caso de que el sistema falle.

### 19.2.3.3 Transact-SQL

Esta es una versión de SQL usado como lenguaje de programación para SQL Server. SQL es un conjunto de comandos que permite especificar la información que se desea restaurar o modificar. Con transact-SQL se puede tener acceso a la información, realizar búsquedas, actualizar y administrar sistemas de Base de Datos Relacionales.

Para una mejor comprensión de lo antes mencionado se explica lo siguiente:

Cuando una consulta se encuentra lista para ser procesada por SQL Server, el administrador de SQL la busca en le cache<sup>30</sup>, de no encontrarla, se debe compilar. El proceso de compilación engloba varios aspectos. En primer lugar, el análisis y la normalización. El análisis consiste en la disección de la instrucción SQL para convertirla en estructuras de datos que el equipo pueda procesar con mayor rapidez. La normalización está dirigida principalmente a resolver los asuntos a los que se hace referencia en el código SQL, es decir, para indicar las características reales de los mismos en la Base de Datos y para comprobar si la semántica solicitada tiene sentido.

---

<sup>30</sup> Véase “Cache” en el Glosario, Página N° 158

El siguiente paso consiste en la compilación del código Transact-SQL. Los términos Transact-SQL y SQL suelen confundir a los usuarios. Sin embargo, existe una diferencia importante. SQL engloba a todas las instrucciones DML (INSERT, UPDATE, DELETE y SELECT) mientras que transact-SQL, el lenguaje de SQL Server, reúne estas instrucciones DML y permite la creación de procedimientos (instrucciones IF y While, declaraciones de variables locales) que se tratan de forma muy distinta dentro del servidor, ya que la lógica de procedimientos de transact-SQL se compila a través de un motor específico para estas tareas.

#### 19.2.4 ASP .Net

ASP.Net es la última presentación de ASP, sin embargo no es completamente compatible con las versiones anteriores de ASP, es una nueva forma de programación totalmente reescrita. Las versiones anteriores de ASP tienen más en común a PHP que al propio ASP.Net, la cual es una plataforma tecnológica para la construcción de aplicaciones Web.

Una de las flexibilidades de este lenguaje es la de elegir el lenguaje de programación a seguir; ASP.Net soporta lenguajes tales como VBScript, JScript, PerlScript y pitón, a si como lenguajes tales como VB, C#, Cobol y LISP. Esta nueva plataforma utiliza un lenguaje común de ejecución (CLR); el código fuente de los programas elaborados es compilado a código fuente de lenguaje intermedio de Microsoft, el cual ejecuta el CLR.

Esta plataforma tecnológica también ofrece una verdadera OOP<sup>31</sup>, herencia, polimorfismos y encapsulamiento son otras de los métodos soportados. La clase .Net está organizada en clases heredables divididas o estratificadas para tareas determinadas, para trabajar con código XML por ejemplo.

---

<sup>31</sup> Programación Orientada a Objetos (OPP)

Además del lenguaje de programación y la metodología, el acceso a los datos es otra de las preocupaciones principales. La programación en ASP .Net está totalmente integrada con bases de datos, lo cual puede ser alcanzado a través de enlaces ODBC el cual ayuda al establecimiento de una serie de funciones que facilitan el acceso a la base de datos.

Las fortalezas de ASP .Net descansan en su diseño limpio y fácil implementación. Es un lenguaje completamente orientado a objetos, con flexibilidad en el lenguaje y sofisticadas características. Los programadores pueden obtener el soporte de una gran comunidad de desarrolladores de esta tecnología, adicionalmente las características sofisticadas de depuración de errores son muy evolucionadas. Pero lo que se gana con robustez, se paga con eficiencia. ASP .Net es exigente en lo que respecta al uso de la memoria y el tiempo de ejecución.

Para aplicaciones basadas en Web, estas limitaciones pueden ser un gran problema, ya que se necesita el acceso de miles y miles de usuarios por segundo en algunos casos. El uso de la memoria puede llegar a convertirse en un elemento en consideración en el servidor Web. ASP .Net es una tecnología desarrollada por Microsoft para crear páginas Web de contenido dinámico apoyándose de Scripts ejecutados en el servidor. Básicamente una página ASP .Net es una mezcla entre una página HTML y un programa que da como resultado una página HTML que es enviada al cliente (Navegador).

## 19.3 Ventajas y Desventajas del Software utilizado

### 19.3.1 Ventajas del Internet Information Server

Ventajas	Descripción
Escalable y confiable	IIS proporciona un entorno de servidor Web inteligente y confiable. Esta ajustado para proporcionar unas posibilidades de consolidación y escalabilidad optimizadas que sacan el máximo provecho de cada servidor Web.
Seguro y administrable	IIS proporciona una seguridad y capacidad de administración significativamente mejoradas. Las mejoras de seguridad incluyen cambios tecnológicos y procesamiento de solicitudes. Además, se ha mejorado la autenticación y la autorización. Proporciona unas capacidades de administración orientadas aumentadas, una administración mejorada con la metabase xml y nuevas.
Desarrollo y compatibilidad internacional mejorados	Con Windows server e IIS los desarrolladores de aplicaciones se benefician de un entorno de alojamiento de aplicaciones integrado, con una compatibilidad total con las características.

**Tabla 14.** Ventajas y Desventajas de los Servicios IIS.

### 19.3.2 Principales razones para utilizar Windows 2003 Server

#### a) Seguridad

Este beneficio proporciona una infraestructura integrada que ayuda a asegurar que la información estará segura. Además de proporcionar fiabilidad, disponibilidad, y escalabilidad para que las personas puedan ofrecer la infraestructura de red que los usuarios necesitan.

## **b) Productividad**

Este beneficio proporciona herramientas flexibles que ayudaran a ajustar el diseño e implementación a las necesidades organizativas y de red. Ayuda a administrar las redes al reforzar las políticas, tareas automatizadas y simplificación de actualizaciones, por lo que además ayuda a mantener bajos los gastos generales al permitir a los usuarios trabajar más por sus propios medios.

## **c) Conectividad**

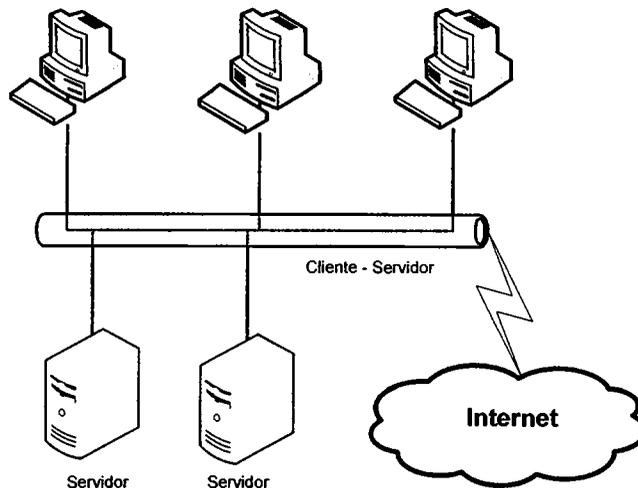
Este beneficio proporciona un servidor Web integrado y un servidor de transmisión de multimedia en tiempo real para ayudar crear más rápido, fácil y segura una intranet dinámica y sitios de internet. Proporciona un servidor de aplicaciones integrado que le ayudará a desarrollar, implementar y administrar servicios Web en XML más fácilmente. Brinda herramientas que le permitirán conectar servicios Web aplicaciones internas, proveedores y socios.

## **d) Valor de Negocio**

Este beneficio proporciona una guía de fácil uso para soluciones que permitan poner rápidamente la tecnología a trabajar. Ayuda a consolidar servidores aprovechando lo último en metodologías, software y hardware para optimizar la implementación de un servidor.

### 19.3.3 Ventajas de SQL Server 2005

#### 19.3.3.1 Plataformas para SQL



**Esquema 9.** Plataforma SQL

#### 19.3.3.2 Integración de SQL con Microsoft Windows

SQL se encuentra totalmente integrado con Windows y toma ventaja de muchas de sus características:

##### a) Soporte de Transacciones

Una transacción consiste en una interacción con una estructura de datos que, aún siendo compleja y estar compuesta por varios procesos que se deben aplicar uno después del otro, por lo que necesitamos que sea equivalente a una interacción atómica. Es decir, que se realice de una sola vez y que la estructura a medio manipular no sea jamás alcanzable por el resto del sistema.

##### b) Estabilidad

En informática, se dice que un sistema es estable cuando su nivel de fallos disminuye por debajo de un determinado umbral, que varía dependiendo de estabilidad que se requiera.

### **c) Seguridad**

La seguridad informática, consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera en que se ha decidido. La seguridad informática busca la protección contra los riesgos ligados a la informática. Los riesgos son en función de varios elementos:

- Amenazas que pesan sobre los activos (datos) a proteger.
- Las vulnerabilidades de estos activos.
- Su sensibilidad, la cual es la conjunción de diferentes factores:
  - ✓ La confidencialidad
  - ✓ La integridad
  - ✓ La disponibilidad o accesibilidad
  - ✓ Revisión anticipada de la información

### **d) Escalabilidad**

Es la capacidad de un sistema informático de adaptarse a un número de usuarios cada vez mayor, sin perder calidad en los servicios.

En general, se puede definir como la capacidad del sistema informático de cambiar su tamaño o configuración para adaptarse a las circunstancias cambiantes. Por ejemplo, una empresa, que establece una red de usuarios por internet, no solamente quiere que su sistema informático tenga capacidad para acoger a los actuales clientes, sino también a los clientes que puedan tener en el futuro.

#### **e) Procedimientos almacenados**

Es un programa o procedimiento, el cual es almacenado físicamente en una base de datos. La ventaja de un procedimiento almacenado es que al ser ejecutado, en respuesta a una petición de usuario, es ejecutado directamente en el motor de la base de datos, el cual usualmente corre en un servidor separado.

#### **f) Soporte Multiprocesador**

SQL Server soporta las capacidades de multiprocesamiento simétrico(SMP) de Windows NT, SQL Server automáticamente toma ventaja de cualquier procesador adicional que sea agregado al servidor.

#### **g) Microsoft Cluster Server**

Es un componente de Windows NT Enterprise Edition. Soporta la conexión de dos servidores, o nudos, en un clúster para aumentar las habilidades y tener un mejor manejo de la información y las aplicaciones. SQL Server trabaja en conjunto con el clúster Server para intercambiar papeles automáticamente en caso de que el nodo primario falle.

## **20. Diseño de la Base de Datos**

Después del diseño conceptual en donde se han incluido los Diagramas de Flujo de Datos, corresponde la etapa de creación del modelo de base de datos que se utilizará para almacenar la información; por lo que se han considerado los procesos involucrados en cada módulo.

El modelo está basado en un diagrama entidad-relación cuya documentación estará definida en el diccionario de datos.

## 20.1 Entidad Relación

Para visualizar la lógica y el diseño implementado en la base de datos, se ha dividido el diagrama E-R en secciones que corresponden a los módulos del sistema.

- Inicialización de Auditoría
- Estudio Preliminar
- Recursos Involucrados
- Planificación
- Desarrollo de Auditoría
- Seguimiento de Auditoría

## 20.2 Descripción por módulos de la Base de Datos

### 20.2.1 Módulo de Inicio o Parametrización Catálogos

En este módulo se incluyen todas las tablas de mantenimiento de los catálogos, datos básicos del proyecto, las áreas a auditar, las características de la empresa a auditar.

Tb\_Objetivos

Tb\_Dominio

Tb\_Dominio\_Proceso\_Proyecto

Tb\_Dominio\_por\_Proyecto

Tb\_Preguntas\_Ini\_A

Tb\_Perfil

Tb\_Criterios

Tb\_Procedimiento

Tb\_Procesos

Tb\_Preguntas\_Ini\_Do

Tb\_RespPreguntas\_Ini\_Dom

Tb\_Areas

Tb\_Resp\_Preguntas\_Ini\_A

Tb\_Audidores

Tb\_Recursos

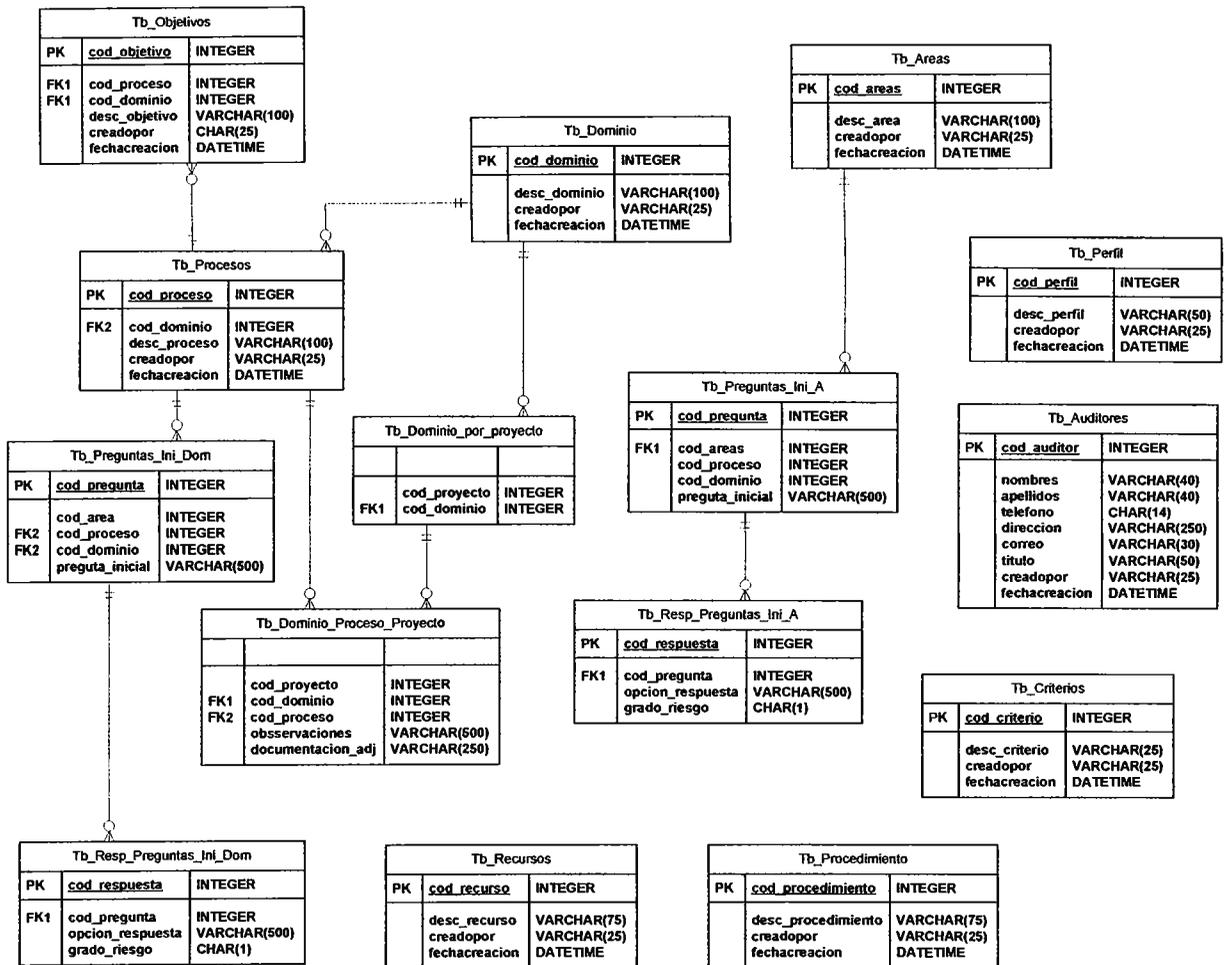


Diagrama 7. E-R Módulo de Inicio o Parametrización Catálogos.

## 20.2.2 Módulo de Inicialización de Auditoría

En este módulo se incluyen todas las tablas transaccionales que involucran el inicio de una auditoría.

Las tablas involucradas en este módulo son:

Tb\_Clientes

Tb\_Proyectos

Tb\_Areas\_por\_proyecto

Tb\_Areas

Tb\_Dominio\_Proceso\_Proyecto

Tb\_Opcion\_Resp\_Ini\_Dom

Tb\_Sectores\_A\_Ini

Tb\_Opcion\_Resp\_Ini\_A

Tb\_Dominio\_por\_Proyecto

Tb\_Dominio

Tb\_Procesos

Tb\_Sectores\_Domi\_Ini

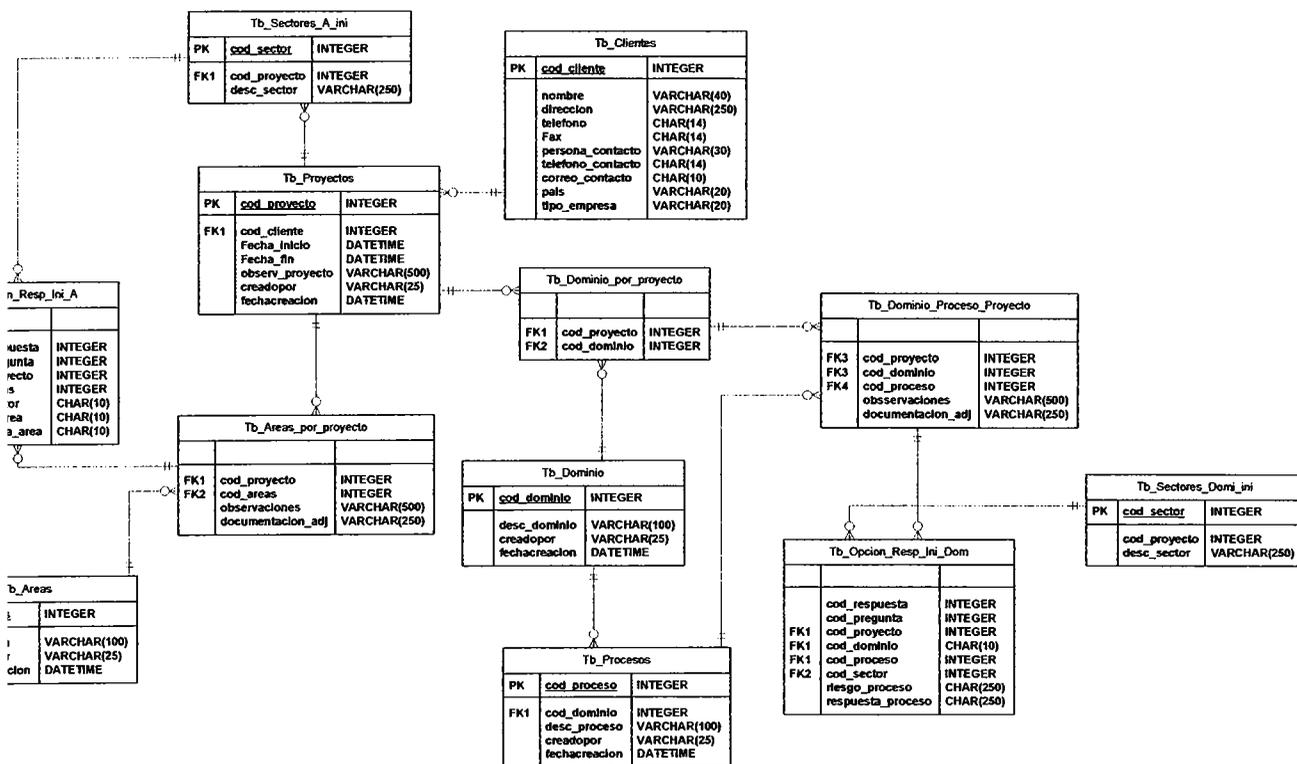


Diagrama 8. E-R para el módulo de inicialización de auditoría.

## 20.2.3 Módulos de Estudio Preliminar y Recursos

Las tablas involucradas en estos módulos son las siguientes:

Tb_Dominio	Tb_Dominio_Proyecto	Tb_Areas
Tb_Procesos	Tb_Dom_Personal_Audit	Tb_Area_Personal_Audi
Tb_Preguntas_Ini_A	Tb_Resp_Pregunas_Ini_A	Tb_Preguntas_Ini_Dom
Tb_Recursos_Procesos	Tb_resp_Preguntas_Ini_Dom	Tb_Recursos

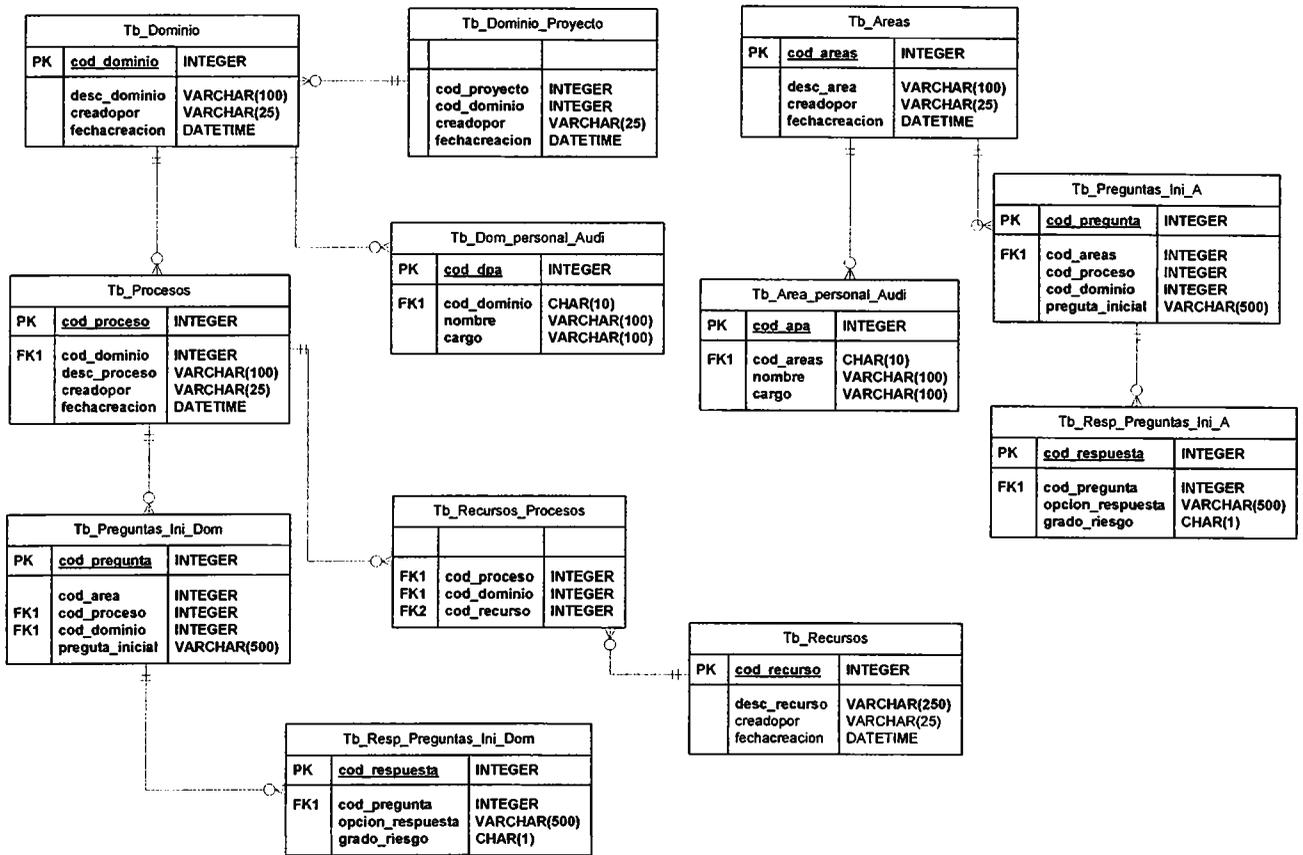


Diagrama 9. E-R Módulos Estudio Preliminar y Recursos.

## 20.2.4 Módulo de Planificación

Las tablas involucradas en este módulo son las siguientes:

Tb\_Audidores

Tb\_Tareas\_por\_proyecto

Tb\_Tareas

Tb\_Proyectos

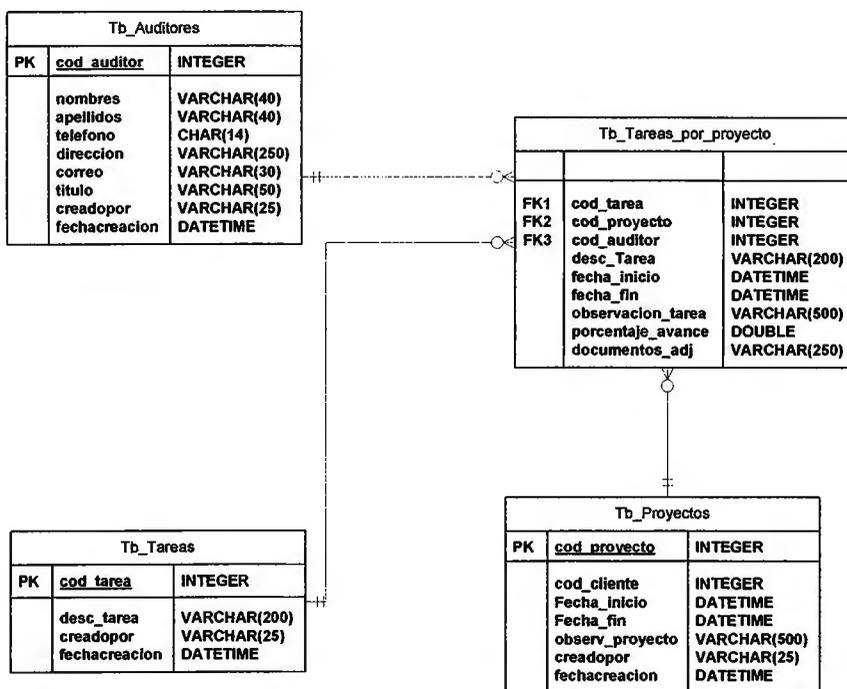


Diagrama 10. E-R Módulo Planificación.

## 20.2.5 Módulos de Desarrollo y Seguimiento

Las tablas involucradas en estos módulos son las siguientes:

- |                             |                            |
|-----------------------------|----------------------------|
| Tb_Area                     | Tb_Areas_por_Proyecto      |
| Tb_Proyectos                | Tb_Preguntas_Prof_A        |
| Tb_Opcion_Resp_Prof_A       | Tb_Dominio_Por_Project     |
| Tb_Dominio_Proceso_Proyecto | Tb_Resp_Preguntas_Prof_A   |
| Tb_Sectores_A_Prof          | Tb_Dominio                 |
| Tb_Opcion_Resp_Prof_Dom     | Tb_Recomendaciones         |
| Tb_Procesos                 | Tb_Resp_Preguntas_Prof_Dom |
| Tb_Preguntas_Prof_Domi      | Tb_Obejtivos               |
| Tb_Secciones_Domi_Ini       |                            |

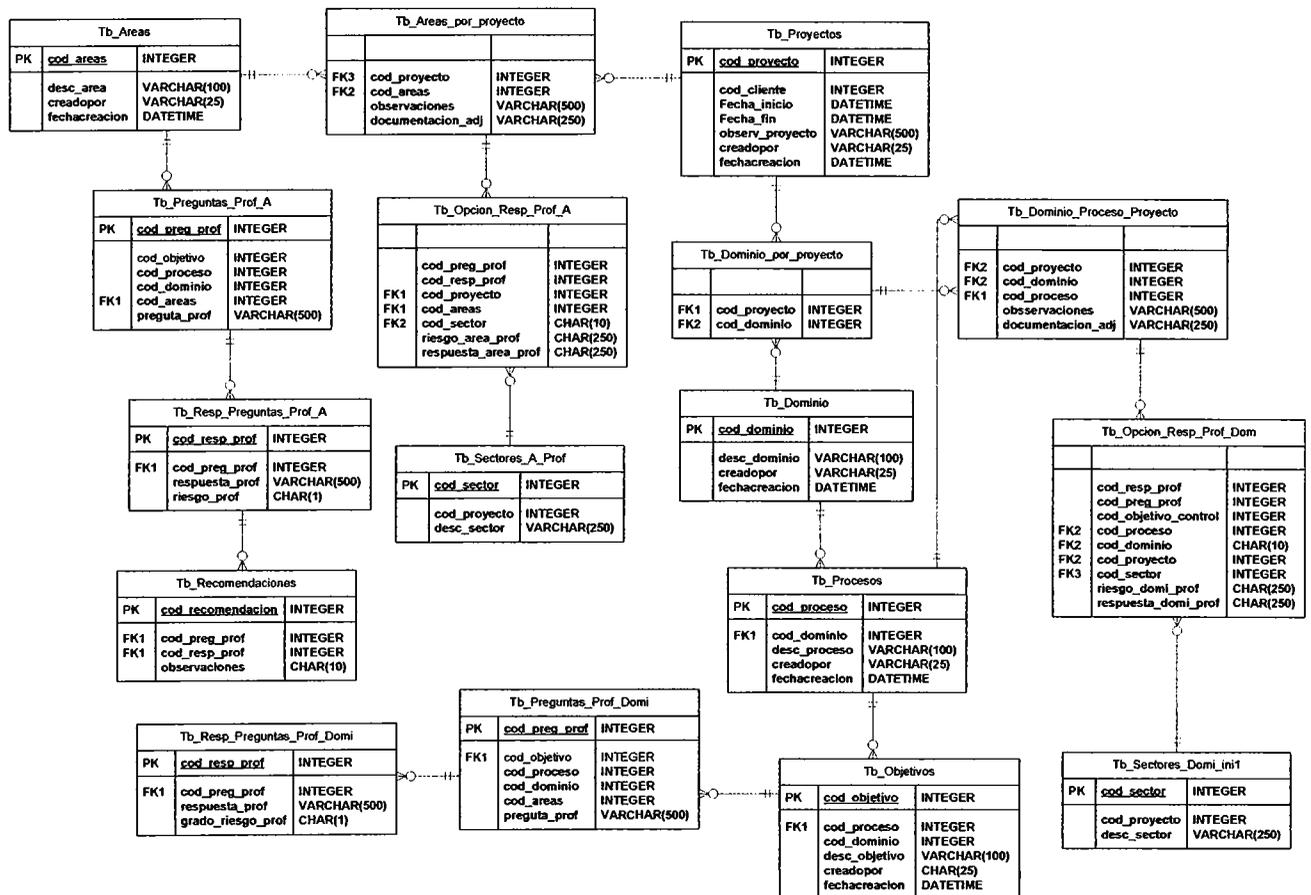


Diagrama 11. E-R Módulos de Desarrollo y Seguimiento.

## 20.3 Diccionario de Datos

### Tb\_AplicacionesWeb

<b>Nombre Tablas</b>	Tb_AplicacionesWeb
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_appWeb
<b>Llave Foránea</b>	

### Columnas

<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Datos</b>	<b>Null</b>	<b>Definición</b>
Cod_appWeb		INTEGER	N	
Aplicacion		INTEGER	N	
FechaIngreso		DATETIME	N	
UsuarioIngreso		VARCHAR(25 )	N	

### Tb\_Areas

<b>Nombre Tabla</b>	Tb_Areas
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_areas
<b>Llave Foránea</b>	

### Columnas

<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Dato</b>	<b>Null</b>	<b>Definición</b>
Cod_areas		INTEGER	N	
Area		NVARCHAR(15)	N	
Desc_area		VARCHAR(40)	Y	
CreadoPor		VARCHAR(25 )	N	

### Tb\_Areas\_por\_proyecto

<b>Nombre Tabla</b>	Tb_Areas_por_proyecto
<b>Nombre Propietario</b>	
<b>Llave primaria</b>	Cod_proyecto
<b>Llave Foránea</b>	Cod_areas

## Columnas

Nombre Columna	Dominio	Tipo Datos	Null	Definición
Cod_proyecto		INTEGER	N	
Cod_areas		INTEGER	N	
Observaciones		CHAR(10)	Y	
documentacion_adj		CHAR(10)	Y	

## Tb\_Audidores

<b>Nombre Tabla</b>	Tb_Audidores
<b>Propietario</b>	
<b>Llave Primaria</b>	Cod_auditor
<b>Llave Foránea</b>	

## Columnas

Nombre Columna	Dominio	Tipo Datos	Null	Definición
Cod_auditor		INTEGER	N	
Nombres		VARCHAR(40)	N	
Apellidos		VARCHAR(40)	N	
Telefono		CHAR(14)	N	
Direccion		VARCHAR(250)	N	
Correo		VARCHAR(30)	Y	
Titulo		VARCHAR(50)	Y	
CreadoPor		VARCHAR(25)	N	
FechaCreacion		DATETIME	N	
Activo		BOOLEAN	N	

## Tb\_Audidores\_por\_Proyecto

<b>Nombre Tabla</b>	Tb_Audidores_por_proyecto
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_proyecto
<b>Llave Foránea</b>	Cod_auditor

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definicion
Cod_proyecto		INTEGER	N	
Cod_auditor		INTEGER	N	

## Tb\_AplicacionesWeb

<b>Nombre Tabla</b>	Tb_AplicacionesWeb
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_AppWeb
<b>Llave Foránea</b>	

### Columnas

<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Dato</b>	<b>Null</b>	<b>Definición</b>
Cod_AppWeb		INTEGER	N	
Aplicación		VARCHAR(100)	N	
FechaIngreso		DATETIME	N	
UsuarioIngreso		NVARCHAR(25)	N	

## Tb\_ArchivoConfig

<b>Nombre Tabla</b>	Tb_ArchivoConfig
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Id
<b>Llave Foránea</b>	

### Columnas

<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Dato</b>	<b>Null</b>	<b>Definición</b>
Id		INTEGER	N	
CodArchivo		NCHAR(10)	N	
ArchivoConfig		NVARCHAR(25)	N	
FechaCreacion		DATETIME	N	

## Tb\_ArchivoSecciones

<b>Nombre Tabla</b>	Tb_ArchivoSecciones
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Id
<b>Llave Foránea</b>	

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Id		INTEGER	N	
CodArchivo		NCHAR(10)	N	
CodSeccion		NVARCHAR(15)	N	
Seccion		NVARCHAR(25)	N	
FechaCreacion		DATETIME	N	

## Tb\_Clientes

<b>Nombre Tabla</b>	Tb_Clientes
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_Cliente
<b>Llave Foránea</b>	

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_cliente		INTEGER	N	
Cliente		VARCHAR(250)	N	
DirecCliente		VARCHAR(500)	N	
NomContacto		NVARCHAR(40)	N	
ApeContacto		NVARCHAR(40)	N	
Cargo		NVARCHAR(75)	Y	
TelContacto		CHAR(14)	N	
Fax		CHAR(14)	Y	
CorreoContacto		CHAR(100)	Y	
Pais		VARCHAR(20)	Y	
TipoEmpresa		VARCHAR(20)	N	
CreadoPor		VARCHAR(25)	N	
FechaCreacion		DATETIME	N	
Estado		BOOLEAN	N	

## Tb\_Criterios

<b>Nombre Tabla</b>	Tb_Criterios
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_Criterio
<b>Llave Foránea</b>	

## Columnas

<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Dato</b>	<b>Null</b>	<b>Definición</b>
Cod_criterio		INTEGER	N	
Nombre		VARCHAR(60)	N	
Desc_Criterio		VARCHAR(2000)	N	
CreadoPor		NVARCHAR(25)	N	
FechaCreacion		DATETIME	N	

## Tb\_Criterios\_Procesos

<b>Nombre Tabla</b>	Tb_Criterios_Procesos
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Id
<b>Llave Foránea</b>	Cod_proceso, Cod_dominio, Cod_criterio

## Columnas

<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Dato</b>	<b>Null</b>	<b>Definición</b>
Cod_proceso		INTEGER	N	
Cod_dominio		INTERGER	N	
Cod_criterio		INTEGER	N	

## Tb\_Dominio

<b>Nombre Tabla</b>	Tb_Dominio
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_dominio
<b>Llave Foránea</b>	

Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_dominio		INTEGER	N	
IDDominio		VARCHAR(3)	N	
Nombre		VARCHAR(30)	N	
Desc_Domino		VARCHAR(100)	N	
CreadoPor		VARCHAR(25)	N	
FechaCreacion		DATETIME	N	

**Tb\_Domino\_por\_Proyecto**

<b>Nombre Tabla</b>	Tb_Domino_por_Proyecto
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	
<b>Llave Foránea</b>	Cod_proyecto, Cod_dominio

Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_proyecto		INTEGER	N	
Cod_dominio		INTERGER	N	

**Tb\_Dominio\_proceso\_proyecto**

<b>Nombre Tabla</b>	Tb_Dominio_proceso_proyecto
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	
<b>Llave Foránea</b>	Cod_proyecto, Cod_dominio, Cod_proceso

Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_proyecto		INTEGER	N	
Cod_dominio		INTEGER	N	
Cod_proceso		INTEGER	N	
Observaciones		VARCHAR(500)	N	
Documentos_adj		VARCHAR(250)	N	

## Tb\_Especialidad

<b>Nombre Tabla</b>	Tb_Especialidad
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_especialidad
<b>Llave Foránea</b>	

### Columna

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_especialidad		INTEGER	N	
Especialidad		VARCHAR(100)	N	
FechaCreacion		DATETIME	N	
CreadoPor		VARCHAR(25)	N	

## Tb\_EspecialidadAuditor

<b>Nombre Tabla</b>	Tb_EspecialidadAuditor
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	
<b>Llave Foránea</b>	Cod_especialidad, Cod_auditor

### Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_especialidad		INTEGER	N	
Cod_auditor		INTEGER	N	

## Tb\_Informe\_Proyecto

<b>Nombre Tabla</b>	Tb_Informe_Proyecto
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	
<b>Llave Foránea</b>	Cod_informe, Cod_proyecto

### Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_informe		INTEGER	N	
Cod_proyecto		INTEGER	N	
Observación		VARCHAR(250)	N	
Fecha_Informe		DATETIME	N	

### Tb\_Item\_Informe

<b>Nombre Tabla</b>	Tb_Item_Informe
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	
<b>Llave Foránea</b>	Cod_item, Cod_informe, Cod_proyecto

### Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_item		INTEGER	N	
Cod_informe		INTEGER	N	
Cod_proyecto		INTEGER	N	
Desc_item		VARCHAR(500)	N	

### Tb\_MenuAppWeb

<b>Nombre Tabla</b>	Tb_MenuAppWeb
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_menu
<b>Llave Foránea</b>	Cod_AppWeb

### Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_menu		INTEGER	N	
Cod_AppWeb		INTEGER	N	
Descripción		INTEGER	N	
FechaCreacion		DATETIME	N	
CreadoPor		NVARCHAR(25)	N	

### Tb\_Objetivos

<b>Nombre Tabla</b>	Tb_Objetivos
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_objetivo
<b>Llave Foránea</b>	Cod_proceso

Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_objetivo		INTEGER	N	
Cod_proceso		INTEGER	N	
Cod_dominio		INTEGER	N	
Desc_objetivo		VARCHAR(2000)	N	
FechaCreacion		DATETIME	N	
CreadoPor		NVARCHAR(25)	N	

**Tb\_Opcion\_resp\_ini\_A**

<b>Nombre Tabla</b>	<b>Tb_Opcion_resp_ini_A</b>
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_respuesta, Cod_pregunta
<b>Llave Foránea</b>	Cod_proyecto, Cod_area, Cod_sector

Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_repuesta		INTEGER	N	
Cod_pregunta		INTEGER	N	
Cod_proyecto		INTEGER	N	
Cod_area		INTEGER	N	
Cod_sector		INTEGER	N	
Riesgo_area		VARCHAR(200)	N	
Respuesta_area		VARCHAR(200)	N	

**Tb\_Opcion\_Resp\_Ini\_Dom**

<b>Nombre Tabla</b>	<b>Tb_Opcion_Resp_Ini_Dom</b>
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_respuesta, Cod_pregunta, Cod_proyecto, Cod_dominio, Cod_proceso, Cod_sector

Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_repuesta		INTEGER	N	
Cod_pregunta		INTEGER	N	
Cod_proyecto		INTEGER	N	
Cod_dominio		INTEGER	N	
Cod_proceso		INTEGER	N	
Cod_sector		INTEGER	N	
Riesgo_proceso		VARCHAR(200)	N	
Respuesta_Proceso		VARCHAR(250)	N	

**Tb\_Opcion\_Resp\_Pof\_Dom**

Nombre Tabla	Tb_Opcion_Resp_Pof_Dom
Nombre Propietario	
Llave Primaria	
Llave Foránea	Cod_proceso, Cod_dominio, Cod_proyecto, Cod_sector

Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_proceso		INTEGER	N	
Cod_dominio		INTEGER	N	
Cod_proyecto		INTEGER	N	
Cod_sector		INTEGER	N	
Cod_resp_prof		INTEGER	N	
Cod_Preg_prof		INTEGER	N	
Cod_Objetivo_Control		INTEGER	N	
Riesgo_domi_prof		CHAR(1)	N	
Respuesta_domi_prof		VARCHAR(250)	N	

**Tb\_Opcion\_Resp\_Prof\_A**

Nombre Tabla	Tb_Opcion_Resp_Prof_A
Nombre Propietario	
Llave Primaria	
Llave Foránea	Cod_proyecto, Cod_areas

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_proyecto		INTEGER	N	
Cod_areas		INTEGER	N	
Cod_preg_prof		INTEGER	N	
Cod_resp_prof		INTEGER	N	
Cod_sector		INTEGER	N	
Riesgo_area_prof		CHAR(1)	N	
Respuesta_area_prof		VARCHAR(250)	N	

## Tb\_OpcionesMenu

Nombre Tabla	Tb_OpcionesMenu
Nombre Propietario	
Llave Primaria	Cod_opcion
Llave Foránea	Cod_menú, Cod_AppWeb

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_opcion		INTEGER	N	
Cod_menu		INTEGER	N	
Cod_AppWeb		INTEGER	N	
Descripción		INTEGER	Y	
OpcionPadreId		INTEGER	Y	
Nivel		INTEGER	Y	
SubNivel		INTEGER	Y	
ExpandedOpcionPadreId		INTEGER	Y	
SelectedIndexOpcion		INTEGER	Y	
Url		NVARCHAR(100)	Y	
ToolTip		NVARCHAR(200)	Y	
BackgroundImageCollapsed		NVARCHAR(100)	Y	
BackgroundImageExpanded		NVARCHAR(100)	Y	
BackgroundImageHoverCollapsed		NVARCHAR(100)	Y	
BackgroundImageHoverExpanded		NVARCHAR(100)	Y	
ImageCollapsed		NVARCHAR(100)	Y	
ImageExpanded		NVARCHAR(100)	Y	
ImageHoverCollapsed		NVARCHAR(100)	Y	
ImageHoverExpanded		NVARCHAR(100)	Y	
ImageCollapsedItem		NVARCHAR(100)	Y	
ImageHoverItem		NVARCHAR(100)	Y	
ImageSelectedItem		NVARCHAR(100)	Y	
ImageDisabledItem		NVARCHAR(100)	Y	
FechaCreacion		DATETIME	N	

## Tb\_Perfil

<b>Nombre Tabla</b>	Tb_Perfil
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Id
<b>Llave Foránea</b>	

### Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Id		INTEGER	N	
Cod_perfil		VARCHAR(10)	N	
Perfil		VARCHAR(25)	N	
Desc_perfil		VARCHAR(300)	N	
Estado		BOOLEAN	N	
CreadoPor		VARCHAR(25)	N	
FechaCreacion		DATETIME	N	

## Tb\_Perfil\_Acceso\_Usuario

<b>Nombre Tabla</b>	Tb_Perfil_Acceso_Usuario
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Id
<b>Llave Foránea</b>	

### Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_appweb		INTEGER	N	
Cod_perfil		VARCHAR(10)	N	
Cod_usuario		INTEGER	N	
EstadoAcceso		BOOLEAN	N	

## Tb\_Perfil\_MenuAppWeb

<b>Nombre Tabla</b>	Tb_Perfil_MenuAppWeb
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	
<b>Llave Foránea</b>	Cod_perfil, Cod_AppWeb, Cod_menú, Cod_Opcion

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_perfil		INTEGER	N	
Cod_AppWeb		INTEGER	N	
Cod_Menu		INTEGER	N	
Cod_Opcion		INTEGER	N	
Estado		BOOLEAN	N	

## Tb\_Perfil\_por\_Proceso

<b>Nombre Tabla</b>	Tb_Perfil_por_Proceso
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_perfil, Cod_proceso, Cod_dominio
<b>Llave Foránea</b>	

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_perfil		INTEGER	N	
Cod_proceso		INTEGER	N	
Cod_dominio		INTEGER	N	

## Tb\_Preguntas\_ini\_A

<b>Nombre Tabla</b>	Tb_Preguntas_ini_A
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_pregunta
<b>Llave Foránea</b>	Cod_areas

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_pregunta		INTEGER	N	
Cod_areas		INTEGER	N	
Cod_proceso		INTEGER	N	
Cod_dominio		INTEGER	N	
Pregunta_inicial		VARCHAR(500)	N	

### Tb\_Preguntas\_ini\_dom

<b>Nombre Tabla</b>	Tb_Preguntas_ini_dom
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_pregunta
<b>Llave Foránea</b>	

### Columnas

<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Dato</b>	<b>Null</b>	<b>Definición</b>
Cod_preguntas		INTEGER	N	
Cod_areas		INTEGER	N	
Cod_proceso		INTEGER	N	
Cod_dominio		INTEGER	N	
Pregunta_inicial		VARCHAR(500)	N	

### Tb\_Preguntas\_prof\_A

<b>Nombre Tabla</b>	Tb_Preguntas_prof_A
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_preg_prof
<b>Llave Foránea</b>	Cod_areas

### Columnas

<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Dato</b>	<b>Null</b>	<b>Definición</b>
Cod_preg_prof		INTEGER	N	
Cod_objetivo		INTEGER	N	
Cod_proceso		INTEGER	N	
Cod_areas		INTEGER	N	
Pregunta_prof		VARCHAR(500)	N	

### Tb\_Preguntas\_prof\_domi

<b>Nombre Tabla</b>	Tb_Preguntas_prof_domi
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_preg_prof
<b>Llave Foránea</b>	

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_preg_prof		INTEGER	N	
Cod_objetivo		INTEGER	N	
Cod_proceso		INTEGER	N	
Cod_areas		INTEGER	N	
Pregunta_prof		VARCHAR(500)	N	

## Tb\_Procedimiento

<b>Nombre Tabla</b>	Tb_Procedimiento
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_procedimiento
<b>Llave Foránea</b>	

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_procedimiento		INTEGER	N	
Desc_procedimiento		VARCHAR(250)	N	
CreadoPor		VARCHAR(25)	N	
FechaCreacion		DATETIME	N	

## Tb\_Procedimiento\_Area

<b>Nombre Tabla</b>	Tb_Procedimiento_Area
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	
<b>Llave Foránea</b>	Cod_areas, Cod_Procedimiento

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_areas		INTEGER	N	
Cod_procedimiento		INTEGER	N	

### Tb\_Procedimiento\_proceso

<b>Nombre Tabla</b>	Tb_Procedimiento_proceso
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	
<b>Llave Foránea</b>	Cod_procedimiento

#### Columnas

<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Dato</b>	<b>Null</b>	<b>Definición</b>
Cod_procedimiento		INTEGER	N	
Cod_proceso		INTEGER	N	
Cod_dominio		INTEGER	N	

### Tb\_Procesos

<b>Nombre Tabla</b>	Tb_Procesos
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_proceso
<b>Llave Foránea</b>	Cod_dominio

#### Columnas

<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Dato</b>	<b>Null</b>	<b>Definición</b>
Cod_proceso		INTEGER	N	
Cod_dominio		INTEGER	N	
IDProceso		VARCHAR(3)	N	
Nombre		VARCHAR(30)	N	
Desc_proceso		VARCHAR(2000)	N	
CreadoPor		VARCHAR(25)	N	
FechaCreacion		DATETIME	N	

### Tb\_Proyectos

<b>Nombre Tabla</b>	Tb_Proyectos
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_proyecto
<b>Llave Foránea</b>	Cod_cliente

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_proyecto		INTEGER	N	
Cod_cliente		INTEGER	N	
Fecha_Inicio		DATETIME	N	
Fecha_Fin		DATETIME	N	
Observ_proyecto		VARCHAR(500)	N	
SNDominio		BOOLEAN	N	
SNArea		BOOLEAN	N	
Objetivos		VARCHAR(2000)	N	
Alcances		VARCHAR(2000)	N	
Estado		BOOLEAN	N	
CreadoPor		VARCHAR(25)	N	
FechaCreacion		DATETIME	N	

## Tb\_Recomendaciones\_Dom

<b>Nombre Tabla</b>	Tb_Recomendaciones_Dom
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_recomendación
<b>Llave Foránea</b>	Cod_resp_prof

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_recomendacion		INTEGER	N	
Cod_preg_prof		INTEGER	N	
Cod_resp_prof		INTEGER	N	
Observaciones		VARCHAR(500)	N	

## Tb\_Recomendaciones\_Area

<b>Nombre Tabla</b>	Tb_Recomendaciones_Area
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_recomendación
<b>Llave Foránea</b>	Cod_resp_prof

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_recomendacion		INTEGER	N	
Cod_preg_prof		INTEGER	N	
Cod_resp_prof		INTEGER	N	
Observaciones		VARCHAR(500)	N	

## Tb\_Recursos

<b>Nombre Tabla</b>	Tb_Recursos
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_recurso
<b>Llave Foránea</b>	

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_recurso		INTEGER	N	
Nombre		VARCHAR(60)	N	
Desc_recurso		VARCHAR(2000)	N	
CreadoPor		VARCHAR(25)	N	
FechaCreacion		DATETIME	N	

## Tb\_Recursos\_Procesos

<b>Nombre Tabla</b>	Tb_Recursos_Procesos
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	
<b>Llave Foránea</b>	Cod_proceso, Cod_recurso

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Id		INTEGER	N	
Cod_proceso		INTEGER	N	
Cod_dominio		INTEGER	N	
Cod_recurso		INTEGER	N	

### Tb\_Resp\_Preguntas\_ini\_A

<b>Nombre Tabla</b>	Tb_Resp_Preguntas_ini_A
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_respuesta
<b>Llave Foránea</b>	Cod_pregunta

#### Columnas

<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Dato</b>	<b>Null</b>	<b>Definición</b>
Cod_respuesta		INTEGER	N	
Cod_pregunta		INTEGER	N	
Opcion_respuesta		VARCHAR(500)	N	
grado_riesgo		CHAR(1)	N	

### Tb\_Resp\_Preguntas\_ini\_Dom

<b>Nombre Tabla</b>	Tb_Resp_Preguntas_ini_Dom
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_respuesta
<b>Llave Foránea</b>	Cod_pregunta

#### Columnas

<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Dato</b>	<b>Null</b>	<b>Definición</b>
Cod_respuesta		INTEGER	N	
Cod_pregunta		INTEGER	N	
Opcion_respuesta		VARCHAR(500)	N	
grado_riesgo		CHAR(1)	N	

### Tb\_Resp\_Preguntas\_Prof\_A

<b>Nombre Tabla</b>	Tb_Resp_Preguntas_Prof_A
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_resp_prof
<b>Llave Foránea</b>	Cod_preg_prof

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_resp_prof		INTEGER	N	
Cod_preg_prof		INTEGER	N	
Respuesta_prof		VARCHAR(500)	N	
grado_riesgo		CHAR(1)	N	

## Tb\_Resp\_preguntas\_prof\_domi

<b>Nombre Tabla</b>	Tb_Resp_Preguntas_Prof_domi
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_resp_prof
<b>Llave Foránea</b>	Cod_preg_prof

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_resp_prof		INTEGER	N	
Cod_preg_prof		INTEGER	N	
respuesta_prof		VARCHAR(500)	N	
grado_riesgo		CHAR(1)	N	

## Tb\_Sectores\_A\_ini

<b>Nombre Tabla</b>	Tb_Sectores_A_ini
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_sector
<b>Llave Foránea</b>	Cod_proyecto

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_sector		INTEGER	N	
Cod_proyecto		INTEGER	N	
desc_sector		VARCHAR(250)	N	

### Tb\_Sectores\_A\_Prof

<b>Nombre Tabla</b>	Tb_Sectores_A_Prof
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_sector
<b>Llave Foránea</b>	Cod_proyecto

#### Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_sector		INTEGER	N	
Cod_proyecto		INTEGER	N	
desc_sector		VARCHAR(250)	N	

### Tb\_Sectores\_domi\_ini

<b>Nombre Tabla</b>	Tb_Sectores_domi_ini
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_sector
<b>Llave Foránea</b>	

#### Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_sector		INTEGER	N	
Cod_proyecto		INTEGER	N	
desc_sector		VARCHAR(250)	N	

### Tb\_SesionGeneradas

<b>Nombre Tabla</b>	Tb_SesionGeneradas
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Id
<b>Llave Foránea</b>	

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Id		INTEGER	N	
SesionGenerada		VARCHAR(25)	N	
EstadoSesion		BOOLEAN	N	
UsrGeneracionSesion		VARCHAR(25)	N	
FechaCreacion		DATETIME	N	

## Tb\_Tarea\_por\_proyecto

<b>Nombre Tabla</b>	Tb_Tarea_por_proyecto
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	
<b>Llave Foránea</b>	Cod_tarea, Cod_proyecto

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_tarea		INTEGER	N	
Cod_proyecto		INTEGER	N	
Cod_auditor		INTEGER	N	
Desc_tarea		VARCHAR(250)	N	
Fecha_inicio		DATETIME	N	
Fecha_fin		DATETIME	N	
Observación_tarea		VARCHAR(250)	N	
Porcentaje_avance		FLOAT	N	
Documentos_adj		VARCHAR(250)	S	

## Tb\_Tareas

<b>Nombre Tabla</b>	Tb_Tareas
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_tarea
<b>Llave Foránea</b>	

## Columnas

Nombre Columna	Dominio	Tipo Dato	Null	Definición
Cod_tarea		INTEGER	N	
Desc_tarea		VARCHAR(250)	N	
CreadoPor		VARCHAR(25)	N	
FechaCreacion		DATETIME	N	

## Tb\_Usuarios

<b>Nombre Tabla</b>	Tb_Usuarios
<b>Nombre Propietario</b>	
<b>Llave Primaria</b>	Cod_usuario
<b>Llave Foránea</b>	

## Columnas

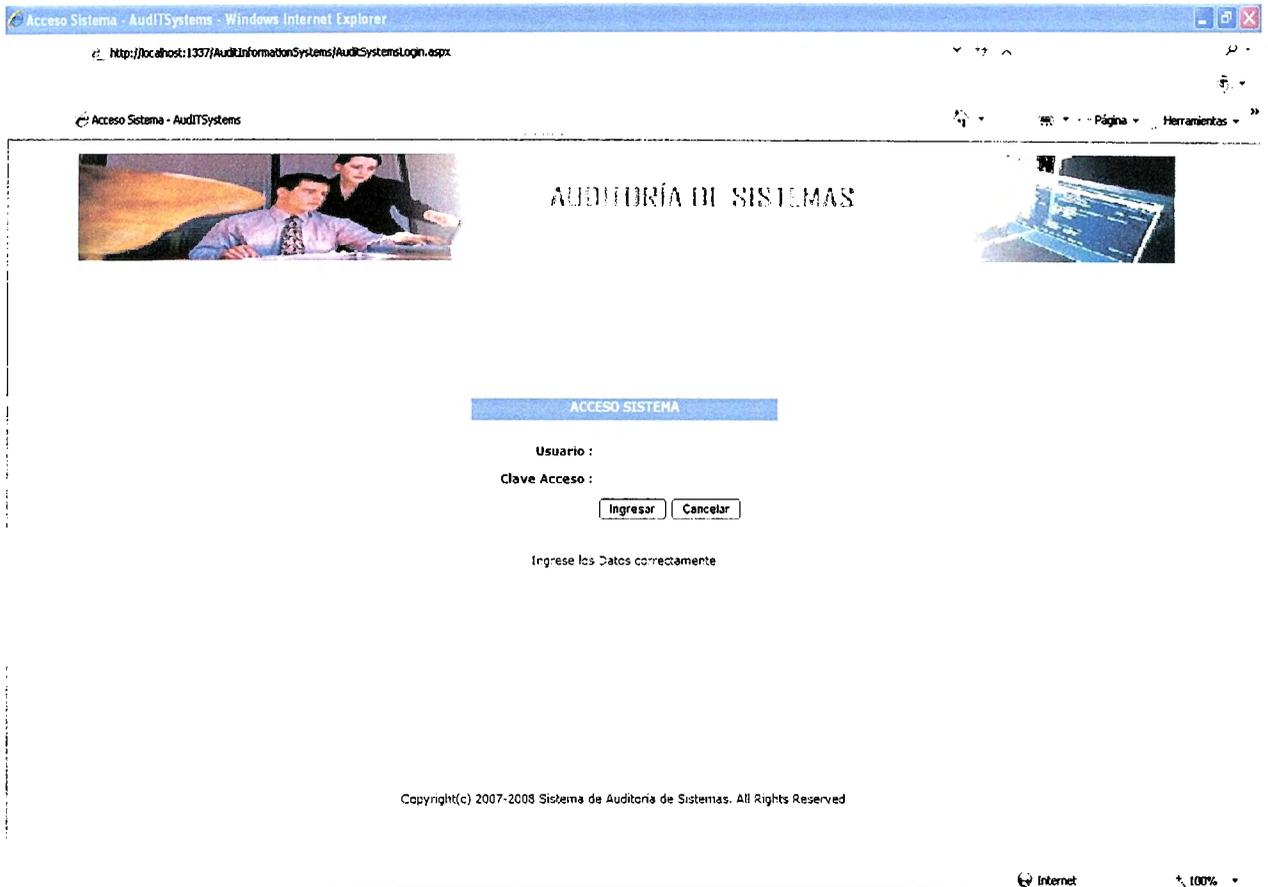
<b>Nombre Columna</b>	<b>Dominio</b>	<b>Tipo Dato</b>	<b>Null</b>	<b>Definición</b>
Cod_usuario		INTEGER	N	
Cod_auditor		INTEGER	N	
Usuario		VARCHAR(25)	N	
ClaveApp		VARCHAR(25)	N	
Estado		BOOLEAN	N	
FechaCreacion		DATETIME	N	
CreadoPor		NVARCHAR(25)	N	
ActualizarClave		BOOLEAN	N	

## 20.4 Diseño de la Interfase Web

Una de las finalidades principales que se buscan además de la funcionalidad del sistema, es la homogeneidad del mismo, lo cual permita a los diferentes usuarios el fácil manejo del sistema.

A continuación se encuentran las principales interfaces del sistema, las cuales no solo permiten tener un mejor panorama de los aspectos relevantes a implementar, sino que a su vez, aportan innovaciones al proceso actual tales como: conexión al sistema, mantenimientos de información, consultas a la base de datos y generación de resultados.

## 20.4.1 Interfase Web



**Imagen 1:** Autenticación de usuarios.

### **Descripción:**

Pantalla inicial de autenticación de usuarios.

### **Funcionalidad:**

Permite la autenticación de todos los usuarios registrados al sistema.

## **Parametrización Sistema**

Configuración

**Seguridad**

**Inicialización Auditoría**

**Estudio Preliminar**

**Recursos**

**Planificación**

**Seguimiento Auditoría**

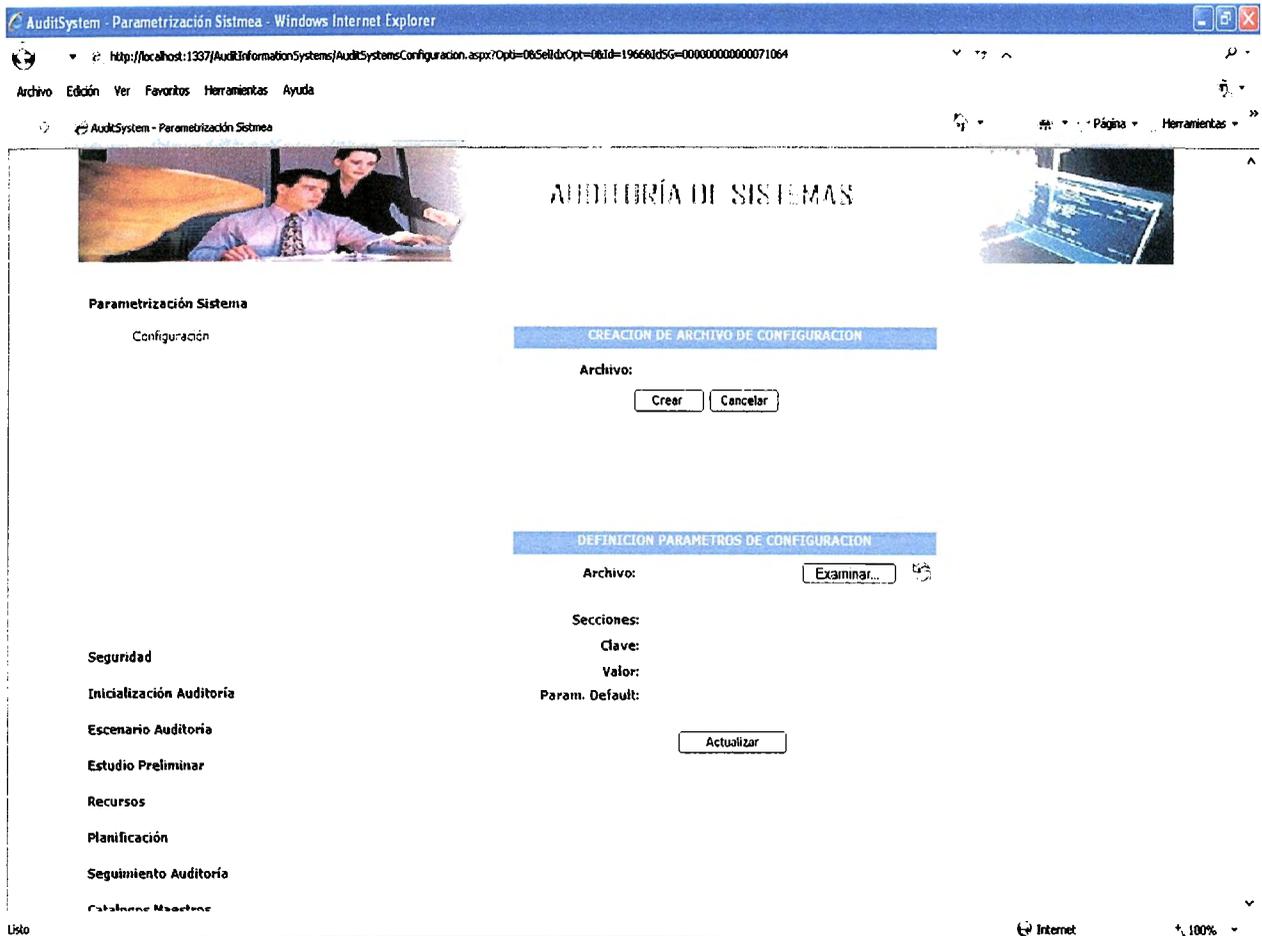
**Catalogos Maestros**

**Imagen 2: Menú Principal.**

El sistema cuenta con un menú principal formado por paneles, este se encuentra ubicado en la parte izquierda del navegador web. Cada panel del menú incluye las diferentes opciones de navegación dentro del sistema.

Las diferentes opciones se muestran de acuerdo a los permisos otorgados al perfil al que pertenece un usuario determinado.

## 20.4.1.1 Panel Parametrización Sistema



**Imagen 3:** Configuración de parámetros de conexión.

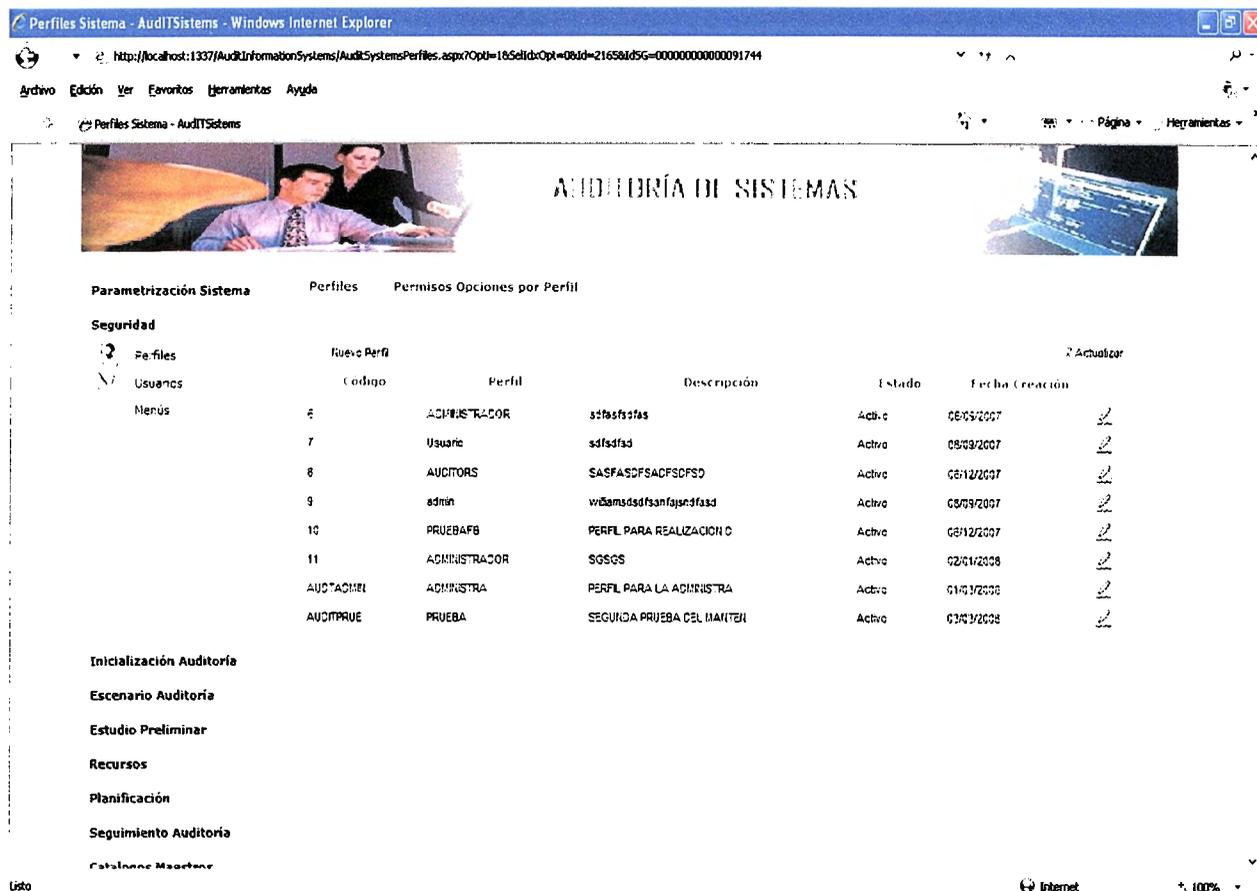
### **Descripción:**

Pantalla de configuración de parámetros de conexión.

### **Funcionalidad:**

Permite la creación de un archivo .ini que almacena los parámetros de conexión hacia la base de datos.

## 20.4.1.2 Panel Seguridad



The screenshot shows a web browser window titled 'Perfiles Sistema - AudITSystems - Windows Internet Explorer'. The address bar shows the URL: <http://localhost:1337/AuditInformationSystems/AuditSystemsPerfiles.aspx?Opt=1&SId=Opt=0&Id=2165&IdSG=0000000000091744>. The page content includes a header with the title 'AUDITORÍA DE SISTEMAS' and a navigation menu with options: 'Parametrización Sistema', 'Perfiles', 'Permisos Opciones por Perfil', 'Seguridad', 'Iniciación Auditoría', 'Escenario Auditoría', 'Estudio Preliminar', 'Recursos', 'Planificación', 'Seguimiento Auditoría', and 'Catálogo Maestro'. The 'Perfiles' section is active, displaying a table of profiles.

Perfiles	Nuevo Perfil	Perfil	Descripción	Estado	Fecha Creación	Actualizar
Menús	6	ADMINISTRADOR	sdfasdfsas	Activo	08/05/2007	
	7	Usuario	sdfasdfsad	Activo	08/03/2007	
	8	AUDITORS	SASFASDFASDFSD	Activo	08/12/2007	
	9	admin	wdsasdfsasfjsefsasf	Activo	09/09/2007	
	10	PRUEBAFB	PERFIL PARA REALIZACION O	Activo	08/12/2007	
	11	ADMINISTRADOR	SGSGS	Activo	02/01/2008	
	AUDTACMEI	ADMINISTRA	PERFIL PARA LA ADMINISTRA	Activo	01/01/2008	
	AUDITPRUE	PRUEBA	SEGUNDA PRUEBA DEL MAINTEN	Activo	01/01/2008	

Imagen 4: Definición de perfiles.

### Descripción:

Pantalla de definición de perfiles.

### Funcionalidad:

Permite el mantenimiento de los perfiles a manejar dentro del sistema. Esta opción se encuentra habilitada solo para el administrador del sistema.

Mantenimiento de Perfiles

**ADICION DE PERFILES**

Id :

Perfil :

Descripción :

Estado :

Agregar Cancelar

**Imagen 5:** Adición de perfiles.

**Descripción:**

Pantalla de adición de perfiles.

**Funcionalidad:**

Permite definir nuevos perfiles dentro del sistema.

Mantenimiento de Perfiles

**ACTUALIZACIÓN DE PERFILES**

Id : AUDTADMIN

Perfil : ADMINISTRA

Descripción : PERFIL PARA LA ADMINISTRA

Estado :

Actualizar Cancelar

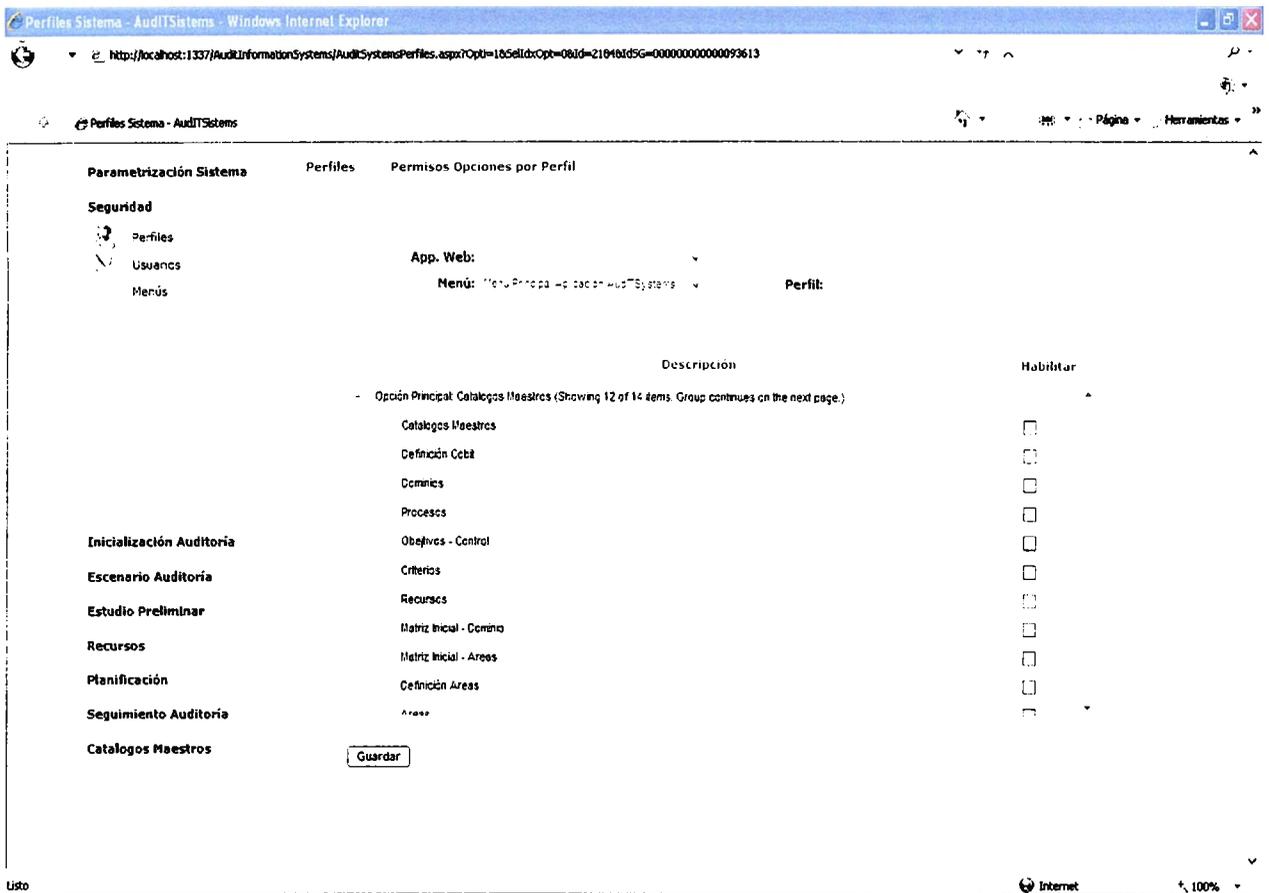
**Imagen 5:** Modificación de perfiles.

**Descripción:**

Pantalla de modificación de perfiles.

**Funcionalidad:**

Permite modificar perfiles existentes en el sistema.



**Imagen 6:** Asignación de opciones a perfiles.

**Descripción:**

Pantalla de asignación de opciones a perfiles.

**Funcionalidad:**

Permite la asignación de opciones a un perfil determinado.

<http://localhost:1337/AuditInformationSystems/AuditSystemUsuarios.aspx?Opt=1&SelIdcOpt=1&Id=2166&IdSG=0000000000064549>

Archivo Edición Ver Favoritos Herramientas Ayuda

AuditSystem - Mantenimiento de Usuarios



# AUDITORÍA DE SISTEMAS



Parametrización Sistema    Mantenimiento Usuarios    Usuarios por Perfil

**Seguridad**

Perfiles	Nuevo Usuario					Actualizar
Usuarios	Código	Nombre	Usuario	Estado		
Menús	22	GERARDO BELTRAN	rbeltran	Alta		
	23	GERARDO BELTRAN	JUDITAX23	Baja		
	30	Isa Lopez	isa	Baja		
	31	VICENTE FERNANDEZ	Fernandez	Alta		
	32	VICENTE FERNANDEZ	prueba	Alta		
	33	Isa Lopez	prueba2	Alta		
	34	VICENTE FERNANDEZ	Prueba hoy	Alta		
	35	GERARDO BELTRAN	PruebaDos	Alta		
<b>Inicialización Auditoría</b>	36	Judith Melgar	kruger799	Baja		
<b>Escenario Auditoría</b>	37	Judith Melgar	fffff	Alta		
<b>Estudio Preliminar</b>	39	GERARDO BELTRAN	freedyyyyy	Alta		

Change page: 1 2 . . Displaying page 1 of 2. Items 1 to 12 of 17.

Recursos  
 Planificación  
 Seguimiento Auditoría  
 Catalogo Maestros

Listo    Internet    100%

**Imagen 7: Mantenimiento de usuarios.**

### Descripción:

Pantalla de mantenimiento de usuarios.

### Funcionalidad:

Permite listar todos los usuarios activos e inactivos, desde esta pantalla se dará mantenimiento a todos los usuarios del sistema.

Mantenimiento de Usuarios

**ADICION DE USUARIOS**

**Id :**  
**Usuario :**  
**Auditor :** ▼  
**Clave :**  
**Confirmación :**  
**Estado :**

**Imagen 8:** Adición de usuarios.

**Descripción:**

Pantalla de adición de usuarios.

**Funcionalidad:**

Permite ingresar nuevos usuarios al sistema.

Mantenimiento de Usuarios

**MODIFICACION DE USUARIOS**

**Id :**  
**Usuario :** Prueba hoy  
**Auditor :** VICENTE FERNANDEZ ▼  
**Clave :**  
**Confirmación :**  
**Estado :**

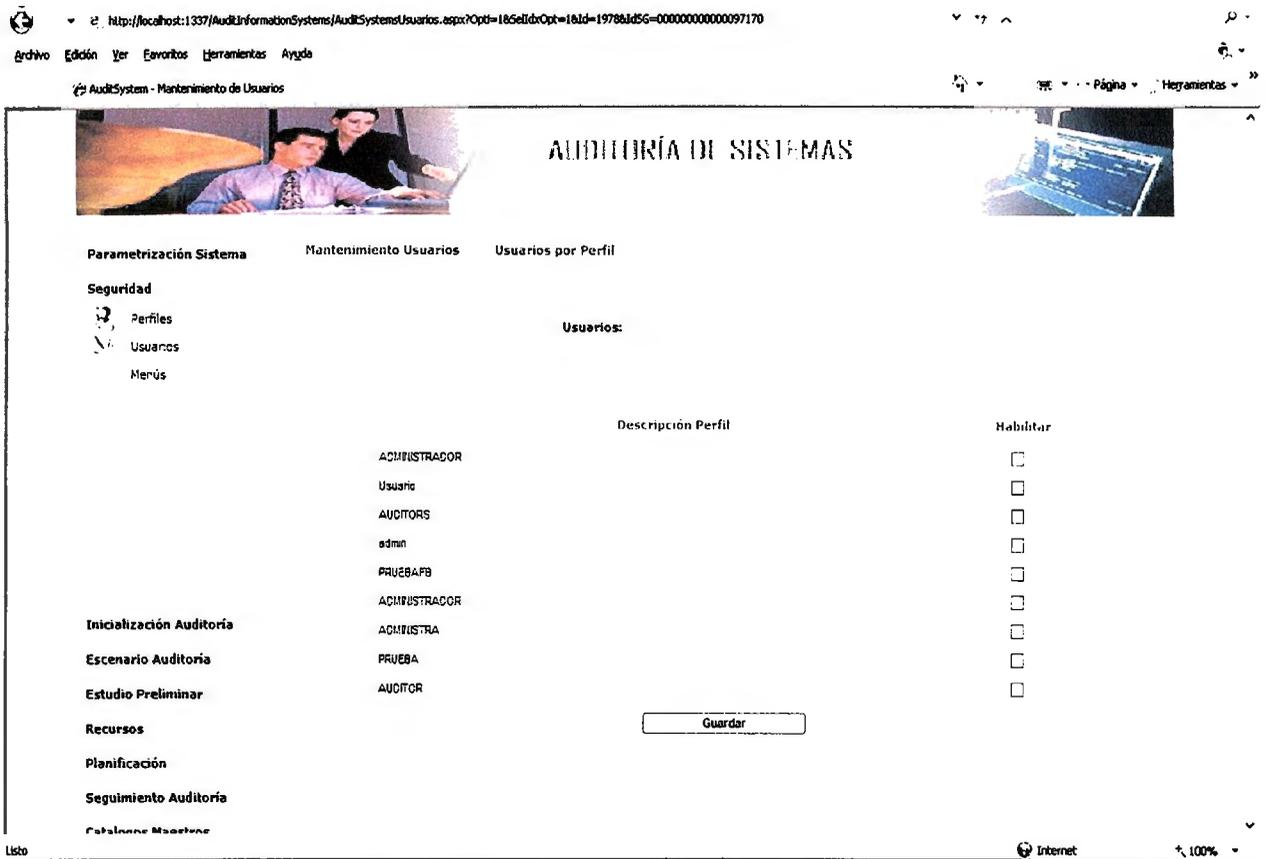
**Imagen 9:** Modificación de usuarios.

**Descripción:**

Pantalla de modificación de usuarios.

**Funcionalidad:**

Permite actualizar usuarios existentes en el sistema.



**Imagen 10:** Usuarios por perfil.

**Descripción:**

Pantalla Usuarios por perfil.

**Funcionalidad:**

Permite relacionar un usuario a un perfil existente dentro del sistema.

## 20.4.1.3 Panel Inicialización Auditoría

The screenshot shows a web browser window with the URL `http://localhost:1337/AuditInformationSystems/AuditSystemsAlcanceObjetivo.aspx?Opt=2&SelId=Opt=0&Id=2171&IdSG=00000000000061475`. The application interface includes a navigation menu with options like 'Parametrización Sistema', 'Datos del Proyecto', 'Datos de Clientes', 'Auditores', 'Auditoría', and 'Informes'. The 'Datos del Proyecto' form contains fields for 'Código del Proyecto', 'Nombre del Proyecto', 'Auditar Por' (with radio buttons for 'Areas' and 'Cobit'), 'Fecha Inicio', 'Fecha Finalización', 'Estado Proyecto' (set to 'Activo'), 'Objetivos', and 'Alcances'. Below the form are 'Guardar' and 'Cancelar' buttons. A table at the bottom lists audit scenarios with columns for 'Código Proyecto', 'Proyecto', 'Fecha Inicio', 'Fecha Fin', and 'Seleccionar'.

	Código Proyecto	Proyecto	Fecha Inicio	Fecha Fin	
Escenario Auditoría	1	guardar	01/09/2007	13/10/2007	Seleccionar
Estudio Preliminar	2	programacion de auditoriascosdesdesdesdes	05/10/2007	17/11/2007	Seleccionar
Recursos	3	Auditoria Sistema Bocadei	01/03/2008	31/03/2008	Seleccionar
Planificación	4	Auditoria Bocadei Prueba	01/03/2008	20/03/2008	Seleccionar
Seguimiento Auditoría	5	Prueba Pruebassssss	13/03/2008	27/03/2008	Seleccionar
Catalogos Maestros	6	Prueba 11032008	03/03/2008	13/03/2008	Seleccionar

Imagen 11: Datos del proyecto.

### Descripción:

Pantalla Alcances y Objetivos – Ficha Datos del Proyecto.

### Funcionalidad:

Permite dar ingreso a nuevos proyectos que estarán disponibles para darles inicio a un proceso de auditoría.

http://localhost:1337/AuditInformationSystems/AuditSystemsAlcanceObjetivo.aspx?Opt=2&SelIdrOpt=0&Id=2172&IdSG=00000000000022658

Archivo Edición Ver Favoritos Herramientas Ayuda

Alcances y Objetivos - AuditSystems

Parameetrización Sistema Datos del Proyecto Datos de Clientes Auditores Auditoría Informes

Seguridad

Inicialización Auditoría

Alcances y Objetivos

Código de Cliente : 4

Empresa : Corporación Panamericana S.A de C.V Estado : Activo

Col. Escalón Teléfono : 22779300

Dirección : Fax : 22779300

Pais : El Salvador

Nombre(s) Contacto : Ricardo Apellido(s) Contacto : Fuentes

Cargo : Jefe Auditoría Interna

Teléfono : 22779376 Correo Electrónico : rfuentes@yahoo.com

Actualizar Cancelar

Escenario Auditoría

Estudio Preliminar

	Código	Cliente	Estado	Proyecto
Recursos	4	Corporación Panamericana S.A de C.V	Alta	Asignada Editar
Planificación	29	BOCADELI S.A DE C.V	Alta	Asignada Editar
Seguimiento Auditoría	30	Empresas Fantasma S.A de C.V	Alta	Asignada Editar

Catalogos Maestros

Listo Internet 100%

**Imagen 12:** Datos de clientes.

## Descripción:

Pantalla Alcances y Objetivos – Ficha Datos de Clientes.

## Funcionalidad:

Permite dar ingreso a los clientes que estarán asociados a un proceso de auditoría.

**ASIGNACION DE PROYECTOS - CLIENTES**

**Cod. Cliente :** 29  
**Cliente :** BOCADELIS.A CE C.V

**Proyecto :**  
**Fecha Inicio :**  
**Fecha Fin :**

Proyecto	Fecha Inicio	Fecha Fin	
Auditoria Bocadeli Prueba	01/03/2008	20/03/2008	Seleccionar
Prueba Prusbasssss	13/03/2008	27/03/2008	Seleccionar

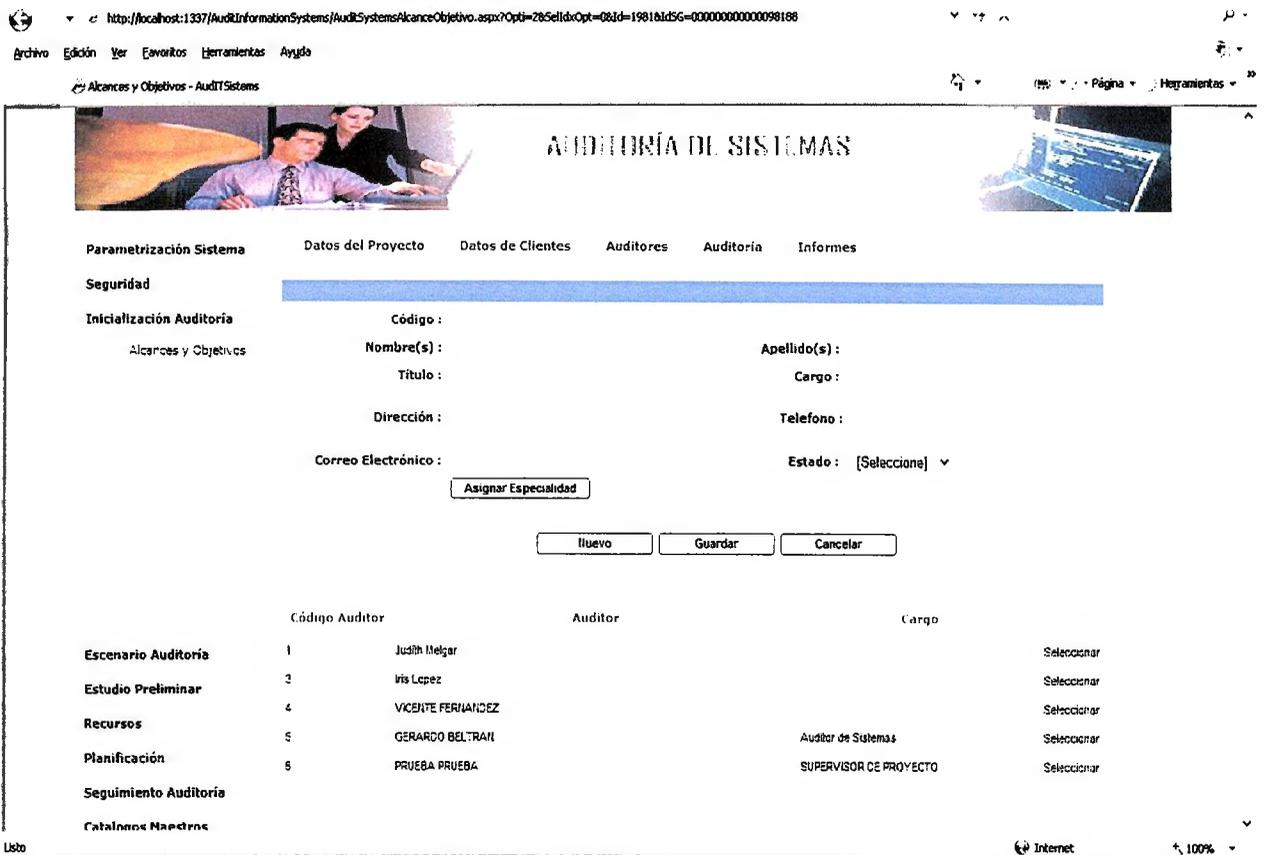
**Imagen 13:** Asignación de proyectos a clientes.

**Descripción:**

Pantalla Alcances y Objetivos – Ficha Auditores – Asignación de proyectos a clientes.

**Funcionalidad:**

Permite asociar los proyectos a los clientes.



**Imagen 14:** Definición de auditores.

### Descripción:

Pantalla Alcances y Objetivos – Ficha Auditores.

### Funcionalidad:

Permite dar ingreso a los auditores que estarán disponibles para realizar procesos de auditoría en el sistema.

Descripción

Habilitar



◀

Guardar

▶

**Imagen 15:** Asignación de especialidades.

**Descripción:**

Pantalla Alcances y Objetivos – Ficha Auditores – Asignación de especialidad.

**Funcionalidad:**

Permite asignar una o varias especialidades a cada auditor, con el fin de tener una serie de auditores clasificados por especialidad.

<http://localhost:1337/AuditInformationSystems/AuditSystemsAlcanceObjetivo.aspx?Opt=2&SelIdxOpt=0&Id=2174&IdSG=00000000000754>

Archivo Edición Ver Favoritos Herramientas Ayuda

Alcances y Objetivos - AuditSystems

## AUDITORÍA DE SISTEMAS

Parametrización Sistema    Datos del Proyecto    Datos de Clientes    Auditores    Auditoría    Informes

**Seguridad**

**Inicialización Auditoría**

	Código	Proyecto	Estado	Fecha Inicio	Fecha Fin
Alcances y Objetivos	1	guardar	En Proceso	01/09/2007	13/10/2007
	2	programacion de auditoria	Iniciada	08/10/2007	17/11/2007

Escenario Auditoría  
 Estudio Preliminar  
 Recursos  
 Planificación  
 Seguimiento Auditoría

Listo    Internet    100%

**Imagen 16:** Auditoría.

**Descripción:**

Pantalla Alcances y Objetivos – Ficha Auditoría.

**Funcionalidad:**

Permite definir el área o dominio COBIT donde se realizará la auditoría.

## Áreas

Proyecto :

Código	Area	
AFI	Auditoría de la Gestión Informática	<input type="checkbox"/>
ASG	Auditoría de la Seguridad General	<input type="checkbox"/>
ORGBJ	Organización Gestión y Base Jurídica	<input type="checkbox"/>
APR	Auditoría de la Producción	<input type="checkbox"/>
AAO	Auditoría de las Aplicaciones Operativas	<input type="checkbox"/>
APD	Auditoría de Proyectos en Desarrollo	<input type="checkbox"/>
AMA	Auditoría del Mantenimiento de Aplicaciones	<input type="checkbox"/>
ACF	Auditoría de la Calidad del Software	<input type="checkbox"/>

}

Imagen 17: Tipos de Auditoría.

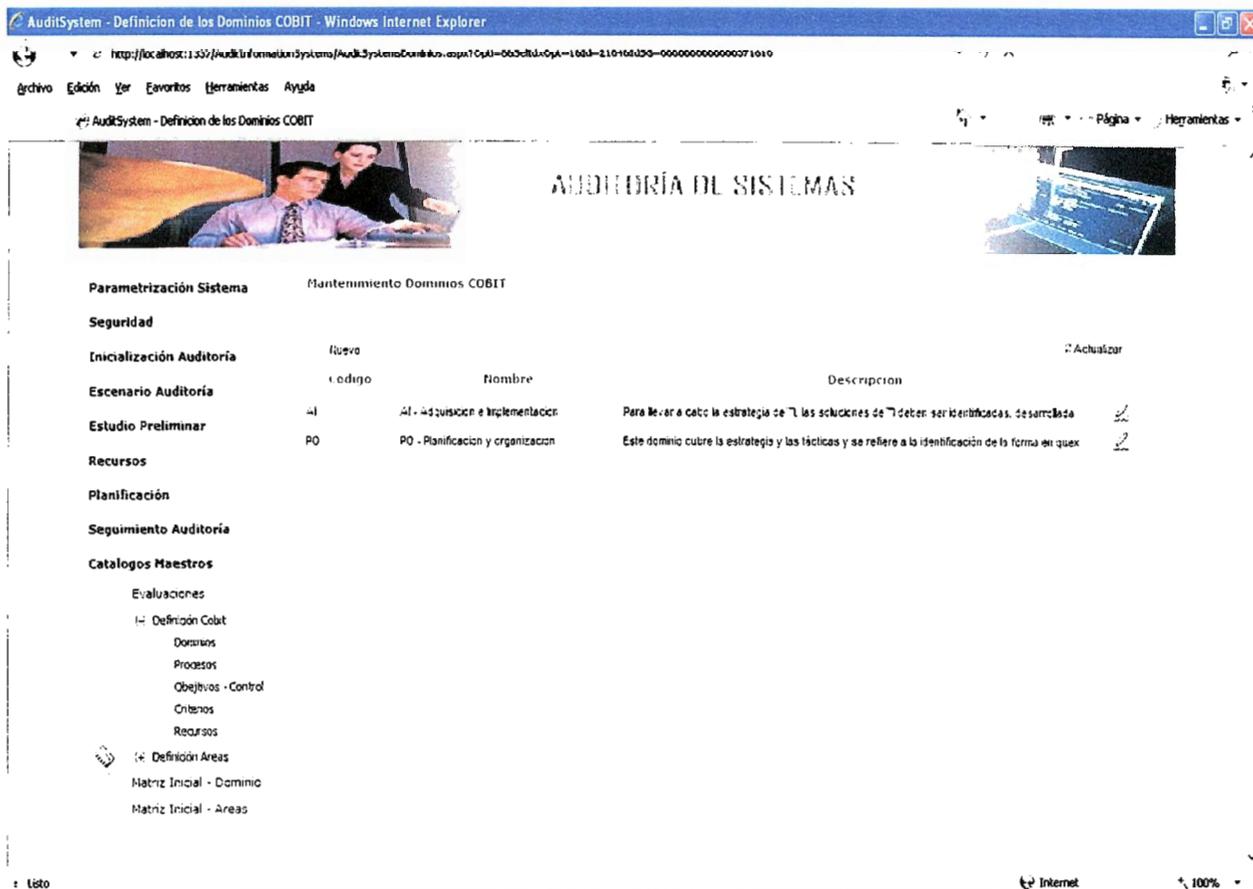
**Descripción:**

Pantalla Alcances y Objetivos – Ficha Auditoría – Tipo de auditoría.

**Funcionalidad:**

Permite definir el área o dominio COBIT donde se realizará la auditoría.

## 20.4.1.4 Panel Módulos Catálogos Maestros



The screenshot shows a web browser window titled 'AuditSystem - Definición de los Dominios COBIT'. The main content area is titled 'AUDITORÍA DE SISTEMAS' and displays a table for 'Mantenimiento Dominios COBIT'. The table has columns for 'Código', 'Nombre', and 'Descripción'. There are also buttons for 'Nuevo' and 'Actualizar'.

Código	Nombre	Descripción	Actualizar
AI	AI - Adquisición e implementación	Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas	
PO	PO - Planificación y organización	Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que	

The left navigation menu includes: Parametrización Sistema, Seguridad, Inicialización Auditoría, Escenario Auditoría, Estudio Preliminar, Recursos, Planificación, Seguimiento Auditoría, and Catálogos Maestros. Under 'Catálogos Maestros', there are sub-menus for Evaluaciones, Definición Cobit, and Definición Areas.

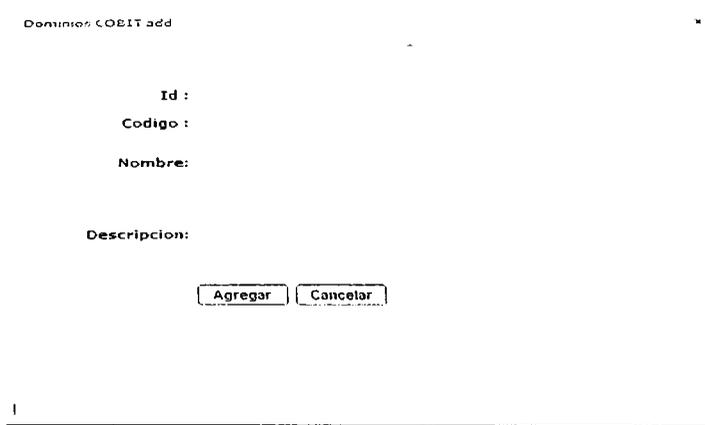
Imagen 18: Mantenimiento de dominios COBIT.

### Descripción:

Mantenimiento de dominios COBIT.

### Funcionalidad:

Esta pantalla es la encargada de dar mantenimiento a los dominios, aquí es donde se muestra una lista de los dominios definidos por el estándar COBIT, que representan las áreas donde se realizarán las auditorías



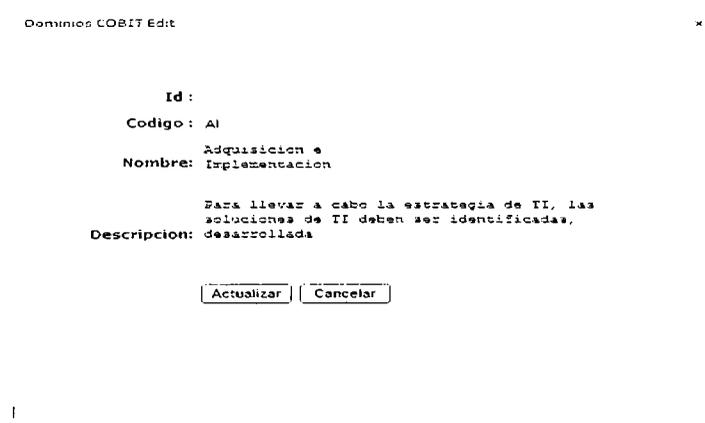
**Imagen 19:** Agregar dominios COBIT

**Descripción:**

Agregar Dominios COBIT.

**Funcionalidad:**

Esta ventana emergente es la encargada de dar Ingreso a un nuevo dominio; solamente se dará ingreso aquellos que estén definidos como dominio, dentro del el estándar COBIT.



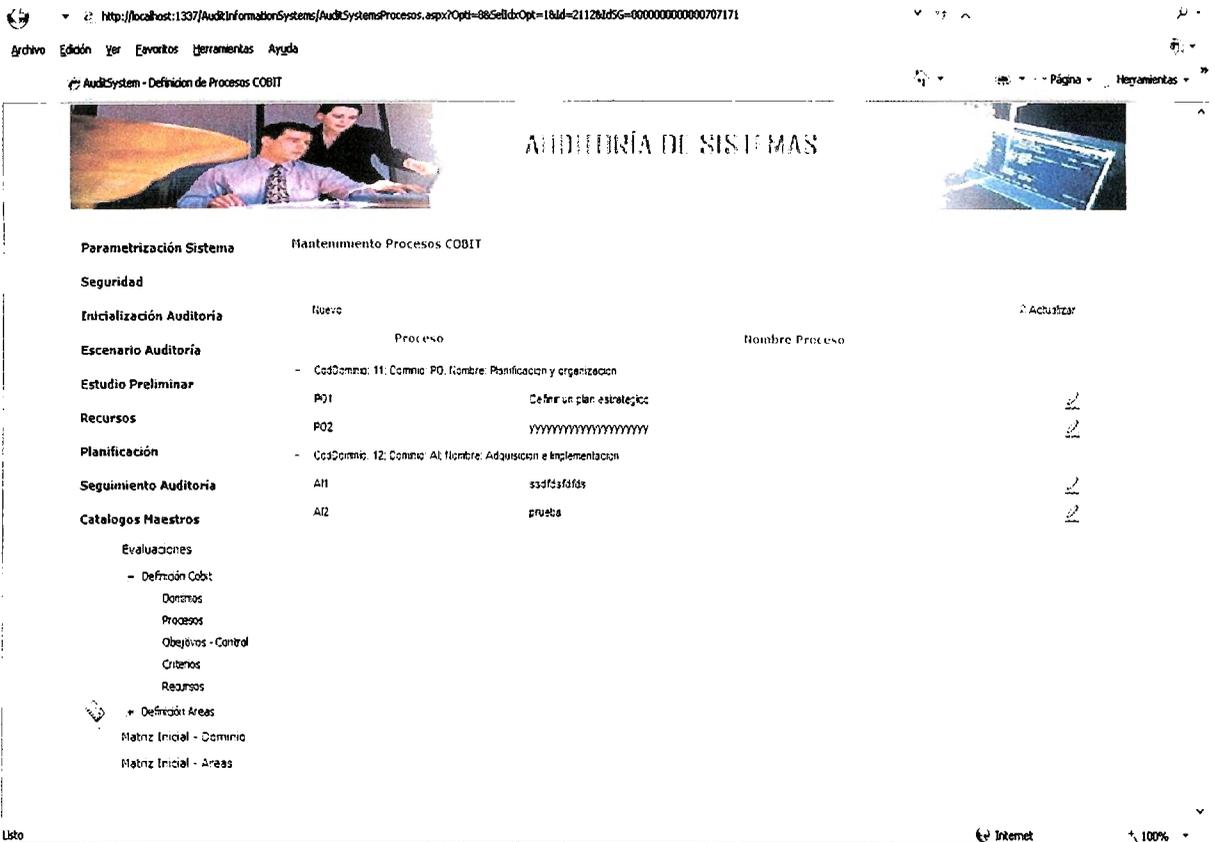
**Imagen 20:** Modificar dominios COBIT

**Descripción:**

Modificar dominios COBIT

**Funcionalidad:**

Esta ventana es la encargada de actualizar los datos de un dominio COBIT.



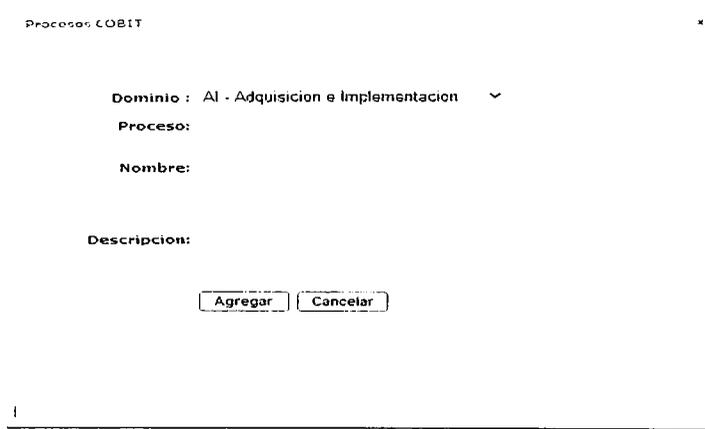
**Imagen 21:** Mantenimiento de procesos COBIT.

**Descripción:**

Mantenimiento de procesos COBIT.

**Funcionalidad:**

Esta pantalla es la encargada de dar mantenimiento a los procesos, aquí es donde se muestra una lista de procesos COBIT, agrupados por dominios, estos procesos representan el conjunto de actividades que se desarrollaran en un determinado dominio.



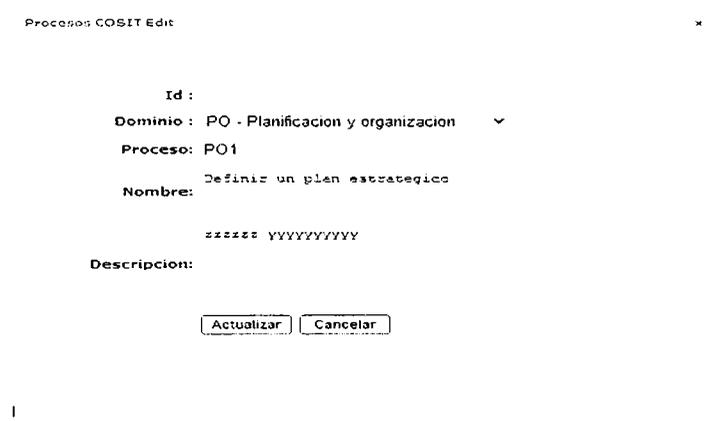
**Imagen 22:** Agregar procesos COBIT.

**Descripción:**

Pantalla Agregar Procesos COBIT.

**Funcionalidad:**

Esta ventana emergente es la encargada de dar Ingreso a un nuevo proceso; se dará ingreso a aquellos que estén definidos como procesos del estándar COBIT.



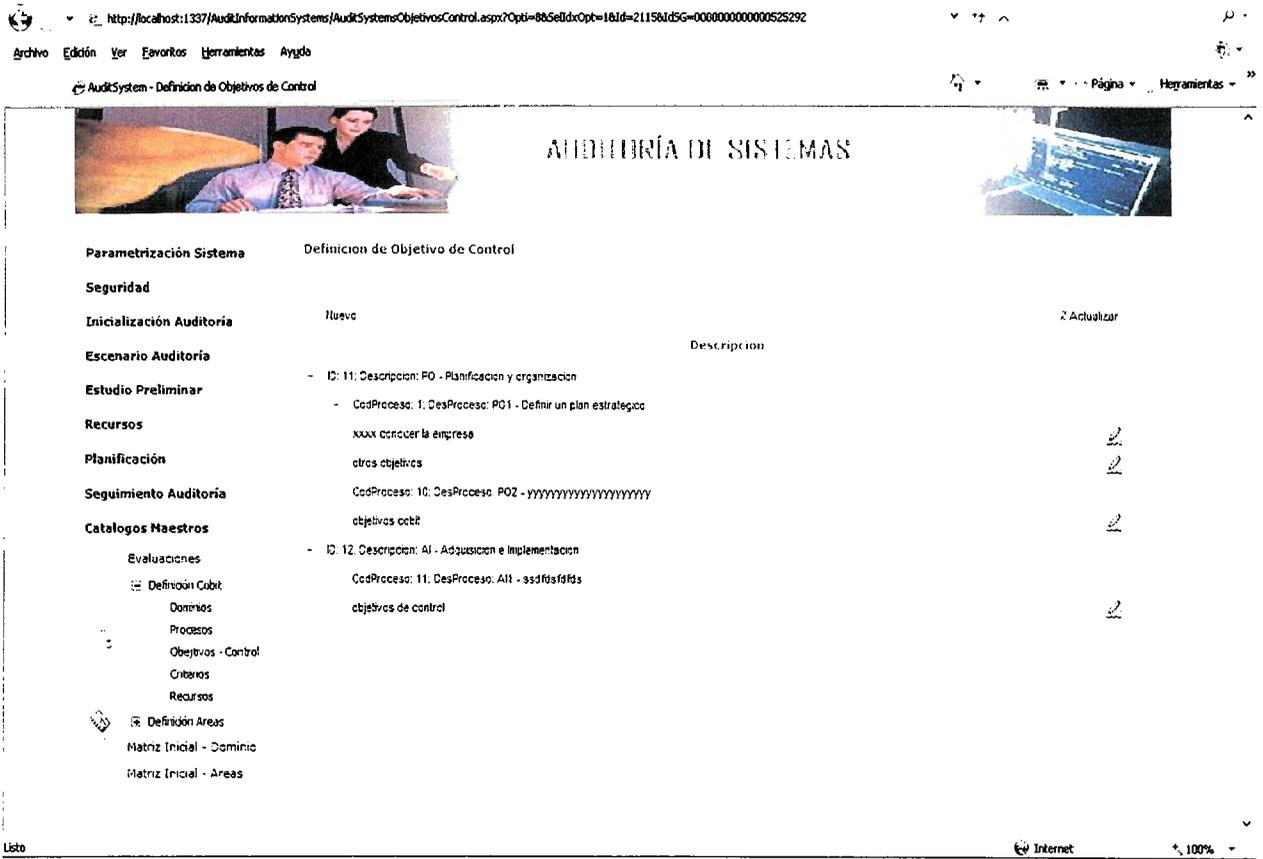
**Imagen 23:** Modificar procesos COBIT.

**Descripción:**

Modificar procesos COBIT.

**Funcionalidad:**

Esta ventana es la encargada de actualizar los datos de un proceso COBIT.



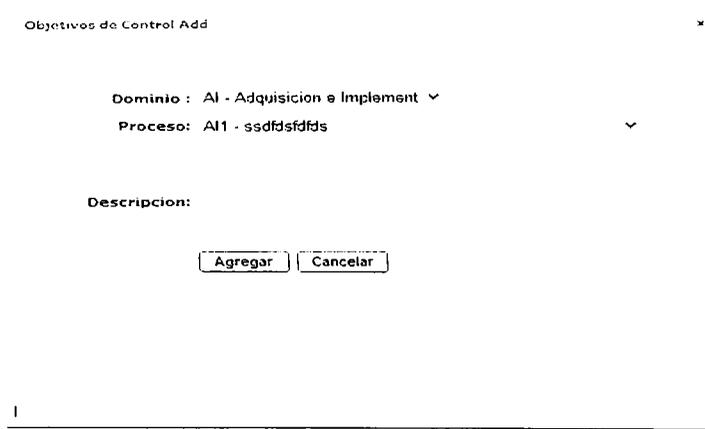
**Imagen 24:** Definición de Objetivos de Control.

**Descripción:**

Definición de los Objetivos de Control.

**Funcionalidad:**

Esta pantalla es la encargada de dar mantenimiento a los objetivos de control, la pantalla muestra una lista de objetivos agrupado por dominio y por proceso COBIT, esta lista representa una definición del resultado o propósito que se desea alcanzar implementando procesos COBIT.



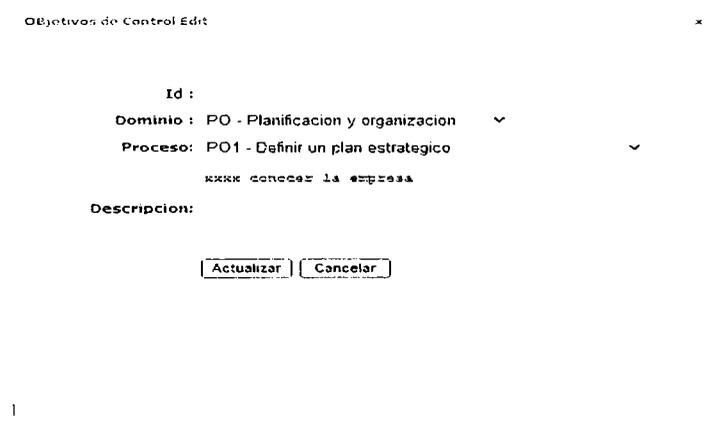
**Imagen 25:** Agregar Objetivos de Control.

**Descripción:**

Pantalla Agregar objetivos de control.

**Funcionalidad**

Esta ventana emergente es la encargada de dar Ingreso a un nuevo objetivo de control.



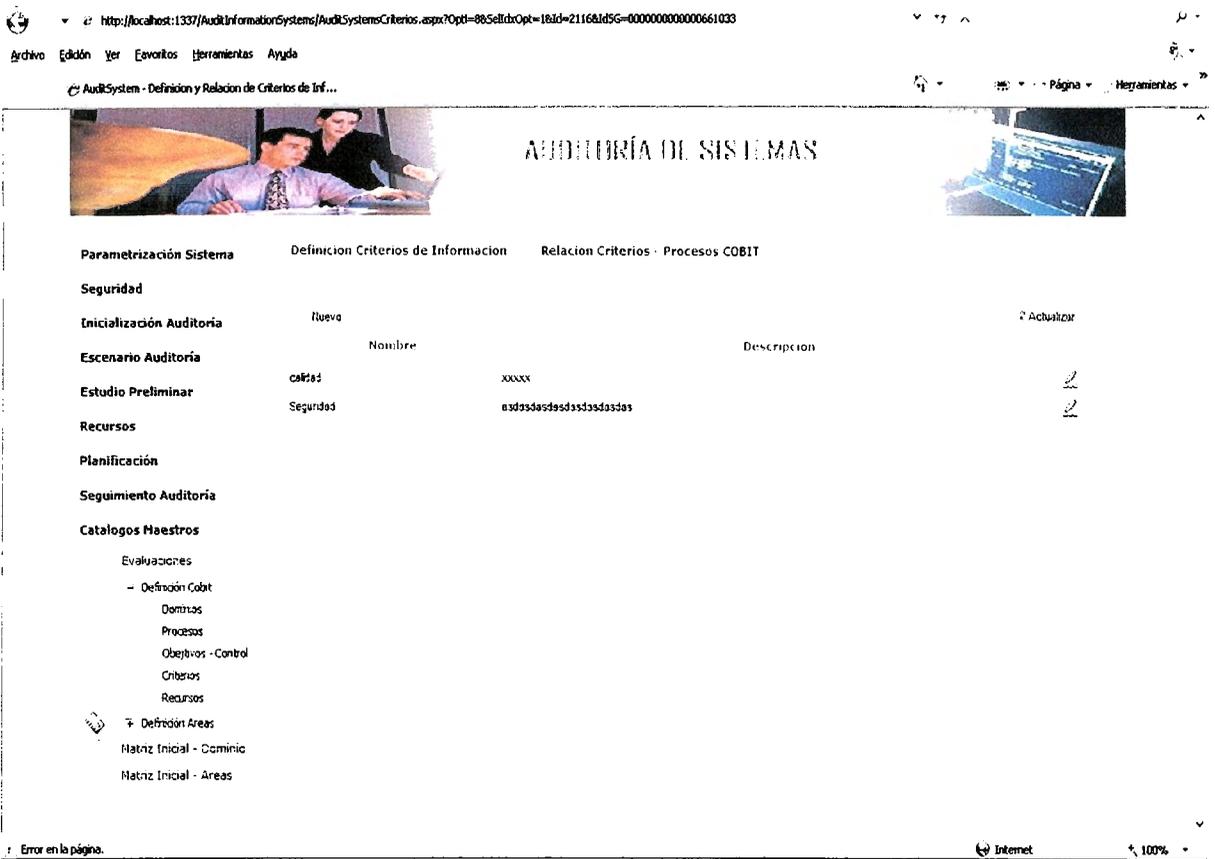
**Imagen 26:** Modificar Objetivos de Control.

**Descripción:**

Pantalla Modificar objetivos de control.

**Funcionalidad:**

Esta ventana es la encargada de actualizar los datos de un Objetivo de Control.



**Imagen 27:** Definición de criterios de información.

**Descripción:**

Definición de criterios de información.

**Funcionalidad:**

Esta pantalla muestra una lista de criterios de información comunes para la seguridad en tecnología de información y es la encargada de dar mantenimiento a:

- Lista de los criterios de información.
- La relación criterios-procesos, los criterios a considerar en cada proceso.

Parametrización Sistema    Definición Criterios de Información    Relación Criterios - Procesos COBIT

Seguridad

Inicialización Auditoría

Escenario Auditoría    Dominio : AI - Adquisición e Implementación

Estudio Preliminar    Proceso:

Recursos    Criterios

Planificación    Descripción:

Seguimiento Auditoría

Catalogos Nuestros   

Evaluaciones

- Definición Cobit
  - Domnios
  - Procesos
  - Objetivos - Control
  - Criterios
  - Recursos
- Definición Areas
  - Matriz Inicial - Dominio
  - Matriz Inicial - Areas

Id	Criterio	Descripcion
12	Descripción: AI - Adquisición e Implementación	
11	CodProceso: 11: DesProceso: AM - ssdfdsfdfs	
	calidad	xxxxxx

Libro    Internet    100%

Imagen 28: Relación criterios - procesos de información.



**Imagen 29:** Mantenimiento definición de recursos.

**Descripción:**

Mantenimiento definición de recursos.

**Funcionalidad:**

Esta pantalla muestra una lista de los recursos necesarios para realizar una auditoría y es la encargada de dar mantenimiento a:

- Lista de los Recursos de tecnología de información.
- La relación Recursos-Procesos, los recursos a considerar en cada proceso.

http://localhost:1337/AuditInformationSystems/AuditSystemRecursos.aspx?Opt=66&IdOpt=1&Id=2140&IdSG=000000000004059504

Archivo Edición Ver Favoritos Herramientas Ayuda

AuditSystem - Definición de Recursos de auditoría

Parametrización Sistema    Mantenimiento Definición de Recursos    Mantenimiento Recursos - Procesos

Seguridad

Inicialización Auditoría

Escenario Auditoría    Dominio : AI - Adquisición e Implementación

Estudio Preliminar    Proceso:

Recursos    Recursos

Planificación    Descripción:

Seguimiento Auditoría

Catalogos Maestros    Nuevo

Evaluaciones

Definición Cobt    Nuevo Registro    Actualizar

Domnios

Procesos

Objetivos - Control

Criterios

Recursos

Definición Areas

Matriz Inicial - Deminc

Matriz Inicial - Areas

Nombre Recurso	Descripción	
E: 12; Descripción: AI - Adquisición e Implementación		
- CodProceso: 11; DesProceso: AI1 - asdfghjkl		
Gente	personas involucradas	Editar
sistemas	todos los sistemas xxxx	Editar
- CodProceso: 12; DesProceso: AI2 - prueba		
Gente	personas involucradas	Editar
Gente	personas involucradas	Editar

Lista    Internet    100%

Imagen 30: Mantenimiento definición de recursos.

Parametrización Sistema      Áreas de Auditoría

Seguridad

Iniciación Auditoría      Id :

Escenario Auditoría      Área:

Estudio Preliminar

Recursos      Descripción:

Planificación

Seguimiento Auditoría      Estado:

Catalogos Maestros

Evaluaciones

Definición Cobit

  Dominios

  Procesos

  Objetivos - Control

  Criterios

  Recursos

Definición Áreas

  Áreas

Matriz Inicial - Dominio

Matriz Inicial - Áreas

Área	Descripción	Estado		
AFI	AFI - Auditoría de la Gestión Informática	ACTIVO	Seleccionar	Eliminar
ASG	ASG - Auditoría de la Seguridad General	ACTIVO	Seleccionar	Eliminar
GRQBJ	GRQBJ - Organización Gestión y Base Jurídica	ACTIVO	Seleccionar	Eliminar
APR	APR - Auditoría de la Producción	ACTIVO	Seleccionar	Eliminar

Listo      Internet      100%

Imagen 31: Mantenimiento Áreas de Auditoría.

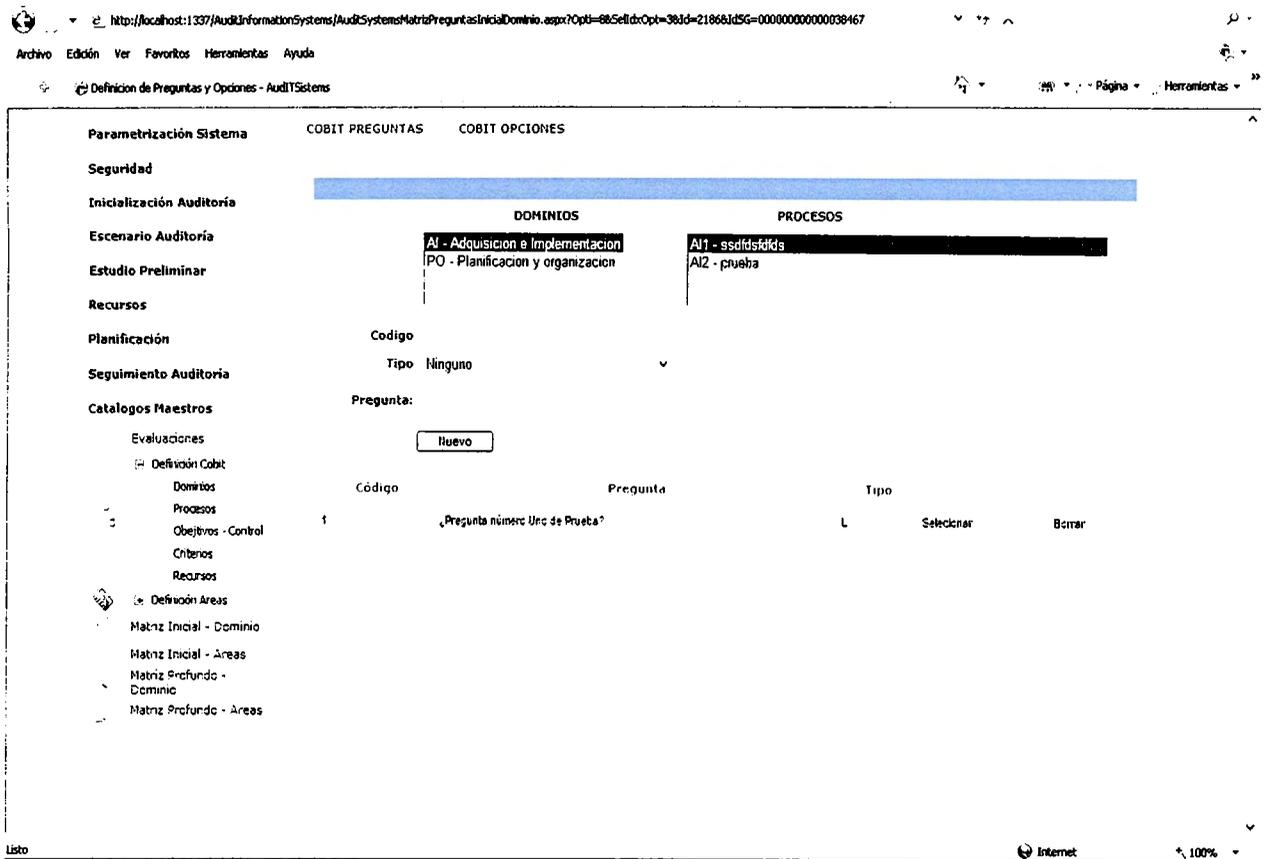
**Descripción:**

Mantenimiento de Áreas de auditoría.

**Funcionalidad:**

Esta pantalla muestra una lista de las áreas donde se desarrollarán las auditorías de sistemas.





**Imagen 33:** Definición de opciones de preguntas por COBIT.

### Descripción:

Definición de preguntas y opciones auditoría por COBIT.

### Funcionalidad:

En esta pantalla se puede observar las preguntas y respuestas que se pueden realizar en una auditoría de forma inicial por COBIT y es la encargada de dar mantenimiento a:

- Preguntas iniciales para una determinada área por COBIT.
- Opciones o posibles respuestas para una determinada pregunta.

Parametrización Sistema

AREAS PREGUNTAS

AREAS OPCIONES

Seguridad

Inicialización Auditoría

Escenario Auditoría

Estudio Preliminar

Recursos

Planificación

Seguimiento Auditoría

Catalogos Maestros

Evaluaciones

Definición Cobit

Domínios

Procesos

Objetivos - Control

Criterios

Recursos

Definición Areas

Matriz Inicial - Dominio

Matriz Inicial - Areas

Matriz Profundo - Dominio

Matriz Profundo - Areas

AREAS

- AFI - Auditoría de la Gestión Informática
- ASG - Auditoría de la Seguridad General
- ORGBJ - Organización Gestión y Base Jurídica
- APR - Auditoría de la Producción

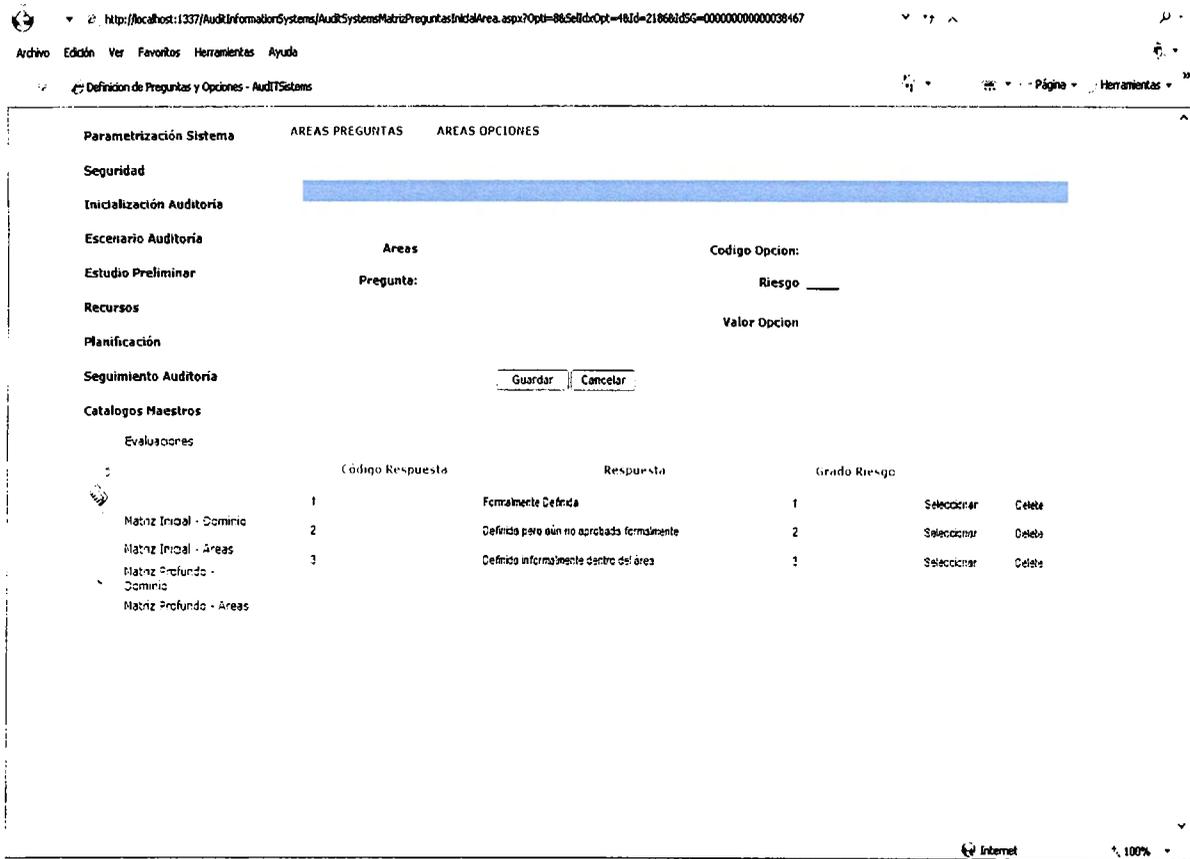
Código

Tipo Ninguno

Pregunta:

Código	Pregunta	Tipo		
1	¿El área de Sistemas cuenta con un Estructura?	chk	Seleccionar	Borrar
2	¿El área de Sistemas dispone de?	chk	Seleccionar	Borrar
3	¿La incorporación de sistemas en el Organismo es realizado por?	chk	Seleccionar	Borrar
4	¿Existe un comité de Informática?	tbl	Seleccionar	Borrar
7	¿El área de Sistemas reviste el carácter de?	chk	Seleccionar	Borrar

Imagen 34: Definición de preguntas por áreas.



**Imagen 35:** Definición de opciones de preguntas por áreas.

### Descripción:

Definición de preguntas y opciones auditoría por áreas.

### Funcionalidad:

En esta pantalla se puede observar las preguntas y respuestas que se pueden realizar en una auditoría de forma inicial por áreas y es la encargada de dar mantenimiento a:

- Preguntas iniciales para una determinada área.
- Opciones o posibles respuestas para una determinada pregunta.

http://localhost:1337/AuditInformationSystems/AuditSystemMatrizPreguntasProfundaDominio.aspx?Opt=685e1f0xOpt=583d=2169&IdSG=00000000000049867

Archivo Edición Ver Favoritos Herramientas Ayuda

Definición de Preguntas y Opciones - AuditSystem

Parametrización Sistema COBIT PREGUNTAS PROFUNDA COBIT OPCIONES PROFUNDA

Seguridad

Inicialización Auditoría

Esenario Auditoría

Estudio Preliminar

Recursos

Planificación

Seguimiento Auditoría

Catalogos Maestros

- Evaluaciones
  - Definición Cobit
    - Dominios
    - Procesos
    - Objetivos - Control
    - Criterios
    - Recursos
  - Definición Areas
    - Matriz Inicial - Dominio
    - Matriz Inicial - Areas
    - Matriz Profundo - Cominio
    - Matriz Profundo - Areas

DOMINIOS

AI - Adquisición e Implementación

PO - Planificación y organización

PROCESOS

AI1 - ssdfdsfdfs

AI2 - prueba

OBJETIVOS DE CONTROL

objetivos de control

Código

Tipo Ninguno

Pregunta:

ltuevo

Código	cod_objetivo	Pregunta	Tipo		
1	4	¿Existe un control estricto de los recursos Tecnológicos?	btn	Seleccionar	Borrar
2	4	¿Existe un Análisis en su empresa?	btn	Seleccionar	Borrar

Listo

Internet 100%

Imagen 36: Definición de de preguntas profundas por COBIT.



**Imagen 37:** Definición de opciones de preguntas profundas por COBIT.

### Descripción:

Definición de preguntas y opciones profundas de auditoría por COBIT.

### Funcionalidad:

En esta pantalla se puede observar las preguntas y respuestas que se pueden realizar en una auditoría de forma profunda por COBIT y es la encargada de dar mantenimiento a:

- Preguntas profunda para una determinada área o dominio COBIT.
- Opciones o posibles respuestas para una determinada pregunta.

http://localhost:1337/AuditInformationSystems/AuditSystem/MatrizPreguntasProfundaArea.aspx?Opt=8&SellId=Opt=6&Id=2206&IdG=00000000000046294

Archivo Edición Ver Favoritos Herramientas Ayuda

Definición de Preguntas y Opciones - AuditSystem

Parametrización Sistema AREAS PREGUNTAS PROFUNDAS AREAS OPCIONES PROFUNDAS

Seguridad

Inicialización Auditoría

Escenario Auditoría

Estudio Preliminar

Recursos

Planificación

Seguimiento Auditoría

Catalogos Maestros

Evaluaciones

- Definición Cobit
  - Domínios
  - Procesos
  - Objetivos - Control
  - Criterios
  - Recursos
- Definición Areas
  - Matriz Inicial - Dominio
  - Matriz Inicial - Areas
  - Matriz Profundo - Dominio
  - Matriz Profundo - Areas

AREAS

AFI - Auditoría de la Gestión Informática ^

ASG - Auditoría de la Seguridad General

ORGBJ - Organización Gestión y Base Jurídica

APR - Auditoría de la Producción v

Código

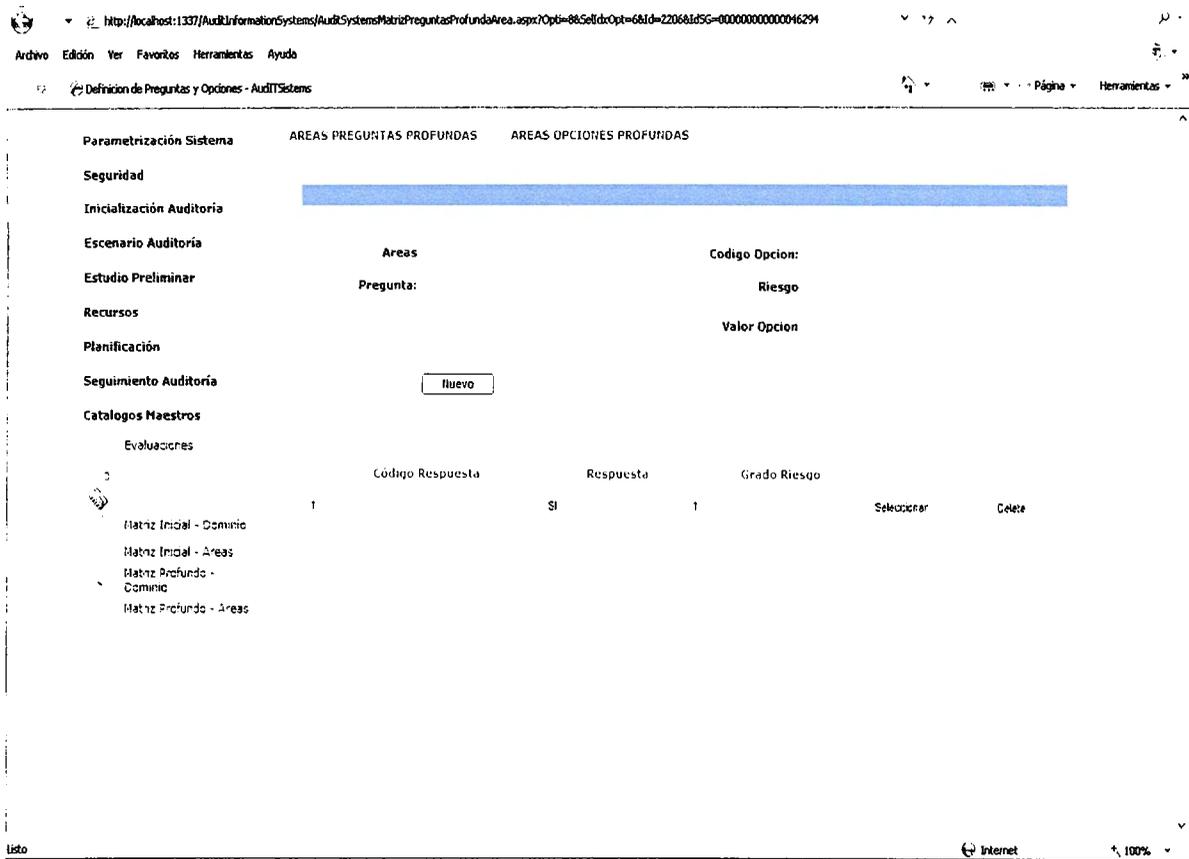
Tipo Sí/No v

Pregunta:

Código	Pregunta	Tipo		
1	¿Pregunta de prueba número de inicio?	bt	Seleccionar	Borrar

Listo Internet 100%

Imagen 38: Definición de preguntas profundas por áreas.



**Imagen 39:** Definición opciones de preguntas profundas por áreas.

### Descripción:

Definición de preguntas y opciones profundas auditoría por áreas.

### Funcionalidad:

En esta pantalla se puede observar las preguntas y respuestas que se pueden realizar en una auditoría de forma profunda por áreas y es la encargada de dar mantenimiento a:

- Preguntas profundas para una determinada área.
- Opciones o posibles respuestas para una determinada pregunta.

## 21. CONCLUSIONES

- El desarrollo del sistema de información distribuido para el apoyo a la auditoría de sistemas permite afirmar que es posible contar con una herramienta software que incorpore los estándares que actualmente se utilizan para realizar auditoría de sistemas.
- La arquitectura del sistema y el hecho que el mismo funcione en un entorno Web, posibilita a auditores de sistemas en general, y a aquellos en particular que realizan sus actividades lejos de su lugar de trabajo y tienen dificultades en su actualización profesional, contar con una herramienta software que les posibilita realizar su tarea de manera eficaz y eficiente.
- El sistema de información desarrollado demuestra que se puede contar con una herramienta software que asista desde el punto de vista metodológico a la auditoría de sistemas y se adapte a los distintos entornos a auditar.
- Es necesario difundir el uso de las técnicas de auditoría asistidas por computadora, ya que las mismas son un soporte fundamental en la tarea que realiza el auditor de sistemas.
- El desarrollo del sistema de información deja claro que se puede utilizar herramientas basadas en tecnología web y que den soporte al desarrollo de auditoría en sistemas apoyados con técnicas asistidas por computadora.

## 22. RECOMENDACIONES

- Mantener siempre actualizado los catálogos maestros del sistema de información, para contar con la información más reciente, al momento de realizar una auditoría en sistemas de información.
- Definir las preguntas con sus opciones basándose en las áreas y las normas COBIT, para el desarrollo de una auditoría, manteniendo siempre en todo momento actualizadas dichas preguntas con sus respuestas.
- Se recomienda la elaboración de un programa de capacitación por parte de los auditores incluyendo los aspectos teóricos, procedimientos y actividades que con llevan a realizar una auditoría en sistemas practicando la forma tradicional y la nueva utilizando el sistema.
- Se recomienda para el diseño y desarrollo de versiones futuras del Sistema de Información Distribuido para el Apoyo a la Auditoría de Sistemas, el uso de software de licencia pública General (GNU GPL) o herramientas de software libre.
- Desarrollar un modulo de alarmas que permita al auditor conocer los proyectos de auditorias que están por concluir o vencer en una determinada fecha y que se permita visualizar a través de un visor de auditorias el cliente, la fecha de inicio y final del proyecto de auditoría.

# GLOSARIO

## A

**Acceso web:** Es la capacidad que tiene un dispositivo, una computadora, PDA, teléfono móvil u otros de conectarse a internet a través de un programa navegador como Internet Explorer, Netscape.

**Auditoría:** Es la revisión y examen de una función, cifra, proceso o reporte, efectuados por personal independiente a la operación, para apoyar la función ejecutiva.

**Auditoría en sistemas:** Es la revisión que se dirige a evaluar los métodos y procedimientos de uso en una entidad, con el propósito de determinar si su diseño y aplicación son correctos; y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; así como para identificar aspectos susceptibles de mejorarse o eliminarse.

**ACID:** se denomina ACID a la propiedad de una base de datos para realizar transacciones seguras.

**API:** una serie de funciones que están disponibles para realizar programas para un cierto entorno.

## B

**Base de datos:** Es una colección de archivos interrelacionados, son creados con un DBMS. El contenido de una base de datos engloba a la información concerniente (almacenadas en archivos) de una organización, de tal manera que los datos estén disponibles para los usuarios, una finalidad de la base de datos es eliminar la redundancia o al menos minimizarla.

**Bluetooth:** Es la norma que define un estándar global de comunicación inalámbrica, que posibilita la transmisión de voz y datos entre diferentes equipos, mediante un enlace por radiofrecuencia.

**Benchmark:** un conjunto de procedimientos (programas de computación) para evaluar el rendimiento de un ordenador

## C

**CheckList:** Listas de control con una serie de preguntas a verificar utilizadas por los auditores como una guía de referencia para asegurar que se han revisado todos los controles.

**Cache:** Es un tipo de memoria especial, más rápida que la RAM normal (y más cara), que se sitúa en el camino de los datos que van del procesador a la memoria RAM.

## D

**Diagrama entidad – relación (E-R):** Denominado por sus siglas como: E-R; este modelo representa a la realidad a través de un esquema gráfico empleando la terminología de entidades, que son los objetos que existen y son elementos principales que se identifican en el problema a resolver con el diagramado.

## G

**GPRS:** General Packet Radio Service o GPRS es una tecnología digital de telefonía móvil que proporciona altas velocidades de transferencia de datos.

## E

**Extranet:** es una red privada virtual que utiliza protocolos de Internet, protocolos de comunicación y probablemente infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, clientes o cualquier otro negocio u organización.

**GPL:** (General Public License o licencia pública general) es una licencia creada por la Free Software Foundation a mediados de los 80, y está orientada principalmente a proteger la libre distribución, modificación y uso de software

## I

**ISACA:** Asociación para la Auditoría y el Control de Sistemas de Información. El objetivo de los Estándares de Auditoría de Sistemas desarrollados por ISACA, es informar a los auditores de sistemas, el nivel mínimo aceptado para resolver las responsabilidades profesionales precisadas en el código de ética profesional de ISACA.

**Internet:** Es una red de redes de computadoras a nivel mundial, esto con el objeto de facilitar el intercambio de información de un lugar a otro que puede estar separado por miles de kilómetros.

**Intranet:** es una red de ordenadores dentro de una red de área local (LAN) privada empresarial o educativa que proporciona herramientas de Internet, teniendo como función principal proveer lógica de negocios.

## O

**On-line:** En línea, accesibilidad y disponibilidad en cualquier momento utilizando como medio Internet.

## P

**PDA (Personal Digital Assistant o Ayudante personal digital):** es un dispositivo de tamaño pequeño, combina un ordenador, teléfono/fax, Internet y conexiones de red.

**Protocolo HTTP1.1:** protocolo usado en cada transacción de la Web (WWW). HTTP fue desarrollado por el consorcio W3C y la IETF.

**Pipelining:** es una técnica que utiliza el protocolo HTTP1.1 para recibir muchas solicitudes respuestas por parte de los clientes y luego escribirlas en determinados sockets.

**Proxy:** permite el acceso a internet a todos los equipos de una organización cuando sólo se dispone de un único equipo conectado, esto es, una única dirección IP.

## S

**Servidor web:** Ordenador que usa el protocolo http para enviar páginas al ordenador de cualquier usuario que las solicite.

**Servidor de base de datos:** Ordenador en el que se encuentra instalado un gestor de base de datos para la administración de un conjunto de base de datos.

**Sistema de información (SI):** Los que logran la automatización de procesos operativos dentro de una organización, son llamados frecuentemente Sistemas Transaccionales por otra parte, los Sistemas de Información que apoyan el proceso de toma de decisiones son los Sistemas de Soporte a la Toma de Decisiones.

**Sistema Gestor de Base de Datos(SGBD):** Conjunto de programas que se encargan de manejar la creación y todos los accesos a una base de datos.

## T

**Tecnología de información (TI):** Una forma de denominar al conjunto de herramientas, habitualmente de naturaleza electrónica, utilizadas para la recogida, almacenamiento, tratamiento, difusión y transmisión de la información.

**Tecnología móvil:** La tecnología móvil permite llevar el trabajo a donde quiera que uno vaya (en el coche, en un avión, en el aeropuerto, en un restaurante o en el parque) y ofrece en todo momento la posibilidad de utilizar las aplicaciones instaladas, exponer presentaciones, crear documentos y datos, y acceder a ellos. Significa llevar siempre consigo el dispositivo que contiene toda su información y que le permite generar los documentos que necesita en todo momento y donde quiera que se encuentre.

**TAACS:** Técnicas de auditoría con ayuda de computadora (TAACs) que usan la computadora como una herramienta de auditoría.

**Triggers:** es un evento que se ejecuta cuando se cumple una condición establecida al realizar una operación de inserción (INSERT), actualización (UPDATE) o borrado (DELETE).

## W

**WiFi:** Abreviatura de Wireless Fidelity, es un conjunto de estándares para redes inalámbricas. Se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad se utilice para acceder a Internet.

**WAP:** Wireless Application Protocol o WAP (Protocolo de aplicaciones inalámbricas) es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, por ejemplo acceso a Internet desde un teléfono móvil.

**Web:** Significa el conjunto de archivos bajo un dominio común que se materializan en la presentación gráfica en la pantalla del usuario de información, servicios u otros contenidos disponibles para su acceso en internet por usuarios en general.

**Wireless:** Es denominada a la tecnología inalámbrica de comunicaciones, funciona por medio de ondas electromagnéticas que comunica dos o varios puntos

# FUENTES DE INFORMACION

## A. BIBLIOGRAFIA

1. Jack J. Champlain. AUDITING INFORMATION SYSTEMS. Segunda edición. publicado por John Wiley & Sons.
2. Mario Piattini. AUDITING INFORMATION SYSTEMS. United States of America. Idea Group Publishing.
3. Piattini, Mario G. Peso Navarro, Emilio. AUDITORIA INFORMATICA. Editorial RA-MA. 1997
4. KENDALL Edward J. y KENDALL Julia A. ANALISIS Y DISEÑO DE SISTEMAS. Tercera Edición. Editorial Prentice May Inc.

## B. SITIOS DE INTERNET

1. [http://www.auditoriasistemas.com/auditoria\\_de\\_sistemas.htm](http://www.auditoriasistemas.com/auditoria_de_sistemas.htm)
2. <http://www.gerencie.com/>, Auditoría en sistemas, todo lo que el contador y el empresario necesita saber
3. <http://www.isaca.org.pe/>, Normas generales para la auditoría en sistemas de información, actualización 2004
4. <http://www.full-on-net.com/articulo.php?id=2>, Artículo, Full On Net, actualización

# **ANEXOS**

# **ANEXO A**

**Talle de Auditoría de Sistemas  
Corte de Cuentas de la República de El Salvador, C.A  
Material de Apoyo**

CORTE DE CUENTAS DE LA REPUBLICA DE EL SALVADOR, C. A.

Organismo Rector del Sistema de Control y Auditoría de la Gestión Pública



# **"TALLER AUDITORÍA DE SISTEMAS"**

*Material de Apoyo*

Octubre, 2005

San Salvador, República de El Salvador



Alfa|group

GRUPO GESTOR CUMBRES

## I. INTRODUCCIÓN

Las organizaciones deben satisfacer para su información, como para todos sus activos, los requerimientos de calidad (calidad, costo, entrega), reportes financieros (efectividad y eficiencia de las operaciones, disponibilidad de la información, ajuste a leyes y regulaciones) y seguridad (confidencialidad, integridad y disponibilidad). La administración debe balancear el uso de los recursos disponibles como personas, facilidades, tecnología, sistemas de aplicación y datos. Para cumplir su responsabilidad, como para alcanzar sus expectativas, la administración debe establecer un adecuado sistema de control interno; tanto en sistemas como en estructura, debe soportar los procesos del negocio y debe ser claro en cómo cada actividad de control impacta los recursos y satisface los requerimientos. El control es responsabilidad de la administración e incluye políticas, estructuras organizacionales, prácticas y procedimientos. Para observar el cumplimiento, es necesario establecer Objetivos de Control, que consisten en una serie de declaraciones de los resultados o propósitos deseados a ser alcanzados por medio de la implementación de procedimientos de control específicos dentro de una actividad que involucre Tecnología de Información.

Partiendo de la premisa "Los recursos de Tecnología de Información necesitan ser administrados por una serie de procesos de negocios naturalmente agrupados para proveer la información que la empresa necesita para alcanzar sus objetivos", la administración de la empresa necesita una estructura de las prácticas de seguridad y control generalmente aceptadas para la Tecnología de Información para comparar su ambiente en TI existente contra el planeado.

## II. GENERALIDADES

### ANTECEDENTES

La función de auditoría de sistemas, emergió debido a cambios en la gestión de la administración de los negocios, tales como:

- Nivel de desarrollo de la Tecnología de Información de las organizaciones
- Reenfoque del establecimiento del ambiente de control interno en la organización
- Alcance de la Auditoría para la evaluación del control interno en los procesos del negocio
- Actualización de métodos y procedimientos de evaluación para la auditoría
- Necesidad de capacitación constante de los auditores

Igualmente, se identifican los siguientes factores por los que las organizaciones requieren establecer la función de la auditoría de sistemas:

- Necesidad de control en un ambiente de constante aumento en el uso de la tecnología de información
- Abuso en la utilización de los recursos tecnológicos
- Riesgo de enfrentar una pérdida de la capacidades de procesamiento informático y su correspondiente funcionalidad
- Riesgo de tomar decisiones incorrectas si la información mantenida y proporcionada por las aplicaciones informáticas es incorrecta
- Riesgo de enfrentar problemas operativos y hasta legales para información o procedimientos incorrectos en los sistemas informáticos
- Necesidad garantizar que se mantiene la seguridad y privacidad de la información

### AMBITO DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

En su función, la auditoría de sistemas requiere evaluar el control interno de las actividades relacionadas con el desarrollo y operación en tecnología de información para promover la eficiencia y eficacia en la utilización de los recursos.

Su ámbito de acción en la evaluación del control interno, se puede resumir en:

- Organización y Gestión del Departamento de TI
- Desarrollo y Funcionamiento de los Sistemas
- Continuidad en la Operación de los Sistemas

## III. GESTIÓN DE LA AUDITORÍA DE TI

### Enfoque

Los Auditores tienen como requisito general, el proporcionar a la Administración y a los dueños de procesos de negocios apoyo para el cumplimiento de los controles en una organización; proporcionar una certeza razonable de que objetivos de control se están cumpliendo; identificar dónde existen debilidades significativas en esos controles; determinar los riesgos que pueden

estar asociados con las debilidades; y, finalmente, recomendar a los ejecutivos sobre las acciones correctivas que se deben tomar.

Los objetivos y prácticas de auditoría varían considerablemente de organización en organización y existen muchos tipos de practicantes envueltos en actividades relacionadas a la auditoría, ej., auditores externos, auditores internos, evaluadores, verificadores de la calidad y asesores técnicos.

### **Objetivos**

Los objetivos de la auditoría son:

- Evaluar la organización y gestión del área de tecnología de información para verificar que estén acorde con los objetivos y políticas de la empresa.
- Fiscalizar que las actividades informáticas se realicen mediante procedimientos establecidos, bien definidos y documentados, de forma tal que procuren un adecuado desarrollo y operación de los sistemas.
- Evaluar la adquisición y utilización eficiente de los recursos tecnológicos.
- Verificar que el desarrollo de sistemas satisfaga los necesidades de información, haciendo un uso eficiente y eficaz de los recursos tecnológicos.
- Evaluar los sistemas automatizados para que guarden la debida confiabilidad, seguridad, integridad y oportunidad de la información.
- Evaluar el acceso a los sistemas y bases de datos.
- Brindar asesoría en aspectos técnicos

Igualmente, pueden ser agrupados por función de TI:

- Administrativos
  - Organización y personal
  - Planificación
  - Análisis de costos y beneficios
  - Desarrollo de procedimientos y definición de controles
  - Aspectos legales
- Requerimientos, desarrollo y mantenimiento de sistemas
  - Aplicación de la metodología
  - Resultados del desarrollo y mantenimiento
- Operaciones informáticas
  - Centro de operaciones
  - Controles de entrada y salida
  - Comunicaciones y redes
  - Soporte técnico
- Sistemas en operación
- Servicios de apoyo

La estructura generalmente aceptada del proceso de auditoría incluye:

- Identificación y documentación
- Evaluación
- Pruebas de cumplimiento
- Pruebas sustantivas

El proceso de TI es entonces auditado por medio de:

- Obtener un entendimiento de los requerimientos del negocio, los riesgos relacionados, y las medidas de control relevantes
- Evaluar lo apropiado de los controles establecidos
- Evaluar el cumplimiento probando si los controles establecidos están trabajando tal y como fueron definidos en forma consistente y continua.

- Probar que no se materializa el riesgo sobre los objetivos de control, utilizando técnicas analíticas y/o consultando fuentes alternativas.

### **Código de Ética Profesional del Auditor de Sistemas de Información**

Los auditores de sistemas deben desempeñarse en una forma profesional, respetando los siguientes patrones de conducta:

- Promover el establecimiento y cumplimiento apropiado de los estándares, procedimientos y controles de las operaciones y sistemas de procesamiento electrónico de datos, los cuales deben operar en una forma consistente y de acuerdo con las prácticas profesionales de aceptación general.
- Promover la necesidad de que la gerencia y la organización cuenten con controles adecuados de procesamiento electrónico de datos.
- Ejecutar las responsabilidades asignadas de una manera honesta y leal y no involucrarse en ningún aspecto que sea deshonesto o ilegal.
- Promover la educación y el entendimiento de las interrelaciones que existen entre el área de procesamiento electrónico de datos y la auditoría.
- Ejecutar el trabajo y comunicar su opinión en una forma objetiva soportada con suficiente documentación y evidencia de acuerdo con su criterio profesional.
- Mantener la confidencialidad de información privilegiada obtenida durante el desarrollo de su trabajo.
- Mantener un alto grado de profesionalismo en el área de procesamiento electrónico de datos y en auditoría, participando en actividades de desarrollo de profesional en esas disciplinas.
- Debe conducirse con altos patrones de conducta y de moral en su vida personal y profesional.
- No debe participar en actividades donde puedan ocasionar conflictos de intereses con las políticas de la organización y sus empleados. Tampoco debe participar en actividades que atenten con su independencia profesional.

### **Efecto**

El trabajo profesional de auditoría, tiene una finalidad y unos objetivos definidos que se desprenden de su propia naturaleza. El auditor es llamado como un técnico independiente y de confianza para opinar sobre cierta información, procedimientos o áreas, a efecto de que su opinión sea una garantía de credibilidad respecto a esa información. En esa virtud, el trabajo de auditoría tiene una finalidad y un objetivo que no depende ni de la voluntad personal del auditor ni de la voluntad personal del cliente, sino que se desprenden de la misma naturaleza de la actividad profesional de la auditoría. Esta característica obliga también a que el trabajo profesional de auditoría se realice dentro de determinadas normas de calidad.

Por consiguiente, la existencia de normas de auditoría y la naturaleza de ellas, reconoce como fuente los siguientes dos hechos:

- ✓ La auditoría es un trabajo de naturaleza profesional
- ✓ La auditoría tiene características y finalidades propias que le son conaturales.

### **Normas de Auditoría**

Son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña y a la información que rinde como resultado de este trabajo.

#### **1) Normas Personales**

Se refieren a las cualidades que el auditor debe tener para poder asumir, dentro de las exigencias que el carácter profesional de la auditoría impone, un trabajo de este tipo. Dentro de estas normas existen cualidades que el auditor debe tener pre-adquiridas antes de poder asumir un trabajo profesional de auditoría y cualidades que debe mantener durante el desarrollo de toda su actividad profesional.

- ✓ **Entrenamiento técnico y capacidad profesional**

El trabajo de auditoría, cuya finalidad es la de rendir una opinión profesional independiente, debe ser desempeñado por personas que, teniendo un título profesional legalmente expedido y reconocido, tengan entrenamiento técnico adecuado y capacidad profesional como auditores.

- ✓ **Cuidado y diligencia profesional**

El auditor está obligado a ejercitar cuidado y diligencia razonables en la realización de su examen y en la preparación de su informe.

✓ Independencia

El auditor está obligado a mantener una actitud de independencia mental en todos los asuntos relativos a sus trabajo profesional.

2) **Normas de Ejecución del Trabajo**

Al tratar las normas personales, se señaló que el auditor está obligado a ejecutar su trabajo con cuidado y diligencia. Aún cuando es difícil definir lo que en cada tarea puede representar un cuidado y diligencia adecuados, existen ciertos elementos que por su importancia, deben ser cumplidos. Estos elementos básicos, fundamentales en la ejecución del trabajo, que constituyen la especificación particular, por lo menos al mínimo indispensable, de la exigencia de cuidado y diligencia, son los que constituyen las normas denominadas de ejecución del trabajo.

✓ Planeación y supervisión

El trabajo de auditoría debe ser planeado adecuadamente y, si se usan ayudantes, éstos deben ser supervisados en forma apropiada.

✓ Estudio y evaluación del control interno

El auditor debe efectuar un estudio y evaluación adecuados del control interno existente, que le sirvan de base para determinar el grado de confianza que va a depositar en él; así mismo, que le permita determinar la naturaleza, extensión y oportunidad que va a dar a los procedimientos de auditoría.

✓ Obtención de evidencia suficiente y competente

Mediante sus procedimientos de auditoría, el auditor debe obtener evidencia comprobatoria suficiente y competente en el grado que requiera para suministrar una base objetiva para su opinión.

3) **Normas de Información**

El resultado final del trabajo del auditor es su dictamen o informe. Mediante él, pone en conocimiento de las personas interesadas los resultados de su trabajo y la opinión que se ha formado a través de su examen. El dictamen o informe del auditor es en lo que va a reposar la confianza de los interesados, para presentarles fe a las declaraciones dadas. Por último, es principalmente, a través del informe o dictamen, como el público y el cliente se dan cuenta del trabajo del auditor y, en muchos casos, es la única parte, de dicho trabajo que queda a su alcance.

**Norma Internacional de Auditoría para TI**

El Comité Internacional de Prácticas de Auditoría ("IAPC") de la Federación Internacional de Contadores emite las Declaraciones internacionales de prácticas de auditoría (IAPS) ("Declaraciones") para proporcionar ayuda práctica a los auditores, con el fin de adaptar y usar las Normas Internacionales de Auditoría ("NIAs") para promover una buena práctica.

El auditor comprende y considera las características de un ambiente de sistema de información de cómputo (tecnología de la información) porque afectan al diseño del sistema de contabilidad y a los controles internos relacionados. Consecuentemente, un ambiente de CIS (Tecnología de la información) de aquí en adelante puede afectar al plan general de auditoría, incluyendo la selección de los controles internos en que el auditor tiene la intención de apoyarse y la naturaleza, oportunidad y alcance de los procedimientos de auditoría.

El AICPA (Instituto Americano de Contadores Públicos Certificados) aprobó esta Declaración internacional de prácticas de auditoría en junio de 2001 para su publicación en julio de 2001.

**NIA 401 – Auditoría en un Ambiente de sistemas de Información por computadora**

Establece normas y proporciona lineamientos sobre los procedimientos a seguir cuando se realiza una auditoría en un ambiente de sistemas de información automatizado. Para fines de las NIA's un ambiente SIC existe cuando está involucrada una computadora en el procesamiento por la entidad de información financiera de importancia para la auditoría.

La NIA 401, considera:

- **Habilidad y competencia** – el auditor deberá tener suficiente conocimiento del SIC para planear, dirigir, supervisar y revisar el trabajo desarrollado. Además, considerar si se necesitan habilidades especializadas en SIC en una auditoría.
- **Planeación** – el auditor deberá obtener una comprensión de los sistemas de contabilidad y de control interno, suficiente para planear la auditoría y desarrollar un enfoque efectivo. Además, deberá obtener una comprensión de la importancia y complejidad de las actividades de SIC y la disponibilidad de datos para uso en la auditoría.
- **Evaluación del Riesgo** – cuando el SIC es significativo, el auditor deberá también obtener una comprensión del ambiente SIC y de si puede influir en la evaluación de los riesgos inherente y de control y que afectan las aseveraciones importantes de los estados financieros.

- **Procedimientos de auditoría** – el auditor deberá considerar el ambiente SIC al diseñar los procedimientos de auditoría para reducir el riesgo de auditoría a un nivel aceptablemente bajo.

## DIPA 1001 - MICROCOMPUTADORES INDEPENDIENTES

La Perspectiva del Sector Público (PSP Public Sector Perspective), emitida por el Comité del Sector Público de la federación Internacional de Contadores, se expone al final de una IAPS (Declaración internacional de prácticas de auditoría. Cuando no hay PSP la Declaración aplica, respecto de todo lo impórtame, al sector público.

### Introducción

1. Esta Declaración describe los efectos que tienen las microcomputadoras independientes sobre el sistema de contabilidad y controles internos relacionados y sobre los procedimientos de auditoría.

### Microcomputadoras independientes

2. Las microcomputadoras pueden ser usadas para procesar transacciones contables y producir informes que son esenciales para la preparación de estados financieros. La microcomputadora puede constituir todo el sistema de contabilidad basado en computadoras, o solamente una parte del mismo.
3. Generalmente, los ambientes de CIS en los que se usan las microcomputadoras son de algún modo diferentes de otros ambientes de CIS. Ciertos controles y medidas de seguridad que se usan para sistemas grandes de computación pueden no ser factibles para las microcomputadoras. En contraste, se hacen más importantes ciertos tipos de controles internos debido a las características de las microcomputadoras y a los ambientes en que se usan.
4. Las computadoras independientes pueden ser operadas por uno o muchos usuarios en movimientos distintos, accediendo al mismo o a diferentes programas en la misma máquina. El usuario de una computadora independiente que procesa aplicaciones de contabilidad realiza muchas funciones (por ejemplo ingresa datos y opera aplicaciones de programas). Aunque típicamente sin conocimientos de programación, los usuarios a menudo pueden utilizar paquetes de software (programas) de terceros o tomados de la biblioteca de programas o paquetes, tales como hojas de cálculo o aplicaciones de bases de datos.
5. La estructura organizacional dentro de la que una microcomputadora independiente se usa es importante para evaluar riesgos y el alcance de los controles requeridos para aminorar dichos riesgos. Por ejemplo, los controles de vigilancia o monitoreo empleados por la administración pueden ser los únicos efectivos para un paquete de software comprado y que usa un negocio pequeño en una microcomputadora independiente, aparte de cualquier tipo de control que se incorpore en el paquete mismo. En contraste, la efectividad de los controles relacionados con una microcomputadora independiente usada dentro de una organización mayor pueden depender de una estructura organizacional que claramente segrega responsabilidades y restringe el uso de las microcomputadoras independientes para funciones específicas.
6. Las consideraciones de control y las características del hardware (equipo físico de cómputo) y del software (programas y sistema de programación) son diferentes cuando se enlaza una microcomputadora a otras computadoras. Estas situaciones a menudo llevan a aumento de riesgos. Esta Declaración no se refiere a la consideración del auditor de la seguridad y controles de una red. Sin embargo, esta Declaración es relevante para microcomputadoras enlazadas con otra computadora, las cuales también pueden usarse como estaciones de trabajo independientes. Muchas microcomputadoras utilizan en forma intercambiable como parte de una red o de modo independiente. Cuando se refiere a estas microcomputadoras, el auditor considera los riesgos adicionales que se encuentran por el acceso mediante una red así como los lineamientos en esta Declaración.

### Control interno en ambientes de microcomputadoras independientes

7. Las microcomputadoras están orientadas a usuarios finales individuales. El grado de precisión y confiabilidad de la información financiera que producen dependerá, en parte, de los controles internos que el usuario adopte, ya sea por voluntad o porque la administración los ha prescrito. Los procedimientos de control establecidos se relacionan con la complejidad del entorno del negocio en que opera la microcomputadora. Normalmente, el ambiente de microcomputadoras independientes es menos estructurado que un ambiente de CIS controlado en forma central. En el primero, los usuarios con sólo habilidades básicas de procesamiento de datos pueden adoptar y poner en marcha los programas de aplicación en forma relativamente rápida, haciendo surgir asuntos tales como lo adecuado de la documentación de sistemas o los procedimientos de control del acceso. Dichos usuarios pueden no considerar como importantes o como de costo efectivo los controles sobre el proceso de desarrollo de la aplicación (por ejemplo, documentación adecuada) y las operaciones (por ejemplo, procedimientos de control de acceso). En tales circunstancias, como la información financiera se procesa en una computadora, los usuarios pueden tender a depositar una confianza injustificada en la misma.

8. En un ambiente típico de microcomputadoras independientes, el nivel de controles generales es más bajo del que se encontraría en un ambiente de computación a mayor escala. No obstante, los procedimientos selectos de seguridad y control pueden ayudar a mejorar el nivel general de control interno.

#### Políticas organizacionales y procedimientos

9. Como parte de haber obtenido una comprensión del ambiente de control, y por tanto del ambiente de CIS para microcomputadoras independientes, el auditor considera la estructura organizacional de la entidad y, en particular, la asignación de responsabilidades para el procesamiento de datos. Las políticas y procedimientos efectivos para la adquisición, desarrollo, operación y mantenimiento de microcomputadoras independientes puede enriquecer el ambiente general de control. La falta de desarrollo de dichas políticas puede llevar a que la entidad use programas obsoletos y a errores en los datos así como de la información derivada de los mismos, lo cual puede llevar al incremento del riesgo de fraude. Dichas políticas y procedimientos incluyen lo siguiente:
  - estándares de adquisición, desarrollo y documentación;
  - entrenamiento del usuario;
  - lineamientos de seguridad, respaldos y almacenamiento;
  - administración de contraseñas (password);
  - políticas de uso personal;
  - estándares de adquisición y uso de software;
  - estándares de protección de datos;
  - mantenimiento de programas y soporte técnico;
  - un nivel apropiado de segregación de funciones y responsabilidades; y
  - protección contra virus. Protección física—equipo
10. Debido a sus características físicas, las microcomputadoras independientes y sus medios de almacenamiento son susceptibles a robo, daño físico, acceso no autorizado o mal uso. Pueden protegerse físicamente de la manera siguiente:
  - cerrándolas bajo llave en un cuarto, gabinete o estuche de protección;
  - usando un sistema de alarma que se active si la microcomputadora es desconectada o movida de su lugar;
  - asegurando la microcomputadora a una mesa;
  - con políticas que expongan los procedimientos apropiados a seguir al salir de viaje con una computadora portátil "laptop" o al usarla fuera de las instalaciones;
  - usando la criptografía para archivos clave;
  - instalando un mecanismo de seguridad para controlar el interruptor de encendido/apagado. Esto quizá no prevenga el robo de la microcomputadora, pero puede ser efectivo para controlar el uso no autorizado; y
  - desarrollando controles ambientales para prevenir daños por desastres naturales, como incendio, inundación, etcétera.

#### Protección física - medios removibles y no removibles

11. Los programas y datos de las microcomputadoras pueden almacenarse en medios de almacenamiento removibles o no removibles. Por ejemplo, los disquetes y CDs pueden removerse físicamente de la microcomputadora independiente, mientras que los discos duros normalmente están integrados en la microcomputadora o en una unidad independiente anexa a la misma. Además, los componentes interiores (incluyendo el hard drive "disco duro") de muchas microcomputadoras, en particular laptops, son fácilmente accesibles. Cuando muchos individuos usan una microcomputadora particular es más probable que los medios de almacenamiento se extravíen, se alteren sin autorización o se destruyan.
12. Es responsabilidad del usuario proteger los medios de almacenamiento removibles, por ejemplo, manteniendo respaldos actualizados de dichos medios en un contenedor a prueba de incendio, ya sea en el lugar de trabajo, fuera de él o en ambos. Esto aplica igualmente a los sistemas operativos, programas de aplicación y datos.

#### Seguridad de programas y datos

13. Cuando muchos usuarios pueden acceder a las microcomputadoras hay un riesgo de que el sistema operativo, los programas y los datos puedan ser alterados sin autorización, o que los usuarios puedan instalar sus propias versiones de programas dando pie a responsabilidades potenciales sobre autorización del software.

14. El grado de características de control y seguridad presentes en un sistema operativo de microcomputadora varía. Aunque algunos sistemas operativos contienen características de seguridad sofisticadas selladas, los utilizados en microcomputadoras independientes generalmente no las tienen. Sin embargo, hay técnicas para ayudar a asegurar que los datos que se procesen y lean sean autorizados, minimizando la destrucción accidental de éstos. Las siguientes técnicas pueden limitar sólo a personal autorizado el acceso a programas y datos:
  - uso de contraseñas-password;
  - desarrollar un paquete de control de acceso;
  - usar medios de almacenamiento removibles;
  - usar directorios y archivos ocultos; y
  - usar la criptografía.
15. Una técnica efectiva de control es usar perfiles y contraseñas que controlen el nivel de acceso concedido a un usuario. Por ejemplo, se puede dar a un usuario un perfil protegido por una contraseña que permita sólo la alimentación de datos, y puede configurarse una microcomputadora independiente para que requiera una contraseña antes de ser "saqueada".
16. En algunos casos, un paquete de control de acceso puede proporcionar control efectivo sobre el acceso y uso de sistemas operativos, programas y datos. Por ejemplo, sólo un usuario específico puede tener acceso al archivo de contraseñas o permitírsele instalar programas. Dichos paquetes pueden también, en forma regular, examinar los programas en la microcomputadora para detectar si se están usando programas o versiones de éstos no autorizados.
17. El uso de medios de almacenamiento removibles para programas y datos críticos y sensibles puede proporcionar una mayor protección, al mantenerse fuera de línea y bajo control independiente hasta ser requeridos. Por ejemplo, los datos sobre salarios en un sistema de nóminas pueden mantenerse fuera de línea y usarse sólo cuando se requiera para el procesamiento de nóminas.
18. Remover los programas y datos de las microcomputadoras con medios de almacenamiento removibles (por ejemplo, disquetes, CDs y cartuchos) es una manera efectiva de mantenerlos seguros. Los medios se colocan después bajo custodia de los bibliotecarios de archivos o de los usuarios responsables de los datos o programas.
19. La criptografía o cifrado es una técnica que generalmente se utiliza cuando se transmiten datos sensibles por las líneas de comunicación, pero puede también usarse en datos almacenados en una microcomputadora independiente.

#### Continuidad de operaciones

20. En un ambiente de microcomputadoras, la administración se apoya típicamente en el usuario para asegurar la disponibilidad continua de los sistemas en caso de una falla, pérdida o destrucción del equipo, sistema operativo, programas o datos.

Esto implicará que;

  - (a) el usuario retenga copias del sistema operativo, programas y datos; cuando menos una almacenada en un lugar seguro, lejos de la microcomputadora; y
  - (b) esté disponible el acceso a un equipo alterno dentro de un tiempo razonable, dado el uso e importancia del sistema fundamental.

#### El efecto de microcomputadoras independientes sobre el sistema de contabilidad y los controles internos relacionados

21. El efecto de las microcomputadoras sobre el sistema de contabilidad y los riesgos asociados generalmente dependerá de:
  - (a) el grado en que se use la microcomputadora para procesar aplicaciones contables;
  - (b) el tipo e importancia de las transacciones financieras que se procesen; y
  - (c) la naturaleza de los programas y datos usados en las aplicaciones,
22. A continuación un resumen de algunas de las consideraciones clave y sus efectos, se presenta tanto sobre los controles generales como sobre los de aplicación,

#### Controles generales - segregación de funciones

23. En un ambiente de microcomputadoras, los usuarios generalmente pueden desempeñar dos o más de las siguientes funciones en el sistema de contabilidad:
  - (a) iniciar documentos fuente;
  - (b) autorizar documentos fuente;
  - (c) alimentar datos al sistema;
  - (d) procesar datos que se han alimentado;

- (e) cambiar programas y datos;
- (f) usar o distribuir datos de salida; y
- (g) modificar los sistemas operativos.

24. En otros ambientes de CIS, estas funciones normalmente se segregarian mediante controles generales apropiados. Esta falla de segregación de funciones en un ambiente de microcomputadoras puede permitir que se dejen de detectar los errores, permitiendo que se cometa y oculte el fraude.

#### Controles de aplicación

25. La existencia y uso de controles apropiados de acceso sobre los programas y datos, combinados con controles sobre la alimentación, procesamiento y salida de datos pueden, en coordinación con las políticas de administración, compensar algunas de las debilidades en los controles generales en ambientes de microcomputadoras. Los controles efectivos incluyen lo siguiente:

- procedimientos de control programados, como verificaciones de límites;
- un sistema de registro de transacciones y contrapartidas de lotes, incluyendo seguimiento y resolución de cualquier excepción;
- supervisión directa, por ejemplo, una revisión de informes; y
- conciliación de recuentos de registros o cifras de control.

26. El control puede establecerse por una función independiente que normalmente:

- (a) recibe todos los datos para procesamiento;
- (b) asegura que todos los datos sean autorizados y registrados;
- (c) hace un seguimiento de todos los errores detectados durante el procesamiento;
- (d) verifica la distribución apropiada de los datos de salida; y
- (e) restringe el acceso físico a los programas de aplicación y datos.

Normalmente se requieren controles separados sobre el archivo maestro y datos de transacciones.

#### El efecto de un ambiente de microcomputadoras independientes sobre los procedimientos de auditoría

27. En un ambiente de microcomputadoras independientes, puede no ser factible o efectivo, desde el punto de vista de costo efectivo para la administración, implementar controles suficientes para reducir a un nivel mínimo los riesgos de errores sin detectar. En esta situación, después de obtener la comprensión del sistema de contabilidad y del ambiente de control requeridos por la NIA 400 "Evaluaciones del Riesgo y Control Interno", el auditor puede encontrar que es más efectivo, desde el punto de vista de costo, no hacer una revisión adicional de los controles generales o de los controles de aplicación, sino concentrar los esfuerzos de auditoría en los procedimientos sustantivos. Esto puede implicar un examen físico más amplio y confirmación de los activos, más pruebas de las transacciones, tamaños mayores de muestras así como mayor uso de TAAC (técnicas de auditoría asistidas por computadora).

28. Cuando el nivel de los controles generales parezca adecuado, el auditor puede decidir adoptar un enfoque diferente. Por ejemplo, una entidad que procesa un gran número de transacciones de ventas en una microcomputadora independiente, puede establecer procedimientos de control que reduzcan el riesgo de control.

29. Las microcomputadoras independientes frecuentemente se encuentran en entidades pequeñas. El IAPS 1005 "Consideraciones especiales en la auditoría de entidades pequeñas", proporciona más lineamientos. Con base en una revisión preliminar de los controles, el plan de auditoría podría incluir someter a prueba los controles en los que el auditor piensa apoyarse.

## DIPA 1002 - SISTEMAS DE COMPUTADORAS EN LINEA

### Introducción

1. Esta Declaración describe los efectos de un sistema de computadoras en línea sobre el sistema de contabilidad, los controles internos relativos y sobre los procedimientos de auditoría.

#### Sistemas de computadoras en línea

2. Los sistemas de computadoras en línea son sistemas de computadoras que posibilitan a los usuarios el acceso a datos y programas directamente a través de aparatos terminales. Dichos sistemas pueden comprender computadoras main-frame (unidades centrales de procesamiento), minicomputadoras o una red de microcomputadoras interconectadas. Cuando la entidad usa un sistema de computadoras en línea, es probable que la tecnología sea compleja y ligada a los planes estratégicos de negocios de la entidad. El equipo de auditoría puede requerir habilidades especiales de CIS para hacer

- investigaciones y para entender las implicaciones de las respuestas que obtenga.<sup>1</sup> Puede ser necesario para el auditor considerar el uso del trabajo de un experto (ver la NIA 620 "Uso del trabajo de un experto").
3. Los sistemas en línea permiten a los usuarios iniciar directamente varias funciones como:
    - alimentar transacciones (por ejemplo, transacciones de ventas en una tienda al menudeo, retiros de efectivo en un banco y embarque de mercancías en una planta);
    - hacer investigaciones (por ejemplo, la cuenta corriente de clientes o información de saldos);
    - solicitar informes (por ejemplo, una lista de partidas de inventario con cantidades negativas "en existencia");
    - actualizar archivos maestros (por ejemplo, establecer cuentas de nuevos clientes y cambiar los códigos del libro mayor); y
    - actividades de comercio electrónico (por ejemplo, colocar pedidos y pagar las mercancías por Internet).
  4. Los sistemas de computadoras en línea usan muchos tipos diferentes de aparatos terminales. Las funciones que desempeñan estos aparatos varían ampliamente, y dependen de sus capacidades de lógica, transmisión, almacenamiento y procesamiento básicos. Los tipos de aparatos terminales son:
    - (a) Terminales para fines generales, como:
      - Teclado básico y monitor —usados para alimentar datos sin validación alguna dentro de la terminal y para desplegar datos del sistema de la computadora en la pantalla. Por ejemplo, al alimentar una orden de venta, la computadora principal valida la clave del producto y el resultado de la validación aparece en la pantalla de la terminal.
      - Terminal inteligente —usada para las funciones del teclado básico y monitor con las funciones adicionales de validación de datos dentro de la terminal, de mantener registros de transacciones y llevar a cabo otros procesamientos locales. En el ejemplo anterior de la orden de venta, la terminal inteligente verifica el número correcto de caracteres en la clave del producto y la computadora principal verifica la existencia de la clave del producto en el archivo maestro.
      - Microcomputadoras—usadas para todas las funciones de una terminal inteligente con capacidades adicionales de procesamiento local y de almacenamiento. Siguiendo con el ejemplo anterior, la microcomputadora puede llevar a cabo todas las verificaciones de la clave del producto.
    - (b) Terminales para fines especiales, como:
      - Aparatos de punto de venta —usados para registrar transacciones de venta cuando éstas ocurren y para transmitirlos a la computadora principal. Las cajas registradoras en línea y scanners ópticos usados en el comercio al menudeo son aparatos típicos de punto de venta.
      - Cajeros automáticos —usados para iniciar, validar, registrar, transmitir y completar diversas transacciones bancarias. Dependiendo del diseño del sistema, algunas de estas funciones son desempeñadas por el cajero automático y otras, en línea, por la computadora principal.
      - Aparatos inalámbricos manuales para alimentar datos desde localidades remotas.
      - Sistemas contestadores de voz —usados para permitir al usuario la interacción con la computadora por una red de telecomunicaciones con base en instrucciones verbales emitidas por la computadora. El cliente se comunica usando un aparato que genera un tono, el cual a menudo es el teclado del teléfono del cliente. Las aplicaciones comunes incluyen sistemas de banca por teléfono y de pago de cuentas.
  5. Los aparatos terminales pueden localizarse ya sea localmente o en sitios remotos. Las terminales locales están conectadas directamente a la computadora por medio de cables, mientras que los aparatos terminales remotos requieren del uso de telecomunicaciones para enlazarlos a la computadora. En algunos casos, sin embargo, aun las terminales locales pueden conectarse usando enlaces de telecomunicaciones o enlaces de comunicación inalámbrica. Los aparatos terminales pueden usarse al mismo tiempo por muchos usuarios, para diferentes propósitos y en diferentes localidades. Los usuarios, como clientes o proveedores, pueden estar dentro o fuera de la entidad. En tales casos, el software de aplicaciones y los datos son mantenidos en línea para satisfacer las necesidades de los usuarios. Estos sistemas también requieren otro software de control de acceso, y para vigilar y controlar los aparatos terminales en línea.
  6. Compartir cada vez más los recursos de sistemas a través de LANs (red de área local) y WANs (red de área ancha) ha llevado al crecimiento del procesamiento en línea distribuido. Los sistemas Cliente/Servidor han dado como resultado que se dividan las aplicaciones, de modo que el procesamiento puede desempeñarse en varias máquinas. En un ambiente de cliente/servidor, el procesamiento de datos tiene lugar en el servidor y en la computadora de escritorio (cliente).
  7. Los empleados, socios de negocios, clientes y otras terceras partes pueden obtener acceso a las aplicaciones en línea de una organización usando la Internet u otros servicios de acceso remoto. Las partes externas pueden tener acceso a las

aplicaciones de la organización a través de intercambio electrónico de datos (EDI Electronic data interchange) u otras aplicaciones comerciales electrónicas.

8. Además de los usuarios de estos sistemas, los programadores pueden usar las capacidades del sistema en línea para desarrollar nuevos programas y mantener los programas existentes. El personal del proveedor de las computadoras puede también tener acceso en línea para proporcionar mantenimiento y servicios de apoyo.

#### Tipos de sistemas de computadoras en línea

9. Los sistemas de computadoras en línea pueden clasificarse de acuerdo a cómo se alimenta la información al sistema, cómo se procesan y cuándo están disponibles los resultados para el usuario. Para fines de esta Declaración, las funciones de los sistemas de computadoras en línea se clasifican como sigue:
  - (a) procesamiento en línea/tiempo real;
  - (b) procesamiento en línea/por lote;
  - (c) actualización en línea/memo (y procesamiento posterior);
  - (d) consultas en línea; y
  - (e) procesamiento de descarga/carga en línea. Procesamiento en línea/tiempo real
10. En un sistema de procesamiento en línea/tiempo real, las transacciones individuales son alimentadas en aparatos terminales, validadas y usadas para actualizar inmediatamente los archivos de computadora relacionados. Un ejemplo es la aplicación de cobros en efectivo directamente de las cuentas de los clientes. Los resultados de este procesamiento están entonces disponibles inmediatamente para consultas o informes.

#### Procesamiento en línea/por Lote

11. En un sistema con alimentación y procesamiento por lote en línea, las transacciones individuales se alimentan en un aparato terminal, sujeto a verificaciones de validación y se añaden a un archivo de transacciones que contiene otras alimentadas durante el periodo. Después, durante un ciclo posterior de procesamiento, el archivo de transacciones puede validarse más aún y luego usarse para actualizar el archivo maestro relevante. Por ejemplo, las entradas del diario pueden alimentarse y validarse en línea y conservarse en un archivo de transacciones, actualizando el archivo maestro del libro mayor sobre una base mensual. Las investigaciones de, o informes generados desde el archivo maestro no incluirán transacciones alimentadas después de la última actualización del archivo maestro.

#### Actualización en línea/memo (y procesamiento posterior)

12. La alimentación en línea con procesamiento de actualización de memo, también conocida como actualización de sombra, combina procesamiento en línea/tiempo real y procesamiento en línea/por lote. Las transacciones individuales inmediatamente actualizan un archivo de memos que contiene información que ha sido extraída de la versión más reciente del archivo maestro. Las consultas se hacen de este archivo de memos. Estas mismas transacciones se añaden a un archivo de transacciones para validación y actualización posteriores del archivo maestro sobre una base por lotes. Por ejemplo, el retiro de efectivo mediante un cajero automático se verifica contra el saldo del cliente en el archivo memo, e inmediatamente se anota en la cuenta del cliente en ese archivo para reducir el saldo por la cantidad del retiro. Desde la perspectiva del usuario, este sistema no parecerá diferente del procesamiento en línea /tiempo real ya que los resultados de datos que se alimentan están disponibles inmediatamente. Sin embargo, las transacciones no han sido sujetas a una validación completa antes de la actualización del archivo maestro.

#### Consultas en línea

13. La consulta en línea restringe al usuario de aparatos terminales de hacer consultas de archivos maestros. En dichos sistemas, los archivos maestros son actualizados por otros sistemas, generalmente sobre una base por lote. Por ejemplo, el usuario puede consultar la situación de crédito de un cliente particular antes de aceptar un pedido de ese cliente.

#### Procesamiento de descarga/carga en línea

14. La descarga en línea se refiere a la transferencia de datos de un archivo maestro a un aparato terminal inteligente para ser procesados adicionalmente por el usuario. Por ejemplo, los datos en la oficina general que representan transacciones de una sucursal pueden ser descargados en un aparato terminal en la sucursal para mayor procesamiento y preparación de informes financieros de la sucursal. Los resultados de este procesamiento y de otros datos procesados localmente pueden entonces cargarse en la computadora de la oficina general.

#### Características de los sistemas de computadoras en línea

Las características de los sistemas de computadoras en línea pueden aplicarse a muchos de los tipos de sistemas en línea discretos en la sección anterior. Las características más importantes se refieren a la entrada y validación de datos en línea, al acceso en línea al sistema por los usuarios, a la posible falta de un rastro visible de las transacciones y al acceso potencial al

sistema por parte de no usuarios, incluyendo a programadores y otras terceras parte (por ejemplo, a través de correo electrónico Internet). Las características particulares de un sistema en línea específico dependerán del diseño de dicho sistema.

Cuando se alimentan los datos en línea, generalmente están sujetos a verificaciones de validación inmediatas. Los datos que no pasen esta validación no se aceptan y puede aparecer un mensaje en la pantalla de la terminal, dando al usuario la posibilidad de corregir los datos y realimentar los datos válidos inmediatamente. Por ejemplo, si el usuario alimenta un número inválido por parte de inventario, aparece un mensaje de error, permitiendo al usuario realimentar un número válido de parte.

Los usuarios pueden tener acceso en línea al sistema lo que les permite desempeñar diversas funciones (por ejemplo, alimentar transacciones y leer, cambiar o suprimir programas y archivos de datos mediante los aparatos terminales). No es deseable el acceso ilimitado a todas estas funciones en una aplicación particular porque da al usuario la capacidad potencial de hacer cambios no autorizados a los datos y programas. El acceso ilimitado impide la segregación de funciones y permite a los usuarios el acceso a todos los niveles de procesamiento y registro de una transacción. El grado de este acceso dependerá de aspectos tales como el diseño de la aplicación particular y la implementación de software diseñado para controlar el acceso al sistema.

18. Un sistema de computadoras en línea puede estar diseñado de modo que no proporcione documentos de soporte para todas las transacciones alimentadas al sistema. Este sistema debe ser capaz de proporcionar detalles de las transacciones a petición o mediante registros de transacciones u otros medios. Los ejemplos de estos tipos de sistemas incluyen órdenes recibidas por un operador telefónico que las alimenta en línea sin órdenes de compra escritas y retiros de efectivo de cajeros automáticos.
19. Los programadores pueden tener acceso al sistema en línea que les permita desarrollar nuevos programas y modificar programas existentes. El acceso no restringido da al programador el potencial de hacer cambios no autorizados a los programas y de obtener acceso no autorizado a otras partes del sistema, representando una seria debilidad del control. El grado de este acceso depende de los requerimientos del sistema. Por ejemplo, en algunos sistemas, los programadores comúnmente tienen acceso sólo a programas mantenidos en una biblioteca separada de desarrollo y mantenimiento de programas. Sin embargo, los programadores pueden estar autorizados a cambiar los programas operacionales en emergencias que requieran cambios a los programas mantenidos en línea. En estos casos, después de la emergencia, se seguirían los procedimientos formales de control para asegurar la autorización y documentación apropiadas de los cambios.

#### Control interno en un sistema de computadoras en línea

20. Las aplicaciones en un ambiente en línea pueden estar más expuestas al acceso no autorizado y a la actualización. La infraestructura de seguridad de una entidad juega un papel importante para asegurar la integridad de la información producida. Por lo tanto, el auditor considera la infraestructura de seguridad antes de examinar los controles generales y de aplicación. La entidad puede necesitar establecer controles generales adecuados para aminorar los riesgos de virus, acceso no autorizado y la destrucción potencial de rastros de auditoría. Así, los controles de acceso son particularmente importantes para el procesamiento en línea.
21. Estos controles pueden incluir el uso de contraseñas password, software especializado de control de acceso, tal como monitores en línea que mantienen el control sobre los menús, tablas de autorización, contraseñas, archivos y programas a los que se permite acceso de los usuarios. Pueden también incluir controles físicos como el uso de cerraduras en los aparatos terminales, cuartos de computadoras cerrados con llave y horarios sin actividad. Otros aspectos importantes de control en un sistema de computadoras en línea incluyen:
  - Controles sobre las contraseñas: procedimientos para la asignación y mantenimiento de contraseñas para restringir el acceso a los usuarios autorizados.
  - Controles de desarrollo y mantenimiento de sistemas: procedimientos adicionales para asegurar que se incluyan en el sistema durante su desarrollo y mantenimiento los controles esenciales para las aplicaciones en línea, tales como contraseñas, controles de acceso, validación de datos y recuperación de procedimientos en línea; los controles están también diseñados para asegurar que los cambios a los sistemas operan según se espera y se hacen de la manera correcta.
  - Controles de programación.
  - Registros de transacciones.
22. Ciertos controles de aplicación son particularmente importantes para el procesamiento en línea. Incluyen los siguientes:
  - Autorización para pre-procesamiento. Autorización para iniciar una transacción, por ejemplo, usar una tarjeta bancaria junto con un número de identificación personal antes de poder hacer un retiro de efectivo mediante un cajero automático.

- Pruebas de edición del aparato terminal, pruebas de razonabilidad y otras de validación. Rutinas programadas que verifican los datos de entrada y los resultados del procesamiento para que esté completo, y para su exactitud y razonabilidad. Estas rutinas incluyen verificaciones de secuencia, límite, rango y razonabilidad y pueden desempeñarse en un aparato terminal inteligente o en la computadora central.
- Informes y manejo de errores de alimentación. Los procedimientos para asegurar que todos los errores de alimentación sean informados, identificados y se les impida seguir el procesamiento, sean corregidos y vueltos a someter para procesamiento oportuno y, todo de una manera apropiada. Estos procedimientos generalmente comprenderán una mezcla de rutinas tanto manuales como automatizadas.
- Procedimientos de corte. Procedimientos que aseguran que las transacciones se procesan en el periodo contable apropiado. Son particularmente necesarios en sistemas que tienen un flujo continuo de transacciones. Por ejemplo, en los sistemas en línea donde los aparatos terminales de diversas localidades registran órdenes de ventas y embarques, hay necesidad de coordinar el embarque real de mercancías, la salida de inventario y el procesamiento de facturas.
- Controles de archivos. Procedimientos que aseguran que se usan los archivos de datos correctos para el procesamiento en línea.
- Controles de archivo maestro. Los cambios a los archivos maestros se controlan por procedimientos similares a los usados para controlar otros datos de entrada de transacciones. Puede ser necesario un reforzamiento más estricto de estos procedimientos de control porque los datos del archivo maestro pueden tener un efecto profundo sobre los resultados del procesamiento.
- Balanceo. El proceso de establecer totales de controles sobre los datos que se someten para procesamiento por medio de los aparatos terminales en línea, y de comparar los totales de controles durante y después del procesamiento para asegurar que se transfieren datos completos y exactos a cada fase del procesamiento. Estos controles de balanceo son importantes para monitorear los controles de totalidad y exactitud en un ambiente de procesamiento en tiempo real. Deberán incluirse en las rutinas automatizadas de programas siempre que sea posible.
- Puede establecerse el control con una función independiente que generalmente:
  - (a) recibe todos los datos para procesamiento;
  - (b) asegura que todos los datos estén autorizados y registrados;
  - (c) hace seguimiento de todos los errores detectados durante el procesamiento;
  - (d) verifica la distribución apropiada de los datos de salida; y
  - (e) restringe el acceso físico a programas y datos de aplicación.

Normalmente se requieren controles separados sobre el archivo maestro y los datos de transacciones así como en los sistemas de computadoras en línea sobre el sistema de contabilidad y los controles internos relacionados

23. El efecto de un sistema de computadoras en línea sobre el sistema de contabilidad y los riesgos asociados generalmente dependerán de:
- (a) el grado en que el sistema en línea está siendo usado para procesar aplicaciones contables;
  - (b) el tipo e importancia de las transacciones financieras que se procesan; y
  - (c) la naturaleza de los archivos y programas que usan las aplicaciones.

La infraestructura de seguridad de la entidad juega un papel importante en el control del efecto de los riesgos creados por el uso en la entidad de un ambiente en línea.

24. Factores como los siguientes pueden reducir el riesgo de errores que ocurren porque la entidad utiliza sistemas en línea:
- Realizar la entrada de datos en o cerca del punto donde se originan las transacciones reduce el riesgo de que no se registren las transacciones.
  - La corrección inmediata y realimentación de transacciones inválidas reduce el riesgo de que dichas transacciones no sean corregidas y vueltas a alimentar rápidamente.
  - La alimentación de datos desempeñada por individuos que entienden la naturaleza de las transacciones implicadas puede ser menos propensa a error que cuando es desempeñada por individuos no familiarizados con la naturaleza de las transacciones.
  - Procesar las transacciones inmediatamente reduce el riesgo de que sean procesadas en el periodo contable equivocado.
  - La revisión de autenticidad y autorización llevada a cabo en o cerca del punto donde las transacciones se originan reduce el riesgo de suplantación u otro acceso no autorizado a los datos o su manipulación.

25. El riesgo de errores en los sistemas de computadoras en línea puede aumentar por las siguientes razones;
- Ubicar los aparatos terminales por toda la entidad aumenta la oportunidad de uso no autorizado de un aparato terminal y la entrada de transacciones no autorizadas.
  - Los aparatos terminales en línea pueden proporcionar una oportunidad más fácil de usos no autorizados como:
    - modificación de transacciones o saldos alimentados previamente;
    - modificación de programas de computadora; o
    - acceso a datos y programas desde localidades remotas.
  - la falta de rastros visibles de las transacciones;
  - procedimientos realizados durante la etapa de planeación de la auditoría (ver párrafo 29);
  - procedimientos de auditoría desempeñados en forma concurrente con
  - el procesamiento en línea (ver párrafo 30); y
  - procedimientos desempeñados después de que ha tenido lugar el proceso de datos (ver párrafo 31).
29. Los procedimientos desarrollados durante la etapa de planeación pueden incluir los siguientes:
- participación en el equipo de auditoría de individuos con pericia técnica en sistemas de computadoras en línea y los controles relativos;
  - identificación de nuevas instalaciones de acceso remotas; y
  - determinación preliminar, durante el proceso de evaluación del riesgo, del impacto del sistema sobre los procedimientos de auditoría.
30. Los procedimientos de auditoría desempeñados en forma concurrente con el procesamiento en línea pueden incluir pruebas de los controles sobre las aplicaciones en línea. Por ejemplo, esto puede ser por medio de alimentar transacciones para prueba mediante los aparatos terminales en línea o con el uso de software de auditoría. Estas pruebas pueden usarse ya sea para confirmar la comprensión del sistema por el auditor o para probar controles como contraseñas y otros controles de acceso. Cuando la entidad permite el acceso mediante Internet, los procedimientos de auditoría pueden incluir pruebas de cortafuegos y otros controles de autorización y acceso, así como pruebas de procesamiento de transacciones. Para evitar alteración inadvertida de registros de clientes, el auditor revisa los procedimientos concurrentes con el personal apropiado de clientes y obtiene aprobación antes de conducir las pruebas.
31. Los procedimientos desempeñados después de tener lugar el procesamiento en línea pueden incluir los siguientes:
- pruebas de los controles sobre las transacciones registradas por el sistema en línea en cuanto a autorización, exactitud, y que estén completas;
  - procedimientos sustantivos que cubran las transacciones y resultados del procesamiento más que pruebas de control, cuando los primeros sean de costo más efectivo o cuando el sistema no esté bien diseñado o controlado; y
  - procesamiento de transacciones ya sea como una prueba de control o como un procedimiento sustantivo.

### **DIPA 1003 - AMBIENTE DE CIS - SISTEMAS DE BASES DE DATOS**

#### **Introducción**

1. Esta Declaración describe los efectos de un sistema de base de datos sobre el sistema de contabilidad y los controles internos relativos y sobre los procedimientos de auditoría.
2. Una base de datos es una colección de datos que se comparten y se usan entre diferentes usuarios para diferentes fines. Cada usuario puede no estar necesariamente enterado de todos los datos almacenados en la base de datos, o de las maneras en que pueden usarse los datos para fines múltiples. Generalmente, los usuarios individuales conocen sólo los datos que usan y pueden considerar los datos como archivos de computadora utilizados para sus aplicaciones.
3. "Cuando una entidad usa un sistema de bases de datos, es probable que la tecnología sea compleja y pueda estar ligada con los planes estratégicos de negocios de la entidad. El equipo de auditoría puede requerir habilidades especiales de CIS para hacer las investigaciones apropiadas y para entender las implicaciones de las respuestas que obtenga". El auditor puede necesitar considerar el empleo del trabajo de un experto (ver NIA 620 "Uso del trabajo de un experto").

#### **Sistemas de bases de datos**

4. Los sistemas de bases de datos consisten principalmente de dos componentes: la base de datos y el sistema de administración de la base de datos (SABs). Los sistemas de bases de datos interactúan con otros aspectos del hardware y software del sistema general de computadoras.
5. El software que crea, mantiene y opera la base de datos es conocido como software SABs. Junto con el sistema operativo, el SABs facilita el almacenamiento físico de los datos, mantiene las interrelaciones entre ellos, y los hace disponibles para

programas de aplicación. También proporciona métodos de acceso controlados para establecer medidas básicas de seguridad sobre los datos. Generalmente, el software SABs es surtido por un proveedor comercial, pero necesitará adaptarse a las necesidades de la entidad.

6. Los lineamientos en esta declaración aplican a los sistemas de base de datos utilizadas en ambientes de usuarios múltiples. Aunque los sistemas de bases de datos pueden residir en cualquier tipo de sistema de computadoras, incluyendo microcomputadoras, esta Declaración no se refiere a ambientes de microcomputadoras con un solo usuario.

#### Características del sistema de base de datos

7. Los sistemas de base de datos se distinguen por dos importantes características: datos compartidos e independencia de datos. Estas características normalmente requieren el uso de un diccionario de datos (párrafo 11) y establecer una función de administración de recursos de datos (párrafos 13-19).

#### Datos compartidos

8. Una base de datos está compuesta de datos que se instalan con relaciones definidas y se organizan para permitir que muchos usuarios utilicen los datos en diferentes programas de aplicación. Las aplicaciones individuales comparten los datos de la base de datos para diferentes fines. Por ejemplo, el costo unitario de una partida de inventario mantenido por la base de datos puede usarse por un programa de aplicación para producir un informe de costo de ventas, y por otro programa para preparar una valuación de inventario.

#### Independencia de datos respecto de los programas de aplicación

9. El SABs registra los datos una vez para el uso de diversos programas de aplicación. Esto crea una necesidad de compartir los datos y una necesidad de independencia de éstos respecto de los programas de aplicación. En sistemas que no son de base de datos se mantienen archivos de datos separados para cada aplicación. Los datos similares usados por varias aplicaciones pueden repetirse un sinnúmero de archivos diferentes. Sin embargo, en un sistema de base de datos un solo archivo de datos (base de datos) es usado por muchas aplicaciones, manteniendo a un mínimo la redundancia de datos.
10. Los SABs difieren en el grado de independencia de datos que proporcionan. El grado de independencia de datos está relacionado con la facilidad con que el personal puede hacer cambios a los programas de aplicación o a la base de datos. La verdadera independencia de datos se logra cuando la estructura de los datos en la base de datos puede cambiarse sin afectar los programas de aplicación y viceversa.

#### Diccionario de datos

11. Una implicación importante de compartir datos y de la independencia de datos es el potencial para el registro de datos sólo una vez para su uso en diversas aplicaciones. Ya que diversos programas de aplicación necesitan tener acceso a estos datos, se requiere una instalación de software para seguir el rastro de la localización de los datos en la base de datos, este software dentro del SABs se conoce como diccionario de datos. También sirve como herramienta para mantener documentación estandarizada y definiciones del ambiente de la base de datos y sistemas de aplicación. Un diccionario de datos proporciona funciones como:
  - un mecanismo para crear/modificar definiciones de datos;
  - validación de las definiciones de datos que se dan para asegurar su integridad;
  - prevención de manipulaciones o accesos no autorizados de las definiciones de datos; y
  - mecanismos de interrogación e informes que permiten al administrador de la base de datos hacer preguntas sobre las definiciones de los datos.
12. Las bases de datos pueden estructurarse como bases de datos de archivos planos (ficheros) o como bases de datos relacionadas. En una base de datos de archivo plano todos los datos relativos a un registro se almacenan como parte de dicho registro. Con una base de datos relacionada, los datos se almacenan como una serie de tablas, con enlaces entre ellas según sea necesario. Las bases de datos relacionadas minimizan la duplicación de datos almacenados, ya que los datos compartidos por más de un registro necesitan almacenarse sólo una vez. Los datos mismos pueden comprender objetos para usarlas con aplicaciones orientadas a objetos. Esto puede llevar a estructuras complicadas de datos.

#### Administración de recursos de datos

13. La administración de los recursos de datos forma un control organizacional esencial para asegurar la integridad y compatibilidad de los datos. En un ambiente de base de datos los métodos de control y uso informativo cambian, de un enfoque orientado a la aplicación a un enfoque a nivel de toda la organización. En contraste con los sistemas tradicionales, donde cada aplicación es un sistema separado con su propia información y controles, en un ambiente de base de datos muchos controles pueden ser centralizados, por lo cual la base de datos se diseña para servir a todas las necesidades de información de la organización.

14. El uso de los mismos datos por diversos programas de aplicación enfatiza la importancia de la coordinación centralizada del uso y definición de datos y el mantenimiento de su integridad, seguridad, exactitud y totalidad. Se requiere una administración de recursos de datos para promover la integridad de datos para la organización como un todo, e incluye la función de administración de datos (ver el párrafo 15) y una función de administración de la base de datos (ver los párrafos 16-19). La función de administración de datos tiene que ver con la "propiedad" de los datos, su significado, relación con otros datos e integridad a nivel de toda la entidad. En contraste, la función de administración de la base de datos se refiere primordialmente a la implementación técnica de la base de datos, las operaciones cotidianas de la misma y las políticas así como a procedimientos que gobiernan su acceso y uso diario.

#### Administración de datos

15. La función de administración de datos administra los datos como un recurso organizacional, e incluye responsabilidades por:
- el desarrollo e implementación de un plan estratégico y políticas de administración de recursos de datos, que respalde los planes de negocios de la entidad al lograr un uso de costo efectivo de los datos de la organización;
  - la creación y mantenimiento de un modelo o arquitectura de datos corporativos (a veces conocido como un modelo de datos de la empresa);
  - la coordinación e integración de modelos de datos del sistema;
  - obtener el acuerdo entre los usuarios sobre las definiciones y el formato de datos;
  - resolver conflictos sobre representación y datos incompatibles;
  - establecer un diccionario de datos a nivel corporación y administrar los estándares de nomenclatura y definición de la organización;
  - establecer los estándares de datos y los procedimientos para:
    - nomenclatura de datos;
    - uso de datos;
    - seguridad de datos;
    - compilación de definición de datos;
    - modelos de datos; y
  - proporcionar entrenamiento y asesoría a los usuarios y a los miembros del equipo de CIS (desarrolladores de sistemas y administradores de base de datos) respecto a todos los aspectos de la administración de recursos de datos.

#### Administración de la base de datos

16. La coordinación es generalmente responsabilidad de un grupo de individuos a quienes se conoce típicamente como "administración de la base de datos", el individuo que encabeza esta función puede conocerse como el "administrador de la base de datos". Generalmente la función de administración de la base de datos tiene la responsabilidad de la definición, estructura, seguridad, control operacional y eficiencia de las bases de datos, incluyendo la definición de las reglas para el acceso y almacenamiento de datos.
17. Las tareas de administración de la base de datos pueden también desempeñarse por individuos que no sean parte de un grupo centralizado de administración de la base de datos. Cuando las tareas de administración de la base de datos se distribuyen entre las unidades organizacionales existentes, en vez de ser centralizadas, las diferentes tareas necesitan aún ser coordinadas.
18. Las tareas de administración de la base de datos incluyen típicamente:
- Definir la estructura de la base de datos y la descripción del modelo de datos. Determinar cómo se definen, almacenan y se accede a los datos, por los usuarios de la base de datos, para asegurar que todos sus requerimientos se cumplan de manera oportuna.
  - Mantener la integridad, seguridad y totalidad de los datos. Desarrollar, implementar y ejecutar las reglas de integridad, totalidad y acceso a los datos. Las responsabilidades incluyen:
    - definir quién es responsable de controlar el origen apropiado de los datos y cómo se desempeña dicho control;
    - definir quién puede acceder a los datos y cómo se logra el acceso (por ejemplo, mediante contraseñas y tablas de autorización);
    - prevenir la inclusión de datos incompletos inválidos;
    - detectar la ausencia de datos;
    - asegurar la base de datos contra acceso no autorizado y destrucción;
    - vigilar y controlar, hacer seguimiento de incidentes de seguridad, así como respaldo regular de datos; y

- organizar la recuperación total en caso de pérdida. En tal circunstancia, es probable que el protocolo de respaldo que cubre las tablas de datos sea complejo.
  - Coordinar operaciones de computadora relacionadas con la base de datos. Asignar responsabilidad por los recursos físicos de computadoras y monitorear su uso, relativo a la operación de la base de datos.
  - Vigilar y controlar el funcionamiento del sistema. Desarrollar mediciones del funcionamiento para monitorear la integridad de los datos, la capacidad de la base de datos de responder a las necesidades de los usuarios y la frecuencia de cambios y acceso a los datos.
  - Proporcionar soporte administrativo. Coordinación y enlace con el vendedor del SABs, evaluando nuevas versiones emitidas por el vendedor del SABs junto con el grado de su efecto sobre la entidad, instalando nuevas versiones y asegurando que se proporcione la instrucción interna apropiada.
19. Algunas aplicaciones pueden usar más de una base de datos. En estas circunstancias, las tareas del grupo de administración de la base de datos incluirán la necesidad de asegurar:
- enlace adecuado entre las bases de datos;
  - coordinación de funciones; y
  - consistencia entre los datos de diferentes bases de datos. Control interno en un ambiente de base de datos
20. La infraestructura de seguridad de una entidad juega un importante papel para asegurar la integridad de la información producida, por lo que el auditor considera dicha infraestructura antes de examinar los controles generales y de aplicación. Generalmente, el control interno en un ambiente de base de datos requiere controles efectivos sobre la base de datos, el SABs y las aplicaciones. La efectividad de los controles internos depende en gran parte de la naturaleza de las tareas de administración de datos y de administración de la base de datos (párrafos 15-19), y de cómo se desempeñan.
21. Debido a que los datos son compartidos, a la independencia de datos y a otras características de los sistemas de base de datos, los controles generales normalmente tienen una mayor influencia que los controles de aplicación. Los controles generales sobre la base de datos, el SABs y las actividades de la administración de recursos de datos (administración de datos y administración de la base de datos) tienen un efecto profundo sobre el procesamiento de las aplicaciones. Como se hace notar en el párrafo 29, el uso de SABs, junto con las funciones integradas en él, pueden ayudar a proporcionar controles efectivos. Los controles generales de importancia particular en un ambiente de base de datos pueden clasificarse en los siguientes grupos:
- (a) enfoque estándar para desarrollo y mantenimiento de programas ó aplicación;
  - (b) modelo de datos y propiedad de los datos;
  - (c) acceso a la base de datos;
  - (d) segregación de funciones;
  - (e) administración de recursos de datos; y
  - (f) seguridad de datos y recuperación de la base de datos.

**Enfoque estándar para desarrollo y mantenimiento de programas de aplicación**

22. Considerando que muchos usuarios comparten los datos, el control puede mejorarse si se usa un enfoque estándar para desarrollar cada nuevo programa de aplicación y modificar los existentes. Esto incluye un enfoque paso a paso, formalizado, al que deben adherirse todos los individuos que desarrollan o modifican un programa de aplicación. También incluye analizar el efecto de transacciones nuevas y existentes sobre la base de datos cada vez que se requiera una modificación. El análisis resultante indicaría los efectos de los cambios sobre la seguridad e integridad de la base de datos. Implementar un enfoque estándar para desarrollar y modificar programas de aplicación es una técnica que puede ayudar a mejorar la exactitud, integridad y totalidad de la base de datos. Los siguientes son algunos de los controles que pueden ayudar a lograr esto:
- Se establecen estándares de definición, los cuales se vigilan y controlan para su cumplimiento.
  - Se establecen y separan en un procedimientos de respaldo y recuperación de datos para asegurar la disponibilidad de la base de datos;
  - Se establecen diversos niveles de control de acceso para partidas de datos, tablas y archivos para prevenir el acceso inadvertido o no autorizado;
  - Se establecen controles para asegurar la exactitud, totalidad y consistencia de los elementos y relaciones de datos en la base de datos. Sin embargo, en los sistemas complejos el diseño de los sistemas no siempre puede proporcionar a los usuarios controles que prueben la totalidad y exactitud de los datos, pudiendo haber un incremento del riesgo de que el SABs no siempre identifique alteraciones de datos o índices; y,

- Se siguen procedimientos de reestructuración de la base de datos cuando se hacen cambios lógicos, físicos y de procedimiento.

#### Modelo de datos y propiedad de datos

23. En un ambiente de base de datos, donde muchos individuos pueden usar programas para alimentar y modificar datos, el administrador de la base de datos necesita asegurarse de que haya una asignación de responsabilidad clara y definida por la exactitud e integridad de cada partida de datos. Deberá asignarse a un solo propietario de los datos la responsabilidad de definir las reglas de acceso y seguridad; quiénes pueden usar los datos (acceso) y qué funciones pueden desempeñar (seguridad). Asignar responsabilidad específica por la propiedad de los datos ayuda a asegurar la integridad de la base de datos. Por ejemplo, puede designarse al gerente de crédito como "propietario" del límite de crédito de un cliente, siendo responsable de determinar los usuarios autorizados de dicha información. Si varios individuos tienen capacidad de tomar decisiones que afecten la exactitud e integridad de los datos dados, aumenta la probabilidad de que éstos sean alterados o se usen de manera no apropiada. También son importantes, cuando se usa un sistema de base de datos, los controles sobre los perfiles de usuarios, no sólo para establecer el acceso autorizado, sino también para detectar violaciones o intentos de violación.

#### Acceso a la base de datos

24. El acceso de usuarios a la base de datos puede restringirse mediante controles de acceso. Estas restricciones aplican a individuos, aparatos terminales y programas. Para que las contraseñas sean efectivas se requieren procedimientos adecuados para cambiarlas, mantener el secreto de las mismas y revisar e investigar los intentos de violación a la seguridad. Relacionar las contraseñas a aparatos terminales, programas y datos definidos ayuda a asegurar que sólo usuarios y programas autorizados puedan tener acceso, corregir o suprimir datos. Por ejemplo, el gerente de crédito puede dar autoridad a los vendedores para referirse al límite de crédito de un cliente, mientras que un dependiente del almacén podría no tener dicha autorización.

25. El acceso de usuarios a los diversos elementos de la base de datos puede controlarse aún más mediante el uso de tablas de autorización. La implementación no apropiada de procedimientos de acceso puede dar como resultado el acceso no autorizado a la base de datos. Los controles apropiados también aseguran que los datos almacenados sean convertibles a un formato legible para las personas, en un tiempo razonable.

#### Segregación defunciones

26. Las responsabilidades para desempeñar las diversas actividades requeridas para diseñar, implementar y operar una base de datos se dividen entre el personal técnico, de diseño, administrativo y de usuarios. Sus funciones incluyen diseño del sistema, diseño, administración y operación de la base de datos. Es necesario mantener la adecuada segregación de estas funciones para asegurar la totalidad, integridad y exactitud de la base de datos. Por ejemplo, los individuos responsables de modificar los programas de personal en la base de datos no deberían ser los mismos que estén autorizados para cambiar las tarifas de pago individuales en la base de datos.

#### Seguridad de los datos y recuperación de la base de datos

27. Es probable que las bases de datos se usen por personas en muy diferentes partes de las operaciones de una entidad. Esto significa que muchas partes de la entidad serán afectadas si los datos no estuvieran disponibles o tuvieran errores. Consecuentemente los controles generales, en los sistemas de base de datos, se convierten en muy importantes para la seguridad de los datos y la recuperación de la base de datos.

#### El efecto de las bases de datos sobre el sistema de contabilidad y los controles internos relacionados

28. El efecto de un sistema de base de datos sobre el sistema de contabilidad y los riesgos asociados generalmente dependerán de factores como;

- el grado en el que las bases de datos se usen para aplicaciones contables;
- el tipo e importancia de las transacciones financieras que se procesen;
- la naturaleza y estructura de la base de datos, el SABs (incluyendo el diccionario de datos) las tareas de administración de la base de datos y las aplicaciones (por ejemplo, actualización por lote o en línea); y,
- los controles generales y de aplicación que sean particularmente importantes en un ambiente de base de datos.

29. Los sistemas de base de datos típicamente dan la oportunidad de mayor confiabilidad en los datos que los sistemas que no son de base de datos. En estos sistemas los controles generales cobran una mayor importancia que los controles de aplicación. Esto puede dar como resultado un riesgo reducido de fraude o error en los sistemas de contabilidad donde se usen bases de datos. Los siguientes factores, combinados con controles adecuados, contribuyen a esta mayor confiabilidad en los datos:

- Se logra mejor consistencia de datos porque los datos se registran y actualizan sólo una vez, en lugar de ser almacenados en varios archivos y actualizados en diferentes momentos por diferentes programas.
  - Se mejorará la integridad de los datos con el uso efectivo de mecanismos incluidos en el SABs, tales como rutinas de recuperación/reinicio, rutinas generalizadas de edición y validación, junto con características de seguridad y control.
  - Otras funciones disponibles con el SABs pueden facilitar los procedimientos de control y auditoría. Estas funciones incluyen generadores de informes que pueden usarse para crear informes de compensación y lenguajes de consulta, los cuales pueden ser usados para identificar inconsistencias en los datos.
30. En forma alterna, puede aumentar el riesgo de representación errónea si los sistemas de base de datos se usan sin los controles adecuados. En un ambiente típico que no sea de base de datos, los controles ejercidos por usuarios individuales pueden compensar las fallas en los controles generales. Sin embargo, en un sistema de base de datos los usuarios individuales no pueden siempre compensar los controles inadecuados de la administración de la base de datos. Por ejemplo, el personal de cuentas por cobrar no puede controlar en forma efectiva los datos de cuentas por cobrar si no se restringe a otros miembros del personal la modificación de los saldos de las cuentas por cobrar en la base de datos.

#### El efecto de las bases de datos sobre los procedimientos de auditoría

31. Los procedimientos de auditoría en un ambiente de base de datos serán afectados principalmente por el grado en el que el sistema de contabilidad use los datos de la base de datos. Cuando aplicaciones contables de importancia usen una base común de datos, el auditor puede encontrar conveniente, desde el punto de vista de su costo, utilizar algunos de los procedimientos listados en los siguientes párrafos.
32. Para obtener una comprensión del ambiente de control de la base de datos y del flujo de transacciones, el auditor puede considerar el efecto de lo siguiente sobre el riesgo de auditoría al planear su auditoría:
- Los controles de acceso relevantes. Personas fuera de la función contable tradicional pueden usar las bases de datos, y el auditor considera los controles de acceso sobre los datos contables y sobre todos los que puedan tener acceso a ellos.
  - El SABs y las aplicaciones contables importantes que usan la base de datos. Otras aplicaciones dentro de la entidad pueden generar o alterar datos que usan las aplicaciones contables. El auditor considera cómo el SABs controla estos datos.
  - Los estándares y procedimientos para desarrollo y mantenimiento de los programas de aplicación que usan la base de datos. Las bases de datos, especialmente las de computadoras independientes, pueden a menudo ser diseñadas e implementadas por personas fuera del ambiente de CIS o de las funciones contables. El auditor considera cómo controla la entidad el desarrollo de estas bases de datos.
  - La función de administración de recursos de datos. Como se describe en los párrafos 13-19, esta función juega un papel importante para mantener la integridad de los datos almacenados en la base de datos.
  - Descripción de puestos, estándares y procedimientos para los individuos responsables del soporte técnico, diseño, administración y operación de la base de datos. Con los sistemas de base de datos es probable que una gama más amplia de individuos tengan importantes responsabilidades sobre los datos, al contrario de los sistemas que no sean de base de datos.
  - Los procedimientos usados para asegurar la integridad, seguridad y totalidad de la información financiera contenida en la base de datos.
  - La disponibilidad de recursos de auditoría dentro del SABs.
  - Los procedimientos que se usan para introducir a la operación nuevas versiones de la base de datos.
33. Al determinar el grado de confiabilidad de los controles internos relacionados con el uso de la base de datos en el sistema de contabilidad, el auditor puede considerar cómo se usan los controles descritos en los párrafos 22-27. Si el auditor posteriormente decide apoyarse en dichos controles, éste diseña y lleva a cabo las pruebas apropiadas.
34. Cuando el auditor decide llevar a cabo pruebas de control o procedimientos sustantivos relacionados con el sistema de base de datos, a menudo será más efectivo hacerlo usando técnicas de auditoría con ayuda de computadora. El hecho de que todos los datos estén almacenados en un lugar, y organizados de una manera consistente, hace más fácil la extracción de muestras. También las bases de datos pueden incluir datos generados fuera de la función contable, lo que ayudará a hacer más efectiva la aplicación de procedimientos analíticos.
35. Los procedimientos de auditoría pueden incluir el uso de las funciones del SABs para:
- poner a prueba los controles de acceso;
  - generar datos para pruebas;
  - proporcionar una pista de auditoría;

- verificar la integridad de la base de datos;
- proporcionar acceso a la base de datos o una copia de partes relevantes de la base de datos para posibilitar el uso de software de auditoría (ver Declaración internacional de prácticas de auditoría 1009 "Técnicas de Auditoría con Ayuda de Computadora", TAAC Computer assisted audit techniques); y
- obtener información necesaria para la auditoría.

Antes de usar los recursos del SABs, el auditor considera si están funcionando en forma adecuada.

36. Si los controles de administración de la base de datos son inadecuados, tal vez no pueda el auditor compensar las fallas de control con alguna cantidad de trabajo sustantivo. Por lo tanto, cuando está claro que los controles en el sistema de base de datos no son confiables, el auditor considera si la realización de procedimientos sustantivos sobre todas las aplicaciones contables importantes que usan la base de datos lograría el objetivo de auditoría. Sí el auditor no puede superar las fallas en el ambiente de control con trabajo sustantivo para reducir el riesgo de auditoría a un nivel aceptablemente bajo, la NIA 700 requiere que el auditor emita su opinión con salvedades o se abstenga de emitirla.
37. Las características de los sistemas de base de datos pueden hacer más efectivo para el auditor practicar una revisión de pre-implementación de nuevas aplicaciones contables más que revisar las aplicaciones después de su instalación. Esta revisión de pre-implementación y revisión del proceso de administración del cambio pueden dar al auditor una oportunidad de solicitar funciones adicionales, tales como rutinas de auditoría o controles integrados dentro del diseño de la aplicación. Puede también dar al auditor tiempo suficiente para desarrollar y poner a prueba procedimientos de auditoría con anticipación al uso del sistema.

## DIPA 1009 - TÉCNICAS DE AUDITORIA CON AYUDA DE COMPUTADORAS

### Introducción

1. Los objetivos y alcance global de una auditoría no cambian cuando se conduce una auditoría en un ambiente de sistemas de información de cómputo (CIS). Sin embargo, la aplicación de procedimientos de auditoría puede requerir que el auditor considere técnicas conocidas como Técnicas de auditoría con ayuda de computadora (TAACs) que usan la computadora como una herramienta de auditoría.
2. Las TAACs pueden mejorar la efectividad y eficiencia de los procedimientos de auditoría. Pueden también proporcionar pruebas de control efectivas y procedimientos sustantivos cuando no haya documentos de entrada o un rastro visible de auditoría, o cuando la población y tamaños de muestra sean muy grandes.
3. El propósito de esta Declaración es proporcionar lineamientos sobre el uso de TAACs. Se aplica a todos los usos de TAACs que requieran el uso de una computadora de cualquier tipo o tamaño. Las consideraciones especiales que se refieren a ambientes de CIS en entidades pequeñas se describen en el párrafo 26.

Descripción de técnicas de auditoría con ayuda de computadora (TAACs —CAATs Computer assisted audit techniques)

4. Esta Declaración describe las técnicas de auditoría con ayuda de computadora incluyendo herramientas de auditoría, conocidas en forma colectiva como TAACs. Las TAACs pueden usarse para desempeñar diversos procedimientos de auditoría, incluyendo los siguientes:
  - pruebas de detalles de transacciones y saldos, por ejemplo, el uso de software de auditoría para recalcular los intereses o la extracción de facturas por encima de un cierto valor de los registros de computadora;
  - procedimientos analíticos, por ejemplo, identificar inconsistencias o fluctuaciones importantes;
  - pruebas de controles generales, por ejemplo, pruebas de la instalación o configuración del sistema operativo o procedimientos de acceso a las bibliotecas de programas o el uso de software de comparación de códigos para verificar que la versión del programa en uso es la versión aprobada por la administración,
  - muestreo de programas para extraer datos para pruebas de auditoría;
  - pruebas de controles de aplicación, por ejemplo, pruebas del funcionamiento de un control programado; y
  - volver a hacer cálculos realizados por los sistemas de contabilidad de la entidad.

Las TAACs son programas y datos de computadora que el auditor usa como parte de los procedimientos de auditoría para procesar datos importantes para la auditoría contenidos en los sistemas de información de una entidad- Los datos pueden ser datos de transacciones, sobre los que el auditor desea realizar pruebas de controles o procedimientos sustantivos, o pueden ser otros tipos de datos. Por ejemplo, los detalles de la aplicación de algunos controles generales pueden mantenerse en forma de archivos de texto u otros archivos por aplicaciones que no sean parte del sistema contable. El auditor puede usar TAACs para revisar dichos archivos para obtener evidencia de la existencia y operación de dichos controles. Las TAACs pueden consistir en programas de paquete, programas escritos para un propósito, programas de utilería o programas de administración

del sistema. Independientemente del origen de los programas, el auditor ratifica que sean apropiados y su validez para fines de auditoría antes de usarlos:

- Los programas en paquete son programas generalizados de computadora diseñados para desempeñar funciones de procesamiento de datos, tales como leer datos, seleccionar y analizar información, hacer cálculos, crear archivos de datos así como dar informes en un formato especificado por el auditor.
- Los programas escritos para un propósito desempeñan tareas de auditoría en circunstancias específicas. Estos programas pueden desarrollarse por el auditor, por la entidad que está siendo auditada o por un programador externo contratado por el auditor. En algunos casos el auditor puede usar los programas existentes de una entidad en su estado original o modificados porque así puede ser más eficiente que desarrollar programas independientes.
- Los programas de utilerías se usan por una entidad para desempeñar funciones comunes de procesamiento de datos, tales como clasificación, creación e impresión de archivos. Estos programas generalmente no están diseñados para propósitos de auditoría y, por lo tanto, pueden no contener características tales como conteos automáticos de registros o totales de control.
- Los programas de administración del sistema son herramientas de productividad mejorada que típicamente son parte de un ambiente sofisticado de sistemas operativos, por ejemplo, software de recuperación de datos o software de comparación de códigos. Como los programas de utilerías, estas herramientas no están diseñadas específicamente para usarlos en auditoría y su uso requiere un cuidado adicional.
- Las rutinas de auditoría incorporadas a veces están integradas en un sistema de computadoras de una entidad para proporcionar datos de uso posterior por el auditor. Incluyen:
  - Fotos instantáneas: Esta técnica implica tomar una foto de una transacción mientras fluye por los sistemas de computadora. Las rutinas del software de auditoría están incorporadas en diferentes puntos de la lógica del procesamiento para capturar imágenes de la transacción mientras avanza por las diversas etapas del procesamiento. Esta técnica permite al auditor rastrear los datos y evaluar los procesos de computadora aplicados a los datos.
  - Archivo de revisión de auditoría del control del sistema. Éste implica incorporar módulos de software de auditoría dentro de un sistema de aplicaciones para proporcionar monitoreo continuo de las transacciones del sistema. La información es reunida en un archivo especial de computadora que el auditor puede examinar.
  - Las técnicas de datos de prueba a veces se usan durante una auditoría, alimentando datos (por ejemplo, una muestra de transacciones) en el sistema de computadora de una entidad y comparando los resultados obtenidos con resultados predeterminados. Un auditor podría usar datos de prueba para:
    - poner a prueba controles específicos en programas de computadora, tales como controles en línea de contraseñas y acceso a datos;
    - poner a prueba transacciones seleccionadas de transacciones previamente procesadas o creadas por el auditor para poner a prueba características específicas de procesamiento de los sistemas de información de una entidad. Dichas transacciones generalmente son procesadas por separado del procesamiento normal de la entidad; y
    - poner a prueba transacciones usadas en un mecanismo integrado de pruebas donde se establece una unidad "modelo" (por ejemplo, un departamento o empleado ficticio), a la cual se le registran las transacciones durante el ciclo de procesamiento normal.

Cuando se procesan los datos de prueba con el procesamiento normal de la entidad, el auditor se asegura de que las transacciones de prueba sean eliminadas posteriormente de los registros contables de la entidad.

El creciente poder y sofisticación de las microcomputadoras, particularmente laptops, ha dado como resultado otras herramientas para uso del auditor. En algunos casos, las laptops serán enlazadas a los sistemas de computadora central del auditor. Ejemplos de estas técnicas incluyen:

- sistemas expertos, por ejemplo en el diseño de programas de auditoría y en la inspección de auditoría y evaluación de riesgos;
- herramientas para evaluar los procedimientos de un cliente para la administración de riesgos;
- papeles de trabajo electrónicos, planeados para la extracción directa de datos de los registros de computadora del cliente, por ejemplo, descargar el libro mayor para pruebas de auditoría; y
- programas de modelaje corporativo y financiero para usar como pruebas predictivas de auditoría.

Estas técnicas son más comúnmente conocidas como "automatización de la auditoría."

### Consideraciones en el uso de TAACs

7. Al planear una auditoría, el auditor puede considerar una combinación apropiada de técnicas de auditoría manuales y con ayuda de computadora. Al evaluar el uso de TAACs, los factores a considerar incluyen:
  - el conocimiento, pericia y experiencia del equipo de auditoría del ambiente de CIS;
  - la disponibilidad de TAACs e instalaciones y datos adecuados de computación;
  - la no imposibilidad de pruebas manuales;
  - efectividad y eficiencia; y
  - oportunidad.

Antes de usar TAACs el auditor considera los controles incorporados en el diseño de los sistemas de computadora de la entidad a los que se aplicarían éstas para determinar si es que, y en ese caso, cómo deberían emplearse.

#### Conocimiento, pericia y experiencia del equipo de auditoría del ambiente de C/S

La NÍA 401, "Auditoría en un Ambiente de Sistemas de Información por Computadora" trata del nivel de habilidades y competencia que necesita el equipo de auditoría para conducir una auditoría en un ambiente de CIS. Proporciona lineamientos para cuando un auditor delega trabajo a ayudantes con habilidades de CIS o cuando se usa el trabajo de otros auditores o expertos con dichas habilidades. Específicamente, el equipo de auditoría deberá tener suficiente conocimiento para planear, ejecutar y usar los resultados de la TAAC particular que se adopte. El nivel de conocimiento requerido depende de la complejidad y naturaleza de la TAAC y del sistema de información de la entidad.

#### Disponibilidad de TAACs e instalaciones adecuadas de computación

9. El auditor deberá considerar la disponibilidad de las TAACs, instalaciones adecuadas de computación (controladas según descrito en párrafos 18-23) y los sistemas de información y datos necesarios basados en computadoras. El auditor puede planear el uso de otras instalaciones de computación cuando el uso de TAACs en una computadora de la entidad no es económico o no es factible, por ejemplo, a causa de una incompatibilidad entre el programa de paquete del auditor y la computadora de la entidad. Además, el auditor puede elegir usar sus propias instalaciones, como microcomputadoras o laptops.
10. Puede requerirse la cooperación del personal de la entidad para proporcionar las instalaciones de procesamiento en un horario cómodo, para ayudar con actividades como la carga y ejecución de las TAACs en el sistema de la entidad, y proporcionar copias de archivos de datos en el formato requerido por el auditor.

#### Imposibilidad de pruebas manuales

11. Quizá no sea posible desempeñar manualmente algunos procedimientos de auditoría porque dependen de un procesamiento complejo (por ejemplo, análisis estadístico avanzado) o implica cantidades de datos que sobrepasarían cualquier procedimiento manual. Además, muchos sistemas de información por computadora desempeñan tareas para las que no hay evidencia de copias impresas disponibles y, por lo tanto, puede no ser factible para el auditor desempeñar las pruebas manualmente. La falta de evidencia en copias impresas puede ocurrir en diferentes etapas del ciclo de negocios.
  - La información de fuente puede ser iniciada electrónicamente por la activación de voz, imágenes electrónicas de datos o transferencia electrónica de fondos en el punto de venta. Además, algunas transacciones como descuentos y cálculo de intereses, pueden generarse directamente por programas de computadora sin autorización específica de las transacciones individuales.
  - Un sistema puede no producir un rastro visible de auditoría que proporcione certeza sobre la totalidad y exactitud de las transacciones procesadas. Por ejemplo, un programa de computadora podría cotejar las notas de entrega con las facturas de proveedores. Además, los procedimientos de control programados como verificación de límites de crédito de clientes, pueden proporcionar evidencia de copia impresa sólo con base en excepciones.
  - Un sistema puede no producir informes en copia impresa. Además, un informe impreso puede contener sólo totales resumidos mientras que los archivos de computadora retienen los detalles de soporte.

#### Efectividad y eficiencia

12. La efectividad y eficiencia de los procedimientos de auditoría pueden mejorarse usando las TAACs para obtener y evaluar la evidencia de auditoría. Las TAACs son a menudo un medio eficiente de poner a prueba un gran número de transacciones o controles sobre grandes poblaciones por medio de:
  - analizar y seleccionar muestras de un gran volumen de transacciones;
  - aplicar procedimientos analíticos; y

- desempeñar procedimientos sustantivos.
13. Los asuntos relacionados con la eficiencia que pueden ser considerados por el auditor incluyen:
- el tiempo para planear, diseñar, ejecutar y evaluar la TAAC;
  - revisión técnica y horas de asistencia;
  - diseño e impresión de formas (por ejemplo, confirmaciones); y
  - disponibilidad de recursos de computación.
14. Al evaluar la efectividad y eficiencia de una TAAC, el auditor puede considerar el uso continuo de la aplicación de la TAAC. La planeación inicial, diseño y desarrollo de una TAAC generalmente beneficiará a las auditorías de periodos posteriores.

#### Oportunidad

15. Ciertos datos, como detalles de transacciones, a menudo se conservan por sólo un corto tiempo, y pueden no estar disponibles en forma legible por la máquina para cuando el auditor lo requiere. Así, el auditor necesitará hacer arreglos para la retención de los datos requeridos, o puede necesitar alterar la programación del trabajo que requiera de estos datos.
16. Cuando el tiempo disponible para desempeñar una auditoría sea limitado, el auditor puede planear el uso de una TAAC, porque cumplirá con su requerimiento de tiempo mejor que otras procedimientos posibles.

#### Utilización de TAACs

17. Los pasos principales que debe tomar el auditor en la aplicación de una TAAC son:
- (a) establecer el objetivo de aplicación de la TAAC;
  - (b) determinar el contenido y accesibilidad de los archivos de la entidad;
  - (c) identificar los archivos específicos o bases de datos que deben examinarse;
  - (d) entender la relación entre las tablas de datos cuando deba examinarse una base de datos;
  - (e) definir las pruebas o procedimientos específicos y transacciones relacionadas y saldos afectados;
  - (f) definir los requerimientos de datos de salida;
  - (g) convenir con el usuario y departamentos de CIS, si es apropiado, en las copias de los archivos relevantes o tablas de bases de datos que deben hacerse en la fecha y momento apropiado del corte;
  - (h) identificar al personal que puede participar en el diseño y aplicación de la TAAC;
  - (i) refinar las estimaciones de costos y beneficios;
  - (j) asegurarse que el uso de la TAAC está controlado y documentado en forma apropiada;
  - (k) organizar las actividades administrativas, incluyendo las habilidades necesarias e instalaciones de computación;
  - (l) conciliar los datos que deban usarse para la TAAC con los registros contables;
  - (m) ejecutar la aplicación de la TAAC; y
  - (n) evaluar los resultados.

#### Control de la aplicación de la TAAC

18. Los procedimientos específicos necesarios para controlar el uso de una TAAC dependen de la aplicación particular. Al establecer el control, el auditor considera la necesidad de:
- (a) aprobar especificaciones y conducir una revisión del trabajo que deba desempeñar la TAAC;
  - (b) revisar los controles generales de la entidad que puedan contribuir a la integridad de la TAAC, por ejemplo, controles sobre cambios a programas y acceso a archivos de computadora. Cuando dichos controles no pueden ser confiables para asegurar la integridad de la TAAC, el auditor puede considerar el proceso de la aplicación de la TAAC en otra instalación de computación adecuada; y
  - (c) asegurar la integración apropiada de los datos de salida dentro del proceso de auditoría por parte del auditor.
19. Los procedimientos llevados a cabo por el auditor para controlar las aplicaciones de la TAAC pueden incluir:
- (a) participar en el diseño y pruebas de la TAAC;
  - (b) verificar, si es aplicable, la codificación del programa para asegurar que esté de acuerdo con las especificaciones detalladas del programa;

- (c) solicitar al personal de computación de la entidad revisar las instrucciones del sistema operativo para asegurar que el software correrá en la instalación de computación de la entidad;
- (d) ejecutar el software de auditoría en pequeños archivos de prueba antes de ejecutarlo en los archivos principales de datos;
- (e) verificar si se usaron los archivos correctos, por ejemplo, verificando la evidencia externa, como totales de controles mantenidos por el usuario, y que dichos archivos estén completos.
- (f) obtener evidencia de que el software de auditoría funcionó según planeado, por ejemplo, revisando los datos de salida y la información de control; y
- (g) establecer medidas apropiadas de seguridad para salvaguardar la integridad y confidencialidad de los datos.

Cuando el auditor tiene la intención de desempeñar procedimientos de auditoría en forma concurrente con procesamiento en línea, el auditor revisa dichos procedimientos con el personal apropiado del cliente y obtiene aprobación antes de conducir las pruebas para ayudar a evitar la alteración inadvertida de los registros del cliente.

- 20. Para asegurar procedimientos de control apropiados, no se requiere necesariamente la presencia del auditor en la instalación de computación durante la ejecución de una TAAC. Sin embargo, esto puede proporcionar ventajas prácticas, como controlar la distribución de los datos de salida y asegurar la corrección oportuna de errores, por ejemplo, si se fuera a usar un archivo de entrada equivocado.
- 21. Los procedimientos de auditoría para controlar las aplicaciones de datos de prueba pueden incluir:
  - controlar la secuencia de presentación de datos de prueba cuando se extienda a varios ciclos de procesamiento;
    - realizar corridas de prueba que contengan pequeñas cantidades de datos de prueba antes de presentar los datos de prueba principales de la auditoría;
    - predecir los resultados de los datos de prueba y compararlos con la salida real de datos de pruebas, para las transacciones individuales y, en total;
    - confirmar que se usó la versión actual de los programas para procesar los datos de prueba; y
    - poner a prueba si los programas usados para procesar los datos de prueba fueron utilizados por la entidad durante el período aplicable de auditoría.
- 22. Cuando el auditor utilice una TAAC, puede requerir la cooperación de personal de la entidad con amplio conocimiento de la instalación de computación. En estas circunstancias, el auditor puede considerar si el personal influyó en forma inapropiada en los resultados de la TAAC.
- 23. Los procedimientos de auditoría para controlar el uso de un software de ayuda para la auditoría pueden incluir:
  - verificar la totalidad, exactitud y disponibilidad de los datos relevantes, por ejemplo, pueden requerirse datos históricos para elaborar un modelo financiero;
  - revisar la razonabilidad de los supuestos usados en la aplicación del conjunto de herramientas, particularmente cuando se usa software de modelaje;
  - verificar la disponibilidad de recursos con habilidad en el uso y control de las herramientas seleccionadas; y
  - confirmar lo adecuado del conjunto de herramientas para el objetivo de auditoría, por ejemplo, puede ser necesario el uso de sistemas específicos para la industria en el diseño de programas de auditoría negocios con para ciclos únicos.

#### Documentación

- 24. El estándar de papeles de trabajo y de procedimientos de retención para una TAAC es consistente con el de la auditoría como un todo (ver NIA 230, "Documentación").
- 25. Los papeles de trabajo necesitan contener suficiente documentación para describir la aplicación de la TAAC, tal como:
  - (a) Planeación
    - objetivos de la TAAC;
    - consideración de la TAAC específica que se va a usar;
    - controles que se van a ejercer; y
    - personal, tiempo, y costo.
  - (b) Ejecución
    - preparación de la TAAC y procedimientos de prueba y controles;

- detalles de las pruebas realizadas por la TAAC;
  - detalles de datos de entrada, procesamiento y datos de salida; e
  - información técnica relevante sobre el sistema de contabilidad de la entidad, tal como la organización de archivos.
- (c) Evidencia de auditoría
- datos de salida proporcionados;
  - descripción del trabajo de auditoría desempeñado en los datos de Salida; y
  - conclusiones de auditoría.
- (d) Otros
- recomendaciones a la administración de la entidad,
  - además, puede ser útil documentar las sugerencias para usar la TAAC en años futuros.

#### Utilización de TAACs en ambientes de CIS en entidades pequeñas

26. Aunque los principios generales explicados en esta Declaración se aplican a ambientes de CIS en entidades pequeñas, los siguientes puntos necesitan consideración especial:
- (a) El nivel de controles generales puede ser tal que el auditor deposite menos confiabilidad en el sistema de control interno. Esto dará como resultado un mayor énfasis sobre pruebas de detalles de transacciones y saldos y procedimientos analíticos de revisión, lo que puede incrementar la efectividad de ciertas TAACs, particularmente software de auditoría,
- (b) Cuando se procesan volúmenes menores de datos, los métodos manuales pueden ser de costo más efectivo.
- (c) Una entidad pequeña quizá no pueda proporcionar al auditor ayuda técnica adecuada, haciendo poco factible el uso de TAACs.
- (d) Ciertos programas de auditoría en paquete pueden no operar en computadoras pequeñas, restringiendo así la opción del auditor en cuanto a TAACs. Sin embargo, los archivos de datos de la entidad pueden copiarse y procesarse en otra computadora adecuada.

#### DIPA 1008 - Evaluación del riesgo y el control interno, características y consideraciones del CIS

##### Introducción

Un entorno de sistema de información de cómputo (CIS) se define en la norma internacional de auditoría (NIA) 401 "Auditoría en un entorno de sistemas de información por computadora", como sigue:

Para los fines de las normas internacionales de auditoría, existe un entorno de CIS cuando hay implicada una computadora de cualquier tipo o tamaño en el procesamiento por parte de la entidad de información financiera de importancia para la auditoría, ya sea que la computadora sea operada por la entidad o por un tercero. La introducción de todos los controles deseados de CIS puede no ser factible cuando el tamaño del negocio es pequeño o cuando se usan microcomputadoras independientemente del tamaño del negocio. También, cuando los datos son procesados por un tercero, la consideración de las características del entorno de CIS puede variar dependiendo del grado de acceso al procesamiento del tercero. Se ha desarrollado una serie de declaraciones internacionales de auditoría para suplementar los siguientes párrafos. Esta serie describe diversos entornos de CIS y su efecto sobre los sistemas de contabilidad y de control interno y sobre los procedimientos de auditoría.

##### Estructura organizacional

En un entorno de CIS, una entidad establecerá una estructura organizacional y procedimientos para administrar las actividades de CIS. Las características de una estructura organizacional de CIS incluyen:

- a) concentración de funciones y conocimiento – aunque la mayoría de los sistemas que emplean métodos de CIS incluye ciertas operaciones manuales, generalmente el número de personas involucradas en el procesamiento de información financiera es significativamente reducido. Más aún, cierto personal de procesamiento de datos pueden ser los únicos con un conocimiento detallado de la interrelación entre las fuente de datos, cómo se procesan y la distribución y uso de los datos de salida. Es también probable que estén conscientes de cualesquiera debilidades en el control interno y por lo tanto, pueden estar en posición de alterar programas o datos mientras están almacenados o durante el procesamiento. Todavía más, pueden no existir muchos controles convencionales basados en la segregación adecuada de funciones incompatibles, o en ausencia de controles de acceso u otros, pueden ser menos efectivos
- b) concentración de programas y datos – a menudo están concentrados los datos por transacción y del archivo maestro, generalmente en forma legible por la máquina, ya sea en una instalación de computadora localizada centralmente o en un

número de instalaciones distribuidas por toda una entidad. Es probable que los programas de computadora que dan la capacidad de obtener acceso a, y de alterar dichos datos estén almacenados en la misma locación que los datos. Por lo tanto, en ausencia de controles apropiados, hay un mayor potencial para acceso no autorizado a, y alteración de programas y datos.

#### Naturaleza del procesamiento

El uso de computadoras puede dar como resultado el diseño de sistemas que proporcionen menos evidencia que aquellos que usen procedimientos manuales. Además, estos sistemas pueden ser accesibles a un mayor número de personas. Las características del sistema que pueden ser resultado de la naturaleza del procesamiento CIS incluyen:

- a) ausencia de documentos de entrada – los datos pueden ser alimentados directamente al sistema por computadora sin documentos que los soporten. En algunos sistemas de transacción en línea, la evidencia por escrito de la autorización de alimentación de datos individuales (por ej. Aprobación para entrada de pedidos) puede ser reemplazada por otros procedimientos, como controles de autorización contenidos en los programas de computadora (por ej. Aprobación de límite de crédito).
- b) Falta de rastro visible de transacciones – ciertos datos pueden mantenerse en archivos de computadora solamente. En un sistema manual, normalmente es posible seguir una transacción a través del sistema examinando los documento fuente, libros de cuentas, registros, archivos y reportes. En un entorno de CIS, sin embargo, el rastro de la transacción puede estar parcialmente en forma legible por máquina y todavía más, puede existir solo por un período limitado de tiempo.
- c) Falta de datos de salida visibles – ciertas transacciones o resultados de procesamiento pueden no imprimirse. En un sistema manual y en algunos sistemas de CIS, es posible normalmente examinar en forma visual los resultados del procesamiento no pueden imprimirse, o pueden imprimirse solo datos resumidos. Así, la falta de datos de salida visibles puede dar como resultado la necesidad de tener acceso a datos retenidos en archivos legibles sólo por computadora.
- d) Facilidad de acceso a datos y programas de computadora – se puede tener acceso a los datos y los programas de computadora y pueden ser alterados, en la computadora o por medio del uso de equipo de computación en locaciones remotas. Por lo tanto, en ausencia de controles apropiados, hay un potencial mayor para el acceso no autorizado a y a la alteración de, datos y programas por personas dentro o fuera de la entidad.

#### Aspectos de diseño y de procedimiento

El desarrollo de sistemas de CIS generalmente dará como resultado el diseño y características de procedimientos que son diferentes de los que se encuentran en los sistemas manuales. Estos aspectos diferentes de diseño y de procedimiento de los sistemas de CIS incluyen:

- a) consistencia de funcionamiento – los sistemas de CIS desempeñan funciones exactamente como se les programe y son potencialmente más confiables que los sistemas manuales, previsto que todos los tipos de transacción y todas las condiciones que puedan ocurrir se anticipen e incorporen en el sistema. Por otra parte, un programa de computadora que no esté correctamente programado y probado puede procesar en forma consistente transacciones u otros datos en forma errónea.
- b) Procedimientos de control programados – la naturaleza de procesamiento por computadora permite el diseño de procedimientos de control interno en los programas de computadora. Estos procedimientos pueden ser diseñados para proporcionar controles con visibilidad limitada (por ej. Se puede dar protección de datos contra acceso no autorizado mediante el uso de palabras clave). Pueden diseñarse otros procedimientos para uso con intervención manual, tales como la revisión de informes impresos para reportar excepciones y errores y verificaciones de razonabilidad y límites de datos.
- c) Actualización sencilla de una transacción en archivos múltiples o de base de datos – una entrada sencilla al sistema de contabilidad puede automáticamente actualizar todos los registros asociados con la transacción (por ej. Los documentos de embarque de mercancías pueden actualizar las ventas y los archivos de cuentas por cobrar a clientes, así como el archivo de inventario). Así, una entrada equivocada en dicho sistema puede crear errores en diversas cuentas financieras.
- d) Transacciones generadas por sistemas – ciertas transacciones pueden iniciarse por el sistema de CIS mismo sin necesidad de un documento de entrada. La autorización de dichas transacciones puede no ser evidenciada con documentos de entrada visibles ni documentada en la misma forma que las transacciones que se inician fuera del sistema de CIS (por ej, el interés puede ser calculado y cargado automáticamente a los saldos de cuentas de clientes con base en términos previamente autorizados contenidos en un programa de computadora)
- e) Vulnerabilidad de datos y medios de almacenamiento de programas – grandes volúmenes de datos y los programas de computadora usados para procesar dichos datos, pueden almacenarse en medios de almacenamiento portátil o fijo, como discos y cintas magnéticos. Estos medios son vulnerables al robo, pérdida o destrucción intencional o accidental.

### Controles internos en un entorno de CIS

El propósito de los controles generales de CIS es establecer un marco de referencia de control global sobre las actividades de CIS y proporcionar un nivel razonable de certeza de que se logran los objetivos globales del control interno. Los controles generales de CIS pueden incluir:

- a) *controles de organización y administración* – diseñados para establecer un marco de referencia organizacional sobre las actividades de CIS, incluyendo:
  - políticas y procedimientos relativos a funciones de control
  - segregación apropiada de funciones incompatibles (por ej. Preparación de transacciones de entrada, programación y operaciones de computadora)
- b) *desarrollo de sistemas de aplicación y controles de mantenimiento* – diseñados para proporcionar certeza razonable de que los sistemas se desarrollan y mantienen de manera eficiente y autorizada. También están diseñados típicamente para establecer control sobre:
  - pruebas, conversión, implementación y documentación de sistemas nuevos o revisados
  - cambios a sistemas de aplicación
  - acceso a documentación de sistemas
  - adquisición de sistemas de aplicación con terceros
- c) *controles de operación de computadoras* – diseñados para controlar la operación de los sistemas y proporcionar certeza razonable de que:
  - los sistemas son usados para propósitos autorizados únicamente
  - el acceso a las operaciones de la computadora es restringido a personal autorizado
  - solo se usan programas autorizados
  - los errores de procesamiento son detectados y corregidos
- d) *controles de software de sistemas* – diseñados para proporcionar razonable certeza de que el software del sistema se adquiere o desarrolla de manera autorizada y eficiente, incluyendo:
  - autorización, aprobación, pruebas, implementación y documentación de software de sistemas nuevos y modificaciones del software de sistemas
  - restricción de acceso a software y documentación de sistemas al personal autorizado
  - controles de entrada de datos y de programas – diseñados para proporcionar razonable certeza de que:
  - hay establecida una estructura de autorización sobre las transacciones que se alimentan al sistema
  - el acceso a datos y programas está restringido a personal autorizado.

Hay otras salvaguardas de CIS que contribuyen a la continuidad del procesamiento de CIS. Estas pueden incluir:

- respaldo de datos y programas de computadora en otro sitio
- procedimientos de recuperación para usarse en caso de robo, pérdida o destrucción intencional o accidental
- provisión para procesamiento externo en caso de desastre

### Controles de aplicación de CIS

El propósito de los controles de aplicación de Cis es establecer procedimientos específicos de control sobre las aplicaciones contables para proporcionar razonable certeza de que todas las transacciones están autorizadas y registradas y son procesadas completamente, con exactitud y oportunidad. Los controles de aplicación de CIS incluyen:

- a) *controles sobre datos de entrada* – diseñados para proporcionar razonable certeza de que:
  - las transacciones son autorizadas en forma apropiada antes de ser procesadas por la computadora
  - las transacciones son convertidas con exactitud a una forma legible por máquina y registradas en los archivos de datos de la computadora
  - las transacciones no están perdidas, añadidas, duplicadas o cambiadas en forma impropia
- b) *controles sobre el procesamiento y sobre archivos de datos de la computadora* – diseñados para proporcionar razonable certeza de que:
  - las transacciones incluyendo las generadas por el sistema, son procesadas en forma apropiada por la computadora
  - las transacciones son convertidas con exactitud a una forma legible por máquina y registradas en los archivos de datos de la computadora
  - los errores de procesamiento son identificados y corregidos oportunamente
- c) *controles sobre los datos de salida* – diseñados para proporcionar razonable certeza de que:
  - los resultados del procesamiento son exactos

- el acceso a los datos de salida se proporcionan al personal autorizado apropiado oportunamente

#### Revisión de controles de aplicación de CIS

Los controles generales de CIS que el auditor puede desear probar se describen en párrafos anteriores. El auditor deberá considerar cómo estos controles generales de CIS afectan las aplicaciones de CIS importantes para la auditoría. Los controles generales de CIS que se relacionan a algunas o todas las aplicaciones son controles típicamente interdependientes en cuanto que su operación es a menudo esencial para la efectividad de los controles de aplicación de CIS. Consecuentemente, puede ser más eficiente revisar el diseño de los controles generales antes de revisar los controles de aplicaciones

#### Revisión de controles de aplicación de CIS

El control sobre los datos de entrada, procesamiento, archivos de datos y datos de salida puede desempeñarse por personal de CIS, por usuarios de sistemas, por un grupo de control separado, o puede ser programado en el software de aplicación. Los controles de aplicación de CIS que el auditor puede desear probar incluyen:

- controles manuales ejercidos por el usuario* – si los controles manuales ejercidos por el usuario del sistema de aplicación tienen la capacidad de dar una certeza razonable de que los datos de salida del sistema son completos, exactos y autorizados, el auditor puede decidir limitar las pruebas de control a estos controles manuales (por ej. Los controles manuales ejercidos por el usuario sobre un sistema computarizado de nóminas para empleados asalariados podría incluir un total anticipado del control de entradas para los pagos brutos, la comprobación de los cálculos de salida de salarios netos, la aprobación de pagos y transferencia de fondos, la comparación con las cifras del registro de nómina y una rápida conciliación bancaria). En este caso, el auditor puede desear probar solo los controles manuales ejercidos por el usuario.
- Controles sobre los datos de salida del sistema – si, además de los controles manuales ejercidos por el usuario, los controles que deben probarse usan información producida por la computadora o están contenidos dentro de programas de computadora, puede ser posible probar dichos controles examinando los datos de salida del sistema usando técnicas de auditoría ya sea manuales o con ayuda de computadora. Dichos datos de salida pueden ser en forma de medios magnéticos, microfilm o impresos (por ej. El auditor puede probar los controles ejercidos por la entidad sobre la conciliación de totales de reportes con las cuentas de control del libro mayor y puede realizar pruebas manuales de dichas conciliaciones). Alternativamente, cuando la conciliación se realiza por computadora, el auditor puede desear probar la conciliación volviendo a ejecutar el control con el uso de técnicas de auditoría con ayuda de computadora (ver declaración de auditoría “Técnicas de Auditoría con Ayuda de Computadora”).
- Procedimientos de control programados – en el caso de ciertos sistemas por computadora, el auditor puede encontrar que no sea posible o, en algunos casos, no sea práctico probar los controles examinando sólo los controles del usuario o los datos de salida del sistema (por ej. En una aplicación que no da resultados impresos de aprobaciones críticas o violaciones a las políticas normales, el auditor puede querer probar los procedimientos de control contenidos dentro del programa de aplicación). El auditor puede considerar llevar a cabo pruebas de control con el uso de técnicas de auditoría con ayuda de computadora, como prueba de los datos reprocesamiento de datos de transacciones o, en situaciones inusuales, examinar la codificación del programa de aplicación.

#### Evaluación

Los controles generales de CIS pueden tener un efecto penetrante en el procesamiento de transacciones en los sistemas de aplicación. Si estos controles no son efectivos, puede haber un riesgo de que pudieran ocurrir representaciones erróneas y no ser detectadas en los sistemas de aplicación. Así, las debilidades en los controles generales de CIS, pueden imposibilitar la prueba de ciertos controles de aplicación de CIS; sin embargo, los procedimientos manuales ejercidos por los usuarios pueden proporcionar control efectivo al nivel de aplicación.

#### **Planificación del Proceso de Auditoría**

Teniendo definido qué se va realizar para auditar y proveer garantía, se debe determinar el enfoque o estrategia más apropiados para desarrollar el trabajo de auditoría. Para cubrirlo, se necesita investigar, analizar y definir con respecto a:

- El proceso de negocio relacionado
- Las plataformas y sistemas de información que apoyan el proceso de negocio, así como la relación con otras plataformas o sistemas
- Los roles y responsabilidades definidos para TI, incluyendo qué se está realizando internamente o en “out-sourcing”
- Riesgos de negocio asociados y estrategias seleccionadas

Luego, deben identificarse los requerimientos de la información que son de una relevancia en particular con respecto a los procesos del negocio; identificar los riesgos de TI inherentes, el nivel de control general que puede ser asociado con el proceso de negocio. Lograr la identificación de:

- Cambios recientes en el ambiente del negocio que tienen impacto en TI

- Cambios recientes al ambiente de TI, nuevos desarrollos, etc.
- Incidentes recientes pertinente a los controles y ambiente del negocio
- Monitoreo de controles en TI aplicados por la administración
- Reportes de auditoría recientes y/ o de certificación
- Resultados recientes de revisiones internas

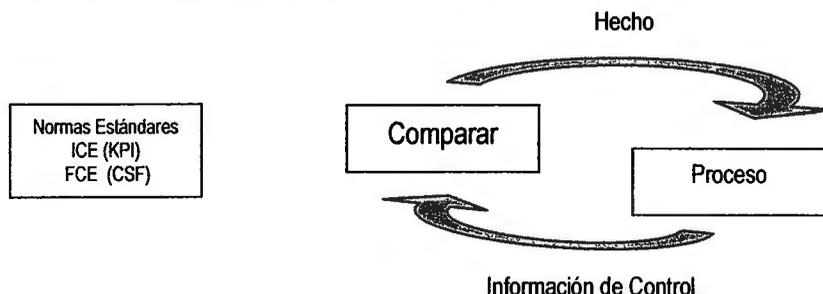
Con base en la información obtenida, se debe determinar una estrategia de auditoría con base en un plan de auditoría detallado, ej. si el enfoque va a ser basado en controles o en pruebas sustantivas. Finalmente, establecer todos los pasos, tareas y puntos de decisión para ejecutar la auditoría que necesitan ser considerados.

<ul style="list-style-type: none"> <li>• Definir el Enfoque de Auditoría</li> </ul>	<ul style="list-style-type: none"> <li>➤ Procesos de Negocio concernientes</li> <li>➤ Plataformas, sistemas y su interconectividad, soportando el proceso</li> <li>➤ Roles, responsabilidades y estructura organizacional</li> </ul>
<ul style="list-style-type: none"> <li>• Identificar los requerimientos de información relevante para el proceso de negocios</li> </ul>	<ul style="list-style-type: none"> <li>➤ Relevancia del proceso de negocios</li> </ul>
<ul style="list-style-type: none"> <li>• Identificar los riesgos inherentes de TI y el nivel de control</li> </ul>	<ul style="list-style-type: none"> <li>➤ Cambios recientes e incidentes en el ambiente de negocios y tecnología</li> <li>➤ Resultados de la auditoría, auto-establecimiento y certificación</li> <li>➤ Monitoreo de controles aplicados por la administración</li> </ul>
<ul style="list-style-type: none"> <li>• Seleccionar los procesos y plataformas para auditar</li> </ul>	<ul style="list-style-type: none"> <li>➤ Procesos</li> <li>➤ Recursos</li> </ul>
<ul style="list-style-type: none"> <li>• Definir la estrategia de Auditoría</li> </ul>	<ul style="list-style-type: none"> <li>➤ Controles x Riesgo</li> <li>➤ Pasos y Tareas</li> <li>➤ Puntos de Decisión</li> </ul>

**Observaciones del Proceso de control**

Los principios generales de control pueden suministrar también un entendimiento adicional. Estos principios se enfocan principalmente en las responsabilidades sobre el proceso y del control, estándares de control y control del flujo de información.

Control, desde el punto de vista de la administración, se define como la determinación de qué está siendo cumplido, qué está evaluando el desempeño y si es necesario aplicar medidas correctivas, de forma tal que el desempeño se cumpla de acuerdo con el plan.



El proceso de control consta de cuatro pasos:

1. Estándar de cómo el desempeño deseado es especificado para un proceso
2. Existen formas de conocer qué está pasando en el proceso, ej. el proceso envía una información de control a la unidad de control
3. La unidad de control compara la información con el estándar.
4. Si está sucediendo un acontecimiento no conforme con el estándar, la unidad de control especifica la acción correctiva a ejecutar, devolviendo la información al proceso.

De este modelo, las siguientes observaciones sobre el control deben considerarse para realizar una auditoría:

1. Para este modelo, la responsabilidad sobre el proceso de negocio (en este caso TI) debe ser claro y esa responsabilidad no debe ser ambigua. Si no, la información de control no fluirá y las acciones correctivas no se ejecutarán

2. Los estándares pueden ser de una gran variedad, desde planes de alto nivel y estrategias con indicadores clave de desempeño (KPI) detalladamente medibles y Factores críticos de éxito Los estándares claramente documentados, mantenidos y comunicados deben ser un requerimiento para el proceso de control Las responsabilidades claras para el custodio de estos estándares también son un requisito para el buen control
3. El proceso de control tiene los mismos requerimientos: bien documentado de cómo trabaja y las responsabilidades claras. Un aspecto importante es la definición clara de lo que puede constituir una excepción, ej. cuáles son los límites de una excepción.
4. La temporalidad, integridad y adecuación de la Información de control, así como de otros datos, es básico para el buen funcionamiento del sistema de control y es algo que el auditor debe identificar.

Tanto la información de control como la información sobre las acciones correctivas, tendrán requerimientos como evidencia para establecer responsabilidades después del hecho.

Estructura básica de un proceso de evaluación de auditoría:

#### OBTENER UN ENTENDIMIENTO

Los pasos de auditoría a ser ejecutados para documentar las actividades para analizar los objetivos de control, así como para identificar las medidas/procedimientos de control aplicadas.

Entrevistar a la administración y al equipo para obtener un entendimiento de:

- Requerimientos del negocio y riesgos asociados
- Estructura Organizacional
- Roles y Responsabilidades
- Políticas y procedimientos
- Leyes y Regulaciones
- Medidas de Control Aplicadas
- Reporte de la Administración (estado, ejecución, puntos de acción)

Documentar el proceso de los recursos de TI relacionados, particularmente afectados por los procesos bajo revisión. Confirmar el entendimiento del proceso bajo revisión, los Indicadores Claves de Desempeño del proceso, Implicaciones de control

#### EVALUACIÓN DE CONTROLES

Los pasos de auditoría a ser ejecutados en el establecimiento de la efectividad de las medidas de control aplicadas o el grado en que los objetivos de control son alcanzados. Básicamente decidiendo que, de qué forma y cómo probarlo

Evaluar lo adecuado de las medidas de control del proceso bajo supervisión, considerando los criterios identificados y las prácticas estándares de la industria, los Factores Críticos de Éxito de las medidas de control y la aplicación del juicio profesional del auditor.

- Documentación de los procesos existentes
  - Entregables existentes apropiados
  - Responsabilidades son claras y efectivas
  - Existen controles compensatorios, donde es necesario
- Concluir el grado donde el objetivo de control es cumplido

#### ESTABLECIMIENTO DE CUMPLIMIENTO

Los pasos de auditoría a ser ejecutados para garantizar que las medidas de control establecidas están trabajando como se determinó, en forma consistente y continua y para concluir con lo adecuado del ambiente de control.

Obtener evidencia de los periodos/items seleccionados para asegurar que los procedimientos han sido cumplidos en el periodo de revisión.

Ejecutar una revisión limitada de la adecuación de los entregables del proceso.

Determinar el nivel de las pruebas sustantivas y del trabajo adicional requerido para proveer garantía de que el proceso de TI es adecuado.

#### PRUEBAS DEL RIESGO

Los pasos de auditoría a ser ejecutados para probar que el riesgo para el objetivo de control no está siendo materializado, utilizando técnicas analíticas y/o fuentes de consulta alternativas. El objetivo es soportar la opinión. Los auditores deben ser creativos en la búsqueda y presentación de esta información sensitiva y confidencial.

Documentar las debilidades de control y las vulnerabilidades y amenazas resultantes.

Identificar y documentar el impacto actual y potencial

Proveer información comparativa

## **Herramientas para la Auditoría**

### **Cuestionarios**

Las auditorías se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la implementación de cuestionarios preimpresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, así como muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzar ambos tipos de información, es una de las bases fundamentales de la auditoría.

Cabe aclarar que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos preimpresos hubieran proporcionado.

### **Entrevistas**

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
2. Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
3. Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importantes del auditor; en ellas, éste recoge más información y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

### **Lista de Chequeo (Checklist)**

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, información cruzada y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Mucho por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la complementación sistemática de sus Cuestionarios, de sus Checklists.

Hay opiniones que descalifican el uso de las Checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de Auditoría Informática guardan sus Checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar la Checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las Checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

a. Checklist de rango

Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo)

*Ejemplo de Checklist de rango:*

Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tiene los siguientes significados:

1 : Muy deficiente.

2 : Deficiente.

3 : Mejorable.

4 : Aceptable.

5 : Correcto.

Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guión. La cumplimentación de la Checklist no debe realizarse en presencia del auditado.

Las Checklists de rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en la checklist binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

b. Checklist Binaria

Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméricamente, equivalen a 1(uno) o 0(cero), respectivamente.

Las Checklists Binarias siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <si o no> frente a la mayor riqueza del intervalo.

No existen Checklists estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

Pistas de Auditoría

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

Muy especialmente, estas "pistas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el Sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo.

Por lo que se refiere al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por Técnica de Sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

No obstante la utilidad de las Trazas, ha de repetirse lo expuesto en la descripción de la auditoría informática de Sistemas: el auditor informático emplea preferentemente la amplia información que proporciona el propio Sistema: Así, los ficheros de <Accounting> o de <contabilidad>, en donde se encuentra la producción completa de aquél, y los <Log> de dicho Sistema, en donde se recogen las modificaciones de datos y se pomenoriza la actividad general. Del mismo modo, el Sistema genera automáticamente exacta información sobre el tratamiento de errores de maquina central, periféricos, etc.

[La auditoría financiero-contable convencional emplea trazas con mucha frecuencia. Son programas encaminados a verificar lo correcto de los cálculos de nóminas, primas, etc.].

### Guía de Auditoría – General

En la guía de Auditoría, se enmarca en el establecimiento de la revisión de procesos específicos en TI con base en los Objetivos del Control recomendados que ayudan a la administración a asegurar donde los controles son suficientes, o aconsejar manejo donde procesos necesitan mejorar. El esquema de utilización de la Guía debe proporcionar una perspectiva "reactiva", en las áreas en que los auditores también necesitan apoyar a la administración de una forma "proactiva". La estructura y las Guías de Auditoría son igualmente aplicables en forma "proactiva" en las fases tempranas de procesos y desarrollo de proyectos.

### Papeles de Trabajo

#### Introducción

El trabajo del auditor queda anotado en una serie de papeles que constituyen en principio la prueba material del trabajo realizado. Además, en ellos se deja constancia de la profundidad de las pruebas y de la suficiencia de los elementos en que se apoyó la opinión, en otras palabras, son evidencia de la calidad profesional del trabajo realizado.

Los papeles de trabajo -de aquí en adelante se seguirán denominando como P/T- son los documentos en que el auditor registra, en orden cronológico, los datos e informaciones obtenidas en su examen; los resultados de las pruebas realizadas; así como las técnicas, métodos y procedimientos utilizados en el desarrollo de su Auditoría o Estudio Especial; en adelante denominados por los siguientes calificativos:

- auditoría
- trabajo;
- examen;
- revisión; o
- estudio.

Además, la tercera norma de las relativas a la ejecución del trabajo, dice: "Obtención de evidencia suficiente y comprobatoria".

Por lo tanto, es obligación del auditor llevar los P/T necesarios para cumplir a cabalidad con lo que pide dicha norma, debido a que la evidencia que debe reunir los conceptos de "comprobación", debe estar recopilada en dichos papeles.

Los P/T deben ajustarse a las circunstancias y a las necesidades del auditor en el trabajo a que se refieren (SAS No. 1, sec.338.04).

Aunque la cantidad, tipo y contenido de los P/T, varía de acuerdo con las circunstancias, deben indicar que el auditor estudió y evaluó el sistema de Control Interno del cliente en la extensión que consideró necesaria, para determinar la naturaleza, alcance y oportunidad de otros procedimientos de auditoría utilizados en el examen que está llevando a cabo.

#### Importancia

Los P/T reflejan su importancia en los siguientes enunciados:

- a. Historia de la labor realizada - Constituyen un registro ordenado, sistemático, estructurado y en detalle de todas las tareas cumplidas o ejecutadas durante el desarrollo de la auditoría.
- b. Registro del resultado de la auditoría - Permiten realizar el registro de la documentación, datos e información, así como de las evidencias encontradas, como sustento de las observaciones, conclusiones y recomendaciones que forman parte sustancial del informe final.
- c. Respaldo del Informe - Los P/T deben ser suficientes en calidad y cantidad, para permitir respaldar el contenido integral del informe final, es importante tomar en cuenta que por ninguna circunstancia, los informes deben estar exentos de los papeles de trabajo; estos por su naturaleza son el fundamento de la evidencia o la ausencia de ella al convalidar o criticar con fundamento y prueba, la validez de las operaciones examinadas, así como del contenido del informe.
- d. Dejan constancia del grado de confianza en el Sistema de Control Interno (CI) - Cuando el auditor, luego de estudiar y evaluar el Sistema de Control Interno, formula sus respectivas apreciaciones y comentarios, deja plasmados en los P/T los comentarios, críticas o inconsistencias del C.I. existentes; al mismo tiempo, consigna su apreciación sobre el grado de confianza o desconfianza en ese C.I. que evaluó.
- e. Como fuente de información - El auditor redacta su informe final, basado en los P/T, por esta razón es que le sirven como fuente principal de información. Pero, no sólo sirven para este fin, sino que también son una fuente muy importante en materia de consulta en el futuro, en la medida que se puedan necesitar datos específicos.
- f. Condicionan una mejora en las auditorías posteriores - La base sustancial de un informe es la calidad de los P/T, los mismos que son capaces -al revelar hechos importantes- de llamar la atención sobre hechos realmente significativos.

- g. Facilidad de revisión y de supervisión - Inmediatamente antes de la emisión de cualquier informe, es necesario e indispensable efectuar la revisión exhaustiva de los P/T, con el fin de verificar la existencia de evidencias que sustenten las observaciones, conclusiones y recomendaciones.
- h. En forma adicional, es posible que cualquier funcionario de auditoría, un Supervisor por ejemplo, pueda examinar o revisar los pormenores encontrados en el desarrollo del trabajo, los mismos que deben quedar registrados en dichos P/T
- i. Contribuyen al Desarrollo Profesional - La corrección y el esmero profesional con que se elaboren los P/T, representa una ayuda importante para lograr el desarrollo profesional del personal de auditoría, especialmente de los que se inician en esta labor especializada.

Los P/T constituyen la imagen de la calidad, cualidad y esmero profesional de cada uno de los auditores que conforman un equipo de auditoría y sirven de base como prueba fehaciente para el reconocimiento de las bondades o debilidades de cada uno de los componentes del grupo, con el propósito de adoptar las medidas correctivas y pertinentes en cada caso.

- j. Respaldo de procesos de orden Judicial - En algunas oportunidades, los informes de auditoría, no sólo contienen observaciones de carácter administrativo/financiero, sino que contienen indicios razonables de comisión de delito; en cuyo caso dichos informes pueden ser utilizados por los Tribunales de Justicia.

El contenido sobre fraudes, apropiaciones ilícitas y otros delitos o irregularidades, puede servir como base para iniciar un juicio.

- k. Constituyen evidencia fundamental - Como constancia de todo el proceso de control, a partir de la evaluación del C.I., la planeación y programación, la ejecución del trabajo y la redacción del informe, el auditor es consciente, que por la naturaleza y trascendencia de su trabajo integral, debe dejar "huellas" de dicha labor, a través de la confección u obtención de P/T, que constituyen EVIDENCIA que fundamenta los objetivos, procedimientos, técnicas, entrevistas, hechos, hallazgos u observaciones, que constituyen el sustento cabal del contenido de los informes

La versión subjetiva y sólo basada en la memoria del ser humano, no constituye elemento de juicio válido en auditoría; por el contrario sería riesgoso e irresponsable consignar detalles en un informe, cuyas evidencias no están registradas en los P/T, sino únicamente en la memoria y en el leal saber y entender del auditor.

Finalmente, es necesario recordar y reafirmar que la calidad de un Informe de Auditoría, es directamente proporcional a la "calidad total" de los Papeles de Trabajo.

- l. Conclusión - La carta de presentación, de la calidad, de la idoneidad y capacidad, tanto académica como técnica, lo constituyen sus Papeles de Trabajo; vale la pena agregar que a partir de ellos, puede ser evaluado por el nivel de exigencia que haya impuesto y esperado la empresa que lo contrató.

En efecto, cuando los P/T están elaborados con el ingrediente del esmero profesional, son ordenados, legibles; con encabezados completos, explicaciones de fuentes de datos y resultados de verificaciones efectuadas, se genera, se ratifica y se acrecienta la confianza en el auditor, así como en el trabajo que efectúa, tanto de parte de sus niveles superiores como del cliente para quien se realiza el examen.

Si por el contrario, los P/T están desordenados, son ilegibles, mal redactados, sin descripciones de labores realizadas ni evidencias obtenidas, en otras palabras, elaborados sin el esmero profesional requerido; ni sus niveles superiores, ni el cliente, ni terceros involucrados, tendrán confianza y respeto en el auditor, en el trabajo realizado, ni en el contenido del informe.

También es importante tomar en cuenta que la evolución del auditor se va materializando, precisamente en sus P/T; en la medida en que todos los auditores se inician en auditoría; en la medida en que vayan adquiriendo, cada vez más experiencia, indudablemente progresarán también en la elaboración de los P/T.

### Evidencia

La evidencia en Auditoría es el conjunto de hechos comprobados que sustentan las conclusiones del auditor. Es la información específica obtenida durante la labor de auditoría a través de:

- la observación
- la inspección
- las entrevistas; y
- el examen detallado de los registros y los hechos. Toda esta información debe quedar recopilada en los P/T

La mayoría de la labor de auditoría se dedica a la obtención de "evidencia", porque es ésta la que provee una base racional para la formulación de conclusiones, de opiniones, de recomendaciones, de mejoras, de beneficios, de ideas, así como de los juicios a emitir en los informes.

La evidencia en auditoría debe ser:

- suficiente;
- relevante;

- competente;
- confiable;
- disponible;
- verificable;
- pertinente, y
- usable

A continuación se proporciona una breve explicación de cada uno de estos conceptos:

- a. Suficiente - Evidencia suficiente es aquella tan veraz, adecuada y convincente que, al ser informado, conllevará a una persona que no es auditor ni tiene conocimiento específico del asunto, a llegar a la misma conclusión del auditor. Suficiencia se refiere no solo al volumen o cantidad de la evidencia, sino también a su grado de "calidad".
- b. Relevante - Consiste en indicar aquellos aspectos sobresalientes y notables como producto del examen que se esté efectuando. Por ejemplo: un paso esencial es determinar los efectos o importancia de una deficiencia: el efecto o efectos pueden ser:
  - mayores costos;
  - no lograr los objetivos previstos;
  - tener una exposición al riesgo de varios "cientos de miles" de colones;
  - reacciones adversas sobre operaciones relacionadas.

Los P/T deben demostrar los efectos en la forma más específica posible, basándose para ello, en computaciones, comparaciones, testimonios, documentación adecuada, informes de auditoría u otras fuentes apropiadas.

- c. Competente - Se refiere este término a que el contenido de los P/T debe ser propio y conveniente al asunto a que se refieren; que está bajo revisión o que se somete a discusión.
- d. La diversidad de la labor de auditoría y los tipos de hallazgos son tan numerosos, que no es factible describir en términos detallados la naturaleza de toda la información que debe incluirse en los P/T; en términos generales. Sin embargo, para que un hallazgo cuente con un respaldo adecuado en los P/T se hace necesario que se efectúen todos los pasos de su desarrollo. Además, los P/T deben contener, para cada paso requerido en el proceso de desarrollo, resúmenes claros o extractos de documentos necesarios para demostrar el trabajo efectuado en cada paso, los resultados obtenidos y las conclusiones alcanzadas.
- e. Confiable - La evidencia recopilada debe ofrecer un grado de confianza máximo para todas las personas que estén relacionadas con ella; no debe contener ambigüedades, ni términos vagos, así como tampoco tachaduras, borrones, ni aspectos negativos que le puedan restar credibilidad. La meta del auditor debe ser obtener, de las mejores fuentes y de aquellas más dignas de confianza, toda la información importante relacionada con sus hallazgos.
- f. Disponible - Los P/T deben estar estructurados de manera tal, que la evidencia pueda ser localizada rápidamente, no sólo por la persona que la recopiló, sino por cualquier otra que esté autorizada a su acceso. De la misma manera, el contenido total de los P/T de una revisión, deben archivar -como legajo- en un lugar de fácil localización y debidamente identificados.
- g. Verificable - La información obtenida debe reunir condiciones para ser verificada posteriormente; recordar muy bien que esa información no se recopila como un fin, sino como un medio para lograr o llegar a algo más; por lo tanto, todos los datos que se trasladen a los P/T deben ser objeto de verificación. Sin embargo, esto no significa que deba dejarse información sin obtener sólo porque al auditor le parezca que no va a poder verificar después; debe recordarse también, que las fuentes de información no deben estar restringidas; se deben considerar y evaluar cuidadosamente los comentarios de todos los empleados de la organización, si no responden directamente a los hallazgos o al asunto bajo estudio, el auditor debe tratar de explicarles mejor, para así obtener comentarios veraces, reales, oportunos y pertinentes.
- h. Pertinente - Este concepto tiende a confundirse con el de competencia, pero se considera oportuno y útil separarlos, especialmente para efectos de explicación y entendimiento. La evidencia pertinente es aquella que es válida y relevante a un hallazgo específico.
- i. Los P/T y toda información relacionada, acumulada al desarrollar un hallazgo o hecho específico, deben tener una relación directa con el mismo y las recomendaciones atinentes. Este requerimiento no excluye el tomar notas apropiadas o hacer observaciones que serán consideradas en otras áreas de investigación o áreas problema que se estudiarán y analizarán. Sin embargo, debe evitarse la acumulación indiscriminada de papeles y documentos que pueden estar relacionados con el tema bajo estudio, pero que no llenen ninguna relación potencial con el hallazgo específico.
- j. Usable - Significa este término, que el contenido de los P/T pueda utilizarse sin reseña alguna en: demostraciones, comprobaciones, fase probatoria, soporte de las recomendaciones; así como en cualquier otra actividad que se desprenda del

examen que se está efectuando. Las otras actividades citadas pueden ser casos elevados a inicios con el debido cuidado que esto implica; otros estudios que se desprenden del actual; otras auditorías; etc.

- k. Diferenciación - Es muy importante diferenciar entre la evidencia de auditoría y la evidencia de tipo legal. En este curso se presentan los fundamentos de la evidencia de auditoría empleada por el auditor en sus labores de campo. En el supuesto caso que ciertos resultados de las labores del auditor, desemboquen en procesos judiciales ante tribunales comunes, la evidencia que el presente ante tal circunstancia, estará sujeta a ser aceptada según las disposiciones vigentes, referentes a la evidencia legal, que en la mayoría de los casos, es muy diferente de la evidencia de auditoría, explicada en este texto.

#### Clases De Evidencia

En términos generales, la evidencia de auditoría se ha clasificado en cuatro tipos:

- a. Evidencia Física - Este tipo de evidencia obtiene por medio de una revisión, inspección u observación directa de:

- las funciones y actividades realizadas por las personas
- los documentos y registros (manuales y o automatizados)
- los hechos relacionados con el objetivo del examen.

Esta evidencia debe documentarse en memoranda que resuma:

- todos los aspectos revisados u observados:
- papeles de trabajo que muestren la naturaleza y alcance de la inspección;
- así como fotografías, cuadros, mapas, y cualquier otra representación gráfica que pueda servir para reafirmar lo revisado.

El obtener y utilizar evidencia de tipo gráfico, es una forma eficaz y eficiente de explicar o describir una situación determinada, ya sea en un informe o en una presentación; por ejemplo, una fotografía de una bodega de almacenamiento, que presente prácticas inapropiadas o ineficientes, tendrá un impacto mucho mayor que las palabras que traten de explicar dichas prácticas.

El auditor debe aprovechar toda oportunidad para observar los aspectos físicos; la habilidad de informar acerca de una condición realmente observada, es mucho más convincente que declaraciones basadas en otros tipos de evidencia.

Es práctica recomendable que dos miembros del equipo de auditoría hagan las inspecciones físicas necesarias; también deben hacerse los arreglos necesarios para que representantes de la organización los acompañen para que ellos mismos puedan corroborar los hallazgos. Si es práctica común y lo consideran necesario, deben firmar un memorando en conjunto sobre los hechos de cada inspección física, con el fin de evitar cualquier controversia acerca de la precisión de los hallazgos.

La utilización eficaz de la técnica de observación, así como el reconocimiento del valor de la evidencia física, depende en gran parte de la persona que lleva a cabo la labor de auditoría. Así por ejemplo, si se mantiene alerta y es curiosa e imaginativa, observará, de manera crítica:

- los inventarios;
- las condiciones de los locales;
- las condiciones de los equipos; y
- las funciones y actividades del personal.

- b. Evidencia Documental - Este tipo de evidencia ha sido la forma más común de evidencia en auditoría, y consiste en documentos clasificados según sea su origen. Esta clasificación se ha dividido en:

- Internos - Son todos aquellos documentos que se originan dentro de la organización y constan de: registros contables, correspondencia que se envía, guías de recepción y comunicación interna.
- Externos - Son todos aquellos documentos que se originan fuera de la entidad y constan de: facturas de vendedores y correspondencia que se recibe.

El auditor debe considerar constantemente la confiabilidad de las formas de evidencia documental utilizada como respaldo de los hallazgos. Para soportarlo anterior, se anota el siguiente ejemplo: un documento externo que se obtenga directamente de su lugar de origen ofrece un mayor grado de confianza que el mismo tipo de documento obtenido por medio de la organización.

Seguidamente se anotan algunos factores importantes a considerar, que afianzan la confiabilidad de la evidencia de origen interno:

- Si los documentos han circulado fuera de la entidad - Los documentos internos que circulen fuera de la empresa, puede tener la misma confiabilidad que la evidencia externa. Algunos ejemplos de estos documentos son: órdenes de compra devueltos con el visto bueno del proveedor; guías de remisión debidamente aceptadas; embarques recibidos por el cargador y pedidos rehechos presentados para retiro de mercadería.

- Si los procedimientos de control interno, son satisfactorios para asumir que la evidencia es precisa y confiable - Los procedimientos internos tienen un efecto importante en la confiabilidad de los documentos que se originan en la compañía y que circula únicamente en ella. Así por ejemplo, una tarjeta de control de asistencia será evidencia confiable, si:
  - el empleado registra su hora de ingreso en el reloj de control;
  - el supervisor respectivo aprueba la marca y la tarjeta;
  - la sección de pago verifica la tarjeta de control, comparándola con la tarjeta de labor o con los horarios de trabajo; y
  - los auditores o la administración efectúan revisiones sorpresivas de asistencia.
  - si la evidencia está sola, o si sirve como soporte para corroborar o otros tipos de evidencia.
- c. Evidencia Testimonial - Esta es la información obtenida de otras personas por medio de cartas o declaraciones recibidas en respuesta a indagaciones, o por medio de entrevistas. Los datos concernientes a entrevistas pueden quedar registrados en los siguientes documentos:
  - Minuta, si fue una entrevista tipo reunión.
  - Memorando, basado en notas tomadas durante la entrevista.
  - Informe, basado en respuestas obtenidas a preguntas específicas; o
  - Transcripciones registradas (en cualquier medio) de todas las conversaciones.En todos los casos de los documentos citados, debe obtenerse la firma de las personas entrevistadas, ya sea en conjunto, con el visto bueno, o como respuesta al documento originado.

Las declaraciones de los funcionarios de una empresa, son fuentes muy valiosas de información, que pueden proporcionar guías que no serían fáciles de obtener por medio de una prueba independiente de auditoría.

Sin embargo, debe tenerse cuidado, debido a que la declaración verbal o escrita de un funcionario de la entidad acerca de un hecho, por ejemplo: la cantidad y estado de los inventarios, tiene un valor limitado como evidencia. Este tipo de declaraciones se vuelven mucho más importantes y adquieren mayor grado de utilidad, si se corroboran por revisiones e inspecciones de los registros y de la toma física de inventarios.
- d. Evidencia Analítica - Esta es la evidencia que obtiene el auditor como producto del análisis a que ha sometido toda la información recopilada según los tipos de evidencia antes citados. Este análisis incluye verificaciones y ajustes a los datos obtenidos, y debe realizar tanto análisis de tipo cuantitativo (de cantidad), como cualitativo (de cualidad). La evidencia de este tipo puede originarse por los resultados de:
  - Computaciones
  - Comparaciones con:
    - normas prescritas
    - operaciones anteriores
    - procedimientos
    - leyes o reglamentos
    - otras operaciones, transacciones o rendimientos, decisiones de tipo legal
    - raciocinio
    - labor analítica de la información dividida en sus componentes

El juicio profesional del auditor, acumulado a través del conocimiento y la experiencia, le puede orientar y facilitar en el análisis.

### Entrevistas

Como un paréntesis, se agrega en este aparte, un aspecto que muy pocas veces se revisa, enseña o practica en los centros de enseñanza superior; este aspecto es el relacionado con las entrevistas, con muy pocas excepciones, los auditores no reciben entrenamiento sobre este tópico tan importante y que, como se vio en la evidencia testimonial es básico para obtener información y sobre todo para confrontarla cuando sea necesario, con la obtenida por otros medios. Aquí se van a revisar algunas técnicas que se consideran importantes para lograr obtener información de personas que pueden ayudar mucho en el proceso de las auditorías.

- a. Plan: en la planificación de la auditoría, así como en el programa de trabajo de la misma, deben estar contempladas todas las entrevistas que se piensan realizar, con nombre completo de la persona a entrevistar, puesto, fecha, hora, duración estimada, tema(s) a tratar. Si en el plan tiene previsto durar, por ejemplo cuatro horas en una entrevista, es conveniente que antes de realizarla, se comunique con el entrevistado y le diga si le puede conceder el tiempo previsto por usted, o que le diga en cuantas entrevistas y de cuánto tiempo pueden disponer.

b. Citas: debe concertar citas con todas las personas que de previo, sabe que va a entrevistar; estas citas deben estar basadas en el plan y comunicadas con suficiente antelación a la fecha y hora de la misma. También debe confirmar estas citas, por lo menos con un día de anticipación.

De la misma manera, al concertar las citas debe respetar el orden jerárquico establecido, significa esto que debe preguntar primero a los jefes si puede entrevistar a sus subalternos y comunicarles las fechas de las citas.

Es claro que lo citado en los puntos anteriores debe realizarse en aquellos casos en que el factor sorpresa no está incluido en el proceso.

c. El proceso: ¿Cómo hacer la entrevista?

- Por teléfono: en este caso no es recomendable que sea muy larga; se pueden realizar por este medio, para aclarar algún concepto o para preguntar algo rápido que no sea de carácter confidencial o muy complejo.
- Por escrito: si se va a hacer uso de este medio, no es recomendable utilizar el cuestionario para ir preguntando directamente, -esta técnica ya pasó a la historia por correr el riesgo de obtener respuestas con monosílabos, como SI, NO, AJA, o de carácter negativo, como NO SE, QUIEN SABE, PUEDE SER, TAL VEZ, QUIZAS, etc.; en lugar de esto, debe tratar "de montar" una conversación fluida e ir tomando nota de los asuntos mediante anotaciones rápidas y claves, o códigos, en lo posible, debe tratar de iniciar la conversación con algo agradable para el entrevistado, pero que la maneje el auditor, para que no se pierda mucho tiempo, tenga siempre presente que es únicamente para "romper el hielo" y entrar de lleno en el asunto que realmente interesa: obtener información.
- No grabar: recuerde que no debe utilizarse ningún medio de grabación, a menos que lo autorice de previo el entrevistado. Tenga presente que estos medios son "intimidadores" y es muy probable que no quieran comprometerse si su conversación o su acción va a quedar grabada.
- No presionar al entrevistado: no obligar al entrevistado a responder sobre cosas de las que no desea hablar, o que de alguna manera está tratando de evitar; no demostrar demasiado interés en algún asunto que le informe con respecto a alguna irregularidad que usted está conociendo hasta ese momento, maneje el asunto con mucha delicadeza, tacto, cautela y buen juicio; escriban juntos un plan de acción sobre lo que debe hacerse y cómo deben manejarlo.
- Hacer que el entrevistado se interese en el asunto: hacerle ver que el trabajo (auditoría) que se está efectuando va a ser de ayuda, le va a servir para mejorar en el futuro, que él puede colaborar a que las cosas vayan mejor en la empresa, que juntos se pueden lograr mejores cosas, que es una labor de equipo, etc.
- Pregunte todo lo que desee saber; pero no repita preguntas innecesarias; si algo no le queda claro. plantee de nuevo la situación, pero no pregunte sobre temas que el entrevistado cree que ya contestó bien; efectúe resúmenes verbales de las situaciones, a manera de contestación y dígame que: "por favor lo corrija si algo no está bien", pero tampoco repita todo, es únicamente aquel o aquellos puntos que necesiten refuerzo.
- No darle chance a hablar de otros asuntos, a menos que puedan dar pistas para otra situación; lo que se trata de evitar es que el entrevistado se convierta en entrevistador y también que se pierda mucho tiempo en la entrevista.
- Recopile información: no debe dejar por fuera ningún tipo de información relacionada con el trabajo, debe obtener todo lo que pueda, no dejar nada a la memoria, ni utilizar la técnica de reconstruir, si el entrevistado le dice que después le envía fotocopia, trate de presionarlo para que se las entregue en el momento de la entrevista u ofrézcase para obtener las fotocopias, pero no lo deje para después porque es probable que no las tenga nunca, o que tenga que hacer esfuerzos adicionales para lograrlo.
- Utilice cuestionarios y listas de verificación; estas herramientas son muy útiles, pero debe tenerse mucho cuidado al hacer uso de ellas; al principio va a ser difícil manejarlas de manera apropiada, pero con el tiempo y la experiencia, la dificultad va disminuyendo. Primero debe tenerlas con usted e ir haciendo las preguntas dentro de la conversación que establezca y poco a poco se las irá aprendiendo de memoria, de manera que ya no va a ser necesario leerlas o ir viendo que sigue para preguntar. Puede armar bloques de preguntas por tema a tratar; también puede sostener la conversación completa sobre el tema e ir tomando notas, luego comparar las notas con el cuestionario o lista para discriminar y tomar nota de algo que quedó claro o no se contestó.
- Aspectos a recordar siempre:
  - No todas las personas a entrevistar reaccionan de la misma manera. La entrevista la dirige y la maneja usted
  - En toda entrevista pueden aparecer "cosas" que nunca se imaginan
  - Una entrevista puede desencadenar acontecimientos diferentes a los del estudio en cuestión
  - Lo que se dice en una entrevista cuesta mucho probarlo
  - No se puede dar por sentado (como un hecho) lo dicho en la entrevista
  - Lo anotado como producto de la entrevista no constituye evidencia

El entrevistado puede decir perfectamente yo no he dicho tal cosa, lo que dije fue otra cosa, pero usted entendió mal o no entendió bien.

No obligue al entrevistado a firmar algún documento producto de la entrevista. Discuta lo dicho antes de anotarlo en firme.

#### Propiedad y Responsabilidad

Los P/T son propiedad del auditor (o de la firma, Entidad u Organización que representa), él los obtuvo, llenó y preparó y son la prueba material del trabajo realizado. Pero esta propiedad no es irrestricta, ya que por contener datos e información que pueden considerarse confidenciales, está obligado a mantener discreción absoluta respecto a la información que contienen.

Esta discreción de mantenerse con el paso del tiempo; el auditor NO debe ser infidente nunca, aún cuando no trabaje para la institución en que realizó el examen; puede a manera de ejemplo, de enseñanza, de colaboración, mencionar el hecho pero, sin dar detalles del mismo, debe omitir nombres, hechos y situaciones que puedan comprometer su condición de confidente.

En otras palabras, los P/T pertenecen al auditor, pero queda obligado por el secreto profesional que estipula "no revelar por "ningún motivo los hechos, datos o circunstancias, aunque tenga conocimiento en el ejercicio, profesión a menos que el o los interesados y ..."

Dada la confidencialidad requerida en cuanto a la formulación, revisión, sustento y archivo de los P/T, la responsabilidad de su custodia y posterior manejo y uso, recae primero que todo en el auditor que los elaboró. Sin embargo, dependiendo de la estructura organizacional que exista y de la entidad que se trate, se puede asignar esta responsabilidad de la siguiente manera:

- en una Firma o Despacho: de acuerdo con los procedimientos de archivo imperantes; el responsable será el Gerente a cargo, con las restricciones que él designe, para verlos, revisarlos, consultarlos, destruirlos, etc.
- en una entidad pública: de acuerdo con los procedimientos y lo que dicten las regulaciones y leyes al respecto.
- en una empresa privada: el responsable es el Jefe de la Auditoría interna.

Cualquiera que sea el responsable de su custodia, nadie más que los responsables del trabajo tienen derecho a trabajar, en el sentido estricto de la palabra, con la información contenida en ellos\*.

#### Contenido y Clasificación

Contenido - Debido a que los P/T son comunes y generales para todo tipo de auditoría, sea cual sea su objetivo; y que para todas debe cumplirse lo estipulado en este curso, se puede decir que en términos de:

- Estudios Especiales
- Auditoría Financiera
- Auditoría Operacional y
- Auditoría de Sistemas de Información

Es necesario hacer una distinción respecto al contenido de los P/T, dada la naturaleza, objetivos, alcance y otras consideraciones que las distinguen. Sin embargo, no se va a ahondar en detalles al respecto, debido a que no se van a revisar P/T para una u otra en particular, sino los aspectos generales de los mismos, sea cual fuere la auditoría a realizar.

Su contenido es generalmente, el siguiente:

##### a. Auditoría Financiera – Operacional y Estudios Especiales

- Informe en borrador de la auditoría o estudio especial
- El Programa de auditoría
- Cuestionarios y listas de verificación sobre evaluación del Control Interno (Aud.Fin.)
- Cuestionarios y listas de verificación sobre entrevistas
- Hoja principal de trabajo o Balance de Comprobación (Aud.Fin.)
- Asientos de ajuste y reclasificaciones recomendadas por el auditor (Aud.Fin.)
- Conciliaciones (Aud.Fin.)
- Cómputos (Aid.Fin.)
- Extractos, copias literales, copias simples o autenticadas, fotocopias, y otros documentos como: copias de leyes y reglamentos, documentos sobre normatividad, copias de actas de sesiones de Junta Directiva, contratos, etc.
- Análisis de cuentas (Aud.Fin.)
- Confirmaciones, versiones o declaraciones de terceros

---

\* Código de Ética Profesional, párrafo 3.01

- Notas y observaciones del auditor, como:
  - procedimientos utilizados;
  - Notas recordatorias para aclarar aspectos que son materia de examen, completar procedimientos, técnicas u orientar mejor la labor del equipo de trabajo;
  - Excepciones existentes y vigentes, incumplimientos de disposiciones legales, comentarios significativos que se vislumbra se pueden convertir en observaciones;
  - Probables recomendaciones a ser discutidas de manera inicial con los auditados y con los niveles pertinentes y posteriormente con el representante del área sometida a examen.
- Todos los documentos o información útil a la obtención de evidencia. Esta información se puede catalogar como "Información voluminosa".

b. Auditoría de Sistemas de Información

Aunque el contenido citado en el punto anterior se puede tomar como base para todas las auditorías, vale la pena mencionar, para este tipo de auditoría en especial, algunas clasificaciones adicionales que es importante tomar en cuenta.

- Planificación, estimación e información relativa a la propuesta, de la auditoría a realizar. En auditoría de sistemas son muchos los tipos de revisiones que pueden realizarse, por lo tanto, debe indicarse aquí de cuál se trata.
- Correspondencia relativa
- Listado de la auditoría e informes de control
- Detalles de fuentes de información
- Consultas y entrevistas efectuadas
- Actas o minutas de reuniones
- Guías de presentaciones

Cabe mencionar que, cualquiera que sea la auditoría a realizar, es el auditor quien deberá distinguir, qué documentos, datos e información tiene trascendencia para la obtención de evidencia y qué otra tiene, solamente importancia relativa, debido a que no toda la documentación que se recopila es una simple transcripción de todos los documentos que existen en la empresa para fines de información, sino que los P/T representan la esencia del historial de las labores de auditoría.

Si se menciona aquí el contenido de los P/T, sólo serán útiles, los que comentan asuntos trascendentales para llegar a constituirse en evidencia suficiente y competente. Se trata por lo tanto, que el volumen de la documentación obtenida no está en razón directa con la calidad de la información útil y aprovechable que contiene.

Se puede resumir indicando que los P/T básicamente contienen dos aspectos fundamentales y complementarios entre sí, incluso se puede agregar, que son indivisibles:

- información necesaria, acumulada u obtenida para soportar con evidencia, el contenido del informe;
- información que demuestra la extensión de las pruebas que se efectuaron.

Clasificación - A los P/T se les acostumbra clasificar desde dos puntos de vista:

a. Por su uso:

- Papeles de uso continuo
- Papeles de uso temporal

b. Por su contenido: aunque en diseño y contenido los P/T son tan variados como la propia imaginación, existe en la secuela del trabajo de auditoría papeles clave cuyo contenido está más o menos definido y que los hace característicos:

- Hojas de trabajo genéricas - Son las que contienen aspectos generales como:
  - la hoja de trabajo, que es la cédula que muestra los grupos o rubros que integran los estados financieros (Aud.Fin.)
  - listas de documentos;
  - cuestionarios;
  - listas de verificaciones o de chequeo;
  - listas de descripciones; etc.
- Hojas sumarias o de resumen - Como lo indica su nombre, resumen las actividades analizadas por el auditor, y que son producto de su trabajo; contienen los puntos finales que le van a dar cuerpo a los informes definitivos; en otras palabras, contienen fortalezas, oportunidades, debilidades y amenazas encontrados a través de la revisión. Para efectos de Auditoría Financiera, son las cédulas que muestran las cuentas de mayor que forman un rubro.

- Hojas de detalle o descriptivas - Listas contienen el detalle de aquellos aspectos que por su incidencia e impacto en la auditoría se convierten en relevantes, como:
  - las cédulas que relacionan las partidas que componen una cuenta de mayor o un saldo cualquiera; (Aud.Fin.)
    - \* descripciones generales de: funciones, operaciones, procedimientos;
    - \* partidas que componen un saldo o una cuenta;
    - \* programas de trabajo detallado;
    - \* informes de progreso;
    - \* comentarios;
    - \* organigramas;
    - \* actas, etc.
- Hojas de análisis o comprobación - Contienen el trabajo efectuado para la verificación de:
  - una partida u operación específica (Aud.Fin.)
  - cifras;
  - partidas;
  - documentos;
  - listados de salidas;
  - listas de documentos de entrada;
  - listas de programas;
  - flujogramas;

así como correcciones a los mismos

Por su utilidad, más o menos permanente a este tipo de papeles se les acostumbra conservar en un expediente especial, particularmente cuando los servicios del auditor son requeridos por varios ejercicios, o para efectos del enfoque de Auditoría Interna; a este expediente, normalmente se le llama: Archivo Permanente

De la misma manera los P/T pueden contener información útil solamente para un ejercicio determinado, como por ejemplo:

- confirmaciones de saldos a una fecha dada;
- contratos y convenios a plazo fijo menor de un año;
- cuestionarios;
- conciliaciones bancarias;
- pruebas;
- cifras de control; etc.;

En este caso, tales papeles se agrupan para integrar el expediente de la auditoría del ejercicio a que se refieran.

#### Clases de papeles de trabajo

También se ha establecido otra clasificación de P/T ordenándolos por clases, éstas se anotan a continuación;

a. P/T Genéricos - Se ubican bajo este nombre los P/T que tienen una característica y utilidad de propósito general.

Ejemplos:

- Programa de auditoría
- Resultado del estudio y evaluación del Control Interno
- Hoja de trabajo o balance de comprobación (Aud.Fin.)
- Asientos de ajustes y de reclasificación (Aud Fin.)
- Resúmenes de entrevistas
- Informe en borrador

b. P/T Específicos - Son los que se relacionan o contienen datos, información o documentación de una transacción específica, como una cuenta, operación, asunto o algún detalle, que sea útil como evidencia sobre un hallazgo concreto detectado por el auditor.

Ejemplos:

- cédulas de las cuentas del mayor general confeccionadas por el auditor (Aud.Fin.)

- análisis de cuentas, del auditor o de la empresa (Aud.Fin.)
- conciliaciones
- memoranda o respuestas a ellos, cursados por el auditor pidiendo datos específicos relacionados con su examen
- confirmaciones recibidas
- resultados de pruebas efectuadas
- cualquier análisis de cuenta o actividad
- resúmenes de entrevistas, declaraciones y otras pruebas de carácter testimonial
- cualquier otro documento o cédula específica que respalde un asumo y que constituya un hecho particular.

Es necesario aclarar que no existe un "patrón" o "machote" estándar, debido a que varían de acuerdo con;

- El objetivo;
  - La naturaleza de la auditoría;
  - La actividad o entidad examinada;
  - Los estándares de la organización, firma o despacho; y
  - Al gusto, juicio y criterio del auditor.
- c. Otros Papeles de Trabajo - Aunque el auditor debe tener acceso a todo tipo de documentos, incluyendo aquellos de carácter legal o reglamentario, como minutas de comités, actas de sesiones de Juntas Directivas, planillas confidenciales, contratos, resoluciones tanto internas como externas y valores, éstos NO necesariamente deben pasar a ser propiedad del auditor; por lo tanto, debe buscar opciones que le permitan recopilar los datos contenidos en ellos, de acuerdo con las necesidades de evidencia y acorde también con la naturaleza y grado de acceso de cada documento.

En circunstancias descritas, puede obtener copias textuales o fotocopias de todo el documento o de la parte que le interesa y tiene pertinencia para él. Es importante que siempre se considere certificar su autenticidad. En otras oportunidades, deber a preparar extractos manuscritos de partes de importancia de los documentos que le son de interés; debe tener el cuidado de dejar marcas -si le es posible y se lo permiten- en los originales en donde quede constancia que los datos fueron tomados de ese documento; también debe anotar con suficiente claridad, en sus P/T todas las marcas necesarias para saber de dónde tomó la información.

Indicaciones a tomar en cuenta:

- la documentación que se genere debe constituir verdaderos P/T; se anota esto así debido a que los resúmenes, extractos o porciones específicas son más elegibles que los documentos fuente; por ejemplo; leyes, reglamentos, resoluciones y cualquier otro documento de tipo legal.
- es mejor obtener fotocopias -en cuanto sea posible-, debido a que el extraer y resumir textos largos, consume mucho tiempo; también es importante tomar en cuenta que, a veces es preferible tomar de las fotocopias, sólo lo indispensable.
- aprovechar las cédulas preparadas por el cliente, no sólo las que el auditor le solicita, sino aquellas que confeccionan rutinariamente. Ejemplos: los informes mensuales sobre el activo fijo, en cuanto a adiciones, dadas de baja, reclasificaciones, mejoras, traslados, etc., y la reconciliación bancaria.

La recomendación final es, que el auditor identifique y trate de aprovechar al máximo todas las fuentes de información que sean más;

- sencillas;
- accesibles;
- importantes;
- prácticas; y
- económicas;

y que en forma real constituyan el soporte de su trabajo, así como del examen que efectúa.

- d. Notas del auditor - Se ubican bajo este nombre a los P/T que le sirven de ayuda (refrescar la memoria) al auditor, en la medida que le permiten registrar determinados hechos, relevantes para él, cuyo recuerdo escaparía a su memoria, en el momento estratégico; por lo tanto este tipo de papeles le permiten dejar por escrito ideas importantes que pueden ser utilizados en su oportunidad. Las notas del auditor pueden ser:
- Notas recordatorias - Estas se utilizan tanto por el auditor como por el Supervisor, debido a que se trata de aspectos inherentes al trabajo en ejecución, que pueden ser susceptibles de análisis complementario, aclaraciones o indicaciones adicionales sobre determinado asunto, con el fin de ultimar detalles que deben contener los P/R, antes de convertirse en soporte del informe.

- Notas técnicas - Se utilizan para anotar hallazgos, debilidades, fortalezas, deficiencias o simples observaciones, que constituirán según sea el caso, condiciones o sólo observaciones en el informe en borrador, también se han incluido en este aparte, notas sobre conclusiones y recomendaciones a ser incluidas en el informe, aunque esa división no es muy recomendable.

Estas notas, normalmente sirven de base para la "redacción" de una observación o conclusión, en la medida en que haga ganar tiempo, el auditor solamente anula lo que se denomina como **"IDEA FUERZA"**. Es decir, la que hará posible "redondear" y "rematar" la observación.

Ejemplo:

Idea Fuerza:

Observación: No se encontraron documentos sobre políticas

"La revisión realizada mostró que no existen documentos que soporten las políticas, claras y precisas sobre las inversiones y captación de recursos que realiza la institución; esta normatividad es necesaria debido a las siguientes deficiencias encontradas en el examen efectuado... (La observación debe contener; el criterio, la causa, el problema así como el efecto)

Es conveniente recordar, que las notas del auditor son recordatorias y no complementarias, ni sustitutas de los P/T.

#### Ordenamiento y Archivo/Indices

Para facilitar la localización, los P/T se marcan con índices que indiquen claramente la sección del expediente en donde deben ser archivados y consecuentemente, en donde pueden ser localizados cuando se les necesite posteriormente.

En términos generales, el orden que se les da en el expediente varía de un auditor a otro, de una Firma a otra y de una Empresa a otra; pero se puede intentar un orden, más o menos aplicable para cualquiera de ellos; aunque se vuelve un poco difícil lograr un orden como el que se utiliza en las auditorías financieras, en que se asigna de acuerdo como presentar las cuentas en los estados financieros, puede decirse que en el caso de Auditoría de Sistemas, puede hacerse según la revisión que se esté efectuando; así por ejemplo:

- de adquisiciones;
- de la gestión de cómputo;
- de la gestión de Auditoría de Sistemas;
- del Ciclo de Vida del Diseño y Desarrollo de sistemas;
- de sistemas en desarrollo;
- de mantenimiento de sistemas;
- de evaluación de controles;
- del Plan de Contingencias; Etc.

Sin embargo, si se lleva un buen control sobre los índices, serán éstos quienes darán un sentido lógico al orden de los P/T. Los índices se asignan de acuerdo con el criterio anterior y pueden utilizarse para este objetivo: letras, números y combinación de ambos.

- Indices - a continuación se presentan ejemplos de índices utilizando el método alfanumérico, que es uno de los más usados. En este sistema, las letras sencillas representan cuentas de activo; las letras dobles, cuentas de pasivo capital, y los números - representados por decenas- indican las cuentas de resultados; cualquier otro método puede ser utilizado siempre y cuando constituya un estándar para quien lo hace, esto significa que, para cada trabajo debe seguirse el mismo esquema.

Ejemplos:

<u>Letras o Número</u>	<u>Para las Cuentas de:</u>
A	Cajas y Bancos
B	Inversiones Transitorias
C	Cuentas por Cobrar
D	Inventarios
L	Obras en Proceso
AA	Cuentas por Pagar
BB	Impuestos por Pagar
UU	Ventas
10	Reservas
20	Gastos Gerenciales
30	Ingresos Financieros

De igual manera, las cédulas secundarias se asignan a los siguientes índices:

<u>Índice</u>	<u>Cédula</u>
A	Sumaria de Caja y Bancos
A-1	Detalle de Fondos de Caja
A-1-1	Arqueo de los fondos de caja
A1-2	Movimientos no normales Detalle de Bancos
A-2	Conciliación bancaria
A-2-1	Confirmación bancaria
A-2-3	Corte de cheques

<u>De Auditoría de Sistemas Sección</u>	<u>Título de la Sección</u>
A	Planificación y Estimación de la Auditoría
B	Propuesta (emitida e Información relativa)
C	Correspondencia (Externa e Interna)
D	Estado de las Auditorías e informes de control

Tal como se anotó en los dos sub-puntos anteriores, este tipo de índices permite archivar de manera ordenada los diferentes papeles, por más disímiles que parezcan y se convierte en una herramienta de localización muy eficaz.

Por otro lado, los índices permiten también, referenciar o cruzar con gran facilidad las hojas y cédulas, que por tener datos comunes entre sí, que al ser verificados en una, estén debidamente comprobados en la otra.

Ejemplo:

Al revisar el incremento en la cuenta de Depreciación Acumulada, se verifica de manera simultánea, el cargo a las cuentas de Gastos en Resultados y en éstos, para no duplicar el trabajo ya hecho, se anota: refiérase a cálculos en hoja No. J-2-1, que será, como ejemplo, el índice de la cédula u hoja de los cálculos que nos ocupan.

- b. Archivo - Aunque el archivo de los P/T depende en gran medida de los procedimientos internos de cada Firma, Despacho u Organización, conviene mencionar ciertos estándares generales que se han establecido con el propósito de archivar, buscando el mejor método para cada quien, los diferentes documentos que se van generando al realizar toda auditoría y que si no se archivan, de manera correcta, adecuada y apropiada puede terminar en un caos para todos los participantes en la misma. Los P/T se archivan en dos tipos de archivo, a saber:
- Archivo Corriente - Este archivo está constituido por las fases ordinarias y específicas de la auditoría y contiene toda la información de las mismas y que no son considerados de una utilización continua en auditorías posteriores. El material que lo constituye, normalmente es el siguiente:
    - revisiones normales y ordinarias del control interno;
    - memoranda de las discusiones con funcionarios de la entidad;
    - correspondencia ordinaria;
    - el programa de Auditoría;
    - papeles que respalden los análisis realizados;
    - papeles que se van acumulando como respaldo a las observaciones
    - documentos que se acumulan en la preparación del informe; incluye las diferentes versiones en borrador
  - Archivo Permanente - La característica principal de este archivo, es que contiene información de importancia y de gran utilidad para auditorías posteriores. El material que debe estar en este tipo de archivo, es el siguiente:
    - historia legal, desde la generación de la organización, así como sus planes;
    - leyes y reglamentos específicos de la entidad;
    - manuales de Políticas (Estándares y Procedimientos);
    - fuentes de financiamiento;
    - organización y Administración
    - evaluaciones del sistema de control interno;
    - contratos a largo plazo:

- estadísticas sobre desembolsos, aspectos financieros y administrativos que tengan trascendencia,
- y sobre asignaciones;
- análisis de activos fijos;
- plan contable, manuales de contabilidad;
- actas o minutas de Junta Directiva, Reuniones de Coordinación, Comités, etc., que sean de interés permanente, o extractos o resúmenes de las mismas.
- cualquier otro documento que por su interés merezca ser incluido en esie archivo.

Es importante que en el archivo permanente se lleve un registro en donde se indique lo que decidió hacer con el Archivo Corriente de auditorías de años anteriores y la determinación de fechas escalonadas para su destrucción, en el entendido de haber cumplido aquél su "vida útil" también es importante tomar en cuenta que este detalle depende de los procedimientos de destrucción establecidos por la empresa de auditoría o por la entidad, y sin olvidar que los documentos de la administración pública pueden ser destruidos por una entidad asignada para tales efectos; y que los periodos de retención de información están dados por la legislación vigente, debido a que se trata de documentos de carácter financiero, que en su oportunidad pueden ser requeridos, incluso en caso de que lo demanden los tribunales de justicia.

El archivo permanente debe proporcionar información sobre auditorías de años anteriores sobre: áreas cubiertas; fechas de ejecución, referencias a informes; extractos de recomendaciones importantes y de resultados obtenidos; y debe ser mantenido en un lugar de fácil acceso para quienes tengan que consultarlo.

Es necesario que el archivo permanente sea revisado y actualizado de manera periódica, para que no pierda el concepto de su nombre, también para ir eliminando datos y documentos que ya no son necesarios; la información que se va eliminando debe archivarse en el denominado archivo Pasivo y debe identificarse y justificarse su posterior destino.

#### Elementos

Los P/T deben ser claros y concisos respecto de:

- la revisión que se está efectuando;
- la cuenta u operación a que se refieran;
- el trabajo desarrollado.
- el análisis efectuado, y
- las conclusiones obtenidas;

esto se logra estableciendo un mínimo de elementos que es conveniente tomar en cuenta en el momento de su elaboración; seguidamente se listan algunos elementos, que debe contener todo papel de trabajo de auditoría.

- Nombre de la empresa a que se refieren
- Fecha de cierre del ejercicio examinado o de la revisión realizada
- Título o descripción breve de su contenido
- Fecha de preparación
- Nombre de la persona que lo preparó
- Fuente de los datos (en los casos que proceda)
- Descripción resumida del trabajo realizado
- Conclusión

Con el propósito de facilitar la transcripción, así como la interpretación de las funciones efectuadas en toda auditoría, generalmente se suele utilizar verificaciones por medio de marcas físicas (signos peculiares y distintivos), que le permiten al auditor transcribir de una forma sencilla y práctica algunos trabajos, que por repetitivos podrían quitarle más tiempo del debido y permitido. Así por ejemplo, la función de cotejar las cifras que vienen de los auxiliares, contra los auxiliares que les dieron origen, se puede dar por transcrita, con sólo anotar una marca, cuyo significado se anota como que fue verificado el dato, en los auxiliares mismos. La señalización de esta simbología, se efectúa tanto en libros, registros y otros documentos de la entidad, como en los P/T que se han preparado.

Vienen a constituir "el sello", el recuerdo y la evidencia adicional de las funciones y tareas ejecutadas por los auditores.

Esta práctica, también es de gran importancia para los supervisores a la hora de efectuar revisiones del trabajo realizado.

Como estándar, es de gran ayuda el establecimiento de marcas que signifiquen siempre lo mismo, a pesar de se utilice en diferentes papeles de trabajo, estas marcas estándar deben establecerse mediante un procedimiento genérico y quedar debidamente registradas en el manual de estándares, para que todos los auditores las utilicen en el mismo sentido que tienen todas.

Seguidamente, se enumeran algunos trabajos que, por su condición de repetitivos, se pueden estandarizar y transcribir por medio de una marca de las que se han denominado como estándares:

- Cómputos en general, como: sumas, divisiones, multiplicaciones y cualquier otro tipo de cálculo debidamente verificado y hallado correcto.
- Inspección o verificación física realizada.
- Todo documento -sea original, copia o fotocopia- revisado y verificado: incluso con requerimientos legales y fiscales.
- Todos aquellos datos y cifras cotejadas **contra** el mayor respectivo se ha determinado como correcta.
- Toda operación, proceso y procedimiento revisado, con las autorizaciones apropiadas, correctas y adecuadas.
- Todos aquellos datos y cifras cotejadas contra el auxiliar respectivo y se ha determinado como correcta.

Las marcas deben anotarse de la manera más sencilla posible, pero que al mismo tiempo sean verdaderamente distintivas, para que no puedan confundirse entre ellas mismas, y por lo tanto no causar confusión tampoco, entre los funcionarios que tengan relación con el trabajo. Generalmente se recomienda efectuar estas marcas distinguiéndolas con colores, no muchos pero que se puedan distinguir bien: rojo, azul y verde son los colores más utilizados.

Esta simbología, a menudo es utilizada bajo dos significados, pero no es obligatorio el seguir este método, es suficiente saber que se puede utilizar y que es muy conveniente hacerlo. A continuación se citan estos significados.

- Significado Uniforme - La simbología tiene este significado, también llamado permanente, cuando se utilizan con frecuencia en cualquier auditoría y que, de alguna manera han sido "general o uniformemente aceptadas", tanto por las autoridades administrativas de la entidad, como por entidades fiscalizadoras superiores y los departamentos de auditoría interna. Es recomendable que a modo de Índice se consigne el significado de cada una de las marcas a utilizar.
- Significado a Criterio del Auditor - Este significado se le asigna a la simbología que es utilizada por los auditores, de manera convencional y particular, para indicar o señalar conceptos, criterios, técnicas, métodos, procesos o procedimientos utilizados durante el trabajo de auditoría que están realizando. La particularidad de esta simbología, es que cada marca debe consignar en cada tramo de la revisión, su significado o equivalencia; como ejemplo se presentan dos:
  - Verificada la operación matemática y confirmada la existencia física.
  - Confirmada.

Es conveniente indicar que las marcas que deja el auditor como "huella" de su trabajo, sirven también como notas recordatorias del grado de avance de su labor, cuando tenga que dedicarse a varios asuntos y, al tener que interrumpir una actividad, al regresar a ella pueda orientarse por la simbología que dejó cuando tuvo necesidad de interrumpir sus funciones.

Esta manera de hacer las cosas, le evitará incluso **duplicidad de esfuerzos** en el desarrollo del examen que efectúa.

En muchos casos, la simbología debe tener el carácter de confidencial, aunque también se utilice -a futuro- como fuente de información. Cuando las utilice de esta manera, el auditor debe tomar sus precauciones con el fin de evitar interpretaciones no correctas de su trabajo, por ejemplo: "Visto", no significa conformidad del documento; esto es sólo una huella, no una certificación de su conformidad.

### Planeación

Tal como se presenta en el proceso administrativo, en la auditoría también es necesario e imprescindible contar con una adecuada planeación en la confección de los P/T. Este planeamiento, que debe ser esmerado y de mucho cuidado, debe darse desde la fase inicial, tomando en cuenta no sólo ésta, sino también el desarrollo de la labor de auditoría, la culminación del trabajo de campo, el análisis de las fortalezas, oportunidades, debilidades y amenazas y la elaboración del informe.

El auditor tendrá que poner en práctica su poder y facultad de carácter creativo, cuando planea el tipo y diversas formas de los P/T que deberá utilizar, formular o recopilar, de acuerdo con las necesidades de dejar evidencia de su trabajo efectuado de manera fehaciente, sin lugar a dudas, preciso, conciso, exacto y todos los demás atributos indispensables para reflejar su imagen, realista, positiva, de respeto, confianza, profesionalismo; en resumen de verdadera idoneidad y competencia, que lo caracteriza para realizar las labores de auditoría, tal como lo exigen las Normas de Auditoría.

Bajo ningún concepto el auditor debe tratar de improvisar, debido a que esta no es compatible con el trabajo de auditoría; el auditor que pretenda hacerlo, estará arriesgando su imagen personal y profesional y, en el afán de aparentar -autosuficiencia, mayor capacidad y conocimiento, mejor academia- tendrá que buscar en la prisa, una supuesta compensación al adecuado y correcto planeamiento, de un trabajo que se supone, debe ser serio y responsable.

El resultado de una tarea no responsable, será el de perder recursos costosos y escasos, como es el tiempo y los esfuerzos adicionales, debido a que se hará necesario repetir pasos o trabajos sobre los que no se tiene suficiente confianza; esto se presenta así porque los datos, cifras e información recopilada, preparada, codificada, procesada, analizada y presentada, no podrán ser utilizados como evidencia seria, adecuada, suficiente y competente.

Al proporcionar los puntos antes descritos, se está dejando en claro la necesidad que el auditor no se crea, como se mencionó en el párrafo anterior, autosuficiente, sino que con sencillez, profesionalidad y modestia, revise los P/T y toda la documentación pertinente

de las auditorías precedentes -si es que se realizó alguna-, con el fin de determinar si se pueden utilizar para el examen que se apresta a iniciar.

Lo aquí mencionado no quiere decir ni significa que los P/T elaborados para auditorías anteriores, constituirán una fuente única o un patrón invariable; por esta razón es que se enfatiza que el funcionario que va a realizar una auditoría -cualquiera que esta sea-, debe contar con imaginación, creatividad, ingenio, experiencia, confianza en sí mismo; capacidad analítica y esmero profesional, para elaborar los formularios, programas, procedimientos, estándares, diagramas y otras herramientas necesarias para realizar su labor, pero además puede apoyarse y sustentarse en P/T anteriores, aunque no los utilice del todo. Sin embargo, pueden ser útiles para formarse y generar ideas, para conocer y estudiar procedimientos y para tomarlos como base en el diseño y puesta en práctica de los propios.

Especialmente para efectos de auditoría financiera, se considera como de mucha importancia el concepto de uniformidad en el diseño de los P/T; generalmente en los departamentos de auditoría interna; en las firmas de auditoría y en los despachos de contadores públicos, utilizan hojas con varias columnas. 7 a 16, de tipo rayado columnar; asignan hojas de cierto tipo para trabajos comunes; así por ejemplo, para la Hoja Principal o para análisis amplios, utilizan la hoja más ancha.

En aquellos casos que se trate de documentar aspectos como: entrevistas, declaraciones, diagramas, flujos de proceso, revisiones físicas, inspecciones oculares o cualquier otra labor en las que se hace necesario efectuar descripciones detalladas de pasos de trabajo, o efectuar narrativas de situaciones especiales, deben utilizarse hojas de rayado común, hojas en blanco o formularios especialmente diseñados para tales efectos.

También depende de los diferentes estándares que tenga cada organización o entidad, así serán sus P/T; algunos usan papel con ciertas características preimpresas para las diferentes actividades, funciones y auditorías, y hojas en blanco -con los elementos básicos- para aquellos aspectos que son considerados como irregulares o impredecibles.

El planear la forma y contenido de los P/T puede ahorrar tiempo, y resultará en P/T más completos, nítidos, breves y limpios. Antes de planear un trabajo, debemos planteamos las siguientes preguntas, a nosotros mismos.

- a. Que propósito de auditoría se logrará, preparando estos papeles de trabajo?
- b. Es esencial preparar estos P/T para lograr el objetivo de auditoría?
- c. Puedo evitar preparar estos P/T comprobando los registros del cliente e indicando la naturaleza y extensión del trabajo de auditoría, en los documentos del cliente o en un programa de trabajo.
- d. Es necesaria la preparación de los P/T para acumular la información exigida para algún informe especial del cliente, informe de impuestos o anexo?
- e. Después de contestar a estas preguntas, el auditor será capaz de planear la preparación de los P/T necesarios. Las siguientes preguntas se deben considerar, antes de preparar los P/T para el año actual:
  - Puedo adaptar los P/T del año pasado y "arrastrarlos" al año actual?
  - Pueden ser los P/T preparados por el cliente, o puedo utilizar una copia de P/T preparados por el cliente rutinariamente, en su lugar?
  - Facilitará el formato de los P/T, que se puedan volver a utilizar en años futuros, o nos beneficiará en el trabajo preliminar y final de auditorías futuras?

Al planear los P/T para el año actual, se deben revisar los del año anterior, en cuanto a:

- cualquier información que pueda ser de un interés permanente o de alguna continuidad;
- orientación al preparar los P/T para el año actual: frecuentemente el formato de P/T anteriores se puede utilizar, con lo que se ahorrarían recursos; y
- cualquier falta de uniformidad en principios -de contabilidad y de auditoría-, o métodos de aplicación entre períodos de contabilidad.

Sin embargo, debe tenerse precaución cuando se revisen los P/T del año anterior como base para determinar los procedimientos de auditoría para el año actual. No se deben seguir los P/T del año anterior ciegamente, porque los procedimientos que fueron apropiados en años anteriores pueden no serlo o lo que es más, pueden ser inapropiados para el año actual.

#### Otras consideraciones

- a. Propósitos
  - Principal - Proveer documentación del cumplimiento con las Normas del Trabajo, que incluya:
    - planificación y supervisión adecuadas;
    - estudio y evaluación del sistema de Control Interno, y
    - evidencia suficiente y competente obtenida a través de la inspección, observación, indagación y confirmación para proporcionar una base para emitir una opinión.

- Secundarios - Existen también otros propósitos de carácter secundario, como:
  - servir de guía en exámenes o revisiones siguientes;
  - proporcionar información para diferentes tipos de declaraciones;
  - facilitar la revisión de los Estados Financieros y todo otro tipo de información; y
  - destacar cualquier posible sugerencia.
- b. Soporte - Los P/T nos pueden dar soporte o proporcionar ayuda para:
  - Planear, organizar y coordinar el trabajo de auditoría
  - estimar las necesidades de recursos personal y equipos
  - evaluar el Control Interno para determinar la extensión necesaria del trabajo como resultado de la evaluación
  - revisar o ayudar en la preparación de cualquier informe
  - aquilatar la suficiencia de los informes de auditoría relacionados con los asuntos sobre los que se está informando
  - adiestrar a los miembros del personal y evaluar su actuación en el trabajo
  - conducir visiones, exámenes, indagaciones y estudios posteriores; y
  - determinar posibles sugerencias
- c. Papeles de trabajo basados en los programas de auditoría - Los programas de auditoría pueden proporcionar una gran ayuda para que los P/T queden "acabados", para esto se requiere que se preste una atención cuidadosa en la planificación apropiada de los diferentes procedimientos; además:
  - ayudan a asegurar un trabajo de auditoría uniforme y completo;
  - proporcionan un medio conveniente para dar instrucciones pertinentes a los asistentes sobre el trabajo y el cliente específico; especialmente cuando existen muchas operaciones detalladas y relacionadas entre sí;
  - proveen control y seguimiento sobre el trabajo de auditoría, mientras éste progresa, además facilita, agiliza y mejora la sincronización del trabajo, y por último
  - constituyen una constancia lógica del trabajo realizado

Programas del año actual para el futuro - Los programas de auditoría pueden proporcionar ayuda en revisiones o exámenes futuros, al minimizar los requerimientos de tiempos para preparar programas, cédulas y anexos.

Cualidades de un buen programa de auditoría - A continuación se describen algunas de las cualidades que debe tener un programa de auditoría que pretenda ser bueno:

- Establece con detalle suficiente el trabajo que se va a llevar a cabo y por lo tanto, minimiza las posibilidades de mal entendidos u omisiones,
- documenta de manera adecuada el trabajo realizado;
- describe los registros y procedimientos del cliente, siguiendo el flujo de la información que se examina, y organiza esta información en un orden lógico;
- establece aquellos procedimientos que se pueden realizar de manera simultánea;
- incluye un estudio y evaluación del control interno en forma minuciosa y detallada; específicamente relacionado con el área que se está examinando, y por lo tanto, proporciona una base para la extensión de las pruebas;
- indica el trabajo necesario a realizar;

(a no ser que se pretenda examinar un 100%, el término prueba se debe utilizar en forma general, y la extensión de las pruebas y los métodos de selección se deben indicar en forma clara, concisa y detallada).

- evita la utilización de términos ambiguos como: "comprobar", "reparar" y "recorrer con la vista";
- cuando es apropiado, contiene una conclusión.

- d. Constancia de las partidas seleccionadas - Para efectos de la realización de pruebas, los P/T deben indicar:
  - un registro de las partidas, datos y documentos seleccionados: o bien
  - una clara explicación de cómo se hicieron las selecciones.

La cantidad de detalle necesaria variará dependiendo de:

- el área de auditoría o tipo de auditoría a realizar,
- el nivel de riesgo de auditoría envuelto; y

- la probabilidad de que la población sea retenida por el auditado, en una condición inalterada por varios años.
- e. Pruebas utilizando muestreo estadístico - Si se utiliza o piensa utilizar la Técnica de Muestreo Estadístico para efectos de las pruebas, los P/T deben indicar en forma clara y detallada que la información básica de muestreo estadístico consiste de los factores de diseño de la muestra:
  - factor de juicio compuesto;
  - factor de confianza; y
  - el punto de partida al azar; y el método de selección, como:
    - Auditaje;
    - Importes Monetarios Acumulados (TMA);
    - CMA estratificado: o
    - algún método específico diseñado por el auditor

Información estadística adicional que se debe indicar

Para todos los efectos prácticos, la información básica de muestreo estadístico, generalmente constituye suficiente documentación en mención en cuanto a la extensión de las pruebas de sumas y resúmenes de los registros y anexos. Sin embargo, como parte de las pruebas de saldos, al seleccionar muestras de los registros iniciales, de partidas de balances u otros anexos de partidas individuales, se debe decidir si los P/T deben contener también:

- una lista de las partidas seleccionadas (enfoque de listado)
  - información suficiente para reconstruir la muestra (enfoque de reconstrucción)
- f. Enfoques de reconstrucción y de listado

**Enfoques** - Al utilizar el enfoque de reconstrucción, el auditor se debe asegurar que las partidas descritas fueron observadas estrictamente en el proceso de selección. Los P/T deben contener la información básica de muestreo estadístico, el número de partidas seleccionadas y una descripción de por lo menos, las técnicas siguientes:

- la determinación del punto de partida al azar;
- la suma para alcanzar totales predeterminados;
- el tratamiento de los importes negativos;
- la determinación de totales predeterminados;
- el uso de puntos de corte, en el diseño de muestras estratificadas.

Bajo el enfoque de listado, el registro de las partidas seleccionadas, se puede lograr de varias formas:

- aparecer en los P/T, confirmaciones de saldos, marcas de cotejo y controles cruzados en un anexo;
- si se utiliza el Auditaje o cualquier otro programa automatizado, se deben incluir:
  - las hojas impresas que prueban la evidencia de los totales de control; las especificaciones que controlan las selecciones; y
  - detalles de las selecciones:

listados en que se especifiquen las partidas seleccionadas, tales como: números de cheques; número de comprobantes, número de partidas y lotes, número de facturas, etc.

**Obligatoriedad de listar las Partidas** - Independientemente del enfoque que se utilice, es de carácter obligatorio, que listen las partidas y se describan en los papeles de Trabajo, cuando:

- el resultado de la selección es una excepción;
- la selección muestra evidencia o sospecha de una irregularidad;
- la selección sea un asunto de carácter insólito o delicado, como una transacción entre
  - la determinación del punto de partida al azar;
  - la suma para alcanzar totales predeterminados;
- el tratamiento de los importes negativos;
- la determinación de totales predeterminados;
- el uso de puntos de corte, en el diseño de muestras estratificadas.
- la selección sea un asunto de carácter insólito o delicado, como una transacción o entre partes relacionadas, contribución a un partido político o un pago ilegal;

- la selección representa una partida de interés para la auditoría, perteneciente a otra área de auditoría;
- la selección pertenece a un área de auditoría que envuelve asuntos complejos, de un alto discernimiento o de un riesgo considerable, que deben recibir estrecha revisión por parte de auditores con categoría superior.

Bajo el enfoque de listado, el registro de las partidas seleccionadas, se puede lograr de varias formas:

- aparecer en los P/T, confirmaciones de saldos, mareas de cotejo y controles
  - cruzados en un anexo;
  - si se utiliza el Auditaje o cualquier otro programa automatizado se deben incluir las hojas impresas que prueban la evidencia de los totales de control;
  - las especificaciones que controlan las selecciones; y
  - detalles de las selecciones;
  - listados en que se especifiquen las partidas seleccionadas, tales como: números de cheques; número de comprobantes; número de partidas y lotes; número de facturas, etc.
- g. Presentación - A continuación se presentan una serie de aspectos, que por su relevancia se consideran de interés, y que deben ser requisitos esenciales para considerar a los P/T como documentos indispensables para una correcta y adecuada auditoría y que deben -al menos- tratar de cumplir TODOS los auditores, independientemente de su especialidad, si se desea que sean considerados como tales:

**Referencias** - La información contenida en los diferentes P/T debe tener referencias con todos aquellos que se considere necesarios con el fin de evitar duplicaciones, tanto de papeles como de datos, totales, cifras e información, que perfectamente se puede referenciar por medio de marcas debidamente identificadas para relacionar diferentes papeles y datos.

La información pertinente o las cantidades que aparecen en más de un lugar, deben tener o contar con referencias cruzadas. Esto le añade sentido y realiza la organización de los P/T.

Estas referencias deben ser hechas de tal manera que la relación de los P/T sea cruzada, para mostrar de una manera objetiva por medio de los mismos, las conexiones entre los diferentes rubros bajo estudio, llámense éstos cuentas, cédulas, análisis, formularios especiales o procesos.

Esta práctica, hasta el momento muy utilizada en la Auditoría Financiera, puede ser de gran soporte y ayuda en cualquier otro tipo de auditoría, como:

- Operacional;
- Legal
- De Sistemas de información; y
- Los diferentes enfoques de Auditoría Interna y Externa.

**Firmas** - Los P/T deben ser firmados por los siguientes funcionarios:

- el auditor que los preparó;
- los auditores que hayan realizado procedimientos específicos y hayan puesto sus iniciales o marcas de cotejo, o explicaciones correspondientes;
- el auditor encargado; y
- el gerente o socio supervisor.

**Revisión y Aprobación** - Como es lógico suponer, antes de ser firmados por los niveles altos de auditoría, los P/T deben ser sometidos a la revisión y aprobación de esos mismos niveles, ya que el éxito o fracaso de un examen, depende en gran medida, de la revisión y aprobación de los P/T como soporte del informe final. La revisión y aprobación debe regirse por las siguientes normas:

- supervisión puntual que incluya dentro de sus tareas la revisión periódica de los P/T
- oportunidad, que se revise en el momento adecuado al tiempo de la auditoría
- participación de los supervisores en las labores de auditoría, para que tengan conocimiento cabal y pleno de lo que están revisando.
- orientación por parte de los supervisores, de la labor de auditoría incluyendo la generación de los P/T.
- supervisión directa, no se debe realizar el tipo de supervisión denominado "a control remoto" o "de escritorio", sino que debe ser en el campo, ya que los aportes, críticas y sugerencias deben darse en el momento real de los exámenes y no, que al final de la auditoría se dan cuenta que tienen que revisar o supervisar, pero aquí lo único que queda por revisar es el informe final.

- soporte y ayuda por parte de los supervisores, debe recordarse que éstos no son correctores de "estilo" de "presentación", ni de "formas" del informe, si no ha participado directamente en la auditoría, podría hacerlo por medio de sugerencias, correcciones y hasta adiciones, si participó y revisó lo hecho durante el proceso de trabajo de campo.
- lugar de revisión, debe hacerse en las oficinas de la entidad auditada con el fin de completar información adicional requerida en virtud de la revisión.

Este aspecto adquiere especial importancia y es esencial que los P/T lo contengan, debido a que:

- define el alcance del examen
- proporciona conclusiones comprensibles;
- permite seguir el proceso paso a paso;
- mejora la presentación;
- indica profesionalismo; y
- permite que alguien que no esté familiarizado con el trabajo, pueda comprender su contenido y propósito.

A continuación se indican algunas características de la nitidez:

- ortografía correcta y apropiada;
- lenguaje sin adornos e inteligible;
- nombres de compañías, lugares, equipos y objetos deletreados completamente;
- abreviaciones que se entiendan;
- siglas, deletreadas y explicadas; si son en otro idioma, explicar su significado o hacer la cita de: "por sus siglas en ... y el idioma correspondiente,
- esquema lógico de referencias;
- marcas de cotejo explicadas adecuadamente preferiblemente colocadas en una sección identificada como tal
- número mínimo de marcas de cotejo hecho posible ampliando un comentario o utilizando una marca de cotejo para explicar más de un procedimiento realizado, en lugar de especificar marcas aparte para cada uno de ellos.

**Brevedad** - Los elementos principales en los P/T son básicamente dos:

- brevedad de la declaración,
- sin elaboración o detalles superfluos.

Lo anterior significa que los auditores debemos ser concisos y muy cuidadosos para dar una explicación completa, sin andar "con rodeos", del asunto examinado, obviamente con mucha claridad y calidad de carácter convincente.

**Limpieza** - Los elementos claves de este importante aspecto, son:

- caligrafía legible;
- escribir solamente por un lado del papel;
- utilizar una hoja de papel lo suficientemente grande que permita evitar la aglomeración de la información;
- adjuntar las cédulas, documentos y correspondencia preparados por el cliente u otros
- papeles, al papel de tamaño estándar, o doblarlos a un tamaño compatible con nuestros P/T;
- volver a copiar información, que merece conservarse, en papel con tamaño estándar o normal, si esta fue escrita en pedazos de papel.

h. Preparación - En la planeación y preparación de los P/T, debe tomarse en cuenta ciertos aspectos relacionados con la presentación, se incluye algunos otros asuntos que de alguna manera se relacionan con ella. Algunas consideraciones a tener presente son:

- Deben incluir los datos y cifras estrictamente necesarios
- Las aseveraciones que contengan deben estar suficientemente respaldadas o sustentadas
- Deben presentar todos los datos que respalden los registros y operaciones
- Deben cumplir con una serie de atributos, que se anotan en este mismo capítulo
- Deben reunir los elementos, características y componentes de la evidencia

## **Presentación de Resultados**

### **Informe Final**

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad.

Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

### ***Estructura del informe final:***

El informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente.

### ***Definición de objetivos y alcance de la auditoría.***

### ***Enumeración de temas considerados:***

Antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.

### ***Cuerpo expositivo:***

Para cada tema, se seguirá el siguiente orden a saber:

- a) Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real
- b) Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
- c) Puntos débiles y amenazas.
- d) Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
- e) Redacción posterior de la Carta de Introducción o Presentación.

### **Discusión de Resultados**

- El informe debe incluir solamente hechos importantes.

La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.

- El Informe debe consolidar los hechos que se describen en el mismo.

El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

1. El hecho debe poder ser sometido a cambios.
2. Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
3. No deben existir alternativas viables que superen al cambio propuesto.
4. La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

### **Flujo del hecho o debilidad:**

#### **1 – Hecho encontrado.**

- Ha de ser relevante para el auditor y para el cliente.
- Ha de ser exacto, y además convincente.
- No deben existir hechos repetidos.

#### **2 – Consecuencias del hecho**

- Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

#### **3 – Repercusión del hecho**

- Se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

#### **4 – Conclusión del hecho**

- No deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

#### **5 – Recomendación del auditor informático**

- Deberá entenderse por sí sola, por simple lectura.
- Deberá estar suficientemente soportada en el propio texto.

- Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
- La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

*Carta de introducción o presentación del informe final:*

La carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargo o contrato la auditoría.

Así como pueden existir tantas copias del informe Final como solicite el cliente, la auditoría no hará copias de la citada carta de Introducción.

La carta de introducción poseerá los siguientes atributos:

- Tendrá como máximo 4 folios.
- Incluirá fecha, naturaleza, objetivos y alcance.
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- En la carta de Introducción no se escribirán nunca recomendaciones.

## **REVISIÓN DE LA GESTIÓN DE AUDITORÍA EN TECNOLOGÍA DE INFORMACIÓN**

### **Introducción**

Con el propósito de alcanzar los objetivos de auditoría, la gestión de auditoría de sistemas de información debe planearse, organizarse, dirigirse y controlarse, incluyendo la revisión de los papeles de trabajo y los informes de auditoría.

### **Objetivos de auditoría**

Los objetivos que persigue la revisión de la gestión de auditoría de sistemas de información se enumeran a continuación:

- Velar por el uso más eficiente posible de los recursos de auditoría (personal, tiempo y dinero).
- Asegurar que existe una adecuada cobertura de auditoría para los riesgos más altos y exposiciones de peligro en un ambiente de procesamiento electrónico de datos.
- Asegurar que los recursos de procesamiento de datos (hardware, equipo periférico, software, servicios y personal) son utilizados en una forma eficiente para lograr las metas de tecnología de información y de la organización.

### **Prácticas en la gestión de auditoría**

#### **Planeación**

Se debe desarrollar una matriz de planeación de auditoría para determinar cuáles son las áreas auditables de TI. Para lograr esto, debe levantar un perfil del Área de TI y de las aplicaciones en desarrollo, mantenimiento y operación.

Un perfil del Área de TI muestra la estructura organizacional, el presupuesto, la configuración del hardware y equipo periférico, la información del software (de aplicaciones, en desarrollo, mantenimiento o en producción, sistema operativo, herramientas de desarrollo, etc.).

El perfil de las aplicaciones debe ser desarrollado utilizando un método de clasificación de riesgo. Esto se hace asignando a cada factor crítico una puntuación de acuerdo con los siguientes criterios:

- Complejidad de los sistemas (línea o batch).
- Satisfacción del usuario.
- Sistemas aislados o integrados
- Edad de los sistemas
- Porcentaje de errores de entrada
- Ordenes pendientes de cambios o programas
- Impacto financiero en los sistemas
- Horas y costo de desarrollo de los sistemas
- Nivel de los lenguajes de programación
- Número de programas por aplicación.

El resultado final es una lista separada de todas las aplicaciones operacionales y nuevas con un puntaje final para cada sistema.

Esta información clasificada por riesgo servirá de base para fijar las prioridades de la intervención que se realizará en el Area de TI. Los puntajes deben ser ordenados en forma descendente. Esto implica que el puntaje más alto representa el sistema de más alto riesgo y sensitivo, y será el primero en revisarse y así sucesivamente.

Para efectos de planeación e informes de auditoría, los puntajes deben ser convertidos en medidas, a saber, altos, medios y bajos (refiérase al final del módulo a la matriz de riesgo de aplicaciones operacionales y nuevas).

En adición al proceso de planeación iniciado por el gerente de auditoría de sistemas de información, el auditor de sistemas necesita efectuar funciones de planeación al inicio del trabajo. Esto determina el alcance total y los objetivos de la intervención y las expectativas de los auditados en relación con el trabajo de desarrollar por el auditor. También, el auditor de sistemas debe recolectar información relacionada con los antecedentes, políticas y procesamientos de la organización, papeles de trabajo de auditoría anteriores e informes y correspondencia del Area de TI y de los usuarios.

Antes de iniciar el trabajo de campo, el auditor debe efectuar una segunda reunión con los auditados. El propósito de dicha reunión será para:

- Explicar los objetivos y alcance de la revisión en términos gerenciales
- Levantar una lista del personal (usuarios y del Area de TI) y cerciorarse de la disponibilidad de cada uno durante la intervención,
- Entender puntos e vista, problemas e inquietudes de los auditados y de las aplicaciones a revisar.
- Cerciorarse de las expectativas de los auditados.
- Definir la información que desea recolectar.

Como resultado de esta reunión, el auditor de sistemas enviará una copia del alcance y programa tentativo de trabajo a los auditados (usuarios y Area de TI) con el propósito de proveer una clara imagen del trabajo que desarrollará.

#### Selección de personal

Cada organización tiene sus propias políticas de reclutamiento, selección, contratación, retención y evaluación de personal.

La selección de personal es de mucha importancia en la auditoría de sistemas de información. Es la calidad del personal la que determina cuáles sistemas de información auditados son efectivos y eficientes. El personal en esta disciplina debe ser competente y tener requisitos y experiencia en procesamiento electrónico de datos, contabilidad y auditoría.

Cuando el gerente de auditoría de sistemas de información va a reclutar un auditor de sistemas debe considerar ciertos atributos tales como: habilidades profesionales y cualidades de carácter como adaptabilidad, entendimiento e iniciativa.

#### Supervisor

La supervisión oportuna asegura que las actividades de la auditoría de sistemas de información han sido apropiadamente planeadas generando un producto de alta calidad.

Un supervisor, competente puede ayudar en la preparación de planes de auditoría, desarrollar y controlar presupuestos y programas de trabajo, contribuir a mejorar las relaciones entre la auditoría y los auditados, preparar papeles de trabajo consistentes y revisar informes de auditoría.

La supervisión es un proceso continuo que se inicia con la planeación, finalización de la auditoría, discusión y distribución del informe final. Los supervisores debe asistir a la reunión inicial y final con los auditados.

Los supervisores deben aprobar el programa inicial de trabajo y cualquier revisión al programa. También, deben revisar los papeles de trabajo y controlar el presupuesto de horas y los programas de trabajo.

Cuando el supervisor revisa el informe de auditoría debe referirse a los papeles de trabajo para verificar que las evidencia y hechos estén bien soportados.

#### Desarrollo del personal de Auditoría

El proceso de desarrollo del personal de auditoría está compuesto por las siguientes actividades:

- a. Entrenamiento - El área de auditoría de sistemas requiere de una revisión continua de los programas de auditoría. Para mantener un sentido práctico, las actividades de entrenamiento deben responder fácilmente a las condiciones cambiantes de la tecnología de procesamiento electrónico de datos y a las técnicas de auditoría.

Para que el entrenamiento sea efectivo, requiere de una continuidad y actualización de las necesidades actuales y futuras del personal. En este caso, el punto más importante es que el gerente de auditoría de sistemas de información desarrolle "El manual de auditoría de sistemas de información", en donde describirá las políticas, procedimientos, muestras de programas de trabajo de auditoría, etc.

El manual deberá ser utilizado como material de entrenamiento para los nuevos empleados y como de consulta y referencia del auditor de sistemas.

En la definición de los objetivos de entrenamiento se deben reconocer las diferentes capacidades y limitaciones del personal. Idealmente, los objetivos de entrenamiento deben ser desarrollados, tomando en consideración las necesidades individuales del personal y las necesidades de la organización.

Los objetivos de entrenamiento deben ser periódicamente actualizados con base en la retroalimentación obtenida de sesiones anteriores. También, es conveniente reservar tiempo (tres o cuatro semanas) para que el personal asista a seminarios y conferencias.

- b. Asesoramiento y guía - Un programa efectivo de asesoramiento debe identificar las debilidades y limitaciones individuales del personal.

Se requiere de un plan de acción para corregir las debilidades del empleado.

El gerente de auditoría de sistemas debe entender los objetivos de la carrera de cada empleado y trabajar con base en la consecución de esos objetivos.

El asesoramiento debe de ayudar al mejoramiento total del desempeño de los empleados.

Si las técnicas de asesoramiento y guía son utilizados en forma efectiva, motivarán al auditor de sistemas a acelerar su capacidad de aprendizaje y habilidades para avanzar dentro de la organización.

- c. Desarrollo - El auditor de sistemas debe desarrollarse para poder ir asumiendo cada vez tareas más complejas. Esto se puede lograr a través de una diversificación que le permita llegar familiarizarse y conocer los problemas en otras áreas de las funciones de auditoría de sistemas de información.

El supervisor de auditoría de sistemas debe darse en cuenta que la posición que el ocupa es muy fuerte para desarrollar subordinados. Debe explotar su habilidad para llevarse bien con la gente. También, es muy importante que se exprese claramente y venda ideas de soluciones a problemas a los auditados.

El gerente de auditoría de sistemas de información debe delegar lo máximo posible en sus subordinados varias funciones con el propósito de desarrollar sus capacidades.

En forma periódica, el gerente de auditoría de sistemas de información debe efectuar una evaluación del desempeño de sus empleados para efectos de ascensos, aumentos, traslados, etc. Con descripciones de funciones de cada puesto y con base en ellas evaluar a su personal.

La función más importante que debe ejercer el auditor de sistemas es conducir los programas de trabajo de auditoría en una forma muy profesional utilizando un criterio sano.

El sentido común y un acercamiento práctico debe aplicarse durante el desarrollo de la auditoría.

Cualquier atraso, problemas, cambios en el enfoque del trabajo o hallazgos inusuales, deben ser comunicados y aprobados por el gerente de auditoría de sistemas y los auditados.

El auditor de sistemas debe ser una persona con mentalidad amplia, ético y objetivo. Se deben establecer buenas relaciones de trabajo entre el auditor de sistemas y los auditados para que las intervenciones sean exitosas.

Los auditados deben sentir que el auditor de sistemas está tratando de ayudar a corregir problemas y no efectuando una intervención inquisidora.

Para complementar los programas de entrenamiento, el auditor de sistemas debe participar en actividades propias de mejoramiento, tales como pertenecer a asociaciones de auditoría de sistemas, matricularse en cursos formales de procesamiento electrónico de datos, obtener un título profesional o técnico en auditoría informática.

Es muy importante que en el desempeño de sus funciones, el auditor de sistemas se conduzca de una forma profesional muy alta, basado en el código de conducta descrito al final de este módulo.

- d. Herramientas y técnicas gerenciales de auditoría - Las siguientes son algunas herramientas gerenciales de auditoría, técnicas y fuentes de información que serán utilizadas por el gerente de auditoría de sistemas de información.

- **Fuentes de información:**

- Manual de políticas y procedimientos de la organización
- Manual de estándares, políticas y procedimientos del área de TI
- Manual de auditoría de sistemas de información
- Planes a corto y largo plazo de la organización
- Planes a corto y largo plazo de procesamiento electrónico de datos
- Planes a corto y largo plazo de auditoría de sistemas de información.
- Cartas de gerencia y correspondencia de la auditoría externa.

- Minutas de las reuniones del comité de sistemas
- Planes a corto y largo plazo de auditoría interna
- Perfiles de la instalación de cómputo
- Perfiles de aplicaciones nuevas, en desarrollo y operación.
- Matriz de planeación de la auditoría de sistemas.
- Organigrama del Area de TI y de otros departamentos.
- Archivo permanente del auditor de sistemas.
- **Herramientas y técnicas gerenciales de auditoría**
  - Guía de chequeo de auditoría
  - Cuestionario de control interno
  - Entrevistas
  - Observaciones

## **EVALUACIÓN AMBIENTE DE CONTROL AL NIVEL DE TECNOLOGÍA DE INFORMACIÓN**

### **Enfoque**

Aseguramiento de la utilización eficiente de los Recursos de TI -. Debido a la gran dependencia que se tiene de los Recursos de Tecnología de Información como herramienta para el logro de los objetivos del negocio, es necesario garantizar que dichos recursos están siendo utilizados en forma eficiente y efectiva. Los recursos de TI incluyen toda la plataforma tecnológica y la función general de la Dirección de Tecnología de Información en sus diferentes áreas.

### **Objetivo General**

Evaluar si se cuenta con el ambiente de control necesario que satisfaga los objetivos del negocio, establecidos para el Area de Tecnología de Información y la Corporación en General.

### **Objetivos Básicos de Control**

Una estructura apropiada de controles generales que soporte la confianza en los controles específicos, debe satisfacer como mínimo los siguientes objetivos básicos:

1. Principio de confidencialidad: Proteger los datos y la información que residen en los sistemas en producción y desarrollo para garantizar que personas no autorizadas no puedan accederlos.
2. Principio de acceso basado en la necesidad de conocer: Dar acceso a los usuarios del sistema a únicamente aquella información o programas que necesiten para ejecutar sus funciones de trabajo asignadas.
3. Principio de segregación de funciones: Contar con una adecuada segregación de funciones (y rotación de puestos) para garantizar que una transacción no pueda ser manipulada para beneficio personal. En particular, la separación de ambientes de producción y desarrollo, así como el procedimiento de cambios/mejoras a los sistemas, son aspectos necesarios para alcanzar una adecuada segregación de funciones.
4. Principio de disponibilidad: Los sistemas de cómputo estarán disponibles cuando los usuarios autorizados los necesiten.

### **Alcance**

- Controles Generales
- Políticas y Procedimientos Internos
- Segregación de funciones
- Seguridad Física y Lógica
- Administración de Proyectos TI
- Servicio al Cliente
- Desarrollo y Mantenimiento de Sistemas
- Plan de Contingencia y Recuperación en caso de Desastre

# **ANEXO B**

## **CUESTIONARIOS**

Con la definición de las aéreas y los objetivos de control COBIT para las auditorías, se detectaron los siguientes cuestionarios a utilizar en las auditorías de sistemas de información.

## **1. Recursos Humanos**

1.1 ¿Es suficiente el número de personal para el desarrollo de las funciones del área?

- Si
- No

1.2 ¿Se deja de realizar alguna actividad por falta de personal?

- Si
- No

1.3 ¿Está capacitado el personal para realizar con eficiencia sus funciones?

- Si
- No

1.4 ¿Es eficiente el personal en el cumplimiento de sus funciones?

- Si
- No

1.5 ¿Es frecuente la repetición de trabajos encomendados?

- Si
- No

1.6 ¿El personal es discreto en el manejo de información confidencial?

- Si
- No

1.7 ¿Respetan el personal la autoridad establecida?

- Si
- No

1.8 ¿Existe colaboración del personal para la realización del trabajo?

- Si
- No

1.9 ¿Los programas de capacitación incluyen al personal de?

- Dirección
- Análisis
- Programación
- Operación
- Administración
- DBA
- Redes
- Otros

1.10 ¿En general se adapta el personal al mejoramiento administrativo?

- Si
- No

1.11 ¿En promedio cual es el grado de asistencia y puntualidad del personal?

- Bueno
- Malo
- Regular

1.12 ¿Existe una política de sanción disciplinaria del personal?

- Si
- No

1.13 ¿Existe un proceso formal de comunicación interna entre el personal Informático?

- Cuál es el sistema?
- Cuáles son los obstáculos principales de comunicación entre el personal informático?

1.14 ¿Son adecuadas las condiciones ambientales con respecto a?

- Espacio del área
- Iluminación
- Ventilación
- Mobiliario
- Ruido
- Limpieza y aseo
- Instalación sanitaria
- Instalación de comunicaciones

## 2. Sistemas en desarrollo

2.1 ¿Cuáles son los sistemas que actualmente están en desarrollo?

- Nombre de cada uno
- Breve descripción funcional
- Etapa del desarrollo

2.2 ¿Existe un plan maestro de sistemas?

- Si
- No

2.3 ¿Está relacionado el plan de desarrollo de sistemas con el plan general de desarrollo de la dependencia?

- Si
- No

2.4 ¿Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios?

- Si
- No

2.5 ¿Se llevan a cabo revisiones periódicas de los sistemas en desarrollo para determinar si cumplen los objetivos?

- De análisis
- De programación
- Otros

## 2.6 ¿Quien interviene al diseñar un sistema?

- Usuario
- Analista
- Gerente
- DBA
- Personal de comunicaciones
- Auditores internos
- Asesores
- Otros

## 2.7 ¿Existe un procedimiento formal para realizar las pruebas?

- Si
- No

## 2.8 ¿Participan los usuarios en el proceso de testing?

- Si
- No

## 2.9 ¿Existe un procedimiento formal para realizar la conversión de datos de un sistema en retiro a un nuevo sistema?

- Si
- No

2.10 ¿Existe un procedimiento formal para realizar la implantación de los nuevos sistemas?

- Si
- No

2.11 ¿El software utilizado para el desarrollo de sistemas es legal?

- Si
- No
- Open source

2.12 ¿El motor de base de datos es legal?

- SI
- NO
- Open source

2.13 ¿La función de aseguramiento de la calidad en el desarrollo de sistemas contempla?

- Puntos de revisión en el análisis
- Puntos de revisión en el diseño
- Puntos de revisión en la construcción
- Puntos de revisión en las pruebas
- Puntos de revisión en la implementación

### 3. Operación y soporte

2.1 ¿Cuáles son los sistemas que se operan actualmente?

- Nombre
- Breve descripción funcional
- Lenguaje
- Motor de base de datos
- Fecha de desarrollo
- Desarrollador
- Última actualización
- Ubicación

2.2 ¿La arquitectura del procesamiento es?

- Centralizada
- Descentralizada
- Mixta

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

- Si
- No

2.4 ¿Quién controla la entrada del documento fuente?

- Quien carga
- Otra persona
- No se controla

2.5 ¿Cuándo la carga de trabajo supera la capacidad instalada se requiere?

- Tiempo extra
- Se subcontrata

2.6 ¿Se verifica la calidad de la información recibida para su captura?

- Si
- No

2.7 ¿Existe un procedimiento escrito que indique como tratar la información inválida?

- Si
- No

2.8 ¿Los documentos fuentes de entrada se guardan en lugar seguro?

- Si
- No

2.9 ¿Se controlan separadamente los documentos confidenciales?

- Si
- No

2.10 ¿Se aprovecha adecuadamente el papel de los listados inservibles?

- Si
- No

2.11 ¿Existen procedimientos formales para lo operación de los sistemas?

- Si
- No

2.12 ¿Los retrasos o incumplimientos del programa de operación diaria, se revisa y analiza?

- Si
- No

2.13 ¿Existe un procedimiento formal para la recuperación del sistema en caso de fallas?

- Si
- No

2.14 ¿Opera el personal del área de informática los sistemas en producción?

- Si
- No

#### **4. Hardware**

3.1 ¿Cuántas computadoras, servidores, y periféricos se tienen conectados a la red?

- Cantidad
- Tipo

4.2 ¿Existe un comité para la compra de hardware?

- Si
- No

4.3 ¿Existen políticas formales de adquisición de equipos?

- Si
- No

4.4 ¿El mantenimiento del hardware es?

- Propio
- Por Terceros
- Mixto

4.5 ¿Existe un listado formal del hardware?

- Si
- No

4.6 ¿Se cuenta con manuales técnicos del hardware instalado?

- Servidores
- Estaciones de trabajo
- Otros

4.7 ¿Existe un procedimiento formal para el mantenimiento del hardware?

- Si
- No

## 5. Software

5.1 ¿Hay una lista del software existente en la organización?

- Si
- No

5.2 ¿Se cuenta con manuales del software?

- Si
- No

5.3 ¿Existe un procedimiento formal para actualizar el software instalado en las estaciones de trabajo?

- Si
- No

5.4 ¿Está identificado el software original y las copias?

- Si
- No

5.5 ¿Hay una lista actualizada del software instalado en cada estación de trabajo?

- Si
- No

## 6. Seguridad lógica y física

6.1 ¿El control de acceso a los sistemas está dada por?

- Seguridad del sistema operativo
- Seguridad del sistema
- Ldap
- Ambas
- Otras

6.2 ¿La validación de acceso a los sistemas está dada por?

- Claves de acceso
- Credencial
- Huella dactilar

- Retina
- Voz
- Retina
- Otros

6.3 ¿Cada cuanto se cambian las claves de acceso a los sistemas?

- Semanalmente
- Mensualmente
- Semestralmente
- Anualmente
- Otros

6.4 ¿Cada cuanto se cambian las claves de administradores de los sistemas?

- Semanalmente
- Mensualmente
- Semestralmente
- Anualmente
- Otros

6.5 ¿Cada cuanto se cambian las claves de DBA?

- Semanalmente
- Mensualmente
- Semestralmente
- Anualmente

- 6.6 ¿Las claves de acceso a los sistemas se encuentran almacenadas en algún lugar?
- Si
  - No
- 6.7 ¿Las claves de acceso de los administradores de los sistemas se encuentran almacenadas en algún lugar?
- Si
  - No
- 6.8 ¿Las claves de acceso de los DBA se encuentran almacenadas en algún lugar?
- Si
  - No
- 6.9 ¿Existe acceso a Internet?
- Desde los servidores
  - Desde las estaciones de trabajo
- 6.10 ¿Se encriptan las bases de datos?
- Si
  - No
- 6.11 ¿Existe un plan de contingencias?
- Si
  - No

6.12 ¿Existe una política de prevención contra virus?

- Si
- No

## **7. Parámetros de medición**

7.1 Se tiene un procedimiento formal de seguimiento al desempeño del personal informático, Indique si dicho procedimiento contempla los siguientes puntos

- Parámetros de medición por puesto
- Parámetros de medición por función
- Objetivos y alcances de cada puesto
- Resultados esperados de cada puesto
- Tiempo esperado para la ejecución de cada función
- Responsables de dar seguimiento a cada puesto
- Encuestas a usuarios al final de cada proyecto

# **ANEXO C**

**Listas de Verificación**

Ejemplo de lista de verificación divididas por áreas, dominio y procesos COBIT tomando como base los cuestionarios del anexo anterior.

<b>PREGUNTA</b>
¿Es suficiente el número de personal para el desarrollo de las funciones del área? <ul style="list-style-type: none"><li>• Si</li><li>• No</li></ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"><li>• Recursos Humanos</li></ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"><li>• Planeación y organización</li></ul>
<b>PROCESO</b>
<ul style="list-style-type: none"><li>• Administrar los recursos humanos</li></ul>

<b>PREGUNTA</b>
¿Se deja de realizar alguna actividad por falta de personal? <ul style="list-style-type: none"><li>• Si</li><li>• No</li></ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"><li>• Recursos Humanos</li></ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"><li>• Planeación y organización</li></ul>
<b>PROCESO</b>
<ul style="list-style-type: none"><li>• Administrar los recursos humanos</li></ul>

<b>PREGUNTA</b>
¿Es eficiente el personal en el cumplimiento de sus funciones? <ul style="list-style-type: none"><li>• Si</li><li>• No</li></ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"><li>• Recursos Humanos</li></ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"><li>• Planeación y organización</li></ul>
<b>PROCESO</b>
<ul style="list-style-type: none"><li>• Administrar los recursos humanos</li></ul>

<b>PREGUNTA</b>
¿Es frecuente la repetición de trabajos encomendados? <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Recursos Humanos</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Planeación y organización</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Definir la Organización y las Relaciones TI</li> </ul>

<b>PREGUNTA</b>
El personal es discreto en el manejo de información confidencial <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Recursos Humanos</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Planeación y organización</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Evaluar Riesgos</li> </ul>

<b>PREGUNTA</b>
Los programas de capacitación incluyen al personal de <ul style="list-style-type: none"> <li>• Dirección</li> <li>• Análisis</li> <li>• Programación</li> <li>• Operación</li> <li>• Administración</li> <li>• Redes</li> <li>• Otros</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Recursos Humanos</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Planeación y organización</li> </ul>
<b>PROCESO</b>

<ul style="list-style-type: none"> <li>• Administrar los recursos humanos</li> </ul>
<b>PREGUNTA</b>
<p>En general se adapta el personal al mejoramiento administrativo</p> <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Recursos Humanos</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Planeación y organización</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Comunicar los objetivos y rumbos administrativos</li> </ul>

<b>PREGUNTA</b>
<p>Existe un proceso formal de comunicación interna entre el personal Informático</p> <ul style="list-style-type: none"> <li>• Cuál es el sistema</li> <li>• Cuáles son los obstáculos principales de comunicación entre el personal informático</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Recursos Humanos</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Planeación y organización</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Definir la organización y las relaciones de TI</li> </ul>

<b>PREGUNTA</b>
<p>¿Cuáles son los sistemas que actualmente están en desarrollo?</p> <ul style="list-style-type: none"> <li>• Nombre de cada uno</li> <li>• Breve descripción funcional</li> <li>• Etapa del desarrollo</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Sistemas en desarrollo</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Adquisición e implementación</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Identificar las soluciones</li> </ul>

<b>PREGUNTA</b>
Existe un plan maestro de sistemas <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Sistemas en desarrollo</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Planeación y organización</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Administrar los proyectos</li> </ul>

<b>PREGUNTA</b>
Está relacionado el plan de desarrollo de sistemas con el plan general de desarrollo de la dependencia <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Sistemas en desarrollo</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Planeación Y organización</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Administrar los proyectos</li> </ul>

<b>PREGUNTA</b>
Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Sistemas en desarrollo</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Planeación Y organización</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Administrar los proyectos</li> </ul>

<b>PREGUNTA</b>
Se llevan a cabo revisiones periódicas de los sistemas en desarrollo para determinar si cumplen los objetivos. <ul style="list-style-type: none"> <li>• De análisis</li> <li>• De programación</li> <li>• Otros</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Sistemas en desarrollo</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Adquisición e Implementación</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Manejar los cambios</li> </ul>

<b>PREGUNTA</b>
Quien interviene al diseñar un sistema <ul style="list-style-type: none"> <li>• Usuario</li> <li>• Analista</li> <li>• Gerente</li> <li>• DBA</li> <li>• Personal de comunicaciones</li> <li>• Auditores internos</li> <li>• Asesores</li> <li>• Otros</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Sistemas en desarrollo</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Adquisición e Implementación</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Adquirir y dar mantenimiento al software de aplicación</li> </ul>

<b>PREGUNTA</b>
Existe un procedimiento formal para realizar las pruebas <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Sistemas en desarrollo</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Adquisición e Implementación</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Instalar y Acreditar los sistemas</li> </ul>

<b>PREGUNTA</b>
El software utilizado para el desarrollo de sistemas es legal <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> <li>• Open source</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Sistemas en desarrollo</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Adquisición e Implementación</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Adquirir y dar mantenimiento a la arquitectura tecnológica.</li> </ul>

<b>PREGUNTA</b>
El motor de base de datos es legal <ul style="list-style-type: none"> <li>• SI</li> <li>• NO</li> <li>• Open Source</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Sistemas en desarrollo</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Adquisición e Implementación</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Adquirir y dar mantenimiento a la arquitectura tecnológica.</li> </ul>

<b>PREGUNTA</b>
La función de aseguramiento de la calidad en el desarrollo de sistemas contempla <ul style="list-style-type: none"> <li>• Puntos de revisión en el análisis</li> <li>• Puntos de revisión en el diseño</li> <li>• Puntos de revisión en la construcción</li> <li>• Puntos de revisión en las pruebas</li> <li>• Puntos de revisión en la implementación</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Sistemas en desarrollo</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Planeación y Organización</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Administrar la calidad</li> </ul>

<b>PREGUNTA</b>
Existen normas que definan el contenido de los instructivos de captación de datos <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Operación y soporte</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Suministro y soporte</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Manejar los datos</li> </ul>

<b>PREGUNTA</b>
Quien controla la entrada del documento fuente <ul style="list-style-type: none"> <li>• Quien carga</li> <li>• Otra persona</li> <li>• No se controla</li> </ul>
<b>TIPO DE AUDITORÍA</b>
<ul style="list-style-type: none"> <li>• Operación y soporte</li> </ul>
<b>DOMINIO</b>
<ul style="list-style-type: none"> <li>• Suministro y soporte</li> </ul>
<b>PROCESO</b>
<ul style="list-style-type: none"> <li>• Manejar los datos</li> </ul>

<b>PREGUNTA</b>
<p>Cuando la carga de trabajo supera la capacidad instalada se requiere</p> <ul style="list-style-type: none"> <li>• Tiempo extra</li> <li>• Se subcontrata</li> </ul>
<b>TIPO DE AUDITORÍA</b>
• Operación y soporte
<b>DOMINIO</b>
• Suministro y soporte
<b>PROCESO</b>
• Manejar los problemas e incidentes

<b>PREGUNTA</b>
<p>Existe un procedimiento escrito que indique como tratar la información invalida</p> <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>
<b>TIPO DE AUDITORÍA</b>
• Operación y soporte
<b>DOMINIO</b>
• Suministro y soporte
<b>PROCESO</b>
• Manejar los datos
<b>PREGUNTA</b>
<p>Se aprovecha adecuadamente el papel de los listados inservibles</p> <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>
<b>TIPO DE AUDITORÍA</b>
• Operación y soporte
<b>DOMINIO</b>
• Suministro y soporte
<b>PROCESO</b>
• Asegurar la seguridad de los sistemas

<b>PREGUNTA</b>
<p>Existen procedimientos formales para lo operación de los sistemas</p> <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>

<b>TIPO DE AUDITORÍA</b>
• Operación y soporte
<b>DOMINIO</b>
• Suministro y soporte
<b>PROCESO</b>
• Manejar las operaciones

<b>PREGUNTA</b>
Los retrasos o incumplimientos del programa de operación diaria, se revisa y analiza. <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>
<b>TIPO DE AUDITORÍA</b>
• Operación y soporte
<b>DOMINIO</b>
• Suministro y soporte
<b>PROCESO</b>
• Manejar las operaciones

<b>PREGUNTA</b>
Cuántas computadoras, servidores, y periféricos se tienen conectados a la red <ul style="list-style-type: none"> <li>• Cantidad</li> <li>• Tipo</li> </ul>
<b>TIPO DE AUDITORÍA</b>
• Hardware
<b>DOMINIO</b>
• Planeación y organización
<b>PROCESO</b>
• Determinar el rumbo tecnológico

<b>PREGUNTA</b>
Existen políticas formales de adquisición de equipos <ul style="list-style-type: none"> <li>• Si</li> <li>• No</li> </ul>
<b>TIPO DE AUDITORÍA</b>
• Hardware
<b>DOMINIO</b>
• Suministro y soporte
<b>PROCESO</b>
• Manejar los servicios de terceros

---

**PREGUNTA**

---

El mantenimiento del hardware es

- Propio
- Terceros
- Mixto

---

**TIPO DE AUDITORÍA**

---

• Hardware

---

**DOMINIO**

---

• Planeación y organización

---

**PROCESO**

---

• Determinar el rumbo tecnológico

---

---

**PREGUNTA**

---

Se cuenta con manuales técnicos del hardware instalado

- Servidores
- Estaciones de trabajo
- Otros

---

**TIPO DE AUDITORÍA**

---

• Hardware

---

**DOMINIO**

---

• Planeación y organización

---

**PROCESO**

---

• Determinar el rumbo tecnológico

---

---

**PREGUNTA**

---

Existe un procedimiento formal para el mantenimiento del hardware

- Si
- No

---

**TIPO DE AUDITORÍA**

---

• Hardware

---

**DOMINIO**

---

• Planeación y organización

---

**PROCESO**

---

• Determinar el rumbo tecnológico

---

---

**PREGUNTA**

---

Cada cuanto se cambian las claves de acceso a los sistemas

- Semanalmente
- Mensualmente
- Semestralmente
- Anualmente o Otros

---

**TIPO DE AUDITORÍA**

- 
- Seguridad lógica y física

---

**DOMINIO**

- 
- Suministro y soporte

---

**PROCESO**

- 
- Asegurar la seguridad de los sistemas
- 

---

**PREGUNTA**

Cada cuanto se cambian las claves de administradores de los sistemas

- Semanalmente
- Mensualmente
- Semestralmente
- Anualmente
- Otros

---

**TIPO DE AUDITORÍA**

- 
- Seguridad lógica y física

---

**DOMINIO**

- 
- **Suministro y soporte**

---

**PROCESO**

- 
- Asegurar la seguridad de los sistemas
- 

---

**PREGUNTA**

Las claves de acceso a los sistemas se encuentran almacenadas en algún lugar

- Si
- No

---

**TIPO DE AUDITORÍA**

- 
- Seguridad lógica y física

---

**DOMINIO**

- 
- Suministro y soporte

---

**PROCESO**

- 
- Asegurar la seguridad de los sistemas
- 

---

**PREGUNTA**

Las claves de acceso de los dba se encuentran almacenadas en algún lugar

- Si
- No

**TIPO DE AUDITORÍA**

- Seguridad lógica y física

**DOMINIO**

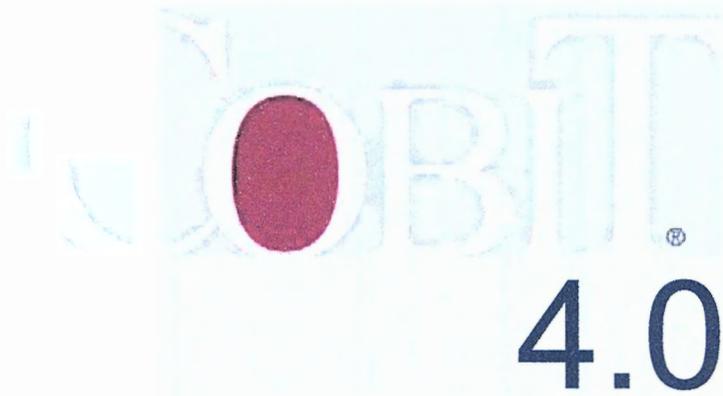
- Suministro y soporte

**PROCESO**

- Asegurar la seguridad de los sistemas

# **ANEXO D**

**COBIT 4.0**



COSO  
4.0

Objetivos de Control  
Directrices Gerenciales  
Modelos de Madurez

# RESUMEN EJECUTIVO

Para muchas empresas, la información y la tecnología que las soportan representan sus más valiosos activos, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI.

La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del gobierno de la empresa. El valor, el riesgo y el control constituyen la esencia del gobierno de TI.

**El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que la TI de la empresa sostiene y extiende las estrategias y objetivos organizacionales.**

Más aún, el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI de la empresa sirve como base a los objetivos del negocio. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas. Estos resultados requieren un marco de referencia para controlar la TI, que se ajuste y sirva como soporte al Committee Of Sponsoring Organisations Of The Treadway Commission *Control interno—Marco de Referencia integrado*, el marco de referencia de control ampliamente aceptado por gobierno de la empresa y para la administración de riesgos, así como a marcos compatibles similares.

Las organizaciones deben satisfacer la calidad, los requerimientos fiduciarios y de seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas. Para descargar estas responsabilidades, así como para lograr sus objetivos, la dirección debe entender el estatus de su arquitectura empresarial para la TI y decidir qué tipo de gobierno y de control debe aplicar.

*Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT\*)* brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones facilitadas por la TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

Para que la TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implantar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

- Estableciendo un vínculo con los requerimientos del negocio
- Organizando las actividades de TI en un modelo de procesos generalmente aceptado
- Identificando los principales recursos de TI a ser utilizados
- Definiendo los objetivos de control gerenciales a ser considerados

La orientación al negocio que enfoca COBIT consiste en vincular las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los propietarios de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

En resumen, para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural.

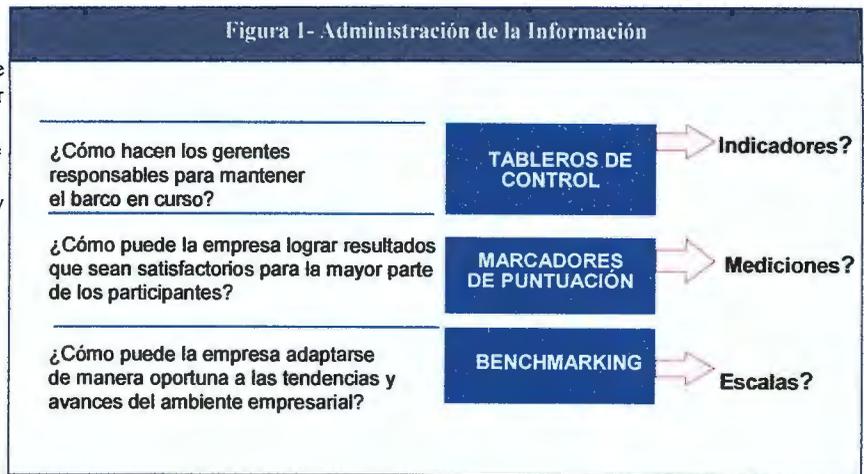
Pero, ¿cómo puede la empresa poner bajo control la TI de tal manera que genere la información que la empresa necesita? ¿Cómo puede administrar los riesgos y asegurar los recursos de TI de los cuales depende tanto? ¿Cómo puede la empresa asegurar que TI logre sus objetivos y soporte los del negocio?

Primero, la dirección requiere objetivos de control que definan la última meta de implantar políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar un nivel razonable para garantizar que:

- Se alcancen los objetivos del negocio.
- Se prevengan o se detecten y corrijan los eventos no deseados.

En segundo lugar, en los complejos ambientes de hoy en día, la dirección busca continuamente información oportuna y condensada, para tomar decisiones difíciles respecto a riesgos y controles, de manera rápida y exitosa. ¿Qué se debe medir y cómo? Las empresas requieren una medición objetiva de dónde se encuentran y dónde se requieren mejoras, y deben implantar una caja de herramientas gerenciales para monitorear esta mejora.

La **figura 1** muestra algunas preguntas frecuentes y las herramientas gerenciales de información usadas para encontrar las respuestas, aunque estos tableros de control requieren indicadores, los marcadores de puntuación requieren mediciones y los Benchmarking requieren una escala de comparación.



Una respuesta a los requerimientos de determinar y monitorear el nivel apropiado de control y desempeño de TI son las definiciones específicas de COBIT de los siguientes conceptos:

- **Benchmarking** de la capacidad de los procesos de TI, expresada como modelos de madurez, derivados del Modelo de Madurez de la Capacidad del Instituto de Ingeniería de Software
- **Metas y métricas** de los procesos de TI para definir y medir sus resultados y su desempeño, basados en los principios de balanced business Scorecard de Robert Kaplan y David Norton
- **Metas de actividades** para controlar estos procesos, con base en los objetivos de control detallados de COBIT

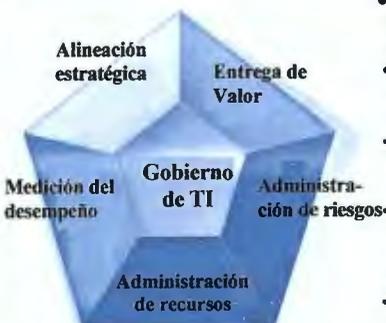
La evaluación de la capacidad de los procesos basada en los modelos de madurez de COBIT es una parte clave de la implementación del gobierno de TI. Después de identificar los procesos y controles críticos de TI, el modelado de la madurez permite identificar y demostrar a la dirección las brechas en la capacidad. Entonces se pueden crear planes de acción para llevar estos procesos hasta el nivel objetivo de capacidad deseado.

COBIT da soporte al gobierno de TI (**figura 2**) al brindar un marco de trabajo que garantiza que:

- TI está alineada con el negocio
- TI capacita el negocio y maximiza los beneficios
- Los recursos de TI se usen de manera responsable
- Los riesgos de TI se administren apropiadamente

La medición del desempeño es esencial para el gobierno de TI. COBIT le da soporte e incluye el establecimiento y el monitoreo de objetivos que se puedan medir, referentes a lo que los procesos de TI requieren generar (resultado del proceso) y cómo lo generan (capacidad y desempeño del proceso). Muchos estudios han identificado que la falta de transparencia en los costos, valor y riesgos de TI, es uno de los más importantes impulsores para el gobierno de TI. Mientras las otras áreas consideradas contribuyen, la transparencia se logra de forma principal por medio de la medición del desempeño.

**Figura 2 – Áreas Focales del Gobierno de TI**



- **Alineación estratégica** se enfoca en garantizar el vínculo entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.
- **Entrega de valor** se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.
- **Administración de recursos** se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI: aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.
- **Administración de riesgos** requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del deseo de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.
- **Medición del desempeño** rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas que se puedan medir más allá del registro convencional.

Estas áreas focales de gobierno de TI describen los tópicos en los que la dirección ejecutiva requiere poner atención para gobernar la TI en sus empresas. La dirección operacional usa procesos para organizar y administrar las actividades cotidianas de TI. COBIT brinda un modelo de procesos genéricos que representa todos los procesos que normalmente se encuentran en las funciones de TI, ofreciendo un modelo de referencia común entendible para los gerentes operacionales de IT y del negocio. Se establecieron equivalencias entre los modelos de procesos COBIT y las áreas focales del gobierno de TI (vea apéndice II), ofreciendo así un puente entre lo que los gerentes operacionales deben realizar y lo que los ejecutivos desean gobernar.

Para lograr un gobierno efectivo, los ejecutivos esperan que los controles a ser implementados por los gerentes operacionales se encuentren dentro de un marco de control definido para todo los procesos de TI. Los objetivos de control de TI de COBIT están organizados por proceso de TI; por lo tanto, el marco de trabajo brinda un vínculo claro entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

COBIT se enfoca en qué se requiere para lograr una administración y un control adecuado de TI, y se posiciona en un nivel alto. COBIT ha sido alineado y armonizado con otros estándares y mejores prácticas más detallados de TI, (vea apéndice IV). COBIT actúa como un integrador de todos estos materiales guía, resumiendo los objetivos clave bajo un mismo marco de trabajo integral que también se vincula con los requerimientos de gobierno y de negocios.

COSO (y similares marcos de trabajo) es generalmente aceptado como el marco de trabajo de control interno para las empresas. COBIT es el marco de trabajo de control interno generalmente aceptado para TI.

Los productos COBIT se han organizado en tres niveles (figura 3) diseñados para dar soporte a:

- Administración y consejos ejecutivos
- Administración del negocio y de TI
- Profesionales en Gobierno, aseguramiento, control y seguridad.

Es de interés primordial para los ejecutivos:

- *El resumen informativo al consejo sobre el gobierno de TI, 2da Edición*—Diseñado para ayudar a los ejecutivos a entender porqué el gobierno de TI es importante, cuáles son sus intereses y sus responsabilidades para su administración

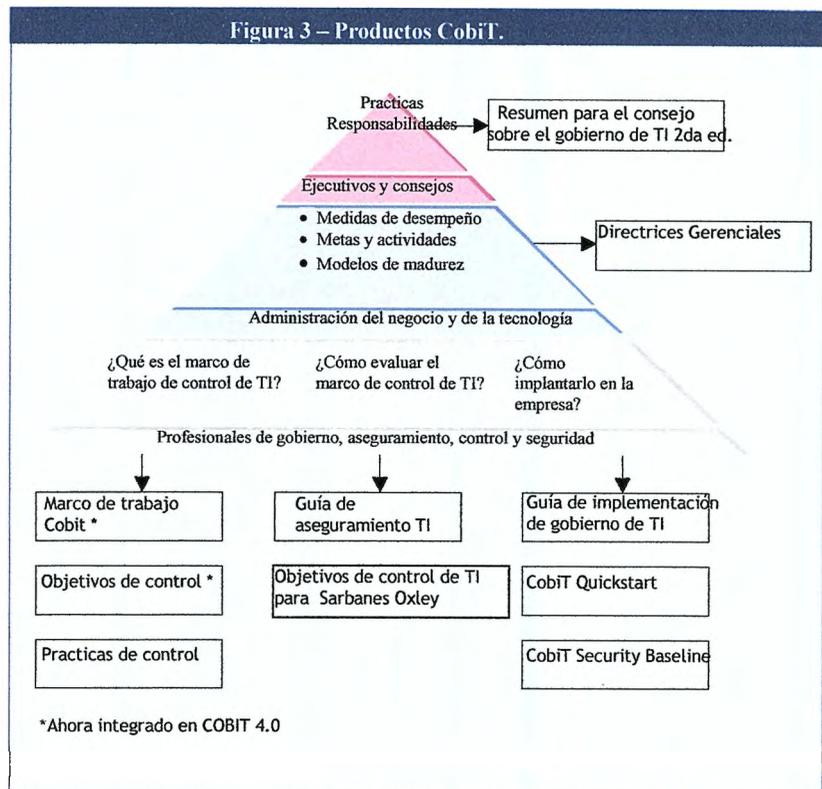
Es de primordial interés para la dirección del negocio y de tecnología:

- *Directrices Gerenciales*—Herramientas para ayudar a asignar responsabilidades, medir el desempeño, llevar a cabo benchmarks y manejar brechas en la capacidad. Las directrices ayudan a brindar respuestas a preguntas comunes de la administración: ¿Qué tan lejos podemos llegar para controlar la TI?, y ¿el costo justifica el beneficio? ¿Cuáles son los indicadores de un buen desempeño? ¿Cuáles son las prácticas administrativas clave a aplicar? ¿Qué hacen otros? ¿Cómo medimos y comparamos?

Es de primordial interés para los profesionales de gobierno, aseguramiento, control y seguridad:

- *Marco de Referencia*—Explicar cómo COBIT organiza los objetivos de gobierno y las mejores prácticas de TI con base en dominios y procesos de TI, y los vincula a los requerimientos del negocio
- *Objetivos de control*—Brindar objetivos a la dirección basados en las mejores prácticas genéricas para todas las actividades de TI
- *Prácticas de control*—Brindar guía de por qué vale la pena implementar controles y cómo implantarlos
- *Guía de aseguramiento de TI*—Ofrecer un enfoque genérico de auditoría y una guía de soporte para la auditoría de todos los procesos TI de COBIT
- *Objetivos de control de IT para Sarbanes-Oxley*—Proporcionar una guía sobre cómo garantizar el cumplimiento para el ambiente de TI basado en los objetivos de control COBIT
- *Guía de implementación del Gobierno de TI*—Ofrecer un mapa genérico para implementar el gobierno de TI usando los recursos COBIT y un juego de herramientas de soporte
- *COBIT Quickstart*<sup>TM</sup>—Brindar una línea base de control para pequeñas organizaciones y un posible primer paso para las grandes
- *COBIT Security Baseline*<sup>TM</sup>—Enfocar la organización a los pasos esenciales para implementar la seguridad de la información dentro de la Empresa

Figura 3 – Productos CobIT.





# MARCO DE TRABAJO COBIT

## LA NECESIDAD DE UN MARCO DE TRABAJO PARA EL CONTROL DEL GOBIERNO DE TI

### *Por qué*

Cada vez más, la alta dirección se está dando cuenta del impacto significativo que la información puede tener en el éxito de una empresa. La dirección espera un alto entendimiento de la manera en que la tecnología de información (TI) es operada y de la posibilidad de que sea aprovechada con éxito para tener una ventaja competitiva. En particular, la alta dirección necesita saber si con la información administrada en la empresa es posible que:

- Garantice el logro de sus objetivos
- Tenga suficiente flexibilidad para aprender y adaptarse
- Cuente con un manejo juicioso de los riesgos que enfrenta
- Reconozca de forma apropiada las oportunidades y actúe de acuerdo a ellas

Las empresas exitosas entienden los riesgos y aprovechan los beneficios de TI, y encuentran maneras para:

- Alinear la estrategia de TI con la estrategia del negocio
- Lograr que toda la estrategia de TI, así como las metas fluyan de forma gradual a toda la empresa
- Proporcionar estructuras organizacionales que faciliten la implementación de estrategias y metas
- Crear relaciones constructivas y comunicaciones efectivas entre el negocio y TI, y con socios externos
- Medir el desempeño de TI

Las empresas no pueden responder de forma efectiva a estos requerimientos de negocio y de gobierno sin adoptar e implementar un marco de Referencia de gobierno y de control para TI, de tal manera que:

- Se forme un vínculo con los requerimientos del negocio
- El desempeño real con respecto a los requerimientos sea transparente
- Organice sus actividades en un modelo de procesos generalmente aceptado
- Identifique los principales recursos a ser aprovechados
- Se definan los objetivos de control Gerenciales a ser considerados

Además, el gobierno y los marcos de trabajo de control están siendo parte de las mejores prácticas de la administración de TI y sirven como facilitadores para establecer el gobierno de TI y cumplir con el constante incremento de requerimientos regulatorios.

Las mejores prácticas de TI se han vuelto significativas debido a un número de factores:

- Directores de negocio y consejos directivos que demandan un mayor retorno de la inversión en TI, es decir, que TI genere lo que el negocio necesita para mejorar el valor de los participantes
- Preocupación por el creciente nivel de gasto en TI
- La necesidad de satisfacer requerimientos regulatorios para controles de TI en áreas como privacidad y reportes financieros (por ejemplo, Sarbanes-Oxley Act, Basel II) y en sectores específicos como el financiero, farmacéutico y de atención a la salud
- La selección de proveedores de servicio y el manejo de Outsourcing y de Adquisición de servicios
- Riesgos crecientemente complejos de la TI como la seguridad de redes
- Iniciativas de gobierno de TI que incluyen la adopción de marcos de referencia de control y de mejores prácticas para ayudar a monitorear y mejorar las actividades críticas de TI, aumentar el valor del negocio y reducir los riesgos de éste
- La necesidad de optimizar costos siguiendo, siempre que sea posible, un enfoque estandarizado en lugar de enfoques desarrollados especialmente
- La madurez creciente y la consecuente aceptación de marcos de trabajo respetados tales como COBIT, ITIL, ISO 17799, ISO 9001, CMM y PRINCE2
- La necesidad de las empresas de valorar su desempeño en comparación con estándares generalmente aceptados y con respecto a su competencia (Benchmarking)

## Quién

Un marco de referencia de gobierno y de control requiere servir a una variedad de interesados internos y externos, cada uno de los cuales tiene necesidades específicas:

- Interesados dentro de la empresa que tengan un interés en generar valor de las inversiones en TI:
  - Aquellos que tomen decisiones de inversiones
  - Aquellos que deciden respecto a los requerimientos
  - Aquellos que utilicen los servicios de TI
- Interesados internos y externos que proporcionen servicios de TI:
  - Aquellos que administren la organización y los procesos de TI
  - Aquellos que desarrollen capacidades
  - Aquellos que operen los servicios
- Interesados internos y externos con responsabilidades de control/riesgo:
  - Aquellos con responsabilidades de seguridad, privacidad y/o riesgo
  - Aquellos que realicen funciones de cumplimiento
  - Aquellos que requieran o proporcionen servicios de aseguramiento

## Qué

Para satisfacer los requerimientos previos, un marco de referencia para el gobierno y el control de TI deben satisfacer las siguientes especificaciones generales:

- Brindar un enfoque de negocios que permita la alineación entre los objetivos de negocio y de TI.
- Establecer una orientación a procesos para definir el alcance y el grado de cobertura, con una estructura definida que permita una fácil navegación en el contenido.
- Ser generalmente aceptable al ser consistente con las mejores prácticas y estándares de TI aceptados, y que sea independiente de tecnologías específicas.
- Proporcionar un lenguaje común, con un juego de términos y definiciones que sean comprensibles en lo general para todos los Interesados.
- Ayudar a satisfacer requerimientos regulatorios, al ser consistente con estándares de gobierno corporativo generalmente aceptados (COSO) y con controles de TI esperados por agentes reguladores y auditores externos.

## COMO SATISFACE COBIT LA NECESIDAD

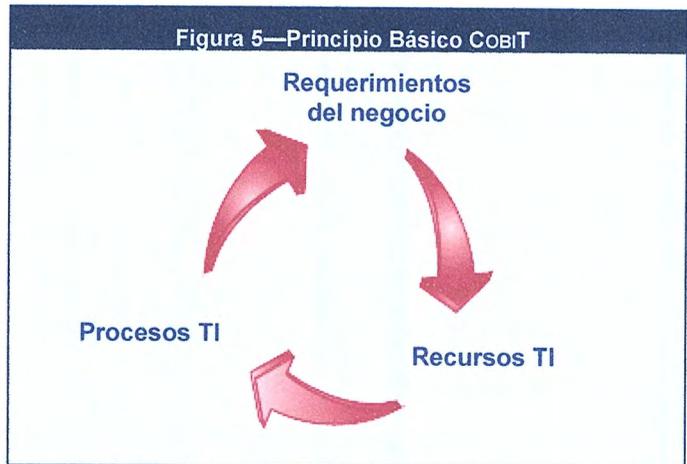
Como respuesta a las necesidades descritas en la sección anterior, el marco de trabajo COBIT se creó con las características principales de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

### Orientado al negocio

La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no solo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los propietarios de los procesos de negocio.

El marco de trabajo COBIT se basa en el siguiente principio (figura 5): proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de información.

El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.



### CRITERIOS DE INFORMACIÓN DE COBIT

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

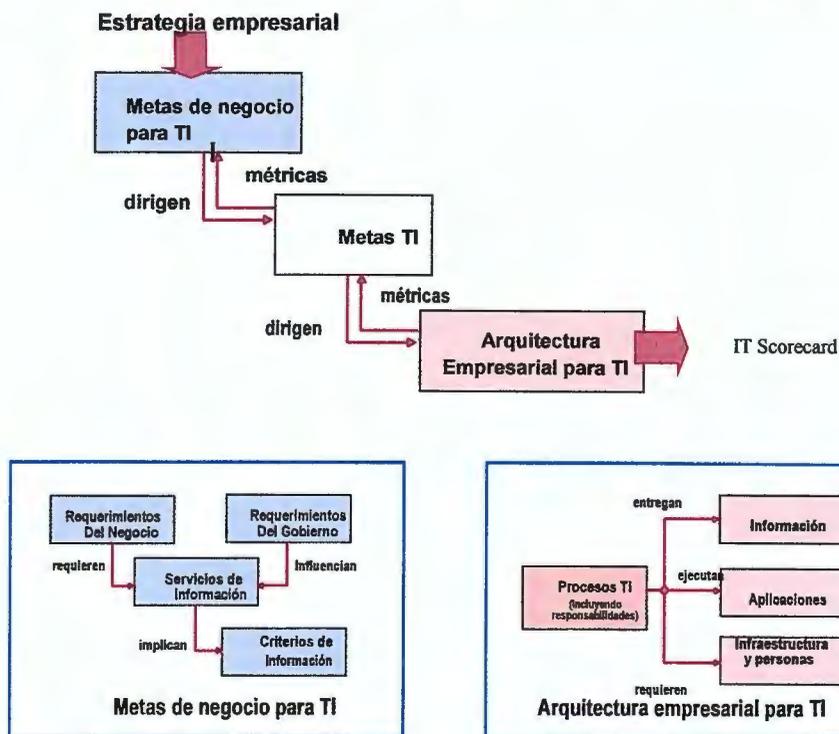
- La efectividad tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- La eficiencia consiste en que la información sea generada optimizando los recursos (más productivo y económico).
- La confidencialidad se refiere a la protección de información sensible contra revelación no autorizada.
- La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne con la protección de los recursos y las capacidades necesarias asociadas.
- El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
- La confiabilidad significa proporcionar la información apropiada para que la gerencia administre la entidad y ejercite sus responsabilidades fiduciarias y de gobierno.

### METAS DE NEGOCIOS Y DE TI

Mientras que los criterios de información proporcionan un método genérico para definir los requerimientos del negocio, la definición de un conjunto de metas genéricas de negocio y de TI ofrece una base más refinada y relacionada con el negocio para el establecimiento de requerimientos de negocio y para el desarrollo de métricas que permitan la medición con respecto a estas metas. Cada empresa usuaria de TI, habilita las iniciativas del negocio y estas pueden ser representadas como metas del negocio para TI. El Apéndice I proporciona una matriz de metas genéricas de negocios y metas de TI y como se asocian con los criterios de la información. Estos ejemplos genéricos se pueden utilizar como guía para determinar los requerimientos, metas y métricas específicas del negocio para la empresa.

Si se pretende que la TI proporcione servicios de forma exitosa para dar soporte a la estrategia de la empresa, debe existir una propiedad y una dirección clara de los requerimientos por parte del negocio (el cliente) y un claro entendimiento para TI, de cómo y qué debe entregar (el proveedor). La Figura 6 ilustra como la estrategia de la empresa se debe traducir por parte del negocio en objetivos para su uso de iniciativas facilitadas por TI (Las metas de negocio para TI). Estos objetivos a su vez, deben conducir a una clara definición de los propios objetivos de la TI (las metas de TI), y luego éstas a su vez definir los recursos y capacidades de TI (la arquitectura empresarial para TI) requeridos para ejecutar de forma exitosa la parte que le corresponde a TI de la estrategia empresarial. Todos estos objetivos se deben expresar en términos de negocios significativos para el cliente, y esto, combinado con una alineación efectiva de la jerarquía de objetivos, asegurará que el negocio pueda confirmar que TI puede, con alta probabilidad, dar soporte a las metas del negocio.

Figura 6—Definiendo metas de TI y arquitectura empresarial para TI



Una vez que las metas alineadas han sido definidas, requieren ser monitoreadas para garantizar que la entrega cumple con las expectativas. Esto se logra con métricas derivadas de las metas y capturadas en scorecard de TI que el cliente pueda entender y seguir, y que permita al proveedor enfocarse en sus propios objetivos internos.

El apéndice I ofrece una visión global de cómo las metas genéricas del negocio se relacionan con las metas de TI, con los procesos de TI y con los criterios de la información. La tabla ayuda a demostrar el alcance de COBIT y la relación general de negocios entre COBIT y los impulsores del negocio.

### RECURSOS DE TI

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio. Estos recursos, junto con los procesos, constituyen una arquitectura empresarial para TI, como se muestra en la figura 6.

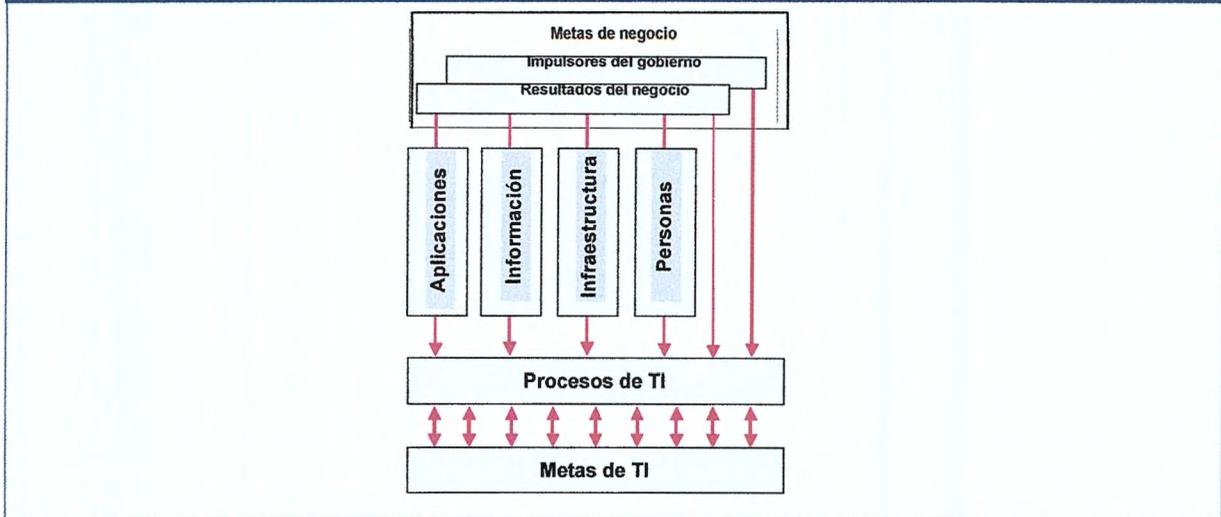
Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una capacidad técnica adecuada (ej., un sistema de planeación de recursos empresariales) para dar soporte a la capacidad del negocio (ej., implementando una cadena de suministro) que genere el resultado deseado (ej., mayores ventas y beneficios financieros).

Los recursos de TI identificados en COBIT se pueden definir como sigue:

- Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- La información son los datos en todas sus formas de entrada, procesados y generados por los sistemas de información, en cualquier forma en que son utilizados por el negocio.
- La infraestructura es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- Las personas son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

La figura 7 resume cómo las metas de negocio para TI influyen la manera en que se manejan los recursos necesarios de TI por parte de los procesos de TI para lograr las metas de TI.

Figura 7. Administración de los recursos de TI para garantizar las metas de TI



### Procesos orientados

COBIT define las actividades de TI en un modelo genérico de procesos en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que cada uno en la empresa visualice y administre las actividades de TI. La incorporación de un modelo operacional y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. También brinda un marco de trabajo para la medición y monitoreo del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas administrativas. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Éstos se pueden resumir como sigue:

#### PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

#### ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

- ¿Los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?
- ¿Los nuevos proyectos son entregados a tiempo y dentro del presupuesto?
- ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
- ¿Los cambios afectarán las operaciones actuales del negocio?

## ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. Por lo general aclara las siguientes preguntas de la gerencia:

- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
- ¿Están optimizados los costos de TI?
- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
- ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

## MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia:

- ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
- ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?
- ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?
- ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

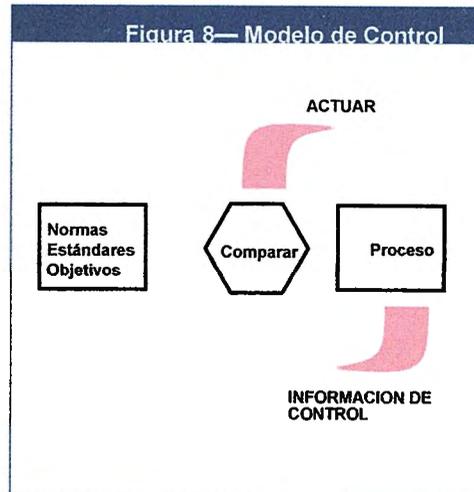
## Basado en controles

### LOS PROCESOS REQUIEREN CONTROLES

Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de IT.

La guía se puede obtener del modelo de control estándar mostrado en la **figura 8**. Sigue los principios que se evidencian en la siguiente analogía: cuando se ajusta la temperatura ambiente (estándar) para el sistema de calefacción (proceso), el sistema verificará de forma constante (comparar) la temperatura ambiente (inf. de control) e indicará (actuar) al sistema de calefacción para que genere más o menos calor.



La gerencia operacional usa los procesos para organizar y administrar las actividades de TI en curso. COBIT brinda un modelo genérico de procesos que representa todos los procesos que normalmente se encuentran en las funciones de TI, proporcionando un modelo de referencia general y entendible para la gerencia operacional de TI y para la gerencia administrativa. Para lograr un gobierno efectivo, los gerentes operacionales deben implementar los controles necesarios dentro de un marco de control definido para todos los procesos de TI. Ya que los objetivos de control de TI de COBIT están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y un número de objetivos de control detallados. Como un todo, representan las características de un proceso bien administrado.

Los objetivos de control detallados se identifican por dos caracteres que representan el dominio más un número de proceso y un número de objetivo de control. Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCn, que significa número de control de proceso. Se deben tomar como un todo junto con los objetivos de control del proceso para tener una visión completa de los requerimientos de control.

### PC1 Dueño del proceso

Asignar un dueño para cada proceso COBIT de tal manera que la responsabilidad sea clara.

### PC2 Reiterativo

Definir cada proceso COBIT de tal forma que sea repetitivo.

### PC3 Metas y objetivos

Establecer metas y objetivos claros para cada proceso COBIT para una ejecución efectiva.

#### *PC4 Roles y responsabilidades*

Definir roles, actividades y responsabilidades claros en cada proceso COBIT para una ejecución eficiente.

#### *PC5 Desempeño del proceso*

Medir el desempeño de cada proceso COBIT en comparación con sus metas.

#### *PC6 Políticas, planes y procedimientos*

Documentar, revisar, actualizar, formalizar y comunicar a todas las partes involucradas cualquier política, plan ó procedimiento que impulse un proceso COBIT.

Los controles efectivos reducen el riesgo, aumentan la probabilidad de la entrega de valor y aumentan la eficiencia debido a que habrá menos errores y un enfoque administrativo más consistente.

Además, COBIT ofrece ejemplos ilustrativos para cada proceso, los cuales no son exhaustivos o anticuados / caducos, de:

- Entradas y salidas genéricas
- Actividades y guías sobre roles y responsabilidades en una gráfica RACI
- Metas de actividades clave (las cosas más importantes a realizar)
- Métricas

Además de evaluar qué controles son requeridos, los propietarios de procesos deben entender qué entradas requieren de otros procesos y que requieren otros de sus procesos. COBIT brinda ejemplos genéricos de las entradas y salidas clave para cada proceso incluyendo los requerimientos externos de TI. Existen algunas salidas que son entradas a todos los demás procesos, marcadas como 'TODOS' en las tablas de salidas, pero no se mencionan como entradas en todos los procesos, y por lo general incluyen estándares de calidad y requerimientos de métricas, el marco de trabajo de procesos de TI, roles y responsabilidades documentados, el marco de control empresarial de TI, las políticas de TI, y roles y responsabilidades del personal.

El entendimiento de los roles y responsabilidades para cada proceso es clave para un gobierno efectivo. COBIT proporciona una gráfica RACI (quién es responsable, quién rinde cuentas, quién es consultado y quien informado) para cada proceso. Rendir cuentas significa 'la responsabilidad termina aquí'—esta es la persona que provee autorización y direccionamiento a una actividad. Responsabilidad se refiere a la persona que realiza la actividad. Los otros dos roles (consultado e informado) garantizan que todas las personas que son requeridas están involucradas y dan soporte al proceso.

### **CONTROLES DEL NEGOCIO Y CONTROLES DE TI**

El sistema empresarial de controles internos impacta a TI en tres niveles:

- Al nivel de dirección ejecutiva, se fijan los objetivos de negocio, se establecen políticas y se toman decisiones de cómo aplicar y administrar los recursos empresariales para ejecutar la estrategia de la compañía. El enfoque genérico hacia el gobierno y el control se establece por parte del consejo y se comunica a todo lo largo de la empresa. El ambiente de control de TI es guiado por este conjunto de objetivos y políticas de alto nivel.
- Al nivel de procesos de negocio, se aplican controles para actividades específicas del negocio. La mayoría de los procesos de negocio están automatizados e integrados con los sistemas aplicativos de TI, dando como resultado que muchos de los controles a este nivel estén automatizados. Estos se conocen como controles de las aplicaciones. Sin embargo, algunos controles dentro del proceso de negocios permanecen como procedimientos manuales, como la autorización de transacciones, la separación de funciones y las conciliaciones manuales. Los controles al nivel de procesos de negocio son, por lo tanto, una combinación de controles manuales operados por el negocio, controles de negocio y controles de aplicación automatizados. Ambos son responsabilidad del negocio en cuanto a su definición y administración aunque los controles de aplicación requieren que la función de TI dé soporte a su diseño y desarrollo.
- Para soportar los procesos de negocio, TI proporciona servicios, por lo general de forma compartida, por varios procesos de negocio, así como procesos operacionales y de desarrollo de TI que se proporcionan a toda la empresa, y mucha de la infraestructura de TI provee un servicio común (es decir, redes, bases de datos, sistemas operativos y almacenamiento). Los controles aplicados a todas las actividades de servicio de TI se conocen como controles generales de TI. La operación formal de estos controles generales es necesaria para que dé confiabilidad a los controles en aplicación. Por ejemplo, una deficiente administración de cambios podría poner en riesgo (por accidente o de forma deliberada) la confiabilidad de los chequeos automáticos de integridad.

### **CONTROLES GENERALES DE TI Y CONTROLES DE APLICACION**

Los controles generales son aquellos que están incrustados en los procesos y servicios de TI. Algunos ejemplos son:

- Desarrollo de sistemas
- Administración de cambios
- Seguridad
- Operación del computador

Los controles incluidos en las aplicaciones del proceso de negocios se conocen por lo general como controles de aplicación. Ejemplos:

- Integridad (Compleitud)
- Precisión
- Validez
- Autorización
- Segregación de funciones

COBIT asume que el diseño e implementación de los controles de aplicación automatizados son responsabilidad de TI, y están cubiertos en el dominio de Adquirir e Implementar, con base en los requerimientos de negocio definidos, usando los criterios de información de COBIT. La responsabilidad operacional de administrar y controlar los controles de aplicación no es de TI, sino del propietario del proceso de negocio.

TI entrega y da soporte a los servicios de las aplicaciones y a las bases de datos e infraestructura de soporte.

Por lo tanto, los procesos de TI de COBIT abarcan a los controles generales de TI, pero no los controles de las aplicaciones, debido a que son responsabilidad de los dueños de los procesos del negocio, y como se describió anteriormente, están integrados en los procesos de negocio.

La siguiente lista ofrece un conjunto recomendado de objetivos de control de las aplicaciones identificados por ACn, número de Control de Aplicación (por sus siglas en inglés):

### **Controles de origen de datos/ autorización**

#### *AC1 Procedimientos de preparación de datos*

Los departamentos usuarios implementan y dan seguimiento a los procedimientos de preparación de datos. En este contexto, el diseño de los formatos de entrada asegura que los errores y las omisiones se minimicen. Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable que los errores y las irregularidades son detectadas, reportadas y corregidas.

#### *AC2 Procedimientos de autorización de documentos fuente*

El personal autorizado, actuando dentro de su autoridad, prepara los documentos fuente de forma adecuada y existe una segregación de funciones apropiada con respecto a la generación y aprobación de los documentos fuente.

#### *AC3 Recolección de datos de documentos fuente*

Los procedimientos garantizan que todos los documentos fuente autorizados son completos y precisos, debidamente justificados y transmitidos de manera oportuna para su captura.

#### *AC4 Manejo de errores en documentos fuente*

Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable la detección, el reporte y la corrección de errores e irregularidades.

#### *AC5 Retención de documentos fuente*

Existen procedimientos para garantizar que los documentos fuente originales son retenidos o pueden ser reproducidos por la organización durante un lapso adecuado de tiempo para facilitar el acceso o reconstrucción de datos así como para satisfacer los requerimientos legales.

### **Controles de entrada de datos**

#### *AC6 Procedimientos de autorización de captura de datos*

Los procedimientos aseguran que solo el personal autorizado capture los datos de entrada.

#### *AC7 Verificaciones de precisión, integridad y autorización*

Los datos de transacciones, ingresados para ser procesados (generados por personas, por sistemas o entradas de interfases) están sujetos a una variedad de controles para verificar su precisión, integridad y validez. Los procedimientos también garantizan que los datos de entrada son validados y editados tan cerca del punto de origen como sea posible.

#### *AC8 Manejo de errores en la entrada de datos*

Existen y se siguen procedimientos para la corrección y re-captura de datos que fueron ingresados de manera incorrecta.

### **Controles en el Procesamiento de datos**

#### *AC9 Integridad en el procesamiento de datos*

Los procedimientos para el procesamiento de datos aseguran que la separación de funciones se mantiene y que el trabajo realizado de forma rutinaria se verifica. Los procedimientos garantizan que existen controles de actualización adecuados, tales como totales de control de corrida-a-corrida, y controles de actualización de archivos maestros.

#### *AC10 Validación y edición del procesamiento de datos*

Los procedimientos garantizan que la validación, la autenticación y la edición del procesamiento de datos se realizan tan cerca como sea posible del punto de generación. Los individuos aprueban decisiones vitales que se basan en sistemas de inteligencia artificial.

#### *AC11 Manejo de errores en el procesamiento de datos*

Los procedimientos de manejo de errores en el procesamiento de datos permiten que las transacciones erróneas sean identificadas sin ser procesadas y sin una indebida interrupción del procesamiento de otras transacciones válidas.

#### **Controles de salida de datos**

##### *AC12 Manejo y retención de salidas*

El manejo y la retención de salidas provenientes de aplicaciones de TI siguen procedimientos definidos y tienen en cuenta los requerimientos de privacidad y de seguridad.

##### *AC13 Distribución de salidas*

Los procedimientos para la distribución de las salidas de TI se definen, se comunican y se les da seguimiento.

##### *AC14 Cuadre y conciliación de salidas*

Las salidas cuadran rutinariamente con los totales de control relevantes. Las pistas de auditoría facilitan el rastreo del procesamiento de las transacciones y la conciliación de datos alterados.

##### *AC15 Revisión de salidas y manejo de errores*

Los procedimientos garantizan que tanto el proveedor como los usuarios relevantes revisan la precisión de los reportes de salida. También existen procedimientos para la identificación y el manejo de errores contenidos en las salidas.

##### *AC16 Provisión de seguridad para reportes de salida*

Existen procedimientos para garantizar que se mantiene la seguridad de los reportes de salida, tanto para aquellos que esperan ser distribuidos como para aquellos que ya están entregados a los usuarios.

#### **Controles de límites**

##### *AC17 Autenticidad e integridad*

Se verifica de forma apropiada la autenticidad e integridad de la información generada fuera de la organización, ya sea que haya sido recibida por teléfono, por correo de voz, como documento en papel, fax o correo electrónico, antes de que se tomen medidas potencialmente críticas.

##### *AC18 Protección de información sensitiva durante su transmisión y transporte*

Se proporciona una protección adecuada contra accesos no autorizados, modificaciones y envíos incorrectos de información sensitiva durante la transmisión y el transporte.

## **Generadores de mediciones**

Una necesidad básica de toda empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar la empresa.

La obtención de una visión objetiva del nivel de desempeño propio de una empresa no es sencilla. ¿Qué se debe medir y cómo? Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear esta mejora.

Para decidir cuál es el nivel correcto, la gerencia debe preguntarse a sí misma: ¿Qué tan lejos debemos ir, y está justificado el costo por el beneficio?

COBIT atiende estos temas por medio de:

- Modelos de madurez que facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad
- Metas y mediciones de desempeño para los procesos de TI, que demuestran cómo los procesos satisfacen las necesidades del negocio y de TI, y cómo se usan para medir el desempeño de los procesos internos basados en los principios de un marcador de puntuación balanceado (balanced scorecard)
- Metas de actividades para facilitar el desempeño efectivo de los procesos

## MODELOS DE MADUREZ

Cada vez con más frecuencia, se les pide a los directivos de empresas corporativas y públicas que se considere qué tan bien se está administrando TI. Como respuesta a esto, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información. Aunque pocos argumentarían que esto no es algo bueno, se debe considerar el equilibrio del costo beneficio y éstas preguntas relacionadas:

- ¿Qué están haciendo nuestra competencia en la industria, y cómo estamos posicionados en relación a ellos?
- ¿Cuáles son las mejores prácticas aceptables en la industria, y cómo estamos posicionados con respecto a estas prácticas?
- Con base en estas comparaciones, ¿se puede decir que estamos haciendo lo suficiente?
- ¿Cómo identificamos lo que se requiere hacer para alcanzar un nivel adecuado de administración y control sobre nuestros procesos de TI?

Puede resultar difícil proporcionar respuestas significativas a estas preguntas. La gerencia de TI está buscando constantemente herramientas de evaluación por benchmarking y herramientas de auto-evaluación como respuesta a la necesidad de saber qué hacer de manera eficiente. Comenzando con los procesos y los objetivos de control de alto nivel de COBIT, el propietario del proceso se debe poder evaluar de forma progresiva, contra los objetivos de control. Esto responde a tres necesidades:

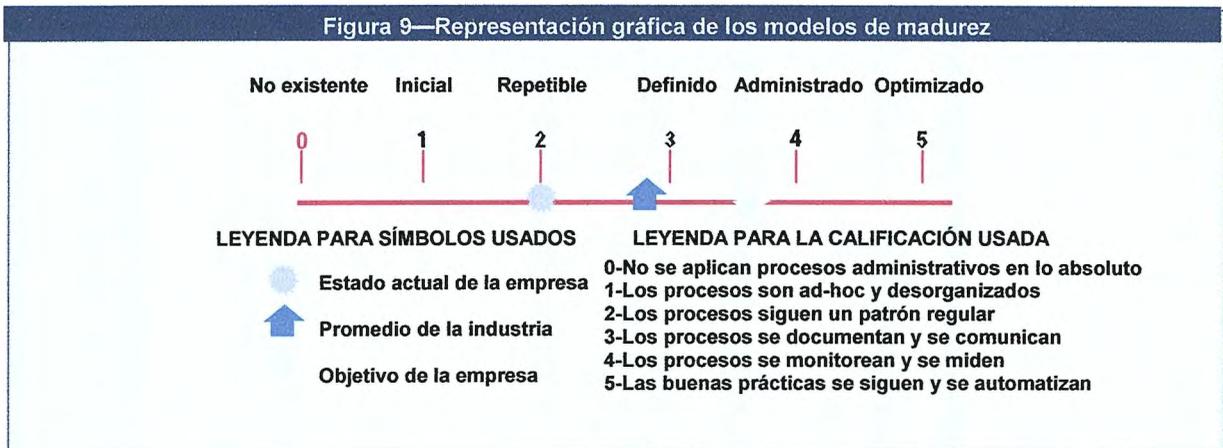
1. Una medición relativa de dónde se encuentra la empresa
2. Una manera de decidir hacia dónde ir de forma eficiente
3. Una herramienta para medir el avance contra la meta

El modelado de la madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es evaluar el nivel de adherencia a los objetivos de control.

Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Si se usan los procesos de madurez desarrollados para cada uno de los 34 procesos TI de COBIT, la administración podrá identificar:

- El desempeño real de la empresa—Dónde se encuentra la empresa hoy
- El estatus actual de la industria—La comparación
- El objetivo de mejora de la empresa—Dónde desea estar la empresa

Para hacer que los resultados sean utilizables con facilidad en resúmenes gerenciales, donde se presentarán como un medio para dar soporte al caso de negocio para planes futuros, se requiere contar con un método gráfico de presentación (figura 9).



Se ha definido un modelo de madurez para cada uno de los 34 procesos de TI, con una escala de medición creciente a partir de 0, no existente, hasta 5, optimizado. El desarrollo se basó en las descripciones del modelo de madurez genérico descritas en la figura 10.

COBIT es un marco de referencia desarrollado para la administración de procesos de TI con un fuerte enfoque en el control. Estas escalas deben ser prácticas en su aplicación y razonablemente fáciles de entender. El tema de procesos de TI es esencialmente complejo y subjetivo, por lo tanto, es más fácil abordarlo por medio de evaluaciones fáciles que aumenten la conciencia, que logren un consenso amplio y que motiven la mejora. Estas evaluaciones se pueden realizar ya sea contra las descripciones del modelo de madurez como un todo o con mayor rigor, en cada una de las afirmaciones individuales de las descripciones. De cualquier manera, se requiere experiencia en el proceso de la empresa que se está revisando.

**0 No existente.** Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

**1 Inicial.** Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

**2 Repetible.** Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

**3 Definido.** Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

**4 Administrado.** Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

**5 Optimizado.** Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

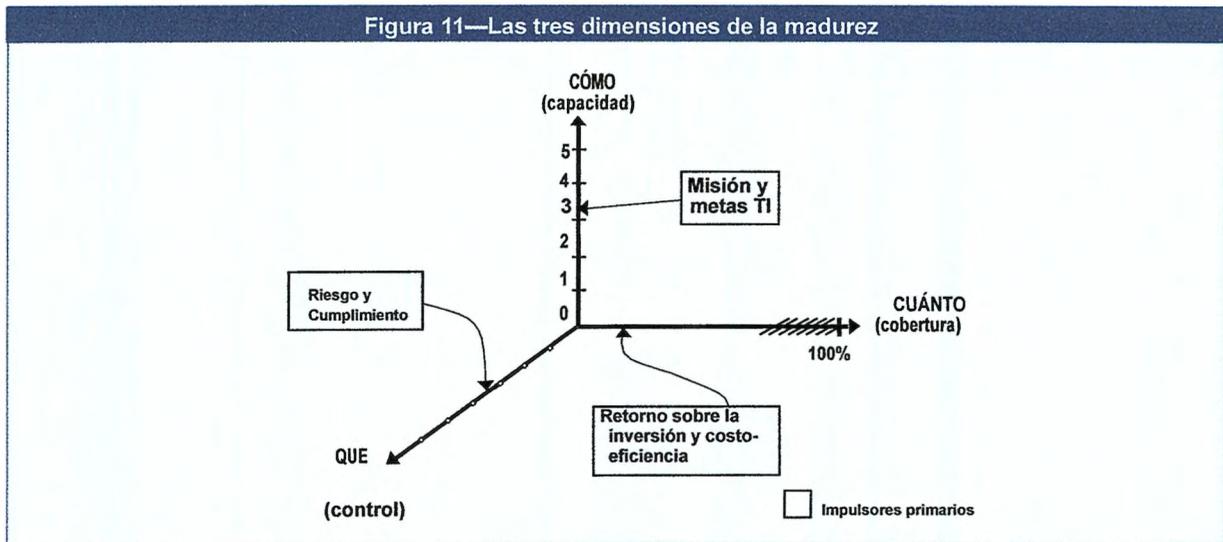
La ventaja de un modelo de madurez es que es relativamente fácil para la dirección ubicarse a sí misma en la escala y evaluar qué se debe hacer si se requiere desarrollar una mejora. La escala incluye al 0 ya que es muy posible que no existan procesos en lo absoluto. La escala del 0-5 se basa en una escala de madurez simple que muestra como un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada.

Sin embargo, la capacidad administrativa de un proceso no es lo mismo que el desempeño. La capacidad requerida, como se determina en el negocio y en las metas de TI, puede no requerir aplicarse al mismo nivel en todo el ambiente de TI, es decir, de forma inconsistente o solo a un número limitado de sistemas o unidades. La medición del desempeño, como se cubre en los próximos párrafos, es esencial para determinar cual es el desempeño real de la empresa en sus procesos de TI.

Aunque una capacidad aplicada de forma apropiada reduce los riesgos, una empresa debe analizar los controles necesarios para asegurar que el riesgo sea mitigado y que se obtenga el valor de acuerdo al apetito de riesgo y a los objetivos del negocio. Estos controles son dirigidos por los objetivos de control de COBIT. El apéndice III brinda un modelo de madurez para el control interno que ilustra la madurez de una empresa con respecto al establecimiento y desempeño del control interno. Con frecuencia, este análisis se inicia como respuesta a impulsores externos, aunque idealmente debería ser institucionalizado como se documenta en los procesos de COBIT PO6 *Comunicar los objetivos y el rumbo de la dirección* y ME2 *Monitorear y evaluar el control interno*.

La capacidad, el desempeño y el control son dimensiones de la madurez de un proceso como se ilustra en la **figura 11**.

Figura 11—Las tres dimensiones de la madurez



El modelo de madurez es una forma de medir qué tan bien están desarrollados los procesos administrativos, esto es, qué tan capaces son en realidad. Qué tan bien desarrollados o capaces deberían ser, principalmente dependen de las metas de TI y en las necesidades del negocio subyacentes a la cuales sirven de base. Cuánta de esa capacidad es realmente utilizada actualmente para retomar la inversión deseada en una empresa. Por ejemplo, habrá procesos y sistemas críticos que requieren de una mayor administración de la seguridad que otros que son menos críticos. Por otro lado, el grado y sofisticación de los controles que se requiere aplicar en un proceso están más definidos por el apetito de riesgo de una empresa y por los requerimientos aplicables.

Las escalas del modelo de madurez ayudarán a los profesionales a explicarle a la gerencia dónde se encuentran los defectos en la administración de procesos de TI y a establecer objetivos donde se requieran. El nivel de madurez correcto estará influenciado por los objetivos de negocio de una empresa, por el ambiente operativo y por las prácticas de la industria. Específicamente, el nivel de madurez en la administración se basará en la dependencia que tenga la empresa en la TI, en su sofisticación tecnológica y, lo más importante, en el valor de su información.

Un punto de referencia estratégico para una empresa que ayuda a mejorar la administración y el control de los procesos de TI se puede encontrar observando los estándares internacionales y las mejores prácticas. Las prácticas emergentes de hoy en día se pueden convertir en el nivel esperado de desempeño del mañana y por lo tanto son útiles para planear dónde desea estar la empresa en un lapso de tiempo.

Los modelos de madurez se desarrollan empezando con el modelo genérico cualitativo (consulte la **figura 10**) al cual se añaden, en forma creciente, algunos principios contenidos en los siguientes atributos, a través de niveles:

- Conciencia y comunicación
- Políticas, estándares y procedimientos
- Herramientas y automatización
- Habilidades y experiencia
- Responsabilidad y rendición de cuentas
- Establecimiento y medición de metas

La tabla de atributos de madurez que se muestra en la **figura 12** lista las características de cómo se administran los procesos de TI y describe cómo evolucionan desde un proceso no existente hasta uno optimizado. Estos atributos se pueden usar para una evaluación más integral, para un análisis de brechas y para la planeación de mejoras.

En resumen, los modelos de madurez brindan un perfil genérico de las etapas a través de las cuales evolucionan las empresas para la administración y el control de los procesos de TI, estos son:

- Un conjunto de requerimientos y los aspectos que los hacen posibles en los distintos niveles de madurez
- Una escala donde la diferencia se puede medir de forma sencilla
- Una escala que se presta a sí misma para una comparación práctica
- La base para establecer el estado actual y el estado deseado
- Soporte para un análisis de brechas para determinar qué se requiere hacer para alcanzar el nivel seleccionado
- Tomado en conjunto, una vista de cómo se administra la TI en la empresa

Los modelos de madurez COBIT se enfocan en la capacidad, y no necesariamente en el desempeño. No son un número al cual hay que llegar, ni están diseñados para ser una base formal de certificación con niveles discretos que formen umbrales difíciles de atravesar. Sin embargo, se diseñaron para ser aplicables siempre, con niveles que brindan una descripción que una empresa pueda reconocer como la mejor para sus procesos. El nivel correcto está determinado por el tipo de empresa, por su medio ambiente y por la estrategia.

El desempeño, o la manera en que la capacidad se usa y se implanta, es una decisión de rentabilidad. Por ejemplo, un alto nivel de administración de la seguridad quizá se tenga que enfocar sólo en los sistemas empresariales más críticos.

Para finalizar, mientras los niveles de madurez más altos aumentan el control del proceso, la empresa aún necesita analizar, con base en los impulsores de riesgo y de valor, cuáles mecanismos de control debe aplicar. Las metas genéricas de negocio y de TI, como se definen en este marco de trabajo, ayudarán a realizar este análisis. Los objetivos de control de COBIT guían los mecanismos de control y éstos se enfocan en qué se hace en el proceso; los modelos de madurez se enfocan principalmente en qué tan bien se administra un proceso. El apéndice III brinda un modelo de madurez genérico que muestra el estatus del ambiente de control interno y el establecimiento de controles en una empresa.

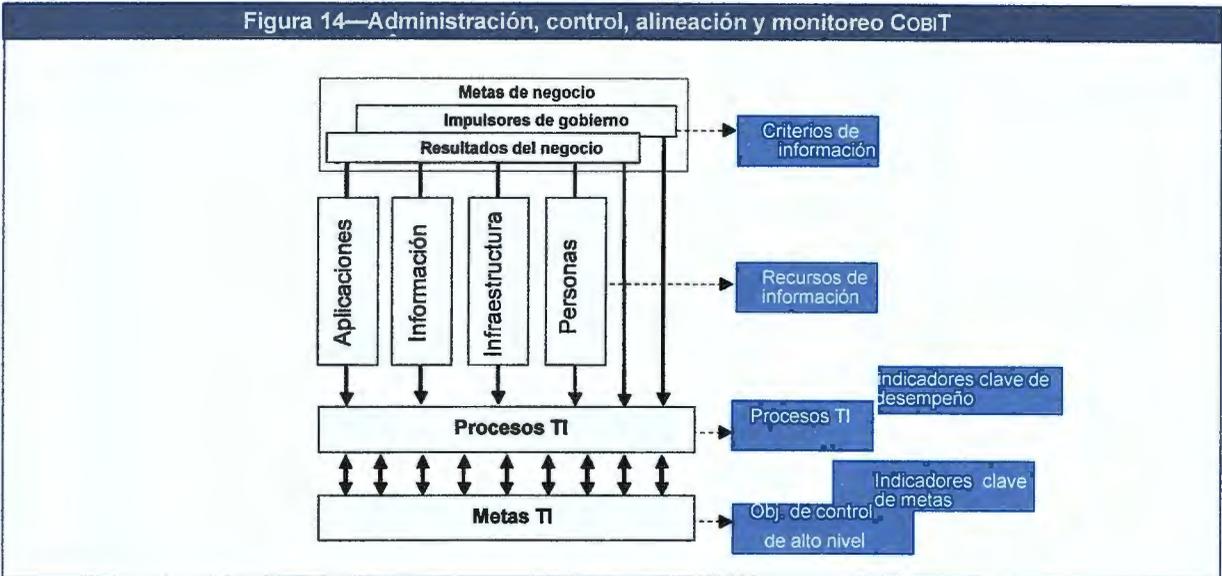
Un ambiente de control implantado de forma adecuada, se logra cuando se han conseguido los tres aspectos de madurez (capacidad, desempeño y control). El incremento en la madurez reduce el riesgo y mejora la eficiencia, generando menos errores, más procesos predecibles y un uso rentable de los recursos.



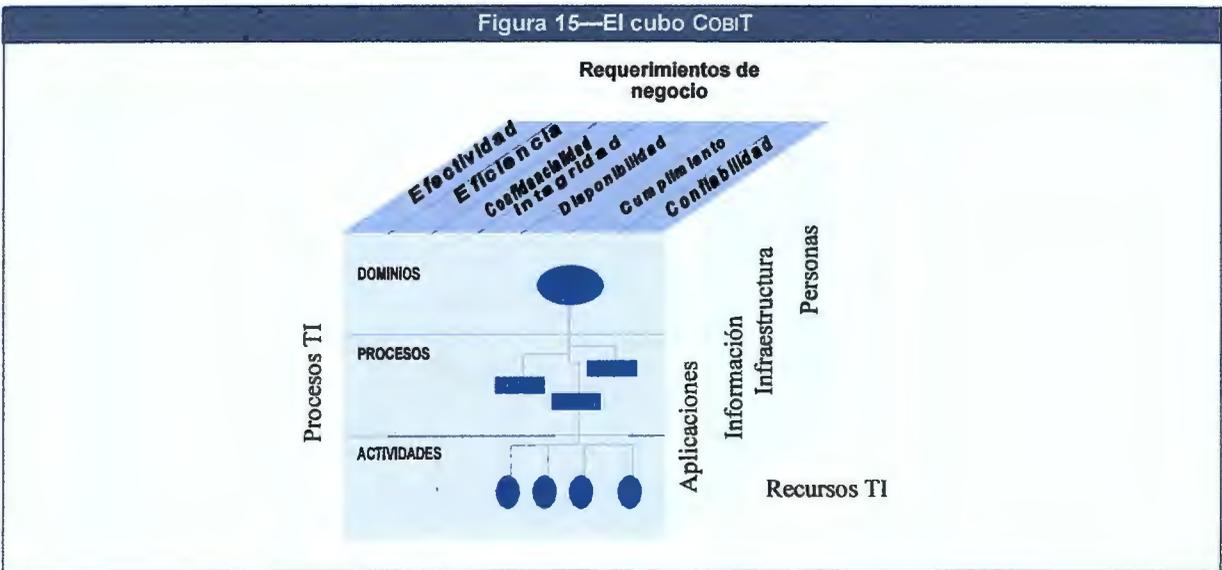
Las metas se definen de arriba hacia abajo con base en las metas de negocio que determinarán el número de metas que soportará TI, las metas de TI decidirán las diferentes necesidades de las metas de proceso, y cada meta de proceso establecerá las metas de las actividades. El logro de metas se mide con las métricas de resultado (llamadas indicadores clave de metas, o KGIs) y dirigen las metas de más alto nivel. Por ejemplo, la métrica que midió el logro de la meta de la actividad es un motivador de desempeño (llamado indicador clave de desempeño, o KPI) para la meta del proceso. Las métricas permiten a la gerencia corregir el desempeño y realinearse con las metas.

### El modelo del marco de trabajo COBIT

El marco de trabajo COBIT, por lo tanto, relaciona los requerimientos de información y de gobierno a los objetivos de la función de servicio de TI. El modelo de procesos COBIT permite que las actividades de TI y los recursos que los soportan sean administrados y controlados basados en los objetivos de control de COBIT, y alineados y monitoreados usando las métricas KGI y KPI de COBIT, como se ilustra en la figura 14.

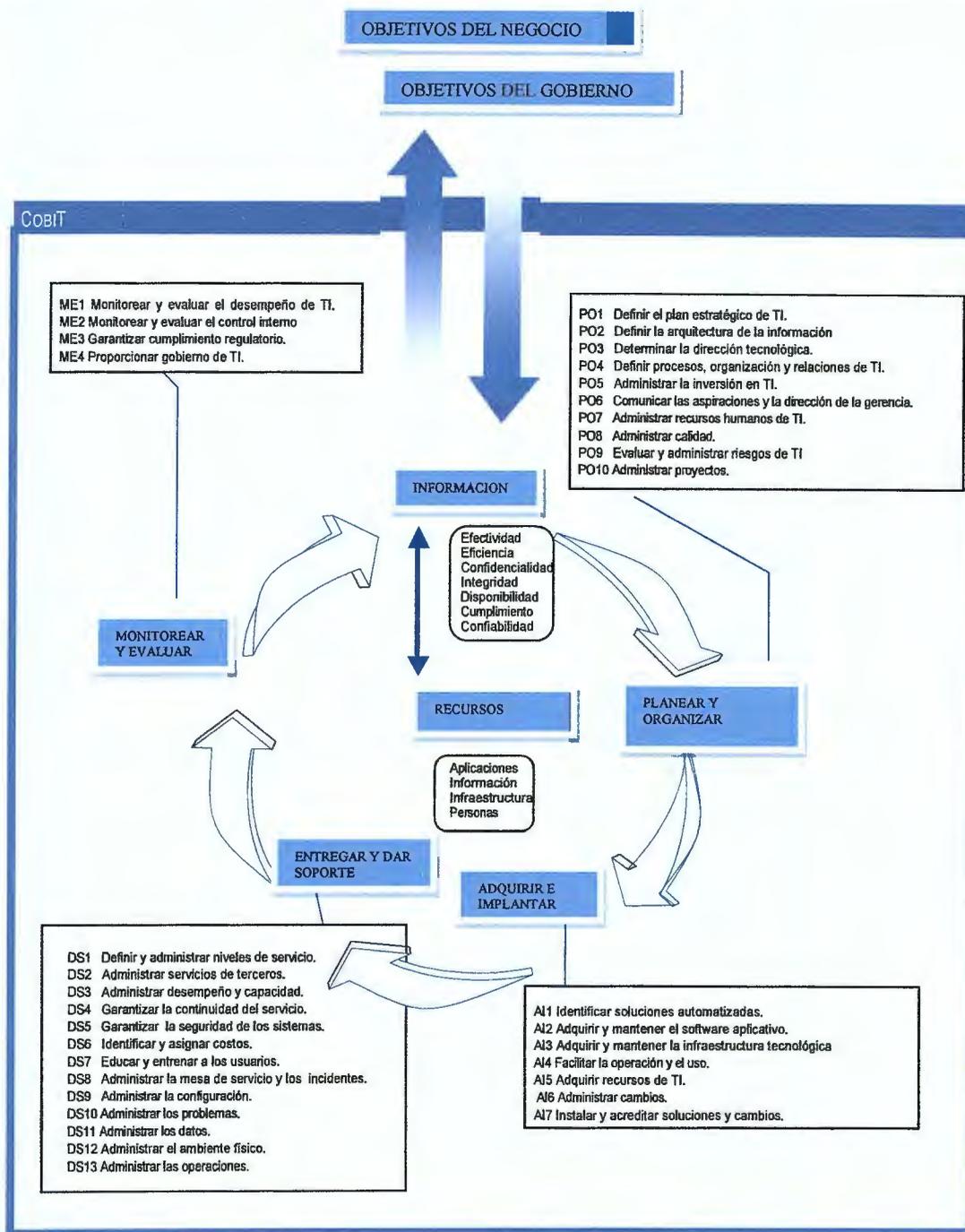


Para resumir, los recursos de TI son manejados por procesos de TI para lograr metas de TI que respondan a los requerimientos del negocio. Este es el principio básico del marco de trabajo COBIT, como se ilustra en el cubo COBIT (figura 15)



En detalle, el marco de trabajo general COBIT se muestra gráficamente en la **figura 16**, con el modelo de procesos de COBIT compuesto de cuatro dominios que contienen 34 procesos genéricos, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

Figura 16—Marco de trabajo general de COBIT



## Nivel de aceptabilidad general de COBIT

COBIT se basa en el análisis y armonización de estándares y mejores prácticas de TI existentes y se adapta a principios de gobierno generalmente aceptados. Está posicionado a un nivel alto, impulsado por los requerimientos del negocio, cubre el rango completo de actividades de TI, y se concentra en lo que se debe lograr en lugar de cómo lograr un gobierno, administración y control efectivos. Por lo tanto, funciona como un integrador de prácticas de gobierno de TI y es de interés para la dirección ejecutiva; para la gerencia del negocio, para la gerencia y gobierno de TI; para los profesionales de aseguramiento y seguridad; así como para los profesionales de auditoría y control de TI. Está diseñado para ser complementario y para ser usado junto con otros estándares y mejores prácticas.

La implantación de las mejores prácticas debe ser consistente con el gobierno y el marco de control de la empresa, debe ser apropiada para la organización, y debe estar integrada con otros métodos y prácticas que se utilicen. Los estándares y las mejores prácticas no son una panacea y su efectividad depende de cómo hayan sido implantados en realidad y de cómo se mantengan actualizados. Son más útiles cuando se aplican como un conjunto de principios y como un punto de partida para adaptar procedimientos específicos. La gerencia y el equipo deben entender qué hacer, cómo hacerlo y porqué es importante hacerlo para garantizar que se utilicen las prácticas.

Para lograr la alineación de las mejores prácticas con los requerimientos del negocio, se recomienda que COBIT se utilice al más alto nivel, brindando así un marco de control general basado en un modelo de procesos de TI que debe ser aplicable en general a toda empresa. Las prácticas y los estándares específicos que cubren áreas discretas, se pueden equiparar con el marco de trabajo de COBIT, brindando así una jerarquía de materiales guía.

COBIT resulta de interés a distintos usuarios:

- Dirección ejecutiva—Para obtener valor de las inversiones y riesgos de TI y para controlar la inversión en un ambiente de TI con frecuencia impredecible
- Gerencia del negocio—Para obtener certidumbre sobre la administración y control de los servicios de TI, proporcionados internamente o por terceros
- Gerencia de TI—Para proporcionar los servicios de TI que el negocio requiere para dar soporte a la estrategia del negocio de una forma controlada y administrada
- Auditores—Para respaldar sus opiniones y/o para proporcionar asesoría a la gerencia sobre controles internos

Un instituto de investigación sin fines de lucro desarrolló COBIT y lo mantiene actualizado, tomando la experiencia de los miembros de sus asociaciones afiliadas, de los expertos de la industria, y de los profesionales de control y seguridad. Su contenido se basa en una investigación continua sobre las mejores prácticas de TI y se le da un mantenimiento continuo, proporcionando así un recurso objetivo y práctico para todo tipo de usuario.

COBIT está orientado a los objetivos y al alcance del gobierno de TI, asegurando que su marco de control sea integral, que esté alineado con los principios de gobierno empresariales y, por lo tanto, que sea aceptable para los consejos directivos, para la dirección ejecutiva, para los auditores y reguladores. En el apéndice II, se ofrece un mapa que muestra cómo los objetivos de control detallados de COBIT se relacionan con las cinco áreas focales del gobierno de TI y con las actividades de control de COSO.

La **figura 17** resume cómo los distintos elementos del marco de trabajo de COBIT se relacionan con las áreas focales del gobierno de TI.

**Figura 17 Marco de trabajo COBIT y áreas focales del gobierno de TI**

	Metas	Métricas	Prácticas	Modelos de madurez
Alineación estratégica	P	P		
Transferencia de valor		P	S	P
Administración de riesgos		S	P	S
Administración de recursos		S	P	P
Medición del desempeño	P	P		S

P = Facilitador primario    S = Facilitador secundario

# PLANEAR Y ORGANIZAR

- PO1 Definir un plan estratégico de TI
- PO2 Definir la arquitectura de la información
- PO3 Determinar la dirección tecnológica
- PO4 Definir los procesos, organización y relaciones de TI
- PO5 Administrar la inversión en TI
- PO6 Comunicar las aspiraciones y la dirección de la gerencia
- PO7 Administrar recursos humanos de TI
- PO8 Administrar la calidad
- PO9 Evaluar y administrar los riesgos de TI
- PO10 Administrar proyectos

## Objetivo de control de alto nivel

### PO1 Definir un plan estratégico para TI

Se requiere una planeación estratégica de TI para administrar y dirigir todos los recursos de TI de acuerdo con la estrategia del negocio y las prioridades. La función de TI y los participantes del negocio son responsables de garantizar que se materialice el valor óptimo de los portafolios de proyectos y servicios. El plan estratégico debe mejorar el entendimiento de los interesados clave respecto a las oportunidades y limitaciones de TI, evaluar el desempeño actual y aclarar el nivel de inversión requerido. La estrategia de negocio y las prioridades se deben reflejar en los portafolios y deben ser ejecutadas por los planes tácticos de TI, los cuales establecen objetivos, planes y tareas específicas, entendidas y aceptadas tanto por el negocio como por TI.



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

#### Control sobre el proceso TI de

Definir un plan estratégico para TI

que satisface el requisito del negocio de TI para

sostener o extender los requerimientos de gobierno y de la estrategia del negocio, al mismo tiempo que se mantiene la transparencia sobre los beneficios, costos y riesgos

enfocándose en

la incorporación de TI y de la gerencia del negocio en la traducción de los requerimientos del negocio a ofertas de servicio, y el desarrollo de estrategias para otorgar estos servicios de una forma transparente y rentable

se logra con

- La intervención con la alta gerencia y con la gerencia del negocio para alinear la planeación estratégica de TI con las necesidades del negocio actuales y futuras
- El entendimiento de las capacidades actuales de TI
- La aplicación de un esquema de prioridades para los objetivos del negocio que cuantifique los requerimientos del negocio

y se mide con

- El porcentaje de objetivos de TI en el plan estratégico de TI, que dan soporte al plan estratégico del negocio
- El porcentaje de proyectos TI en el portafolio de proyectos que se pueden rastrear hacia el plan táctico de TI
- El retraso entre las actualizaciones del plan estratégico de TI y las actualizaciones de los planes tácticos de TI



# Objetivos de control detallados

## PO1 Definir un plan estratégico de TI

### PO1.1 Administración del valor de TI

Trabajar con el negocio para garantizar que el portafolio de inversiones de TI de la empresa contenga programas con casos de negocio sólidos. Reconocer que existen inversiones obligatorias, de sustento y discrecionales que difieren en complejidad y grado de libertad en cuanto a la asignación de fondos. Los procesos de TI deben proporcionar una entrega efectiva y eficiente de los componentes TI de los programas y advertencias oportunas sobre las desviaciones del plan, incluyendo costo, calendario o funcionalidad, que pudieran impactar los resultados esperados de los programas. Los servicios de TI se deben ejecutar contra acuerdos de niveles de servicios equitativos y exigibles. La rendición de cuentas del logro de los beneficios y del control de los costos es claramente asignada y monitoreada. Establecer una evaluación de los casos de negocio que sea justa, transparente, repetible y comparable, incluyendo el valor financiero, el riesgo de no cumplir con una capacidad y el riesgo de no materializar los beneficios esperados.

### PO1.2 Alineación de TI con el negocio

Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades. Asegurarse de que el rumbo del negocio al cual está alineado la TI está bien entendido. Las estrategias de negocio y de TI deben estar integradas, relacionando de manera clara las metas de la empresa y las metas de TI y reconociendo las oportunidades así como las limitaciones en la capacidad actual, y se deben comunicar de manera amplia. Identificar las áreas en que el negocio (estrategia) depende de forma crítica de la TI, y mediar entre los imperativos del negocio y la tecnología, de tal modo que se puedan establecer prioridades concertadas.

### PO1.3 Evaluación del desempeño actual

Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.

### PO1.4 IT Plan estratégico de TI

Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo la TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo la TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operacionales. Define cómo se cumplirán y medirán los objetivos y recibirá una autorización formal de los interesados. El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de procuración, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI.

### PO1.5 IT Planes tácticos de TI

Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos describen las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados. Los planes tácticos deben tener el detalle suficiente para permitir la definición de planes proyectados. Administrar de forma activa los planes tácticos y las iniciativas de TI establecidas por medio del análisis de los portafolios de proyectos y servicios. Esto incluye el equilibrio de los requerimientos y recursos de forma regular, comparándolos con el logro de metas estratégicas y tácticas y con los beneficios esperados, y tomando las medidas necesarias en caso de desviaciones.

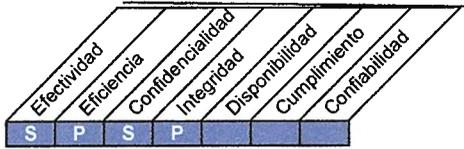
### PO1.6 IT Administración del portafolio de TI

Administrar de forma activa, junto con el negocio, el portafolio de programas de inversión de TI requerido para lograr objetivos de negocio estratégicos y específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas. Esto incluye clarificar los resultados de negocio deseados, garantizar que los objetivos de los programas den soporte al logro de los resultados, entender el alcance completo del esfuerzo requerido para lograr los resultados, definir una rendición de cuentas clara con medidas de soporte, definir proyectos dentro del programa, asignar recursos y financiamiento, delegar autoridad, y licenciar los proyectos requeridos al momento de lanzar el programa.

# Objetivo de control de alto nivel

## PO2 Definir la arquitectura de información

La función de los sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias del negocio. Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades



### Control sobre el proceso TI de

Definir la arquitectura de la información

**que satisface el requisito de negocio de TI para**

agilizar la respuesta a los requerimientos, proporcionar información confiable y consistente, para integrar de forma transparente las aplicaciones dentro de los procesos del negocio

**enfocándose en**

el establecimiento de un modelo de datos empresarial que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos

**se logra con**

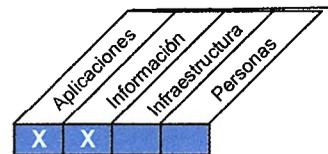
- El aseguramiento de la exactitud de la arquitectura de la información y del modelo de datos
- La asignación de propiedad de datos
- La clasificación de la información usando un esquema de clasificación acordado

**y se mide con**

- El porcentaje de elementos de datos redundantes / duplicados
- El porcentaje de aplicaciones que no cumplen con la arquitectura de la información
- La frecuencia de actividades de validación de datos



■ Primaria □ Secundaria



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

## Objetivos de control detallados

### PO2 Definir la arquitectura de la información

#### PO2.1 Modelo de arquitectura de información empresarial

Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI como se describen en P01. El modelo facilita la creación, uso y compartición óptimas de la información por parte del negocio de una manera que conserva la integridad y es flexible, funcional, rentable oportuna segura y tolerante a fallas.

#### PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos

Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización. El diccionario facilita la compartición de elementos de datos entre las aplicaciones y los sistemas, fomenta un entendimiento común de datos entre los usuarios de TI y del negocio, y previene la creación de elementos de datos incompatibles.

#### PO2.3 Esquema de clasificación de datos

Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o encriptación.

#### PO4.4 IT Administración de la integridad

Definir e implantar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.

## Objetivo de control de alto nivel

### PO3 Determinar la dirección tecnológica

La función de servicios de información debe determinar la dirección tecnológica para dar soporte al negocio. Esto requiere de la creación de un plan de infraestructura tecnológica y de un consejo de arquitectura que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación. El plan se debe actualizar de forma regular y abarca aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias. Esto permite contar con respuestas oportunas a cambios en el ambiente competitivo, economías de escala para consecución de personal de sistemas de información e inversiones, así como una interoperabilidad mejorada de las plataformas y de las aplicaciones.



#### Control sobre el proceso TI de

Determinar la dirección tecnológica

que satisface el requisito de negocio de TI para

contar con sistemas aplicativos estándar, bien integrados, rentables y estables, así como recursos y capacidades que satisfagan requerimientos de negocio actuales y futuros

enfocándose en

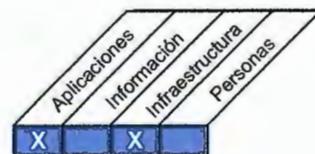
la definición e implantación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas

se logra con

- El establecimiento de un foro para dirigir la arquitectura y verificar el cumplimiento
- El establecimiento de un plan de infraestructura tecnológica equilibrado versus costos, riesgos y requerimientos
- La definición de estándares de infraestructura tecnológica basados en requerimientos de arquitectura de información

y se mide con

- El número y tipo de desviaciones con respecto al plan de infraestructura tecnológica
- Frecuencia de las revisiones /actualizaciones del plan de infraestructura tecnológica
- Número de plataformas de tecnología por función a través de toda la empresa



# Objetivos de control detallados

## PO3 Determinar la dirección tecnológica

### PO3.1 Planeación de la dirección tecnológica

Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiado tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio. También identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.

### PO3.2 Plan de infraestructura tecnológica

Crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos. También toma en cuenta los cambios en el ambiente competitivo, las economías de escala en la obtención de equipo de sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones.

### PO3.3 Monitoreo de tendencias y regulaciones futuras

Establecer un proceso para monitorear las tendencias ambientales del sector / industria, tecnológicas, de infraestructura, legales y regulatorias. Incluir las consecuencias de estas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.

### PO3.4 Estándares tecnológicos

Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección de la tecnología, y medir el cumplimiento de estos estándares y directrices. Este foro impulsa los estándares y las prácticas tecnológicas con base en su importancia y riesgo para el negocio y en el cumplimiento de requerimientos externos.

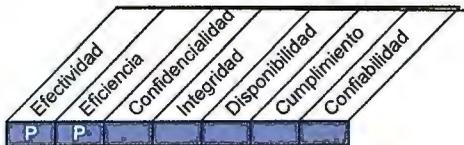
### PO3.4 Consejo de arquitectura

Establecer un consejo de arquitectura de TI que proporcione directrices sobre la arquitectura y asesoría sobre su aplicación y que verifique el cumplimiento. Esta entidad orienta el diseño de la arquitectura de TI garantizando que facilite la estrategia del negocio y tome en cuenta el cumplimiento regulatorio y los requerimientos de continuidad. Estos aspectos se relacionan con la arquitectura de la información

## Objetivo de control de alto nivel

### PO4 Definir los procesos, organización y relaciones de TI

Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, delegación, autoridad, roles, responsabilidades y supervisión. La organización estará incrustada en un marco de trabajo de procesos de TI que asegura la transparencia y el control, así como el involucramiento de los altos ejecutivos y de la gerencia del negocio. Un comité estratégico debe garantizar la vigilancia del consejo directivo sobre la TI, y uno ó más comités administrativos, en los cuales participan tanto el negocio como TI, deben determinar las prioridades de los recursos de TI alineados con las necesidades del negocio. Deben existir procesos, políticas administrativas y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de tareas. Para garantizar el soporte oportuno de los requerimientos del negocio, TI se debe involucrar en los procesos importantes de decisión.



#### Control sobre el proceso TI de

Definir los procesos, organización y relaciones de TI

que satisface el requisito de negocio de TI para

agilizar la respuesta a las estrategias del negocio mientras al mismo tiempo cumple con los requerimientos de gobierno y se establecen puntos de contacto definidos y competentes

enfocándose en

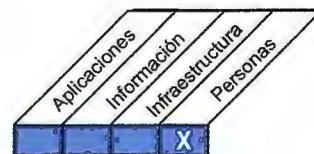
el establecimiento de estructuras organizacionales de TI transparentes, flexibles y responsables, y en la definición e implantación de procesos de TI con los propietarios, y en la integración de roles y responsabilidades hacia los procesos de negocio y de decisión

se logra con

- La definición de un marco de trabajo de procesos de TI
- El establecimiento de un cuerpo y una estructura organizacional apropiada
- La definición de roles y responsabilidades

y se mide con

- El porcentaje de roles con descripciones de puestos y autoridad documentados
- El número de unidades/procesos de negocio que no reciben soporte de TI y que deberían recibirlo, de acuerdo a la estrategia
- Número de actividades clave de TI fuera de la organización de TI que no son aprobadas y que no están sujetas a los estándares organizacionales de TI



## Objetivos de control detallados

### PO4 Definir los procesos, la organización y las relaciones de TI

#### PO4.1 Marco de trabajo del proceso

Definir un marco de trabajo para el proceso de TI para ejecutar el plan estratégico de TI. Este marco incluye estructura y relaciones de procesos de TI (administrando brechas y superposiciones de procesos), propiedad, medición del desempeño, mejoras, cumplimiento, metas de calidad y planes para alcanzarlas. Proporciona integración entre los procesos que son específicos para TI, administración del portafolio de TI, procesos de negocio y procesos de cambio del negocio. El marco de trabajo de procesos de TI debe estar integrado en un sistema de administración de calidad y en un marco de trabajo de control interno.

#### PO4.2 Comité estratégico

Establecer un comité estratégico de TI a nivel del consejo directivo. Este comité garantiza que el gobierno de TI, como parte del gobierno corporativo, se maneja de forma adecuada, asesora sobre la dirección estratégica y revisa las inversiones principales a nombre del consejo directivo.

#### PO4.3 Comité directivo (Steering Committee)

Establecer un comité directivo de TI (o su equivalente) compuesto por la gerencia ejecutiva, del negocio y de TI para:

- Determinar las prioridades de los programas de inversión de TI alineadas con la estrategia y prioridades de negocio de la empresa
- Hacer seguimiento al estatus de los proyectos y resolver los conflictos de recursos
- Monitorear los niveles de servicio y las mejoras del servicio

#### PO4.4 Ubicación organizacional de la función de TI

Ubicar a la función de TI dentro de la estructura organizacional general con un modelo de negocios supeditado a la importancia de TI dentro de la empresa, en especial en función de que tan crítica es para la estrategia del negocio y el nivel de dependencia operativa sobre TI. La línea de reporte del CIO es proporcional con la importancia de TI dentro de la empresa.

#### PO4.5 Estructura organizacional

Establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además implantar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos de negocio esperados y las circunstancias cambiantes.

#### PO4.6 Roles y responsabilidades

Definir y comunicar los roles y las responsabilidades para todo el personal en la organización con respecto a los sistemas de información para permitir que ejerzan los roles y responsabilidades asignados con suficiente autoridad. Crear y actualizar periódicamente la descripción de roles. Estas descripciones deben estar alineadas con la responsabilidad y la autoridad incluyendo definiciones de habilidades y experiencia necesarias en cada posición y que serán aplicables en el uso y evaluación del desempeño.

#### PO4.7 Responsabilidad de aseguramiento de calidad de TI

Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad y proporcionar al grupo de aseguramiento los sistemas de aseguramiento de calidad, los controles y la experiencia para comunicarlos. La ubicación organizacional y las responsabilidades y tamaño del grupo de aseguramiento de calidad satisfacen los requerimientos de la organización.

#### PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento

Incluir la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel senior apropiado. Definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento. Establecer responsabilidad sobre la administración del riesgo y la seguridad a nivel de toda la organización para manejar los problemas a nivel de toda la empresa. Puede ser necesario asignar responsabilidades adicionales de administración de la seguridad a nivel de sistema específico para manejar problemas relacionados con seguridad. Obtener orientación de la alta dirección con respecto al apetito de riesgo de TI y la aprobación de cualquier riesgo residual de TI.

#### PO4.9 Propiedad de datos y de sistemas

Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información. Los propietarios toman decisiones sobre la clasificación de la información y de los sistemas y sobre cómo protegerlos de acuerdo a esta clasificación.

**PO4.10 Supervisión**

Implantar prácticas adecuadas de supervisión dentro de la función de TI para garantizar que los roles y las responsabilidades se ejerzan de forma apropiada, para evaluar si todo el personal cuenta con la suficiente autoridad y recursos para ejecutar sus roles y responsabilidades y para revisar en general los indicadores clave de desempeño.

**PO4.11 Segregación de funciones**

Implantar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice solo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas.

**PO4.12 Personal de TI**

Evaluar los requerimientos de personal de forma regular o cuando existan cambios importantes en el ambiente de negocios, operativo o de TI para garantizar que la función de TI cuente con un número suficiente de personal competente. La consecución de personal toma en cuenta la co-ubicación de personal de negocios / TI, el entrenamiento cruzado- funcional, la rotación de puestos y las oportunidades de personal externo.

**PO4.13 Personal clave de TI**

Definir e identificar al personal clave de TI y minimizar la dependencia excesiva en ellos. Debe existir un plan para contactar al personal clave en caso de emergencia.

**PO4.14 Políticas y procedimientos para personal contratado**

Definir e implantar políticas y procedimientos para controlar las actividades de los consultores y otro personal contratado por la función de TI para garantizar la protección de los activos de información de la empresa y satisfacer los requerimientos contractuales.

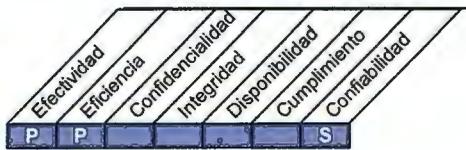
**PO4.15 Relaciones**

Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre la función de TI y otras funciones dentro y fuera de la función de TI, tales como el consejo directivo, ejecutivos, unidades de negocio, usuarios individuales, proveedores, oficiales de seguridad, gerentes de riesgo, el grupo corporativo de cumplimiento, los contratistas externos y la gerencia externa (offsite).

## Objetivo de control de alto nivel

### PO5 Administrar la inversión en TI

Establecer y mantener un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal formal y administración contra ese presupuesto. Trabajar con los interesados para identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, y tomar medidas correctivas según sean necesarias. El proceso fomenta la sociedad entre TI y los interesados del negocio, facilita el uso efectivo y eficiente de recursos de TI, y brinda transparencia y responsabilidad dentro del costo total de la propiedad, la materialización de los beneficios del negocio y el retorno sobre las inversiones en TI.



#### Control sobre el proceso TI de

Administrar la inversión en TI

que satisface el requisito de negocio de TI para

mejorar de forma continua y demostrable la rentabilidad de TI y su contribución a la rentabilidad del negocio con servicios integrados y estandarizados que satisfagan las expectativas del usuario

enfocándose en

decisiones de portafolio e inversión en TI efectivas y eficientes, y por medio del establecimiento y seguimiento del presupuestos de TI de acuerdo a la estrategia de TI y a las decisiones de inversión

se logra con

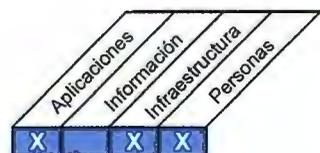
- El pronóstico y la asignación de presupuestos
- La definición de criterios formales de inversión (retorno de inversión -ROI, periodo de reintegro, valor presente neto -NPV)
- La medición y evaluación del valor del negocio en comparación con el pronóstico

y se mide con

- El porcentaje de reducción en el costo unitario del servicio de TI
- Porcentaje del valor de la desviación respecto al presupuesto en comparación con el presupuesto total
- Porcentaje de gasto de TI expresado en impulsores de valor del negocio (Ej. Incremento en ventas / servicios debidos a la mejora en conectividad)



■ Primaria □ Secundaria



## Objetivos de control detallados

### PO5 Administrar la inversión en TI

#### PO5.1 Marco de trabajo para la administración financiera

Establecer un marco de trabajo financiero para TI que impulse el presupuesto y el análisis de rentabilidad, con base en los portafolios de inversión, servicios y activos. Dar mantenimiento a los portafolios de los programas de inversión de TI, de servicios y de activos de TI, los cuales forman la base para el presupuesto corriente de TI. Brindar información de entrada hacia los casos de negocio de nuevas inversiones, tomando en cuenta los portafolios actuales de activos y servicios de TI. Las nuevas inversiones y el mantenimiento a los portafolios de servicios y de activos influenciarán el futuro presupuesto de TI. Comunicar los aspectos de costo y beneficio de estos portafolios a los procesos de priorización de presupuestos, administración de costos y administración de beneficios.

#### PO5.2 Prioridades dentro del presupuesto de TI

Implantar un proceso de toma de decisiones para dar prioridades a la asignación de recursos a TI para operaciones, proyectos y mantenimiento, para maximizar la contribución de TI a optimizar el retorno del portafolio empresarial de programas de inversión en TI y otros servicios y activos de TI.

#### PO5.3 Proceso presupuestal

Establecer un proceso para elaborar y administrar un presupuesto que refleje las prioridades establecidas en el portafolio empresarial de programas de inversión en TI, incluyendo los costos recurrentes de operar y mantener la infraestructura actual. El proceso debe dar soporte al desarrollo de un presupuesto general de TI así como al desarrollo de presupuestos para programas individuales, con énfasis especial en los componentes de TI de esos programas. El proceso debe permitir la revisión, el refinamiento y la aprobación constantes del presupuesto general y de los presupuestos de programas individuales.

#### PO5.4 IT Administración de costos

Implantar un proceso de administración de costos que compare los costos reales con los presupuestados. Los costos se deben monitorear y reportar. Cuando existan desviaciones, estas se deben identificar de forma oportuna y el impacto de esas desviaciones sobre los programas se debe evaluar y, junto con el patrocinador del negocio para estos programas, se deberán tomar las medidas correctivas apropiadas y, en caso de ser necesario, el caso de negocio del programa de inversión se deberá actualizar.

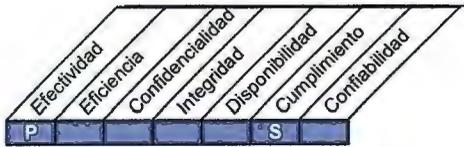
#### PO5.5 Administración de beneficios

Implantar un proceso de monitoreo de beneficios. La contribución esperada de TI a los resultados del negocio, ya sea como un componente de programas de inversión en TI o como parte de un soporte operativo regular, se debe identificar, acordar, monitorear y reportar. Los reportes se deben revisar y, donde existan oportunidades para mejorar la contribución de TI, se deben definir y tomar las medidas apropiadas. Siempre que los cambios en la contribución de TI tengan impacto en el programa, o cuando los cambios a otros proyectos relacionados impacten al programa, el caso de negocio deberá ser actualizado.

## Objetivo de control de alto nivel

### PO6 Comunicar las aspiraciones y la dirección de la gerencia

La dirección debe elaborar un marco de trabajo de control empresarial para TI, y definir y comunicar las políticas. Un programa de comunicación continua se debe implantar para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc., aprobados y apoyados por la dirección. La comunicación apoya el logro de los objetivos de TI y asegura la concientización y el entendimiento de los riesgos de negocio y de TI. El proceso debe garantizar el cumplimiento de las leyes y reglamentos relevantes.



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

#### Control sobre el proceso TI de

Comunicar las aspiraciones y la dirección de la gerencia

que satisface el requisito de negocio de TI para

una información precisa y oportuna sobre los servicios de TI actuales y futuros, los riesgos asociados y las responsabilidades

enfocándose en

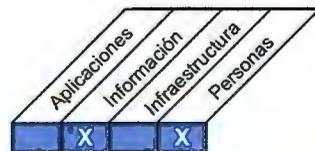
proporcionar políticas, procedimientos, directrices y otra documentación aprobada, de forma precisa y entendible y que se encuentre dentro del marco de trabajo de control de TI a los interesados

se logra con

- La definición de un marco de trabajo de control para TI
- La elaboración e implantación de políticas para TI
- El refuerzo de políticas de TI

y se mide con

- El número de interrupciones en el negocio debidas a interrupciones en el servicio de TI
- Porcentaje de interesados que entienden el marco de trabajo de control de TI de la empresa
- Porcentaje de stakeholders que no cumple las políticas



## Objetivos de control detallados

### PO6 Comunicar las aspiraciones y la dirección de la gerencia

#### PO6.1 Ambiente de políticas y de control

Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa. Estos elementos incluyen las expectativas / requerimientos respecto a la entrega de valor proveniente de las inversiones en TI, el apetito de riesgo, la integridad, los valores éticos, la competencia del personal, la rendición de cuentas y la responsabilidad. El ambiente de control se basa en una cultura que apoya la entrega de valor, mientras que al mismo tiempo administra riesgos significativos, fomenta la colaboración inter-divisional y el trabajo en equipo, promueve el cumplimiento y la mejora continua de procesos, y maneja las desviaciones (incluyendo las fallas) de forma adecuada.

#### PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI

Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial general hacia los riesgos y hacia el control interno para entregar valor mientras al mismo tiempo se protegen los recursos y sistemas de TI. El marco de trabajo debe estar integrado por el marco de procesos de TI y el sistema de administración de calidad, y debe cumplir los objetivos generales de la empresa. Debe tener como meta maximizar el éxito de la entrega de valor mientras minimiza los riesgos para los activos de información por medio de medidas preventivas, la identificación oportuna de irregularidades, la limitación de pérdidas y la oportuna recuperación de activos del negocio.

#### PO6.3 Administración de políticas para TI

Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir la intención de las políticas, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Las políticas deben incluir tópicos clave como calidad, seguridad, confidencialidad, controles internos y propiedad intelectual. Su relevancia se debe confirmar y aprobar de forma regular.

#### PO6.4 Implantación de políticas de TI

Asegurarse de que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales. Los métodos de implantación deben resolver necesidades e implicaciones de recursos y concientización.

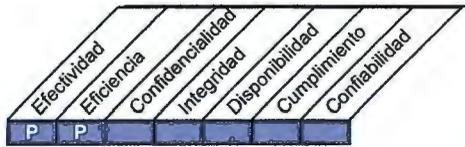
#### PO6.5 Comunicación de los objetivos y la dirección de TI

Asegurarse de que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a toda la organización. La información comunicada debe abarcar una misión claramente articulada, los objetivos de servicio, la seguridad, los controles internos, la calidad, el código de ética y conducta, políticas y procedimientos, etc., y se deben incluir dentro de un programa de comunicación continua, apoyado por la alta dirección con acciones y palabras. La dirección debe dar especial atención a comunicar la conciencia sobre la seguridad de TI y el mensaje de que la seguridad de TI es responsabilidad de todos.

## Objetivo de control de alto nivel

### PO7 Administrar los recursos humanos de TI

Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio. Esto se logra siguiendo prácticas definidas y aprobadas que apoyan el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación. Este proceso es crítico, ya que las personas son activos importantes, y el ambiente de gobierno y de control interno depende fuertemente de la motivación y competencia del personal.



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

#### Control sobre el proceso TI de

Administrar los recursos humanos de TI

que satisface el requisito de negocio de TI para

personas competentes y motivadas para crear y entregar servicios de TI

enfocándose en

la contratación y entrenamiento del personal, la motivación por medio de planes de carrera claros, la asignación de roles que correspondan a las habilidades, el establecimiento de procesos de revisión definidos, la creación de descripción de puestos y el aseguramiento de la conciencia de la dependencia sobre los individuos

se logra con

- La revisión del desempeño del personal
- La contratación y entrenamiento de personal de TI para apoyar los planes tácticos de TI
- La mitigación del riesgo de sobre-dependencia de recursos clave

y se mide con

- El nivel de satisfacción de los interesados respecto a la experiencia y habilidades del personal
- La rotación de personal de TI
- Porcentaje de personal de TI certificado de acuerdo a las necesidades del negocio



## Objetivos de control detallados

### PO7 Administrar los recursos humanos de TI

#### PO7.1 Reclutamiento y Retencion del Personal

Asegurarse que los procesos de reclutamiento del personal de TI estén de acuerdo a las políticas y procedimientos generales de personal de la organización (ej. contratación, un ambiente positivo de trabajo y orientación). La gerencia implementa procesos para garantizar que la organización cuente con una fuerza de trabajo posicionada de forma apropiada, que tenga las habilidades necesarias para alcanzar las metas organizacionales.

#### PO7.2 Competencias del personal

Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso.

#### PO7.3 Asignacion de roles

Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requisito de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales. Los términos y condiciones de empleo deben enfatizar la responsabilidad del empleado respecto a la seguridad de la información, al control interno y al cumplimiento regulatorio. El nivel de supervisión debe estar de acuerdo con la sensibilidad del puesto y el grado de responsabilidades asignadas.

#### PO7.4 Entrenamiento del personal de TI

Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales.

#### PO7.5 Dependencia sobre los individuos

Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal.

#### PO7.6 Procedimientos de Investigación del personal

Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI. El grado y la frecuencia de estas verificaciones dependen de que tan delicada ó crítica sea la función y se deben aplicar a los empleados, contratistas y proveedores.

#### PO7.7 Evaluación del desempeño del empleado

Es necesario que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto. Los empleados deben recibir adiestramiento sobre su desempeño y conducta, según sea necesario.

#### PO7.8 Cambios y terminación de trabajo

Tomar medidas expeditas respecto a los cambios en los puestos, en especial las terminaciones. Se debe realizar la transferencia del conocimiento, reasignar responsabilidades y se deben eliminar los privilegios de acceso, de tal modo que los riesgos se minimicen y se garantice la continuidad de la función.

## Objetivo de control de alto nivel

### PO8 Administrar la calidad

Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo y de adquisición. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, proporcionando requerimientos, procedimientos y políticas claras de calidad. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables. La mejora continua se logra por medio del constante monitoreo, corrección de desviaciones y la comunicación de los resultados a los interesados. La administración de calidad es esencial para garantizar que TI está dando valor al negocio, mejora continua y transparencia para los interesados.



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

#### Control sobre el proceso TI de

Administrar la calidad

que satisface el requisito de negocio de TI para

la mejora continua y medible de la calidad de los servicios prestados por TI

enfocándose en

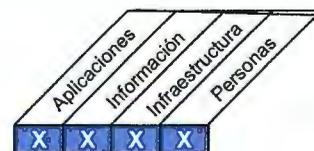
la definición de un sistema de administración de calidad (QMS, por sus siglas en inglés), el monitoreo continuo del desempeño contra los objetivos predefinidos, y la implantación de un programa de mejora continua de servicios de TI

se logra con

- La definición de estándares y prácticas de calidad
- El monitoreo y revisión interna y externa del desempeño contra los estándares y prácticas de calidad definidas
- Mejorar el QMS de manera continua

y se mide con

- Porcentaje de participantes satisfechos con la calidad (ponderado por importancia)
- Porcentaje de procesos de TI revisados de manera formal por aseguramiento de calidad de modo periódico que satisfaga las metas y objetivos de calidad
- Porcentaje de procesos que reciben revisiones de aseguramiento de calidad (QA)



## Objetivos de control detallados

### PO8 Administrar la calidad

#### PO8.1 Sistema de administración de calidad

Establecer y mantener un QMS que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad, que esté alineado con los requerimientos del negocio. El QMS identifica los requerimientos y los criterios de calidad, los procesos claves de TI, y su secuencia e interacción, así como las políticas, criterios y métodos para definir, detectar, corregir y prevenir las no conformidades. El QMS debe definir la estructura organizacional para la administración de la calidad, cubriendo los roles, las tareas y las responsabilidades. Todas las áreas clave desarrollan sus planes de calidad de acuerdo a los criterios y políticas, y registran los datos de calidad. Monitorear y medir la efectividad y aceptación del QMS y mejorarla cuando sea necesario.

#### PO8.2 Estándares y prácticas de calidad

Identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del QMS. Usar las mejores prácticas de la industria como referencia al mejorar y adaptar las prácticas de calidad de la organización.

#### PO8.3 Estándares de desarrollo y de adquisición

Adoptar y mantener estándares para todo el desarrollo y adquisición que siguen el ciclo de vida, hasta el último entregable e incluyen la aprobación en puntos clave con base en criterios de aprobación acordados. Los temas a considerar incluyen estándares de codificación de software, normas de nomenclatura; formatos de archivos, estándares de diseño para esquemas y diccionario de datos; estándares para la interfaz de usuario; inter-operabilidad; eficiencia de desempeño de sistemas; escalabilidad; estándares para desarrollo y pruebas; validación contra requerimientos; planes de pruebas; y pruebas unitarias, de regresión y de integración.

#### PO8.4 IT Enfoque en el cliente

Garantiza que la administración de calidad se enfoque en los clientes, al determinar sus requerimientos y alinearlos con los estándares y prácticas de TI. Se definen los roles y responsabilidades respecto a la resolución de conflictos entre el usuario/cliente y la organización de TI.

#### PO8.5 Mejora continua

Se elabora y comunica un plan global de calidad que promueva la mejora continua, de forma periódica.

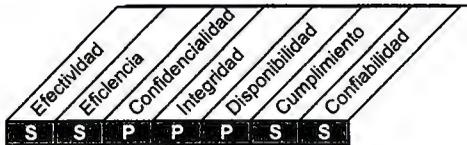
#### PO8.6 Medición, monitoreo y revisión de la calidad

Definir, planear e implantar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que QMS proporciona. La medición, el monitoreo y el registro de la información deben ser usados por el dueño del proceso para tomar las medidas correctivas y preventivas apropiadas.

## Objetivo de control de alto nivel

### PO9 Evaluar y administrar los riesgos de TI

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales acordados. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los participantes y se debe expresar en términos financieros, para permitir a los participantes alinear los riesgos a un nivel aceptable de tolerancia.



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

#### Control sobre el proceso TI de

Evaluar y administrar los riesgos de TI

que satisface el requisito de negocio de TI para

analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de negocio

enfocándose en

la elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales

se logra con

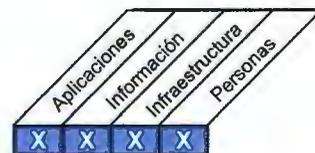
- La garantía de que la administración de riesgos está incluida completamente en los procesos administrativos, tanto interna como externamente, y se aplica de forma consistente
- La realización de evaluaciones de riesgo
- Recomendar y comunicar planes de acciones para mitigar riesgos

y se mide con

- Porcentaje de objetivos críticos de TI cubiertos por la evaluación de riesgos
- Porcentaje de riesgos críticos de TI identificados con planes de acción elaborados
- Porcentaje de planes de acción de administración de riesgos aprobados para su implantación



■ Primaria □ Secundaria



## Objetivos de control detallados

### PO9 Evaluar y administrar los riesgos de TI

#### PO9.1 Alineación de la administración de riesgos de TI y del negocio

Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización

#### PO9.2 Establecimiento del contexto del riesgo

Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

#### PO9.3 Identificación de eventos

Identificar todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto – positivo, negativo o ambos – y dar mantenimiento a esta información.

#### PO9.4 IT Evaluación de riesgos

Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

#### PO9.5 Respuesta a los riesgos

Identificar los propietarios de los riesgos y a los dueños de procesos afectados, y elaborar y mantener respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continua. La respuesta a los riesgos debe identificar estrategias de riesgo tales como evitar, reducir, compartir o aceptar. Al elaborar la respuesta, considerar los costos y beneficios y seleccionar respuestas que limiten los riesgos residuales dentro de los niveles de tolerancia de riesgos definidos.

#### PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos

Asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Buscar la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas son propiedad del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

## Objetivo de control de alto nivel

### P010 Administrar proyectos

Establecer un programa y un marco de control administrativo de proyectos para la administración de todos los proyectos de TI. El marco de trabajo debe garantizar la correcta asignación de prioridades y la coordinación de todos los proyectos. El marco de trabajo debe incluir un plan maestro, asignación de recursos, definición de entregables, aprobación de los usuarios, un enfoque de entrega por fases, aseguramiento de la calidad, un plan formal de pruebas, revisión de pruebas y revisión post-implantación después de la implantación para garantizar la administración de los riesgos del proyecto y la entrega de valor para el negocio. Este enfoque reduce el riesgo de costos inesperados y de cancelación de proyectos, mejora la comunicación y el involucramiento del negocio y de los usuarios finales, asegura el valor y la calidad de los entregables de los proyectos, y maximiza su contribución a los programas de inversión en TI.



#### Control sobre el proceso TI de

Administrar proyectos

que satisface el requisito de negocio de TI para

la entrega de resultados de proyectos dentro de marcos de tiempo, presupuesto y calidad acordados

enfocándose en

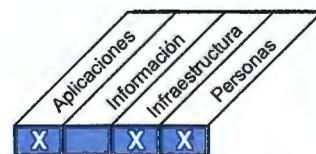
un programa y un enfoque de administración de proyectos definidos, el cual se aplica a todos los proyectos de TI, lo cual facilita la participación de los interesados y el monitoreo de los riesgos y los avances de los proyectos

se logra con

- La definición e implantación de marcos y enfoques de programas y de proyectos
- La emisión de directrices administrativas para proyectos
- La planeación de proyectos para todos los proyectos incluidos en el portafolio de proyectos

y se mide con

- Porcentaje de proyectos que satisfacen las expectativas de los stakeholders (a tiempo, dentro del presupuesto, y con satisfacción de los requerimientos – ponderados por importancia)
- Porcentaje de proyectos con revisión post-implantación
- Porcentaje de proyectos que siguen los estándares y las prácticas administrativas de los proyectos



## Objetivos de control detallados

### **P010 Administrar proyectos**

#### **P010.1 Marco de trabajo para la administración de programas**

Mantener el programa de los proyectos, relacionados con el portafolio de programas de inversión en TI, por medio de la identificación, definición, evaluación, otorgamiento de prioridades, selección, inicio, administración y control de los proyectos. Asegurarse de que los proyectos apoyen los objetivos del programa. Coordinar las actividades e interdependencias de múltiples proyectos, administrar la contribución de todos los proyectos dentro del programa hasta obtener los resultados esperados, y resolver los requerimientos y conflictos de recursos.

#### **P010.2 Marco de trabajo para la administración de proyectos**

Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas a cada proyecto emprendido. Las metodologías deben cubrir, como mínimo, el inicio, la planeación, la ejecución, el control y el cierre de las etapas de los proyectos, así como los puntos de verificación y las aprobaciones. El marco de trabajo y las metodologías de soporte se deben integrar con la administración del portafolio empresarial y con los procesos de administración de programas.

#### **P010.3 Enfoque de administración de proyectos**

Establecer un enfoque de administración de proyectos que corresponda al tamaño, complejidad y requerimientos regulatorios de cada proyecto. La estructura de gobierno de proyectos puede incluir los roles, las responsabilidades y la rendición de cuentas del patrocinador del programa, patrocinadores del proyecto, comité de dirección, oficina de proyectos, y gerente del proyecto, así como los mecanismos por medio de los cuales pueden satisfacer esas responsabilidades (tales como reportes y revisiones por etapa). Asegurarse que todos los proyectos de TI cuenten con patrocinadores con la suficiente autoridad para apropiarse de la ejecución del proyecto dentro del programa estratégico global.

#### **P010.4 Compromiso de los interesados**

Obtener el compromiso y la participación de los interesados afectados en la definición y ejecución del proyecto dentro del contexto del programa global de inversión en TI.

#### **P010.5 Estatuto de alcance del proyecto**

Definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar, entre los interesados, un entendimiento común del alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa global de inversión en TI. La definición se debe aprobar de manera formal por parte de los patrocinadores del programa y del proyecto antes de arrancar el proyecto.

#### **P010.6 Inicio de las fases del proyecto**

Asegurarse que el arranque de las etapas importantes del proyecto se apruebe de manera formal y se comunique a todos los interesados. La aprobación de la fase inicial se debe basar en las decisiones de gobierno del programa. La aprobación de las fases subsiguientes se debe basar en la revisión y aceptación de los entregables de la fase previa, y la aprobación de un caso de negocio actualizado en la próxima revisión importante del programa. En el caso de fases traslapadas, se debe establecer un punto de aprobación por parte de los patrocinadores del programa y del proyecto, para autorizar así el avance del proyecto.

#### **P010.7 Plan integrado del proyecto**

Establecer un plan integrado para el proyecto, aprobado y formal (que cubra los recursos de negocio y de los sistemas de información) para guiar la ejecución y el control del proyecto a lo largo de la vida del éste. Las actividades e interdependencias de múltiples proyectos dentro de un mismo programa se deben entender y documentar. El plan del proyecto se debe mantener a lo largo de la vida del mismo. El plan del proyecto, y las modificaciones a éste, se deben aprobar de acuerdo al marco de trabajo de gobierno del programa y del proyecto.

#### **P010.8 Recursos del proyecto**

Definir las responsabilidades, relaciones, autoridades y criterios de desempeño de los miembros del equipo del proyecto y especificar las bases para adquirir y asignar a los miembros competentes del equipo y/o a los contratistas al proyecto. La obtención de productos y servicios requeridos para cada proyecto se debe planear y administrar para alcanzar los objetivos del proyecto, usando las prácticas de adquisición de la organización.

#### **P010.9 Administración de riesgos del proyecto**

Eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, identificación, análisis, respuestas, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados. Los riesgos afrontados por el proceso de administración de proyectos y el producto entregable del proyecto se deben establecer y registrar de forma central.

**PO10.10 Plan de calidad del proyecto**

Preparar un plan de administración de la calidad que describa el sistema de calidad del proyecto y cómo será implantado. El plan debe ser revisado y acordado de manera formal por todas las partes interesadas para luego ser incorporado en el plan integrado del proyecto.

**PO10.11 Control de cambios del proyecto**

Establecer un sistema de control de cambios para cada proyecto, de tal modo que todos los cambios a la línea base del proyecto (ej. costos, cronograma, alcance y calidad) se revisen, aprueben e incorporen de manera apropiada al plan integrado del proyecto, de acuerdo al marco de trabajo de gobierno del programa y del proyecto.

**PO10.12 Planeación del proyecto y métodos de aseguramiento**

Identificar las tareas de aseguramiento requeridas para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado. Las tareas deben proporcionar la seguridad de que los controles internos y las características de seguridad satisfagan los requerimientos definidos.

**PO10.13 Medición del desempeño, reportes y monitoreo del proyecto**

Medir el desempeño del proyecto contra los criterios clave del proyecto (ej. alcance, calendario, calidad, costos y riesgos); identificar las desviaciones con respecto al plan; evaluar su impacto sobre el proyecto y sobre el programa global; reportar los resultados a los interesados clave; y recomendar, implantar y monitorear las medidas correctivas, según sea requerido, de acuerdo con el marco de trabajo de gobierno del programa y del proyecto.

**PO10.14 Cierre del proyecto**

Solicitar que al finalizar cada proyecto, los interesados del proyecto se cercioren de que el proyecto haya proporcionado los resultados y los beneficios esperados. Identificar y comunicar cualquier actividad sobresaliente requerida para alcanzar los resultados planeados del proyecto y los beneficios del programa, e identificar y documentar las lecciones aprendidas a ser usadas en futuros proyectos y programas

# ADQUIRIR E IMPLANTAR

- AI1** Identificar soluciones automatizadas
- AI2** Adquirir y mantener software aplicativo
- AI3** Adquirir y mantener infraestructura tecnológica
- AI4** Facilitar la operación y el uso
- AI5** Adquirir recursos de TI
- AI6** Administrar cambios
- AI7** Instalar y acreditar soluciones y cambios

## Objetivo de control de alto nivel

### AI1 Identificar soluciones automatizadas

La necesidad de una nueva aplicación o función requiere de análisis antes de la compra o desarrollo para garantizar que los requisitos del negocio se satisfacen con un enfoque efectivo y eficiente. Este proceso cubre la definición de las necesidades, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de costo-beneficio y concluye con una decisión final de “desarrollar” o “comprar”. Todos estos pasos permiten a las organizaciones minimizar el costo para adquirir e implantar soluciones, mientras que al mismo tiempo facilitan el logro de los objetivos del negocio.



#### Control sobre el proceso TI de

Identificar soluciones automatizadas

que satisface el requisito de negocio de TI para

traducir los requerimientos funcionales y de control a un diseño efectivo y eficiente de soluciones automatizadas

enfocándose en

la identificación de soluciones técnicamente factibles y rentables

se logra con

- La definición de los requerimientos técnicos y de negocio
- Realizar estudios de factibilidad como se define en los estándares de desarrollo
- Aprobar (o rechazar) los requerimientos y los resultados de los estudios de factibilidad

y se mide con

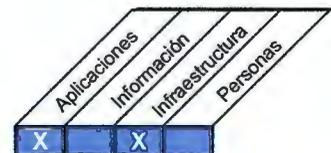
- Número de proyectos donde los beneficios establecidos no se lograron debido a suposiciones de factibilidad incorrectas
- Porcentaje de estudios de factibilidad autorizados por el propietario del proceso
- Porcentaje de usuarios satisfechos con la funcionalidad entregada

Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar



## Objetivos de control detallados

### A11 Identificar soluciones automatizadas

#### **A11.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio.**

Identificar, dar prioridades, especificar y acordar los requerimientos de negocio funcionales y técnicos que cubran el alcance completo de todas las iniciativas requeridas para lograr los resultados esperados de los programas de inversión en TI. Definir los criterios de aceptación de los requerimientos. Estas iniciativas deben incluir todos los cambios requeridos dada la naturaleza del negocio, de los procesos, de las aptitudes y habilidades del personal, su estructura organizacional y la tecnología de apoyo.

Los requerimientos toman en cuenta las necesidades funcionales, la dirección tecnológica, el desempeño, el costo, la confiabilidad, la compatibilidad, la auditoría, la seguridad, la disponibilidad y continuidad, la ergonomía, la funcionalidad, la seguridad y la legislación de la empresa. Establecer procesos para garantizar y administrar la integridad, exactitud y la validez de los requerimientos del negocio, como base para el control de la adquisición y el desarrollo continuo de sistemas. Estos requerimientos deben ser propiedad del patrocinador del negocio.

#### **A11.2 Reporte de análisis de riesgos**

Identificar, documentar y analizar los riesgos asociados con los procesos del negocio como parte de los procesos organizacionales para el desarrollo de los requerimientos. Los riesgos incluyen las amenazas a la integridad, seguridad, disponibilidad y privacidad de los datos, así como el cumplimiento de las leyes y reglamentos.

#### **A11.3 Estudio de factibilidad y formulación de cursos de acción alternativos**

Desarrollar un estudio de factibilidad que examine la posibilidad de implantar los requerimientos. Debe identificar los cursos alternativos de acción para el software, hardware, servicios y habilidades que satisfagan los requerimientos establecidos, tanto funcionales como técnicos, y evaluar la factibilidad tecnológica y económica (costo potencial y análisis de beneficios) de cada uno de los cursos de acción identificados en el contexto de inversión en TI. Es posible que existan varias iteraciones en el desarrollo del estudio de factibilidad, a medida que factores tales como los cambios a los procesos del negocio, la tecnología y las habilidades son evaluados. La administración del negocio, apoyada por la función de TI, debe evaluar la factibilidad y los cursos alternativos de acción y realizar recomendaciones al patrocinador del negocio.

#### **A11.4 Requerimientos, decisión de factibilidad y aprobación.**

El patrocinador del negocio aprueba y autoriza los requisitos de negocio, tanto funcionales como técnicos, y los reportes del estudio de factibilidad en las etapas clave predeterminadas. Cada autorización va después de la terminación de las revisiones de calidad. El patrocinador del negocio tiene la decisión final con respecto a la elección de la solución y al enfoque de adquisición.

## Objetivo de control de alto nivel

### AI2 Adquirir y mantener software aplicativo

Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la configuración en sí de acuerdo a los estándares. Esto permite a las organizaciones apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctas.



#### Control sobre el proceso TI de

Adquirir y dar mantenimiento a software aplicativo

**que satisface el requisito de negocio de TI para**

construir las aplicaciones de acuerdo con los requerimientos del negocio y haciéndolas a tiempo y a un costo razonable

**enfocándose en**

garantizar que exista un proceso de desarrollo oportuno y confiable

**se logra con**

- La traducción de requerimientos de negocio a especificaciones de diseño
- La adhesión a los estándares de desarrollo para todas las modificaciones
- La separación de las actividades de desarrollo, de pruebas y operativas

**y se mide con**

- Número de problemas en producción por aplicación, que causan tiempo perdido significativo
- Porcentaje de usuarios satisfechos con la funcionalidad entregada



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

## Objetivos de control detallados

### AI2 Adquirir y mantener software aplicativo

#### AI2.1 Diseño de alto nivel

Traducir los requerimientos del negocio a una especificación de diseño de alto nivel para desarrollo de software, tomando en cuenta las directivas tecnológicas y la arquitectura de información dentro de la organización, y aprobar las especificaciones de diseño para garantizar que el diseño de alto nivel responde a los requerimientos.

#### AI2.2 Diseño detallado

Preparar el diseño detallado y los requerimientos técnicos del software de aplicación. Definir el criterio de aceptación de los requerimientos. Aprobar los requerimientos para garantizar que corresponden al diseño de alto nivel. Los conceptos a considerar incluyen, pero no se limitan a, definir y documentar los requerimientos de entrada de datos, definir interfaces, la interface de usuario, el diseño para la recopilación de datos fuente, la especificación de programa, definir y documentar los requerimientos de archivo, requerimientos de procesamiento, definir los requerimientos de salida, control y auditabilidad, seguridad y disponibilidad, y pruebas. Realizar una reevaluación para cuando se presenten discrepancias técnicas o lógicas significativas durante el desarrollo o mantenimiento.

#### AI2.3 Control y auditabilidad de las aplicaciones

Asegurar que los controles del negocio se traduzcan correctamente en controles de aplicación de manera que el procesamiento sea exacto, completo, oportuno, aprobado y auditable. Los aspectos que se consideran especialmente son: mecanismos de autorización, integridad de la información, control de acceso, respaldo y diseño de pistas de auditoría.

#### AI2.4 Seguridad y disponibilidad de las aplicaciones.

Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados, de acuerdo con la clasificación de datos, la arquitectura de seguridad en la información de la organización y el perfil de riesgo. Los asuntos a considerar incluyen derechos de acceso y administración de privilegios, protección de información sensible en todas las etapas, autenticación e integridad de las transacciones y recuperación automática.

#### AI2.5 Configuración e implantación de software aplicativo adquirido

Personalizar e implantar la funcionalidad automatizada adquirida con el uso de procedimientos de configuración, aceptación y prueba. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.

#### AI2.6 Actualizaciones importantes en sistemas existentes

Seguir un proceso de desarrollo similar al de desarrollo de sistemas nuevos en el caso que se presenten modificaciones importantes en los sistemas existentes, que resulten en un cambio significativo de los diseños y/o funcionalidad actuales. Los aspectos a considerar incluyen análisis de impacto, justificación costo/beneficio y administración de requerimientos.

#### AI2.7 Desarrollo de software aplicativo

Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación y los requerimientos de calidad. Aprobar y autorizar cada etapa clave del proceso de desarrollo de software aplicativo, dando seguimiento a la terminación exitosa de revisiones de funcionalidad, desempeño y calidad. Los aspectos a considerar incluyen aprobar las especificaciones de diseño que satisfacen los requerimientos de negocio, funcionales y técnicos; aprobar las solicitudes de cambio; y confirmación de que el software aplicativo es compatible con la producción y está listo para su migración. Además, garantizar que se identifican y consideran todos los aspectos legales y contractuales para el software aplicativo que desarrollan terceros.

#### AI2.8 Aseguramiento de la Calidad del Software

Desarrollar, implantar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización. Los asuntos a considerar en el plan de aseguramiento de calidad incluyen especificar el criterio de calidad y los procesos de validación y verificación, incluyendo inspección, revisión de algoritmos y código fuente y pruebas.

#### AI2.9 Administración de los requerimientos de aplicaciones

Garantizar que durante el diseño, desarrollo e implantación, se da seguimiento al estatus de los requerimientos particulares (incluyendo todos los requerimientos rechazados), y que las modificaciones a los requerimientos se aprueban a través de un proceso establecido de administración de cambios.

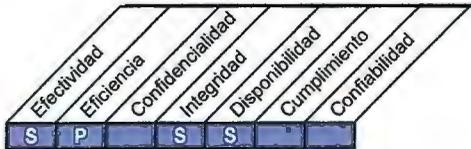
#### AI2.10 Mantenimiento de software aplicativo

Desarrollar una estrategia y un plan para el mantenimiento y liberación de aplicaciones de software. Los asuntos a considerar incluyen liberación planeada y controlada, planeación de recursos, reparación de defectos de programa y corrección de fallas, pequeñas mejoras, mantenimiento de documentación, cambios de emergencia, interdependencia con otras aplicaciones e infraestructura, estrategias de actualización, condiciones contractuales tales como aspectos de soporte y actualizaciones, revisión periódica de acuerdo a las necesidades del negocio, riesgos y requerimientos de seguridad.

## Objetivo de control de alto nivel

### AI3 Adquirir y mantener infraestructura tecnológica

Las organizaciones deben contar con procesos para adquirir, implantar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.



#### Control sobre el proceso TI de

Adquirir y dar mantenimiento a la infraestructura tecnológica

que satisface el requisito de negocio de TI para

adquirir y dar mantenimiento a una infraestructura integrada y estándar de TI

enfocándose en

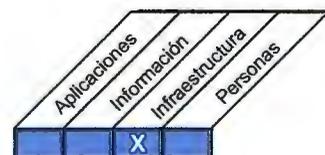
proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología

se logra con

- El establecimiento de un plan de adquisición de tecnología que se alinea con el plan de infraestructura tecnológica
- La planeación de mantenimiento de la infraestructura
- La implantación de medidas de control interno, seguridad y auditabilidad

y se mide con

- El porcentaje de plataformas que no se alinean con la arquitectura de TI definida y los estándares de tecnología
- El número de procesos de negocio críticos soportados por infraestructura obsoleta (o que pronto lo será)
- El número de componentes de infraestructura que ya no se pueden soportar (o que ya no se podrán en el futuro cercano)



# Objetivos de control detallados

## **AI3 Adquirir y mantener infraestructura tecnológica**

### **AI3.1 Plan de adquisición de infraestructura tecnológica**

Generar un plan para adquirir, implantar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica.

### **AI3.2 Protección y disponibilidad del recurso de infraestructura**

Implantar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensibles por todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso.

### **AI3.3 Mantenimiento de la Infraestructura**

Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

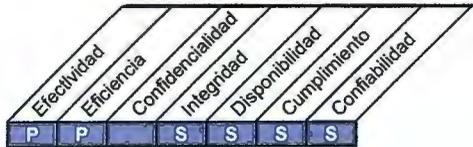
### **AI3.4 Ambiente de prueba de factibilidad**

Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo. Hay que considerar la funcionalidad, la configuración de hardware y software, pruebas de integración y desempeño, migración entre ambientes, control de las versiones, datos y herramientas de prueba y seguridad.

## Objetivo de control de alto nivel

### AI4 Facilitar la operación y el uso

El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la infraestructura.



#### Control sobre el proceso TI de

Facilitar la operación y el uso

que satisface el requisito de negocio de TI para

garantizar la satisfacción de los usuarios finales mediante ofrecimientos de servicios y niveles de servicio, y de forma transparente integrar las soluciones de aplicación y tecnología dentro de los procesos del negocio.

enfocándose en

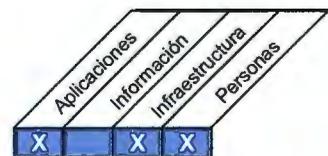
proporcionar manuales efectivos de usuario y de operación y materiales de entrenamiento para transferir el conocimiento necesario para la operación y el uso exitosos del sistema.

se logra con

- El desarrollo y la disponibilidad de documentación para transferir el conocimiento
- Comunicación y entrenamiento a usuarios y a la gerencia del negocio, al personal de apoyo y al personal de operación
- La generación de materiales de entrenamiento

y se mide con

- El número de aplicaciones en que los procedimientos de TI se integran en forma transparente dentro de los procesos de negocio
- El porcentaje de propietarios de negocios satisfechos con el entrenamiento de aplicación y los materiales de apoyo.
- El número de aplicaciones que cuentan con un adecuado entrenamiento de apoyo al usuario y a la operación



## Objetivos de control detallados

### AI4 Facilitar la operación y el uso

#### AI4.1 Plan para soluciones de operación

Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los interesados puedan tomar la responsabilidad oportunamente por la producción de procedimientos de administración, de usuario y operacionales, como resultado de la introducción o actualización de sistemas automatizados o de infraestructura.

#### AI4.2 Transferencia de conocimiento a la gerencia del negocio

Transferir el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos y ejercer la responsabilidad por la entrega y calidad del servicio, del control interno, y de los procesos administrativos de la aplicación. La transferencia de conocimiento incluye la aprobación de acceso, administración de privilegios, segregación de tareas, controles automatizados del negocio, respaldo/recuperación, seguridad física y archivo de la documentación fuente.

#### AI4.3 Transferencia de conocimiento a usuarios finales

Transferencia de conocimiento y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de aplicación como apoyo a los procesos del negocio. La transferencia de conocimiento incluye el desarrollo de un plan de entrenamiento que aborde al entrenamiento inicial y al continuo, así como el desarrollo de habilidades, materiales de entrenamiento, manuales de usuario, manuales de procedimiento, ayuda en línea, asistencia a usuarios, identificación del usuario clave, y evaluación.

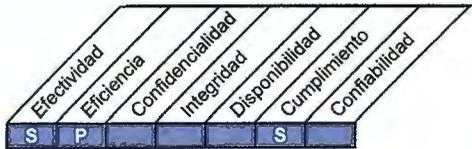
#### AI4.4 Transferencia de conocimiento al personal de operaciones y soporte

Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos. La transferencia del conocimiento debe incluir al entrenamiento inicial y continuo, el desarrollo de las habilidades, los materiales de entrenamiento, los manuales de operación, los manuales de procedimientos y escenarios de atención al usuario.

## Objetivo de control de alto nivel

### AI5 Adquirir recursos de TI

Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.



#### Control sobre el proceso TI de

Adquirir recursos de TI

que satisface el requisito de negocio de TI para

mejorar la rentabilidad de TI y su contribución a la utilidad del negocio.

enfocándose en

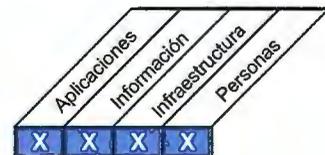
adquirir y mantener las habilidades de TI que respondan a la estrategia de entrega, en una infraestructura TI integrada y estandarizada, y reducir el riesgo de adquisición de TI

se logra con

- La obtención de asesoría profesional legal y contractual
- La definición de procedimientos y estándares de adquisición
- La adquisición de hardware, software y servicios requeridos de acuerdo con los procedimientos definidos

y se mide con

- El número de controversias en relación con los contratos de adquisición
- La reducción del costo de compra
- El porcentaje de interesados clave satisfechos con los proveedores



Planear y  
organizar

Adquirir e  
implantar

Entregar y dar  
soporte

Monitorear y  
evaluar

## Objetivos de control detallados

### AI5 Adquirir recursos de TI

#### AI5.1 Control de adquisición

Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición, para garantizar que la adquisición de infraestructura, instalaciones, hardware, software y servicios relacionados con TI, satisfagan los requerimientos del negocio.

#### AI5.2 Administración de contratos con proveedores

Formular un procedimiento para establecer, modificar y concluir contratos que apliquen a todos los proveedores. El procedimiento debe cubrir, al mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad de propiedad intelectual y de conclusión, así como obligaciones (que incluya cláusulas de penalización). Todos los contratos y las modificaciones a contratos las deben revisar asesores legales.

#### AI5.3 Selección de proveedores

Seleccionar proveedores mediante una práctica justa y formal para garantizar la escogencia del mejor con base en los requerimientos que se han desarrollado con información de proveedores potenciales y acordados entre el cliente y el(los) proveedor(es).

#### AI5.4 Adquisición de software

Garantizar que se protegen los intereses de la organización en todos los acuerdos contractuales de adquisición. Incluir y reforzar los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de software involucrados en el suministro y uso continuo de software. Estos derechos y obligaciones pueden incluir la propiedad y licencia de propiedad intelectual, mantenimiento, garantías, procedimientos de arbitraje, condiciones para la actualización y aspectos de conveniencia que incluyen seguridad, custodia y derechos de acceso.

#### AI5.5 Adquisición de recursos de desarrollo

Garantizar la protección de los intereses de la organización en todos los acuerdos contractuales de adquisición. Incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de recursos de desarrollo. Estos derechos y obligaciones pueden incluir la propiedad y licenciamiento de propiedad intelectual, aspectos de conveniencia incluyendo metodologías de desarrollo, lenguajes, pruebas, procesos de administración de calidad que comprenden los criterios de desempeño requeridos, revisión de desempeño, términos de pago, garantías, procedimientos de arbitraje, administración de recursos humanos y cumplimiento con las políticas de la organización.

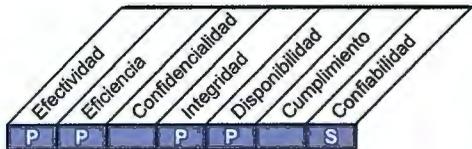
#### AI5.6 Adquisición de infraestructura, instalaciones y servicios relacionados

Incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales, que comprendan los criterios de aceptación, para la adquisición de infraestructura, instalaciones y servicios relacionados. Estos derechos y obligaciones pueden abarcar los niveles de servicio, procedimientos de mantenimiento, controles de acceso, seguridad, revisión de desempeño, términos de pago y procedimientos de arbitraje.

## Objetivo de control de alto nivel

### AI6 Administrar cambios

Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.



#### Control sobre el proceso TI de

Administrar cambios

#### que satisface el requisito de negocio de TI para

responder a los requerimientos del negocio de acuerdo con la estrategia de negocio, mientras se reducen los defectos y la repetición de trabajos en la prestación del servicio y en la solución.

#### enfocándose en

controlar la evaluación de impacto, autorización e implantación de todos los cambios a la infraestructura de TI, aplicaciones y soluciones técnicas, minimizando errores que se deben a especificaciones incompletas de la solicitud y detener la implantación de cambios no autorizados

#### se logra con

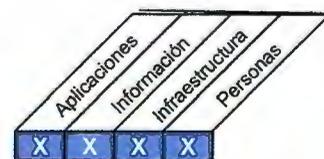
- La definición y comunicación de los procedimientos de cambio, que incluyen cambios de emergencia
- La evaluación, la asignación de prioridad y autorización de cambios
- Seguimiento del estatus y reporte de los cambios

#### y se mide con

- El número de interrupciones o errores de datos provocados por especificaciones inexactas o una evaluación de impacto incompleta
- La repetición de aplicaciones o infraestructura debida a especificaciones de cambio inadecuadas
- El porcentaje de cambios que siguen procesos de control de cambio formales



■ Primaria □ Secundaria



## Objetivos de control detallados

### AI6 Administrar cambios

#### AI6.1 Estándares y procedimientos para cambios

Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y patches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.

#### AI6.2 Evaluación de impacto, priorización y autorización

Garantizar que todas las solicitudes de cambio se evalúan de una estructurada manera en cuanto a impactos en el sistema operacional y su funcionalidad. Esta evaluación deberá incluir categorización y priorización de los cambios. Previo a la migración hacia producción, los interesados correspondientes autorizan los cambios.

#### AI6.3 Cambios de emergencia

Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia.

#### AI6.4 Seguimiento y reporte del estatus de cambio

Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales.

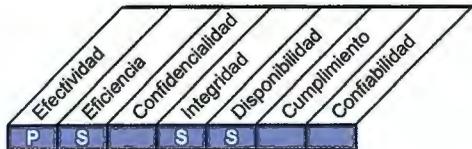
#### AI6.5 Cierre y documentación del cambio

Siempre que se implantan cambios al sistema, actualizar el sistema asociado y la documentación de usuario y procedimientos correspondientes. Establecer un proceso de revisión para garantizar la implantación completa de los cambios.

## Objetivo de control de alto nivel

### AI7 Instalar y acreditar soluciones y cambios

Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la post-implantación. Esto garantiza que los sistemas operacionales estén en línea con las expectativas convenidas y con los resultados.



#### Control sobre el proceso TI de

Instalar y acreditar soluciones y cambios

que satisface el requisito de negocio de TI para

contar con sistemas nuevos o modificados que trabajen sin problemas importantes después de la instalación

enfocándose en

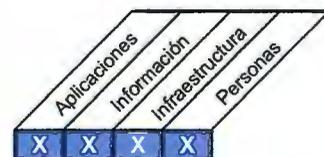
probar que las soluciones de aplicaciones e infraestructura son apropiadas para el propósito deseado y estén libre de errores, y planear las liberaciones a producción

se logra con

- El establecimiento de una metodología de prueba
- Realizar la planeación de la liberación (release)
- Evaluar y aprobar los resultados de las pruebas por parte de la gerencia del negocio
- Ejecutar revisiones posteriores a la implantación

y se mide con

- Tiempo perdido de la aplicación o problemas de datos provocados por pruebas inadecuadas
- Porcentaje de sistemas que satisfacen los beneficios esperados, medidos en el proceso posterior a la implantación
- Porcentaje de proyectos con plan de prueba documentado y aprobado



## Objetivos de control detallados

### AI7 Instalar y acreditar soluciones y cambios

#### AI7.1 Entrenamiento

Entrenar al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de desarrollo, implantación o modificación de sistemas de información.

#### AI7.2 Plan de prueba

Establecer un plan de pruebas y obtener la aprobación de las partes relevantes. El plan de pruebas se basa en los estándares de toda la organización y define roles, responsabilidades y criterios de éxito. El plan considera la preparación de pruebas (incluye la preparación del sitio), requerimientos de entrenamiento, instalación o actualización de un ambiente de pruebas definido, planear / ejecutar / documentar / retener casos de prueba, manejo y corrección de errores y aprobación formal. Con base en la evaluación de riesgos de fallas en el sistema y en la implantación, el plan deberá incluir los requerimientos de prueba de desempeño, stress, de usabilidad, piloto y de seguridad.

#### AI7.3 Plan de implantación

Establecer un plan de implantación y obtener la aprobación de las partes relevantes. El plan define el diseño de versiones (release), construcción de paquetes de versiones, procedimientos de implantación / instalación, manejo de incidentes, controles de distribución (incluye herramientas), almacenamiento de software, revisión de la versión y documentación de cambios. El plan deberá también incluir medidas de respaldo/ y vuelta atrás.

#### AI7.4 Ambiente de prueba

Establecer un ambiente de prueba separado para pruebas. Este ambiente debe reflejar el ambiente futuro de operaciones (por ejemplo, seguridad similar, controles internos y cargas de trabajo) para permitir pruebas acertadas. Se deben tener presentes los procedimientos para garantizar que los datos utilizados en el ambiente de prueba sean representativos de los datos (se limpian si es necesario) que se utilizarán eventualmente en el ambiente de operación. Proporcionar medidas adecuadas para prevenir la divulgación de datos sensibles. La documentación de los resultados de las pruebas se debe archivar.

#### AI7.5 Conversión de sistema y datos

Garantizar que los métodos de desarrollo de la organización, contemplan para todos los proyectos de desarrollo, implantación o modificación, que todos los elementos necesarios, tales como hardware, software, datos de transacciones, archivos maestros, respaldos y archivos, interfaces con otros sistemas, procedimientos, documentación de sistemas, etc., sean convertidos del viejo al nuevo sistema de acuerdo con un plan preestablecido. Se desarrolla y mantiene una pista de auditoría de los resultados previos y posteriores a la conversión. Los propietarios del sistema llevan a cabo una verificación detallada del proceso inicial del nuevo sistema para confirmar una transición exitosa.

#### AI7.6 Prueba de cambios

Garantizar que se prueban los cambios de acuerdo con el plan de aceptación definido y en base en una evaluación de impacto y recursos que incluye el dimensionamiento del desempeño en un ambiente separado de prueba, por parte de un grupo de prueba independiente (de los constructores) antes de comenzar su uso en el ambiente de operación regular. Las pruebas paralelas o piloto se consideran parte del plan. Los controles de seguridad se prueban y evalúan antes de la liberación, de manera que se pueda certificar la efectividad de la seguridad. Los planes de respaldo/vuelta atrás se deben desarrollar y probar antes de transferir el cambio a producción.

#### AI7.7 Prueba final de aceptación

Garantizar que los procedimientos proporcionan, como parte de la aceptación final o prueba de aseguramientos de la calidad de los sistemas de información nuevos o modificados, una evaluación formal y la aprobación de los resultados de prueba por parte de la gerencia de los departamentos afectados del usuario y la función de TI. Las pruebas deberán cubrir todos los componentes del sistema de información (ejemplo, software aplicativo, instalaciones, procedimientos de tecnología y usuario) y garantizar que los requerimientos de seguridad de la información se satisfacen para todos los componentes. Los datos de prueba se deben salvar para propósitos de pistas de auditoría y para pruebas futuras.

#### AI7.8 Transferencia a producción

Implantar procedimientos formales para controlar la transferencia del sistema desde el ambiente de desarrollo al de pruebas, de acuerdo con el plan de implantación. La gerencia debe requerir que se obtenga la autorización del propietario del sistema antes de que se mueva un nuevo sistema a producción y que, antes de que se descontinúe el viejo sistema, el nuevo haya operado exitosamente a través de ciclos de producción diarios, mensuales, trimestrales y de fin de año.

#### AI7.9 Liberación de software

Garantizar que la liberación del software se regula con procedimientos formales que aseguren la autorización, acondicionamiento, pruebas de regresión, distribución, transferencia de control, rastreo de estatus, procedimientos de respaldo y notificación de usuario.

#### AI7.10 Distribución del sistema

Establecer procedimientos de control para asegurar la distribución oportuna y correcta, y la actualización de los componentes aprobados de la configuración. Esto implica controles de integridad; segregación de funciones entre los que construyen, prueban y operan; y adecuadas pistas de auditoría de todas las actividades.



## Objetivos de control detallados

### **AI7.11 Registro y rastreo de cambios**

Automatizar el sistema utilizado para monitorear cambios a sistemas aplicativos para soportar el registro y rastreo de cambios hechos en aplicaciones, procedimientos, procesos, sistemas y parámetros de servicio, y a las plataformas subyacentes.

### **AI7.12 Revisión posterior a la implantación**

Establecer procedimientos de acuerdo con los estándares de desarrollo y de cambios de la empresa, que requieren una revisión posterior a la implantación del sistema de información en operación para evaluar y reportar si el cambio satisfizo los requerimientos del cliente y entregó los beneficios visualizados, de la forma más rentable.

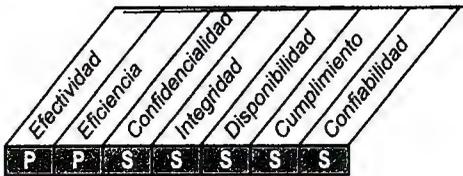
# ENTREGAR Y DAR SOPORTE

- DS1 Definir y administrar los niveles de servicio
- DS2 Administrar los servicios de terceros
- DS3 Administrar el desempeño y la capacidad
- DS4 Garantizar la continuidad del servicio
- DS5 Garantizar la seguridad de los sistemas
- DS6 Identificar y asignar costos
- DS7 Educar y entrenar a los usuarios
- DS8 Administrar la mesa de servicio y los incidentes
- DS9 Administrar la configuración
- DS10 Administrar los problemas
- DS11 Administrar los datos
- DS12 Administrar el ambiente físico
- DS13 Administrar las operaciones

## Objetivo de control de alto nivel

### DS1 Definir y administrar niveles de servicio

Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los participantes sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.



#### Control sobre el proceso TI de

Definir y manejar niveles de servicio

**que satisface el requisito de negocio de TI para**

Asegurar la alineación de los servicios claves de TI con la estrategia del negocio

**enfocándose en**

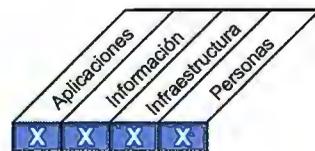
la identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio

**se logra con**

- La formalización de acuerdos internos y externos en línea con los requerimientos y las capacidades de entrega
- La notificación del cumplimiento de los niveles de servicio (reportes y reuniones)
- La identificación y comunicación de requerimientos de servicios actualizados y nuevos para planeación estratégica.

**y se mide con**

- El porcentaje de participantes satisfechos de que la entrega del servicio cumple con los niveles previamente acordados.
- El número de servicios entregados que no están en el catálogo
- El número de reuniones formales de revisión del Acuerdo de Niveles de Servicio (SLA) con las personas de negocio por año



## Objetivos de control detallados

### DS1 Definir y administrar los niveles de servicio

#### DS1.1 Marco de trabajo de la administración de los niveles de servicio

Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el cliente y el prestador de servicio. El marco de trabajo mantiene una alineación continua con los requerimientos y las prioridades de negocio y facilita el entendimiento común entre el cliente y el(los) prestador(es) de servicio. El marco de trabajo incluye procesos para la creación de requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLAs), acuerdos de niveles de operación (OLAs) y las fuentes de financiamiento. Estos atributos están organizados en un catálogo de servicios. El marco de trabajo define la estructura organizacional para la administración del nivel de servicio, incluyendo los roles, tareas y responsabilidades de los proveedores externos e internos y de los clientes.

#### DS1.2 Definición de servicios

Definiciones base de los servicios de TI sobre las características del servicio y los requerimientos de negocio, organizados y almacenados de manera centralizada por medio de la implantación de un enfoque de catálogo/portafolio de servicios.

#### DS1.3 Acuerdos de niveles de servicio

Definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del cliente y las capacidades en TI. Esto incluye los compromisos del cliente, los requerimientos de soporte para el servicio, métricas cualitativas y cuantitativas para la medición del servicio firmado por los interesados, en caso de aplicar, los arreglos comerciales y de financiamiento, y los roles y responsabilidades, incluyendo la revisión del SLA. Los puntos a considerar son disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de continuidad, seguridad y restricciones de demanda.

#### DS1.4 Acuerdos de niveles de operación

Asegurar que los acuerdos de niveles de operación expliquen cómo serán entregados técnicamente los servicios para soportar el (los) SLA(s) de manera óptima. Los OLAs especifican los procesos técnicos en términos entendibles para el proveedor y pueden soportar diversos SLAs.

#### DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio

Monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto.

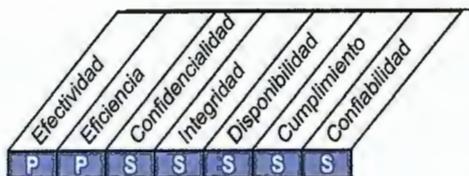
#### DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos

Revisar regularmente con los proveedores internos y externos los acuerdos de niveles de servicio y los contratos de apoyo, para asegurar que son efectivos, que están actualizados y que se han tomado en cuenta los cambios en requerimientos.

## Objetivo de control de alto nivel

### DS2 Administrar los servicios de terceros

La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.



#### Control sobre el proceso TI de

Administrar servicios de terceros

#### que satisface el requisito de negocio de TI para

Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos

#### enfocándose en

el establecimiento de relaciones y responsabilidades bilaterales con proveedores calificados de servicios tercerizados y el monitoreo de la prestación del servicio para verificar y asegurar la adherencia a los convenios.

#### se logra con

- La identificación y categorización de los servicios del proveedor
- La identificación y mitigación de riesgos del proveedor
- El monitoreo y la medición del desempeño del proveedor

#### y se mide con

- El número de quejas de los usuarios debidas a los servicios contratados
- El porcentaje de los principales proveedores que cumplen claramente los requerimientos definidos y los niveles de servicio
- El porcentaje de los principales proveedores sujetos a monitoreo



■ Primaria □ Secundaria



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

# Objetivos de control detallados

## **DS2 Administrar los servicios de terceros**

### **DS2.1 Identificación de las relaciones con todos los proveedores**

Identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad. Mantener documentación formal de las relaciones técnicas y organizacionales incluyendo los roles y responsabilidades, metas, expectativas, entregables esperados y credenciales de los representantes de estos proveedores.

### **DS2.2 Administración de las relaciones con los proveedores**

Formalizar el proceso de administración de relaciones con proveedores por cada proveedor. Los responsables de las relaciones deben coordinar a los proveedores y los clientes y asegurar la calidad de las relaciones con base en la confianza y la transparencia (por ejemplo, a través de acuerdos de niveles de servicio).

### **DS2.3 Administración de riesgos del proveedor**

Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener una efectiva entrega de servicios de forma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los estándares universales del negocio de conformidad con los requerimientos legales y regulatorios. La administración del riesgo debe considerar además acuerdos de confidencialidad (NDAs), contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, etc.

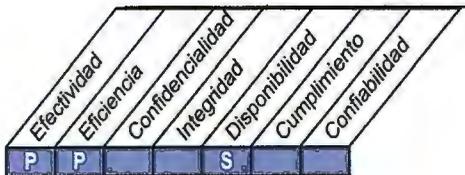
### **DS2.4 Monitoreo del desempeño del proveedor**

Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con los requerimientos del negocio actuales y que se apega de manera continua a los acuerdos del contrato y a los convenios de niveles de servicio, y que el desempeño es competitivo respecto a los proveedores alternativos y a las condiciones del mercado.

## Objetivo de control de alto nivel

### DS3 Administrar el desempeño y la capacidad

La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda la seguridad de que los recursos de información que soportan los requerimientos del negocio están disponibles de manera continua.



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

#### Control sobre el proceso TI de

Administrar el desempeño y la capacidad

que satisface el requisito de negocio de TI para

Optimizar el desempeño de la infraestructura, los recursos y las capacidades de TI en respuesta a las necesidades del negocio.

enfocándose en

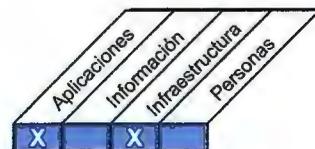
cumplir con los requerimientos de tiempo de respuesta de los acuerdos de niveles de servicio, minimizando el tiempo sin servicio y haciendo mejoras continuas de desempeño y capacidad de TI a través del monitoreo y la medición.

se logra con

- La planeación y la entrega de capacidad y disponibilidad del sistema
- Monitoreando y reportando el desempeño del sistema
- Modelando y pronosticando el desempeño del sistema.

y se mide con

- Número de horas perdidas por usuario por mes, debidas a la falta de planeación de la capacidad
- Porcentaje de picos donde se excede la meta de utilización
- Porcentaje de SLAs de tiempo de respuesta que no se satisfacen



# Objetivos de control detallados

## DS3 Administrar el desempeño y la capacidad

### DS3.1 Planeación del desempeño y la capacidad

Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, con costos justificables, para procesar las cargas de trabajo acordadas tal como se determina en los SLAs. Los planes de capacidad y desempeño deben hacer uso de técnicas de modelado apropiadas para producir un modelo de desempeño, de capacidad y de rendimiento de los recursos de TI, tanto actual como pronosticado.

### DS3.2 Capacidad y desempeño actual

Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados.

### DS3.3 Capacidad y desempeño futuros

Llevar a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño. Identificar también el exceso de capacidad para una posible redistribución. Identificar las tendencias de las cargas de trabajo y determinar los pronósticos que serán parte de los planes de capacidad y de desempeño.

### DS3.4 Disponibilidad de recursos de TI

Brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI. Deben tomarse medidas cuando el desempeño y la capacidad no están en el nivel requerido, tales como dar prioridad a las tareas, mecanismos de tolerancia de fallas y prácticas de asignación de recursos. La gerencia debe garantizar que los planes de contingencia consideran de forma apropiada la disponibilidad, capacidad y desempeño de los recursos individuales de TI.

### DS3.5 Monitoreo y reporte

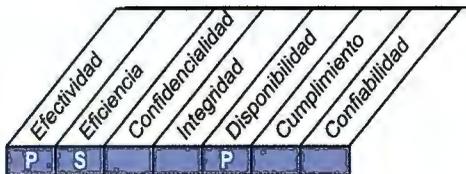
Monitorear continuamente el desempeño y la capacidad de los recursos de TI. La información reunida sirve para dos propósitos:

- Mantener y poner a punto el desempeño actual dentro de TI y atender temas como resiliencia, contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos.
- Para reportar la disponibilidad hacia el negocio del servicio prestado como se requiere en los SLAs. Acompañar todos los reportes de excepción con recomendaciones para llevar a cabo acciones correctivas.

## Objetivo de control de alto nivel

### DS4 Garantizar la continuidad del servicio

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.



#### Control sobre el proceso TI de

Garantizar la continuidad del servicio

que satisface el requisito de negocio de TI para

asegurar el mínimo impacto al negocio en caso de una interrupción de servicios de TI.

enfocándose en

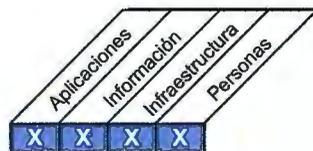
el desarrollo de resistencia (resilience) en las soluciones automatizadas y desarrollando, manteniendo y probando los planes de continuidad de TI

se logra

- Desarrollando y manteniendo (mejorando) los planes de contingencia de TI
- Con entrenamiento y pruebas de los planes de contingencia de TI
- Guardando copias de los planes de contingencia y de los datos fuera de las instalaciones.

y se mide con

- Número de horas perdidas por usuario por mes, debidas a interrupciones no planeadas
- Número de procesos críticos de negocio que dependen de TI, que no están cubiertos por un plan de continuidad.



## Objetivos de control detallados

### DS4 Garantizar la continuidad de los servicios

#### DS4.1 IT Marco de trabajo de continuidad

Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

#### DS4.2 Planes de continuidad de TI

Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

#### DS4.3 Recursos críticos de TI

Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.

#### DS4.4 Mantenimiento del plan de continuidad de TI

Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.

#### DS4.5 Pruebas del plan de continuidad de TI

Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integradas, en pruebas de punta a punta y en pruebas integradas con el proveedor.

#### DS4.6 Entrenamiento del plan de continuidad de TI

Asegurarse de que todas las partes involucradas reciban sesiones de capacitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.

#### DS4.7 Distribución del plan de continuidad de TI

Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre.

#### DS4.8 Recuperación y reanudación de los servicios de TI

Planear las acciones a tomar durante el periodo en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio.

#### DS4.9 Almacenamiento de respaldos fuera de las instalaciones

Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

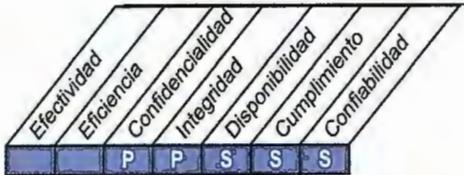
#### DS4.10 Revisión post-reanudación

Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

## Objetivo de control de alto nivel

### DS5 Garantizar la seguridad de los sistemas

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

#### Control sobre el proceso TI de

Garantizar la seguridad de los sistemas

#### que satisface el requisito de negocio de TI para

mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad.

#### enfocándose en

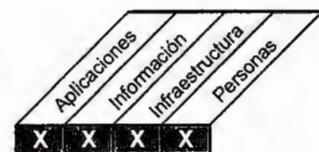
la definición de políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.

#### se logra con

- El entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad.
- La administración de identidades y autorizaciones de los usuarios de forma estandarizada.
- Probando la seguridad de forma regular.

#### y se mide con

- El número de incidentes que dañan la reputación con el público
- El número de sistemas donde no se cumplen los requerimientos de seguridad
- El número de de violaciones en la segregación de tareas.



## Objetivos de control detallados

### DS5 Garantizar la seguridad de los sistemas

#### DS5.1 Administración de la seguridad de TI

Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.

#### DS5.2 Plan de seguridad de TI

Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios.

#### DS5.3 Administración de identidad

Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

#### DS5.4 Administración de cuentas del usuario

Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.

#### DS5.5 Pruebas, vigilancia y monitoreo de la seguridad

Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. El acceso a la información de ingreso al sistema está alineado con los requerimientos del negocio en términos de requerimientos de retención y de derechos de acceso.

#### DS5.6 Definición de incidente de seguridad

Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.

#### DS5.7 Protección de la tecnología de seguridad

Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo. Sin embargo no hay que hacer que la seguridad de los sistemas dependa de la confidencialidad de las especificaciones de seguridad.

#### DS5.8 Administración de llaves criptográficas

Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

#### DS5.9 Prevención, detección y corrección de software malicioso

Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc.).

#### DS5.10 Seguridad de la red

Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

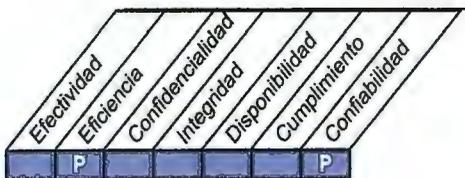
#### DS5.11 Intercambio de datos sensibles

Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.

## Objetivo de control de alto nivel

### DS6 Identificar y asignar costos

La necesidad de un sistema justo y equitativo para asignar costos de TI al negocio, requiere de una medición precisa y un acuerdo con los usuarios del negocio sobre una asignación justa. Este proceso incluye la construcción y operación de un sistema para capturar, distribuir y reportar costos de TI a los usuarios de los servicios. Un sistema equitativo de costos permite al negocio tomar decisiones más informadas respecto al uso de los servicios de TI.



#### Control sobre el proceso TI de

Identificar y asignar costos

#### que satisface el requisito de negocio de TI para

transparentar y entender los costos de TI y mejorar la rentabilidad a través del uso bien informado de los servicios de TI

#### enfocándose en

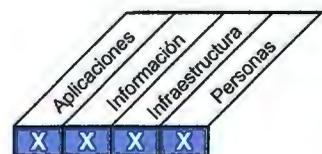
el registro completo y preciso de los costos de TI, un sistema equitativo para asignación acordado con los usuarios de negocio, y un sistema para reportar oportunamente el uso de TI y los costos asignados.

#### se logra con

- La alineación de cargos con la calidad y cantidad de los servicios brindados
- La construcción y aceptación de un modelo de costos completo
- La aplicación de cargos con base en la política acordada.

#### y se mide con

- Porcentaje de facturas de servicios de TI aceptadas/pagadas por la gerencia del negocio.
- Porcentaje de variación entre los presupuestos, pronósticos y costos actuales.
- Porcentaje de costos totales de TI que son distribuidos de acuerdo con los modelos acordados.



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

# Objetivos de control detallados

## **DS6 Identificar y asignar costos**

### **DS6.1 Definición de servicios**

Identificar todos los costos de TI y equiparlos a los servicios de TI para soportar un modelo de costos transparente. Los servicios de TI deben vincularse a los procesos del negocio de forma que el negocio pueda identificar los niveles de facturación de los servicios asociados.

### **DS6.2 Contabilización de TI**

Registrar y asignar los costos actuales de acuerdo con el modelo de costos definido. Las variaciones entre los presupuestos y los costos actuales deben analizarse y reportarse de acuerdo con los sistemas de medición financiera de la empresa.

### **DS6.3 Modelación de costos y cargos**

Con base en la definición del servicio, definir un modelo de costos que incluya costos directos, indirectos y fijos de los servicios, y que ayude al cálculo de tarifas de reintegros de cobro por servicio. El modelo de costos debe estar alineado con los procedimientos de contabilización de costos de la empresa. El modelo de costos de TI debe garantizar que los cargos por servicios son identificables, medibles y predecibles por parte de los usuarios para propiciar el adecuado uso de recursos. La gerencia del usuario debe poder verificar el uso actual y los cargos de los servicios.

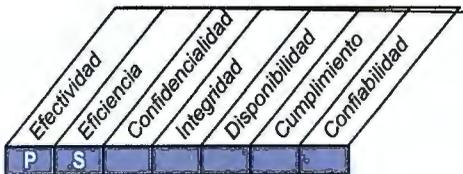
### **DS6.4 Mantenimiento del modelo de costos**

Revisar y comparar de forma regular lo apropiado del modelo de costos/recargos para mantener su relevancia para el negocio en evolución y para las actividades de TI.

## Objetivo de control de alto nivel

### DS7 Educar y entrenar a los usuarios

Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios.



#### Control sobre el proceso TI de

Educar y entrenar a los usuarios

#### que satisface el requisito de negocio de TI para

el uso efectivo y eficiente de soluciones y aplicaciones tecnológicas y el cumplimiento del usuario con las políticas y procedimientos

#### enfocándose en

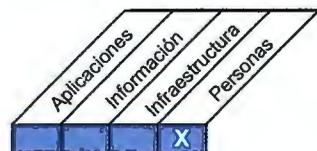
un claro entendimiento de las necesidades de entrenamiento de los usuarios de TI, la ejecución de una efectiva estrategia de entrenamiento y la medición de resultados.

#### se logra con

- Establecer un programa de entrenamiento
- Organizar el entrenamiento
- Impartir el entrenamiento
- Monitorear y reportar la efectividad del entrenamiento.

#### y se mide con

- Número de llamadas de soporte debido a problemas de entrenamiento
- Porcentaje de satisfacción de los participantes con el entrenamiento recibido
- Lapso de tiempo entre la identificación de la necesidad de entrenamiento y la impartición del mismo.



## Objetivos de control detallados

### **DS7 Educar y entrenar a los usuarios**

#### **DS7.1 Identificación de necesidades de entrenamiento y educación**

Establecer y actualizar de forma regular un programa de entrenamiento para cada grupo objetivo de empleados, que incluya:

- Estrategias y requerimientos actuales y futuros del negocio.
- Valores corporativos (valores éticos, cultura de control y seguridad, etc.)
- Implementación de nuevo software e infraestructura de TI (paquetes y aplicaciones)
- Habilidades, perfiles de competencias y certificaciones actuales y/o credenciales necesarias.
- Métodos de impartición (por ejemplo, aula, web), tamaño del grupo objetivo, accesibilidad y tiempo.

#### **DS7.2 Impartición de entrenamiento y educación**

Con base en las necesidades de entrenamiento identificadas, identificar: a los grupos objetivo y a sus miembros, a los mecanismos de impartición eficientes, a maestros, instructores y consejeros. Designar instructores y organizar el entrenamiento con tiempo suficiente. Debe tomarse nota del registro (incluyendo los prerrequisitos), la asistencia, y de las evaluaciones de desempeño.

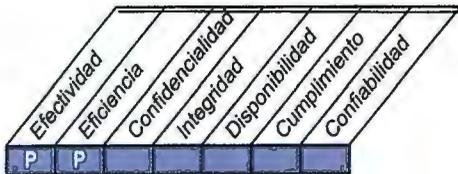
#### **DS7.3 Evaluación del entrenamiento recibido**

Al finalizar el entrenamiento, evaluar el contenido de la capacitación respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor. Los resultados de esta evaluación deben contribuir en la definición futura de los planes de estudio y de las sesiones de entrenamiento.

## Objetivo de control de alto nivel

### DS8 Administrar la mesa de servicio y los incidentes

Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y bien ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raíz y resolución. Los beneficios del negocio incluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo.



#### Control sobre el proceso TI de

Administrar la mesa de servicio y los incidentes

#### que satisface el requisito de negocio de TI para

permitir el efectivo uso de los sistemas de TI garantizando la resolución y el análisis de las consultas de los usuarios finales, incidentes y preguntas.

#### enfocándose en

una función profesional de mesa de servicio, con tiempo de respuesta rápido, procedimientos de escalamiento claros y análisis de tendencias y de resolución.

#### se logra con

- Instalación y operación de un servicio de una mesa de servicios
- Monitoreo y reporte de tendencias
- Definición de procedimientos y de criterios de escalamiento claros

#### y se mide con

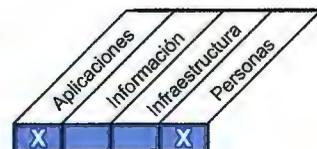
- Satisfacción del usuario con el soporte de primera línea
- Porcentaje de incidentes resueltos dentro de un lapso de tiempo aceptable / acordado.
- Índice de abandono de llamadas

Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar



## Objetivos de control detallados

### **DS8 Administrar la mesa de servicio y los incidentes**

#### **DS8.1 Mesa de Servicios**

Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Deben existir procedimientos de monitoreo y escalamiento basados en los niveles de servicio acordados en los SLAs, que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información. Medir la satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI.

#### **DS8.2 Registro de consultas de clientes**

Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información. Debe trabajar estrechamente con los procesos de administración de incidentes, administración de problemas, administración de cambios, administración de capacidad y administración de disponibilidad. Los incidentes deben clasificarse de acuerdo al negocio y a la prioridad del servicio y enrutarse al equipo de administración de problemas apropiado y se debe mantener informados a los clientes sobre el estatus de sus consultas.

#### **DS8.3 Escalamiento de incidentes**

Establecer procedimientos de mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente de acuerdo con los límites acordados en el SLA y, si es adecuado, brindar soluciones alternas. Garantizar que la asignación de incidentes y el monitoreo del ciclo de vida permanecen en la mesa de servicios, independientemente de qué grupo de TI esté trabajando en las actividades de resolución.

#### **DS8.4 Cierre de incidentes**

Establecer procedimientos para el monitoreo puntual de la resolución de consultas de los clientes. Cuando se resuelve el incidente la mesa de servicios debe registrar la causa raíz, si la conoce, y confirmar que la acción tomada fue acordada con el cliente.

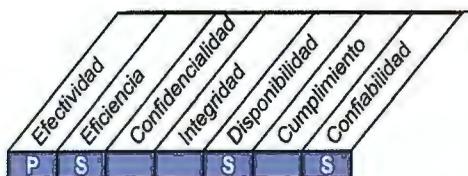
#### **DS8.5 Análisis de tendencias**

Emitir reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.

## Objetivo de control de alto nivel

### DS9 Administrar la configuración

Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite. Una efectiva administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción y resuelve los problemas más rápido.



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

#### Control sobre el proceso TI de

Administrar la configuración

#### que satisface el requisito de negocio de TI para

optimizar la infraestructura, recursos y capacidades de TI, y llevar registro de los activos de TI.

#### enfocándose en

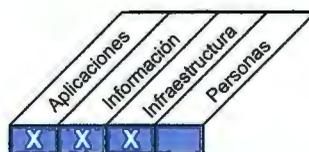
establecer y mantener un repositorio completo y preciso de atributos de la configuración de los activos y de líneas base y compararlos contra la configuración actual.

#### se logra con

- El establecimiento de un repositorio central de todos los elementos de la configuración
- La identificación de los elementos de configuración y su mantenimiento
- Revisión de la integridad de los datos de configuración.

#### y se mide con

- El número de problemas de cumplimiento del negocio debido a inadecuada configuración de los activos.
- El número de desviaciones identificadas entre el repositorio de configuración y la configuración actual de los activos.
- Porcentaje de licencias compradas y no registradas en el repositorio.



## Objetivos de control detallados

### DS9 Administrar la configuración

#### DS9.1 Repositorio de configuración y línea base

Establecer un repositorio central que contenga toda la información referente a los elementos de configuración. Este repositorio incluye hardware, software aplicativo, middleware, parámetros, documentación, procedimientos y herramientas para operar, acceder y utilizar los sistemas y los servicios. La información importante a considerar es el nombre, números de versión y detalles de licenciamiento. Una línea base de elementos de configuración debe mantenerse para cada sistema y servicio, como un punto de control al cual regresar después de realizar cambios.

#### DS9.2 Identificación y mantenimiento de elementos de configuración

Contar con procedimientos en orden para:

- Identificar elementos de configuración y sus atributos
- Registrar elementos de configuración nuevos, modificados y eliminados
- Identificar y mantener las relaciones entre los elementos de configuración y el repositorio de configuraciones.
- Actualizar los elementos de configuración existentes en el repositorio de configuraciones.
- Prevenir la inclusión de software no-autorizado

Estos procedimientos deben brindar una adecuada autorización y registro de todas las acciones sobre el repositorio de configuración y estar integrados de forma apropiada con los procedimientos de administración de cambios y administración de problemas.

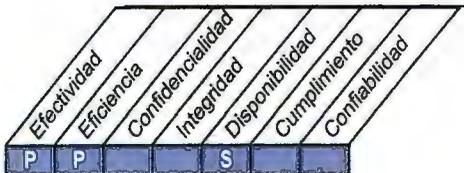
#### DS9.3 Revisión de integridad de la configuración

Revisar y verificar de manera regular, utilizando cuando sea necesario herramientas apropiadas, el estatus de los elementos de configuración para confirmar la integridad de la configuración de datos actual e histórica y para comparar con la situación actual. Revisar periódicamente contra la política de uso de software, la existencia de cualquier software personal o no autorizado de cualquier instancia de software por encima de los acuerdos de licenciamiento actuales. Los errores y las desviaciones deben reportarse, atenderse y corregirse.

## Objetivo de control de alto nivel

### DS10 Administración de problemas

Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la conveniencia y satisfacción del usuario.



#### Control sobre el proceso TI de

Administración de problemas

#### que satisface el requisito de negocio de TI para

garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio, reducir el retrabajo y los defectos en la prestación de los servicios y de las soluciones.

#### enfocándose en

registrar, rastrear y resolver problemas operativos; investigación de las causas raíz de todos los problemas relevantes y definir soluciones para los problemas operativos identificados.

#### se logra

- Realizando un análisis de causas raíz de los problemas reportados
- Analizando las tendencias
- Tomando propiedad de los problemas y con una resolución de problemas progresiva.

#### y se mide con

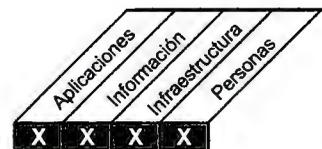
- Número de problemas recurrentes con impacto en el negocio
- Porcentaje de problemas resueltos dentro del período de tiempo solicitado
- Frecuencia de los reportes o actualizaciones sobre un problema en curso, con base en la severidad del problema.

Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar



# Objetivos de control detallados

## DS10 Administración de problemas

### DS10.1 Identificación y clasificación de problemas

Implementar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes. Los pasos involucrados en la clasificación de problemas son similares a los pasos para clasificar incidentes; son determinar la categoría, impacto, urgencia y prioridad. Los problemas deben categorizarse de manera apropiada en grupos o dominios relacionados (por ejemplo, hardware, software, software de soporte). Estos grupos pueden coincidir con las responsabilidades organizacionales o con la base de usuarios y clientes, y son la base para asignar los problemas al personal de soporte.

### DS10.2 Rastreo y resolución de problemas

El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados considerando:

- Todos los elementos de configuración asociados
- Problemas e incidentes sobresalientes
- Errores conocidos y sospechados

Identificar e iniciar soluciones sostenibles indicando la causa raíz, incrementando las solicitudes de cambio por medio del proceso de administración de cambios establecido. En todo el proceso de resolución, la administración de problemas debe obtener reportes regulares de la administración de cambios sobre el progreso en la resolución de problemas o errores. La administración de problemas debe monitorear el continuo impacto de los problemas y errores conocidos en los servicios a los usuarios. En caso de que el impacto se vuelva severo, la administración de problemas debe escalar el problema, tal vez refiriéndolo a un comité determinado para incrementar la prioridad de la solicitud del cambio (RFC) o para implementar un cambio urgente, lo que resulte más pertinente. El avance de la resolución de un problema debe ser monitoreado contra los SLAs.

### DS10.3 Cierre de problemas

Disponer de un procedimiento para cerrar registros de problemas ya sea después de confirmar la eliminación exitosa del error conocido o después de acordar con el negocio cómo manejar el problema de manera alternativa.

### DS10.4 Integración de las administraciones de cambios, configuración y problemas

Para garantizar una adecuada administración de problemas e incidentes, integrar los procesos relacionados de administración de cambios, configuración y problemas. Monitorear cuánto esfuerzo se aplica en apagar fuegos, en lugar de permitir mejoras al negocio y, en los casos que sean necesarios, mejorar estos procesos para minimizar los problemas.

## Modelo de madurez

### DS10 Administración de problemas

**La administración del proceso de *Administrar problemas* que satisfaga el requerimiento de negocio de TI de *garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio, y reducir el retrabajo y los defectos de la prestación de los servicios y de las soluciones* es:**

#### **0 No-existente** cuando

No hay conciencia sobre la necesidad de administrar problemas, y no hay diferencia entre problemas e incidentes. Por lo tanto, no se han hecho intentos por identificar la causa raíz de los incidentes.

#### **1 Inicial/Ad Hoc** cuando

Los individuos reconocen la necesidad de administrar los problemas y de revolver las causas de fondo. Algunos individuos expertos clave brindan asesoría sobre problemas relacionados a su área de experiencia, pero no está asignada la responsabilidad para la administración de problemas. La información no se comparte, resultando en la creación de nuevos problemas y la pérdida de tiempo productivo mientras se buscan respuestas.

#### **2 Repetible pero intuitivo** cuando

Hay una amplia conciencia sobre la necesidad y los beneficios de administrar los problemas relacionados con TI, tanto dentro de las áreas de negocio como en la función de servicios de información. El proceso de resolución ha evolucionado un punto en el que unos cuantos individuos clave son responsables de identificar y resolver los problemas. La información se comparte entre el personal de manera informal y reactiva. El nivel de servicio hacia la comunidad usuaria varía y es obstaculizado por la falta de conocimiento estructurado a disposición del administrador de problemas.

#### **3 Proceso definido** cuando

Se acepta la necesidad de un sistema integrado de administración de problemas y se evidencia con el apoyo de la gerencia y la asignación de presupuesto para personal y capacitación. Se estandarizan los procesos de escalamiento y resolución de problemas. El registro y rastreo de problemas y de sus soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles sin centralizar. Es poco probable detectar las desviaciones de los estándares y de las normas establecidas. La información se comparte entre el personal de manera formal y proactiva. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.

#### **4 Administrado y medible** cuando

El proceso de administración de problemas se entiende a todos los niveles de la organización. Las responsabilidades y la propiedad de los problemas están claramente establecidas. Los métodos y los procedimientos son documentados, comunicados y medidos para evaluar su efectividad. La mayoría de los problemas están identificados, registrados y reportados, y su solución ha iniciado. El conocimiento y la experiencia se cultivan, mantienen y desarrollan hacia un nivel más alto a medida que la función es vista como un activo y una gran contribución al logro de las metas de TI y a la mejora de los servicios de TI. La administración de problemas está bien integrada con los procesos interrelacionados, tales como administración de incidentes, de cambios, y de configuración, y ayuda a los clientes para administrar información, instalaciones y operaciones. Se han acordado los KPIs y KGIs para el proceso de administración de problemas.

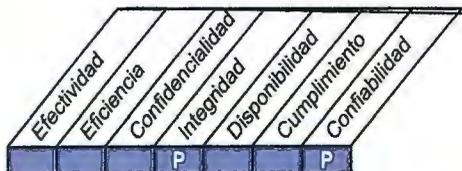
#### **5 Optimizado** cuando

El proceso de administración de problemas ha evolucionado a un proceso proactivo y preventivo, que contribuye con los objetivos de TI. Los problemas se anticipan y previenen. El conocimiento respecto a patrones de problemas pasados y futuros se mantiene a través de contactos regulares con proveedores y expertos. El registro, reporte y análisis de problemas y soluciones está integrado por completo con la administración de datos de configuración. Los KPIs y KGIs son medidos de manera consistente. La mayoría de los sistemas están equipados con mecanismos automáticos de advertencia y detección, los cuales son rastreados y evaluados de manera continua. El proceso de administración de problemas se analiza para buscar la mejora continua con base en los KPIs y KGIs y se reporta a los interesados.

## Objetivo de control de alto nivel

### DS11 Administración de datos

Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.



#### Control sobre el proceso TI de

Administración de datos

#### que satisface el requisito de negocio de TI para

Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.

#### enfocándose en

mantener la integridad, exactitud, disponibilidad y protección de los datos.

#### se logra

- Respaldo de los datos y probando la restauración
- Administrando almacenamiento de datos en sitio y fuera de sitio.
- Desechando de manera segura los datos y el equipo.

#### y se mide con

- Satisfacción del usuario con la disponibilidad de los datos.
- Porcentaje de restauraciones exitosas de datos.
- Número de incidentes en los que tuvo que recuperarse datos sensibles después que los medios habían sido desechados.

Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar



# Objetivos de control detallados

## **DS11 Administración de la información**

### **DS11.1 Requerimientos del negocio para administración de datos**

Establecer mecanismos para garantizar que el negocio reciba los documentos originales que espera, que se procese toda la información recibida por parte del negocio, que se preparen y entreguen todos los reportes de salida que requiere el negocio y que las necesidades de reinicio y reproceso estén soportadas.

### **DS11.2 Acuerdos de almacenamiento y conservación**

Definir e implementar procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables. Los procedimientos deben considerar los requerimientos de recuperación, la rentabilidad, la integridad continua y los requerimientos de seguridad. Para cumplir con los requerimientos legales, regulatorios y de negocio, establecer mecanismos de almacenamiento y conservación de documentos, datos, archivos, programas, reportes y mensajes (entrantes y salientes), así como la información (claves, certificados) utilizada para encriptación y autenticación.

### **DS11.3 Sistema de administración de librerías de medios**

Definir e implementar procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y su uso. Los procedimientos deben permitir la revisión oportuna y el seguimiento de cualquier discrepancia que se perciba.

### **DS11.4 Eliminación**

Definir e implementar procedimientos para prevenir el acceso a datos sensibles y al software desde equipos o medios una vez que son eliminados o transferidos para otro uso. Dichos procedimientos deben garantizar que los datos marcados como borrados o desechados no puedan recuperarse.

### **DS11.5 Respaldo y restauración**

Definir e implementar procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad. Verificar el cumplimiento de los procedimientos de respaldo y verificar la capacidad y el tiempo requerido para tener una restauración completa y exitosa. Probar los medios de respaldo y el proceso de restauración.

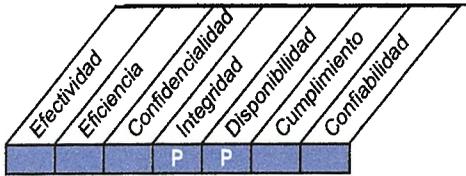
### **DS11.6 Requerimientos de seguridad para la administración de datos**

Establecer mecanismos para identificar y aplicar requerimientos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensibles. Esto incluye registros físicos, transmisiones de datos y cualquier información almacenada fuera del sitio.

# Objetivo de control de alto nivel

## DS12 Administración del ambiente físico

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

### Control sobre el proceso TI de

Administración del ambiente físico

### que satisface el requisito de negocio de TI para

proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio.

### enfocándose en

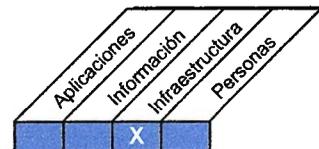
proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo.

### se logra

- Implementando medidas de seguridad físicas.
- Seleccionando y administrando las instalaciones.

### y se mide con

- Tiempo sin servicio ocasionado por incidentes relacionados con el ambiente físico
- Número de incidentes ocasionados por fallas o brechas de seguridad física
- Frecuencia de revisión y evaluación de riesgos físicos.



# Objetivos de control detallados

## **DS12 Administración del ambiente físico**

### **DS12.1 Selección y diseño del centro de datos**

Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.

### **DS12.2 Medidas de seguridad física**

Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.

### **DS12.3 Acceso Físico**

Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.

### **DS12.4 Protección contra factores ambientales**

Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente.

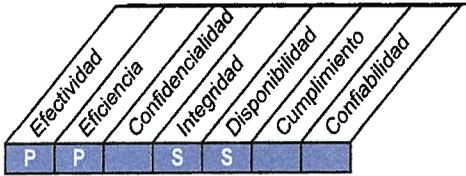
### **DS12.5 Administración de instalaciones físicas**

Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud.

# Objetivo de control de alto nivel

## DS13 Administración de operaciones

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.



### Control sobre el proceso TI de

Administrar operaciones

### que satisface el requisito de negocio de TI para

mantener la integridad de los datos y garantizar que la infraestructura de TI puede resistir y recuperarse de errores y fallas.

### enfocándose en

cumplir con los niveles operativos de servicio para procesamiento de datos programado, protección de datos de salida sensitivos y monitoreo y mantenimiento de la infraestructura.

### se logra

- Operando el ambiente de TI en línea con los niveles de servicio acordados y con las instrucciones definidas
- Manteniendo la infraestructura de TI

### y se mide con

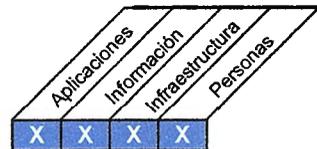
- Número de niveles de servicio afectados a causa de incidentes en la operación.
- Horas no planeadas de tiempo sin servicio a causa de incidentes en la operación.
- Porcentaje de activos de hardware incluidos en los programas de mantenimiento.

Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar



## Objetivos de control detallados

### **DS13 Administración de operaciones**

#### **DS13.1 Procedimientos e instrucciones de operación**

Definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos. Los procedimientos de operación deben cubrir los procesos de entrega de turno (transferencia formal de la actividad, estatus, actualizaciones, problemas de operación, procedimientos de escalamiento, y reportes sobre las responsabilidades actuales) para garantizar la continuidad de las operaciones.

#### **DS13.2 Programación de tareas**

Organizar la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el rendimiento y la utilización para cumplir con los requerimientos del negocio. Deben autorizarse los programas iniciales así como los cambios a estos programas. Los procedimientos deben implementarse para identificar, investigar y aprobar las salidas de los programas estándar agendados.

#### **DS13.3 Monitoreo de la infraestructura de TI**

Definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados. Garantizar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones.

#### **DS13.4 Documentos sensitivos y dispositivos de salida.**

Establecer resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos tales como formas, instrumentos negociables, impresoras de uso especial o dispositivos de seguridad.

#### **DS13.5 Mantenimiento preventivo del hardware**

Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.

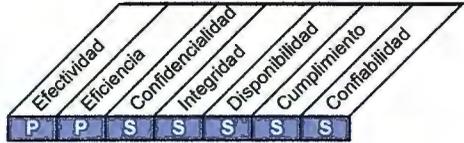
# MONITOREAR Y EVALUAR

<b>ME1</b>	Monitorear y evaluar el desempeño de TI
<b>ME2</b>	Monitorear y evaluar el control interno
<b>ME3</b>	Garantizar el cumplimiento regulatorio
<b>ME4</b>	Proporcionar gobierno de TI

## Objetivo de control de alto nivel

### ME1 Monitorear y evaluar el desempeño de TI

Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas.



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

#### Control sobre el proceso TI de

Monitorear y evaluar el desempeño de TI

que satisface el requisito de negocio de TI para

transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI de acuerdo con los requisitos de gobierno

enfocándose en

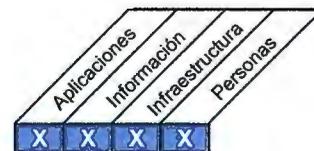
monitorear y reportar las métricas del proceso e identificar e implantar acciones de mejoramiento del desempeño

se logra con

- Cotejar y traducir los reportes de desempeño de proceso a reportes gerenciales
- Comparar el desempeño contra las metas acordadas e iniciar las medidas correctivas necesarias

y se mide con

- Satisfacción de la gerencia y de la entidad de gobierno con los reportes de desempeño
- Número de acciones de mejoramiento impulsadas por las actividades de monitoreo
- Porcentaje de procesos críticos monitoreados



## Objetivos de control detallados

### ME1 Monitorear y evaluar el desempeño de TI

#### ME1.1 Enfoque del Monitoreo

Garantizar que la gerencia establezca un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para monitorear la contribución de TI a los resultados de los procesos de administración de programas y de administración del portafolio empresarial y aquellos procesos que son específicos para la entrega de la capacidad y los servicios de TI. El marco de trabajo se debería integrar con el sistema de administración del desempeño corporativo.

#### ME1.2 Definición y recolección de datos de monitoreo

Garantizar que la gerencia de TI, trabajando en conjunto con el negocio, defina un conjunto balanceado de objetivos, mediciones, metas y comparaciones de desempeño y que estas se encuentren acordadas formalmente con el negocio y otros interesados relevantes. Los indicadores de desempeño deberían incluir:

- La contribución al negocio que incluya, pero que no se limite a, la información financiera
- Desempeño contra el plan estratégico del negocio y de TI
- Riesgo y cumplimiento de las regulaciones
- Satisfacción del usuario interno y externo
- Procesos clave de TI que incluyan desarrollo y entrega del servicio
- Actividades orientadas a futuro, por ejemplo, la tecnología emergente, la infraestructura re-utilizable, habilidades del personal de TI y del negocio

Se deben establecer procesos para recolectar información oportuna y precisa para reportar el avance contra las metas.

#### ME1.3 Método de monitoreo

Garantizar que el proceso de monitoreo implante un método (ej. Balanced Scorecard), que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa.

#### ME1.4 Evaluación del desempeño

Comparar de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes.

#### ME1.5 Reportes al consejo directivo y a ejecutivos

Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño. Los reportes de estatus deben incluir el grado en el que se han alcanzado los objetivos planeados, los entregables obtenidos, las metas de desempeño alcanzadas y los riesgos mitigados. Durante la revisión, se debe identificar cualquier desviación respecto al desempeño esperado y se deben iniciar y reportar las medidas administrativas adecuadas.

#### ME1.6 Acciones correctivas

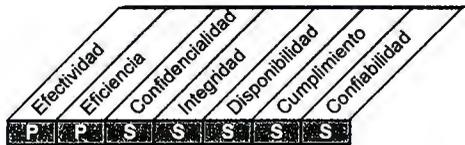
Identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes. Esto incluye el seguimiento de todo el monitoreo, de los reportes y de las evaluaciones con:

- Revisión, negociación y establecimiento de respuestas administrativas
- Asignación de responsabilidades por la corrección
- Rastreo de los resultados de las acciones comprometidas

## Objetivo de control de alto nivel

### ME2 Monitorear y evaluar el control interno

Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.



#### Control sobre el proceso TI de

Monitorear y evaluar el control interno

que satisface el requisito de negocio de TI para

proteger el logro de los objetivos de TI y cumplir las leyes y reglamentos relacionados con TI

enfocándose en

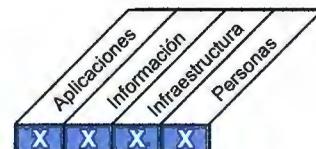
el monitoreo de los procesos de control interno para las actividades relacionadas con TI e identificar las acciones de mejoramiento

se logra con

- La definición de un sistema de controles internos integrados en el marco de trabajo de los procesos de TI
- Monitorear y reportar la efectividad de los controles internos sobre TI
- Reportar las excepciones de control a la gerencia para tomar acciones

y se mide con

- Número de brechas importantes del control interno
- Número de iniciativas para la mejora del control
- Número de cubrimiento de auto evaluaciones de control



Planear y  
organizar

Adquirir e  
implantar

Entregar y dar  
soporte

Monitorear y  
evaluar

# Objetivos de control detallados

## ME2 Monitorear y evaluar el control interno

### ME2.1 Monitorear el marco de trabajo de control interno

Monitorear de forma continua el ambiente de control y el marco de control de TI. Se debe realizar la evaluación usando mejores prácticas de la industria y se debería utilizar benchmarking para mejorar el ambiente y el marco de trabajo de control de TI.

### ME2.2 Revisiones de Auditoría

Monitorear y reportar la efectividad de los controles internos sobre TI por medio de revisiones de auditoría incluyendo, por ejemplo, el cumplimiento de políticas y estándares, seguridad de la información, controles de cambios y controles establecidos en acuerdos de niveles de servicio.

### ME2.3 Excepciones de control

Registrar la información referente a todas las excepciones de control y garantizar que esto conduzca al análisis de las causas subyacentes y a la toma de acciones correctivas. La gerencia debería decidir cuáles excepciones se deberían comunicar al individuo responsable de la función y cuáles excepciones deberían ser escaladas. La gerencia también es responsable de informar a las partes afectadas.

### ME2.4 Auto-evaluación de control

Evaluar la completitud y efectividad de los controles internos de la administración de los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación.

### ME2.5 Aseguramiento del control interno

Obtener, según sea necesario, aseguramiento adicional de la completitud y efectividad de los controles internos por medio de revisiones de terceros. Dichas revisiones pueden ser realizadas por la función de cumplimiento corporativo o, a solicitud de la gerencia, por auditoría interna o por auditores y consultores externos o por organismos de certificación. Se deben verificar las aptitudes de los individuos que realicen la auditoría, por ej. Un Auditor de Sistemas de Información Certificado™ (CISA® por sus siglas en Inglés) debe asignarse.

### ME2.6 Control interno para terceros

Determinar el estado de los controles internos de cada proveedor externos de servicios. Confirmar que los proveedores externos de servicios cumplan con los requerimientos legales y regulatorios y con las obligaciones contractuales. Esto puede ser provisto por una auditoría externa o se puede obtener de una revisión por parte de auditoría interna y por los resultados de otras auditorías.

### ME2.7 Acciones correctivas

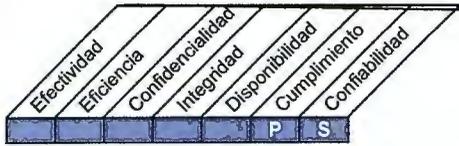
Identificar e iniciar medidas correctivas basadas en las evaluaciones y en los reportes de control. Esto incluye el seguimiento de todas las evaluaciones y los reportes con:

- La revisión, negociación y establecimiento de respuestas administrativas
- La asignación de responsabilidades para corrección (puede incluir la aceptación de los riesgos)
- El rastreo de los resultados de las acciones comprometidas

## Objetivo de control de alto nivel

### ME3 Garantizar el cumplimiento regulatorio

Una supervisión efectiva del cumplimiento regulatorio requiere del establecimiento de un proceso independiente de revisión para garantizar el cumplimiento de las leyes y regulaciones. Este proceso incluye la definición de un estatuto de auditoría, independencia de los auditores, ética y estándares profesionales, planeación, desempeño del trabajo de auditoría y reportes y seguimiento a las actividades de auditoría. El propósito de este proceso es proporcionar un aseguramiento positivo relativo al cumplimiento de TI de las leyes y regulaciones.



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

#### Control sobre el proceso TI de

Garantizar el cumplimiento regulatorio

que satisface el requisito de negocio de TI para

cumplir las leyes y regulaciones

enfocándose en

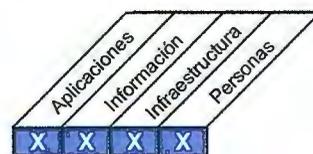
la identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento

se logra con

- La identificación de los requisitos legales y regulatorios relacionados con la TI
- La evaluación del impacto de los requisitos regulatorios
- El monitoreo y reporte del cumplimiento de los requisitos regulatorios

y se mide con

- El costo del no cumplimiento de TI, incluyendo arreglos y multas
- Tiempo promedio de demora entre la identificación de los problemas externos de cumplimiento y su resolución
- Frecuencia de revisiones de cumplimiento



## Objetivos de control detallados

### ME3 Garantizar el cumplimiento regulatorio

#### ME3.1 Identificar las leyes y regulaciones con impacto potencial sobre TI

Definir e implantar un proceso para garantizar la identificación oportuna de requerimientos locales e internacionales legales, contractuales, de políticas y regulatorios, relacionados con la información, con la prestación de servicios de información – incluyendo servicios de terceros – y con la función, procesos e infraestructura de TI. Tomar en cuenta las leyes y reglamentos de comercio electrónico, flujo de datos, privacidad, controles internos, reportes financieros, reglamentos específicos de la industria, propiedad intelectual y derechos de autor, además de salud y seguridad.

#### ME3.2 Optimizar la respuesta a requerimientos regulatorios

Revisar y optimizar las políticas, estándares y procedimientos de TI para garantizar que los requisitos legales y regulatorios se cubran de forma eficiente.

#### ME3.3 Evaluación del cumplimiento con requerimientos regulatorios

Evaluar de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requerimientos legales y regulatorios, con base en la supervisión del gobierno de la gerencia de TI y del negocio y la operación de los controles internos.

#### ME3.4 Aseguramiento positivo del cumplimiento

Definir e implantar procedimientos para obtener y reportar un aseguramiento del cumplimiento y, donde sea necesario, que el propietario del proceso haya tomado las medidas correctivas oportunas para resolver cualquier brecha de cumplimiento. Integrar los reportes de avance y estado del cumplimiento de TI con salidas similares provenientes de otras funciones de negocio

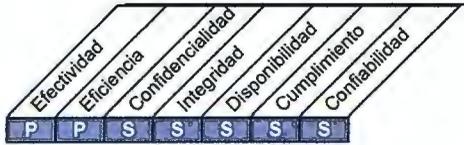
#### ME3.5 Reportes integrados.

Integrar los reportes de TI sobre cumplimiento regulatorio con las salidas similares provenientes de otras funciones del negocio.

## Objetivo de control de alto nivel

### ME4 Proporcionar gobierno de TI

El establecimiento de un marco de trabajo de gobierno efectivo, incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas y de acuerdo con las estrategias y objetivos empresariales.



#### Control sobre el proceso TI de

Proporcionar gobierno de TI

que satisface el requisito de negocio de TI para

la integración de un gobierno de TI con objetivos de gobierno corporativo y el cumplimiento con las leyes y regulaciones

enfocándose en

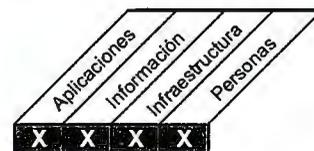
la elaboración de informes para el consejo directivo sobre la estrategia, el desempeño y los riesgos de TI y responder a los requerimientos de gobierno de acuerdo a las directrices del consejo directivo

se logra con

- El establecimiento de un marco de trabajo para el gobierno de TI, integrado al gobierno corporativo
- la obtención de aseguramiento independientes sobre el estatus del gobierno de TI

y se mide con

- La frecuencia de informes del consejo directivo sobre TI a los interesados (incluyendo el nivel de madurez)
- La frecuencia de los reportes de TI hacia el consejo directivo (incluyendo el nivel de madurez)
- Frecuencia de revisiones independientes del cumplimiento de TI



Planear y organizar

Adquirir e implantar

Entregar y dar soporte

Monitorear y evaluar

## Objetivos de control detallados

### ME4 Proporcionar gobierno de TI

#### ME4.1 Establecer un marco de trabajo de gobierno para TI

Trabajar con el consejo directivo para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles y responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI de la empresa ofrezcan y estén alineados con las estrategias y objetivos empresariales. El marco de trabajo debería proporcionar vínculos claros entre la estrategia empresarial, el portafolio de programas de inversiones habilitadas por TI que ejecutan la estrategia, los programas de inversión individual y los proyectos de negocio y de TI que forman los programas. El marco de trabajo debería definir una rendición de cuentas y prácticas incontrovertibles para evitar fallas de control interno y de supervisión. El marco de trabajo debería ser consistente con el ambiente completo de control empresarial y con los principios de control generalmente aceptados y estar basado en el proceso y en el marco de control de TI.

#### ME4.2 Alineamiento estratégico

Facilitar el entendimiento del consejo directivo y de los ejecutivos sobre temas estratégicos de TI tales como el rol de TI, características propias y capacidades de la tecnología. Garantizar que existe un entendimiento compartido entre el negocio y la función de TI sobre la contribución potencial de TI a la estrategia del negocio. Asegurarse de que exista un entendimiento claro de que el valor de TI sólo se obtiene cuando las inversiones habilitadas con TI se administran como un portafolio de programas que incluyen el alcance completo de los cambios que el negocio debe realizar para optimizar el valor proveniente de las capacidades que tiene TI para lograr la estrategia. Trabajar con el consejo directivo para definir e implantar organismos de gobierno, tales como un comité estratégico de TI, para brindar una orientación estratégica a la gerencia respecto a TI, garantizando así que tanto la estrategia como los objetivos se distribuyan en cascada hacia las unidades de negocio y hacia las unidades de TI y que se desarrolle certidumbre y confianza entre el negocio y TI. Facilitar la alineación de TI con el negocio en lo referente a estrategia y operaciones, fomentando la co-responsabilidad entre el negocio y TI en la toma de decisiones estratégicas y en la obtención de los beneficios provenientes de las inversiones habilitadas con TI.

#### ME4.3 Entrega de valor

Administrar los programas de inversión habilitados con TI, así como otros activos y servicios de TI, para asegurar que ofrezcan el mayor valor posible para apoyar la estrategia y los objetivos empresariales. Asegurarse de que los resultados de negocio esperados de las inversiones habilitadas por TI y el alcance completo del esfuerzo requerido para lograr esos resultados esté bien entendido, que se generen casos de negocio integrales y consistentes, y que los aprueben los interesados, que los activos y las inversiones se administren a lo largo del ciclo de vida económico, y que se lleve a cabo una administración activa del logro de los beneficios, tales como la contribución a nuevos servicios, ganancias de eficiencia y un mejor grado de reacción a los requerimientos de los clientes. Implantar un enfoque disciplinado hacia la administración por portafolio, programa y proyecto, enfatizando que el negocio asume la propiedad de todas las inversiones habilitadas con TI y que TI garantiza la optimización de los costos por la prestación de los servicios y capacidades de TI. Asegurar que las inversiones en tecnología estén estandarizadas a mayor grado posible para evitar el aumento en costo y complejidad de una proliferación de soluciones técnicas.

#### ME4.4 Administración de recursos

Optimizar la inversión, uso y asignación de los activos de TI por medio de evaluaciones periódicas, garantizando que TI cuente con recursos suficientes, competentes y capaces para ejecutar los objetivos estratégicos actuales y futuros y seguir el ritmo de los requerimientos del negocio. La dirección debería implantar políticas claras, consistentes y reforzadas sobre recursos humanos y políticas de sustitución para garantizar que se satisfagan los requerimientos de recursos de manera efectiva y para adaptarse a las políticas y estándares de la arquitectura. La infraestructura de TI se debe evaluar periódicamente para asegurar que esté estandarizada siempre que sea posible y que exista la interoperabilidad según sea requiera.

#### ME4.5 Administración de riesgos.

Trabajar en conjunto con el consejo directivo para definir el nivel de riesgo de TI aceptable por la empresa. Comunicar este nivel de riesgo hacia la organización y acordar el plan de administración de riesgos de TI. Integrar las responsabilidades de administración de riesgos en la organización, asegurando que tanto el negocio como TI evalúen y reporten periódicamente los riesgos asociados con TI y su impacto en el negocio. Garantizar que la gerencia de TI haga seguimiento a la exposición a los riesgos, poniendo especial atención en las fallas y debilidades de control interno y de supervisión, así como su impacto actual y potencial en el negocio. La posición de riesgo empresarial en TI debería ser transparente para todos los interesados.

#### ME4.6 Medición del desempeño.

Informar el desempeño relevante del portafolio de los programas de TI al consejo directivo y a los ejecutivos de manera oportuna y precisa. Los informes administrativos que se deben entregar a la alta dirección para su revisión deben incluir el avance de la empresa hacia metas identificadas. Los reportes de estatus deben incluir el grado al cual se han logrado los objetivos planeados, entregables obtenidos, metas de desempeño alcanzadas y los riesgos mitigados. Integrar los informes con salidas similares de otras funciones del negocio. Las mediciones de desempeño deberían ser aprobadas por los interesados clave. El consejo directivo y los ejecutivos deberían cuestionar estos informes de desempeño y la gerencia de TI debería tener la oportunidad de explicar las desviaciones y los problemas de desempeño. Después de la revisión, se deben iniciar y controlar las acciones administrativas apropiadas.

#### ME4.7 Aseguramiento independiente.

Garantizar que la organización establezca y mantenga una función competente y que cuente con el personal adecuado y/o busque servicios de aseguramiento externo para proporcionar al consejo directivo— esto ocurrirá probablemente a través de un comité de auditoría — aseguramiento independiente y oportuno sobre el cumplimiento que tiene TI respecto a sus políticas, estándares y procedimientos, así como con las prácticas generalmente aceptadas.

# **ANEXO E**

## **CRONOGRAMA**

