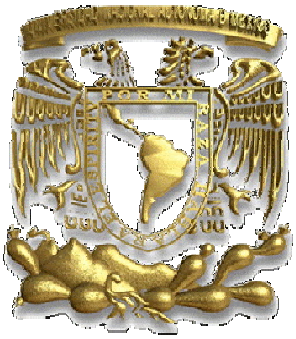

**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

**FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN**

# "MODELO Y DISEÑO DE UNA AUDITORÍA PARA SISTEMAS DE INFORMACIÓN Y SUS MEJORES PRÁCTICAS."

**TESIS**
**PARA OBTENER EL TÍTULO DE**
**INGENIERO MECÁNICO ELECTRICISTA**
**ÁREA: ELÉCTRICA Y ELECTRÓNICA**

**PRESENTA:**
**GAMERO ESPINOZA CARLOS BALTAZAR**


**ASESOR: MTRO. JUAN GASTALDI PÉREZ**

**Bosques de Aragón, Estado de México, Mayo de 2015**

## Objetivo General

Proporcionar un documento que ofrezca una referencia e introducción al análisis y a la práctica de la auditoría de un Sistema de la Información S.I., un área de Tecnología de Información y Comunicaciones o una plataforma tecnológica, enfocado a cualquier área de Tecnologías de la Información T.I., basándose en las directrices y metodologías reconocidas internacionalmente para tal fin, cuya aplicación permitirá la identificación de los elementos de T.I., los niveles de criticidad que guardan en las empresas u organismos, así como los potenciales riesgos que podrían vulnerar los sistemas de información. Obteniendo con lo anterior un conocimiento valioso para apoyar en la implementación y aseguramiento de las mejores prácticas en materia de T.I., y la importancia de la auditoría como herramienta de control y auto-ayuda, abundado en los temas fundamentales como la estructura de un departamento de T.I., roles y responsabilidades y controles inherentes a cada función.

## Objetivos Particulares

- Mencionar al lector que la práctica de auditoría y sus resultados reflejarán el estatus que guarda el sistema durante el periodo de realización, por lo que las medidas para solventar las deficiencias ya sean preventivas o correctivas deben actualizarse constantemente, con fundamento en las mejores prácticas de T.I.
- Ayudar a que las empresas u organizaciones, ya sean públicas o privadas, puedan hacer cabal cumplimiento, mediante las herramientas y equipos informáticos, de los objetivos trazados, así como la misión y visión para cada línea de negocio o en sí para el negocio en general.

**Introducción**

La tecnología está presente en la vida de todos, la sociedad civil y los gobiernos se apoyan en las técnicas desarrolladas por el hombre y la tecnología para desempeñar sus funciones.

En la actualidad las organizaciones y empresas tienen un amplio entendimiento de los beneficios del apoyo tecnológico en sus procesos, a través del uso sistematizado de Tecnologías de la Información y Comunicaciones, bajo una plataforma común de aplicaciones y servicios que permitan satisfacer las demandas del mercado actual. Cuando combinamos el trabajo de técnicas, gente hábil y capacitada, hardware, software, organización y metodología, debemos obtener correctas formas de trabajo, que a su vez requieren de mayores y elevados esquemas de seguridad y supervisión.

La integración adecuada de procesos y procedimientos claros y bien definidos con tecnologías de la información a las líneas de negocio permiten cumplir las metas y objetivos estratégicos de una organización, cumpliendo con la entrega de servicios eficaces y eficientes impulsando el alcance de cada línea de negocios, lo que representa un crecimiento y expansión de la organización.

La administración y manejo de sistemas de información en donde convergen las diferentes aplicaciones de T.I., hoy por hoy son los retos más importantes para los administradores de las tecnologías de la información, ya que requieren contar con un control de procesos, soporte de servicios y administración de riesgos bajo el uso de políticas y procedimientos, así como la continua autoevaluación y la aplicación de las mejores prácticas de los diversos campos de T.I., siempre en apego a las normas y regulaciones correspondientes.

La auditoría de Sistema de la Información (S.I.), auditoría informática o auditoría de sistemas también es un tipo de auditoría consistente en el examen de los sistemas de información, centros de proceso de datos, instalaciones y unidades

informáticas de las organizaciones, con objeto de facilitar la consecución de los objetivos que persiguen, tanto los del área informática como –primordialmente– los del conjunto de la organización. Por lo anterior es muy importante verificar la calidad de los sistemas de información de toda organización y proponer mejoras de los mismos, coherentes con el proyecto de calidad adoptado por la organización, siempre apegado al cumplimiento de normas de calidad o modelo de excelencia en gestión.

El enfoque que se tiene sobre las Tecnologías de la Información T.I. ha evolucionado, siendo una parte fundamental hoy en día y algo cotidiano e imprescindible para casi todo tipo de actividad, hasta en las menos pensadas. Actualmente todas las organizaciones no pueden prescindir de las T.I. para su operación, incluso con una dependencia demasiado alta, por lo que si no se cuenta con áreas de T.I. fuertemente capacitadas para dirigirlas puede traer consecuencias muy altas e incluso puede propiciar un colapso de toda una organización. La información se ha vuelto un activo muy importante para toda corporación y por ello es importante proteger los activos sensibles así como estar prevenidos para todo tipo de eventualidad en caso de que dichos activos sufriesen situaciones no deseadas.

En este documento se ofrece un panorama para que todo aquel que se encuentre relacionado a las TIC se interese por la auditoría de S.I. como una gran área de oportunidad y que, en caso de decidir enfocarse por dicho rubro o ya se esté desempeñando en un área de auditoría, sea este trabajo una herramienta que sirva de guía para llevarla cabo, dejando muy asentado que siempre, para ejecutar un trabajo de auditoría, es requisito apoyarse en las herramientas existentes así como en todas las metodologías internacionalmente reconocidas, las cuales siempre serán las mejores prácticas para la ejecución de la misma.

# Capítulo 1
## Tecnologías de información, Evolución y Gobierno T.I.

Hoy por hoy el término T.I. (Tecnologías de la Información) es muy conocido ya que abarca muchos aspectos de la informática y la tecnología. En este sentido, los profesionales de dicho rubro realizan una variedad de funciones en una organización que entre otras están la instalación de aplicaciones para el diseño de las redes informáticas, gestión de procesos, gestión de datos, redes, administración de hardware, manejo de bases de datos, aseguramiento de la información, así como la entrega y soporte de servicios de T.I., entre otros.

Actualmente las organizaciones cuentan con modelos y planes de optimización del manejo de recursos de T.I. estandarizando procesos, configuraciones y metodologías de trabajo, para lograr niveles mayores de eficiencia, integridad, confiabilidad, estabilidad, flexibilidad, eficacia y rendimiento, coadyuvando como área significativa para el cumplimento de los objetivos de una empresa.

Como antecedente, en la década de los 90 las organizaciones visualizaban la función de T.I. solo como un servicio técnico para los equipos, bajo un esquema aislado e incluso no era considerada parte vital para el desempeño de las mismas. Esta percepción extendida por varios años fue modificándose a través del tiempo, mediante la evaluación y entendimiento de los alcances de la planeación y gestión de T.I. en una organización sacando el máximo provecho del avance tecnológico, llegando hasta el punto de considerar dicha función como una línea de negocios.

Asimismo, el tema de la seguridad física de los elementos y activos de T.I., como equipamiento y documentación, ha evolucionado desde convertirse en barreras físicas hasta incorporar inteligencia y sistemas automatizados para la protección de estos, siendo hoy en día un tema primordial en cualquier organización y empresa.

Actualmente, la inversión en infraestructura y actualización de las aplicaciones de T.I. es parte fundamental para las actividades del área de T.I., desde los administradores que desempeñan esta función dentro de una organización, ya que con el continuo desarrollo de aplicaciones y servicios en entornos de red una organización puede beneficiarse desde nuevas formas para entrega de servicios, hasta el contacto directo con sus clientes, incluso a través de las redes sociales y protección de la información. Lo anterior representa la mejor opción para mantener un nivel máximo de calidad, medido por diversos indicadores que brinden información, ya sea financieros, satisfacción del cliente, entre otros y con ello también la posibilidad de identificar la aplicación de acciones correctivas que se consideren necesarias.

## 1.1 La función de T.I. en una organización.

Los objetivos de T.I. invariablemente deben estar encaminados a proporcionar y mantener una infraestructura tecnológica que permita mantener el negocio operativo y mejorar la calidad al menor costo posible, mediante la disminución de tiempos de entrega, una mejora continua en los procesos, así como la óptima administración de los recursos (Hardware, software, comunicaciones, especialistas de datos, desarrolladores, entre otros), ya sea bajo una arquitectura de servicios centralizada o distribuida. Figura 1.1.

**Figura 1.1 Infraestructura tecnológica**

La función de T.I. en una organización es gestionar los recursos tecnológicos, mediante la planificación a mediano y largo plazo, a fin de determinar los requerimientos para la ejecución de tareas específicas de cada elemento que integra el sistema informático de una organización, así como asegurar un control sobre los procesos inherentes bajo esquemas de seguridad y calidad. Todo esto consolidado en estrategias de negocios, lo cual permitirá un desarrollo informático acorde a las necesidades de la organización.

Un aspecto relevante dentro de las funciones de T.I. es definir una estructura de organización informática con objeto de precisar la administración de los recursos humanos, especificando los perfiles, los roles, el entrenamiento y a su vez conformar la estructura de puestos del personal informático.

La principal necesidad de establecer dicha organización consiste en las actividades e interrelación del personal que se involucra en el área informática, cuyas tareas pueden ser tales como el diseño de sistemas, establecimiento de políticas y procedimientos, administración de bases de datos, administración de servicios, operación del centro de datos, gestión de telecomunicaciones, intercomunicación con los usuarios, entre otras.

### 1.2 Estructura, organización y procesos de T.I.

Basándonos en el marco de trabajo de buenas prácticas que organizan los recursos humanos, los procesos y la tecnología para asegurar la eficacia de la gestión de servicios en la administración de tecnologías de información, se debe establecer una estructura organizacional para facilitar la entrega y soporte de servicios de T.I. a todos los usuarios de una organización. En dicho sentido, actualmente existe una metodología que es reconocida internacionalmente la cual plasma perfectamente lo anteriormente mencionado. Dicha metodología es ITIL (I.T. Infraestructura Library).

ITIL se fundamenta en torno a procesos-modelo de control y gestión de las operaciones y sus recomendaciones fueron desarrolladas en los años 80 por la Central Computer and Telecommunications Agency (CCTA), la cual proporciona información de cómo realizar la gestión de servicios de T.I. El modelo está enfocado a procesos utilizando dos dominios funcionales, que tienen como objetivo asegurar que la organización de T.I. mantenga alineada la operación con la gestión de servicios del negocio.

El primer dominio se refiere al normativo, tomando como referencia las normas y lineamientos que debe seguir la organización de T.I., así como el diseño de la estrategia que seguirá la organización para mejorar los servicios y facilitar los procesos. En este caso la metodología para diseño de procesos se basa en los Objetivos de Control para tecnología de la información y relacionada COBIT (en inglés Control Objectives for Information and Related Technology). El segundo dominio se refiere a la parte operativa en donde las funciones van directamente relacionadas a las acciones sobre la infraestructura tecnológica como supervisión y evaluación de los servicios entregados y/o administrados. Tabla 1.1.

**Tabla 1.1 Dominios normativos y Operativos según ITIL**

| DOMINIO NORMATIVO | DOMINIO OPERATIVO |
|---|---|
| • Planeacion estrategica (Nivel Institucional)<br>• Planeacion Tactica (Nivel Departamental)<br>• Planeacion Operacional<br>• Integracion Tecnologica | • Gestion de niveles de servicio<br>• Gestion de incidentes<br>• Gestionn de Problemas<br>• Gestion de Cambios<br>• Gestion de capacidad<br>• Getion de continuidad<br>• Gestion del Cambio<br>• Gestion de versiones<br>• Gestion financiera |

Asumiendo estos dominios fundamentales se deberán desplegar los procesos relacionados, en donde básicamente aquellos que deriven en planeaciones

pertenecerán al dominio normativo, quedando aquellos procesos de administración incluidos en el dominio de los procesos.

Lo anterior es trascendente en el sentido de que derivado de este análisis se definirán los roles y funciones específicos del personal de T.I., así como la identificación de servicios, la entrega y soporte de los mismos. La estructura organizacional muestra el departamento de sistemas de información típicamente encabezado por un director responsable de información CIO (Chief Information Officer).

### 1.3 Roles y responsabilidades de T.I.

El organigrama representa un elemento importante, ya que con base en éstos se puede tener la ubicación y jerarquía del departamento de S.I., esto aunado a la descripción de cada puesto, y provee una orientación de manera clara para los empleados de este departamento así como para los de otras áreas de una organización. Figura 1.2.

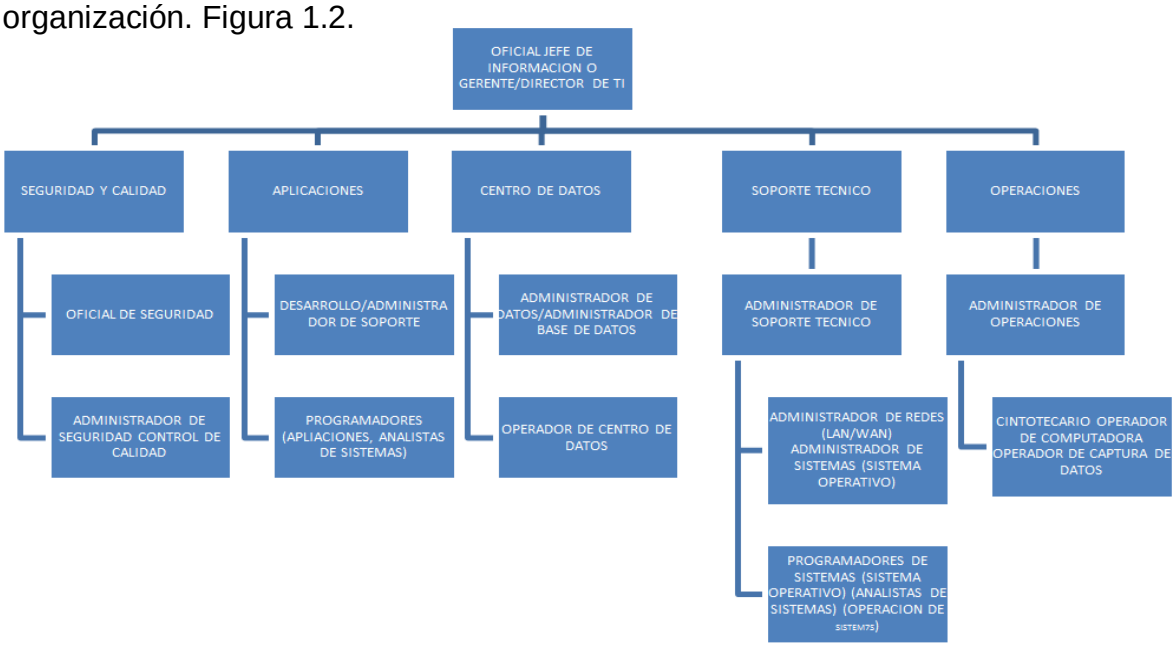


**Figura 1.2 Organización del departamento de sistemas de información.**

- **Gerencia de Desarrollo de Sistemas.** Esta Gerencia es la responsable de los programadores y analistas que implementan los nuevos sistemas y que mantienen los existentes.

- **Mesa de Ayuda (Help Desk).** En el entorno actual de S.I., las compañías deben considerar importante tener la función de help desk, siendo una unidad dentro de cada organización, que responde a preguntas y problemas técnicos que enfrentan los usuarios. El personal de la mesa de ayuda puede utilizar un software especial que les posibilita hallar rápidamente las respuestas a las preguntas más frecuentes.

La administración de mesa de ayuda/soporte incluye las siguientes actividades:

i. Adquisición de Hardware/Software en representación de usuarios finales.
ii. Apoyar a los usuarios finales con las dificultades de Hardware o Software.
iii. Entrenar a los usuarios a usar Hardware y Software.
iv. Responder y resolver las preguntas de los usuarios finales.
v. Monitorear desarrollos técnicos e informar a los usuarios finales de desarrollos que podrían ser pertinentes para ellos.
vi. Determinar la fuente de problemas e informar a los usuarios finales de desarrollos que podrían ser pertinentes para ellos
vii. Informar a los usuarios finales sobre problemas de desarrollos que podrían afectar sus controles por la instalación de actualizaciones (upgrades) de hardware o software.

- **Usuario final.** Responsable de las operaciones relacionadas con los servicios de aplicaciones del negocio, utilizado para distinguir la persona para quien se diseñó el producto de la persona que programa, sirve o instala aplicaciones.

- **Gerencia del Usuario Final**. Responsable del enlace entre departamento de S.I. y los usuarios finales.

- **Administración de Datos**. Responsable de la arquitectura de los datos en los ambientes más grandes de T.I. y encargado de administrar los datos como un activo corporativo.

- **Gerencia de aseguramiento de la Calidad.** Responsable de negociar y facilitar actividades de calidad en todas las áreas de tecnología e información.

- **Cintotecario**. debe registrar, emitir, recibir y custodiar todos los archivos de programa y de datos que sean mantenidos en las cintas de computadora, medios magnéticos y/o en discos o medios externos de memoria. Dependiendo del tamaño de la organización, el cintotecario puede ser una persona de tiempo completo o un miembro de la sección de control de datos que también realiza esta función.

### 1.4 Conceptualización de seguridad física.

Asimismo, como se mencionó al inicio de este capítulo, la conceptualización de la seguridad física aplicado a los sistemas de información en empresas y organizaciones no contemplaba un plan estructurado que incluyera estrategias para mitigar los múltiples riesgos que pudieran representar una amenaza y con esto pérdida o robo de información.

Actualmente la administración de riesgos es un tema amplio; en este documento se mencionará lo referente a la administración de riesgos. De igual manera, se mencionara lo referente a las amenazas físicas de un sistema de información, ya que es primordial la custodia de los activos y del equipamiento

El tema de seguridad física, como se mencionó en el párrafo anterior, se considera parte esencial para asegurar que los elementos físicos del sistema de información que están resguardados de manera adecuada y en este mismo sentido tener la certeza de que las medidas de seguridad son acordes al nivel de riesgo en donde se ubiquen.

En este mismo orden de ideas, para la elaboración de este documento, se considera parte de la actividad de auditoría el revisar constantemente las condiciones de las barreras físicas e instalaciones de resguardo de documentos, equipos y demás elementos que componen un sistema de información S.I., los cuales se mencionaran posteriormente.

Toda empresa u organización debe contar con un programa de seguridad como resultado del análisis, planificación y gestión de los riesgos, en donde se encuentre estructurada la operación de los procesos que involucran las funciones de T.I.

Dentro de la planificación de la gestión de riesgos se encuentran básicamente tres fases para su atención, que incluyen la medida de seguridad de *disuasión* mediante sistemas visibles, la medida de seguridad para la *detección* y en consecuencia la medida de seguridad de *reacción*. Cabe destacar que mayormente estas medidas de seguridad son implementadas mediante sistemas automatizados u operados para tal fin, por lo que nuevamente se hace evidente que es primordial cubrir en las actividades de auditoría, el control y adecuación de los mismos.

Asimismo, es importante recalcar que los sistemas de seguridad deben ser operados por personal calificado, mismo que representan para nuestro caso los usuarios finales y que se encuentran en coexistencia de los administradores de los sistemas de información. Como se mencionó en el punto 1.2. Estructura, organización y procesos de T.I., el departamento de sistemas de información debe

tener una estructura clara para garantizar el correcto flujo de información de acuerdo a cada función.

Aunado a lo anterior y como parte de lo relativo a las medidas para la continuidad de negocio y recuperación de desastres, así como la recuperación de los sistemas de Información, lo cual se abundará en el Capítulo 3. Protección y Continuidad de Activos y Sistemas de Información, los administradores de S.I. deben garantizar la operación continua de los equipos de respaldo. En este sentido, es nuevamente donde toman relevancia las actividades de auditoría, toda vez que nos permitirán llevar el control y monitoreo de las condiciones de cada equipo e identificar las oportunidades de mejora, tanto en los procesos como particularmente en los procedimientos y condiciones físicas.

### 1.5 Gobierno de T.I. y su importancia estratégica.

El modelo de gobierno de T.I. no es más que una práctica de gobierno corporativo, el cual es definido como un comportamiento ético por parte de los directores o encargados del gobierno, cuyo objetivo es el crear y entregar beneficios para todos los clientes de una organización, a través de la distribución de derechos y responsabilidades entre los diferentes integrantes de la misma. Es de resaltar que el término de gobierno de T.I. incluye sistemas de información, tecnología, comunicación, negocio, estándares, aspectos legales y normativos, entre otros. Así mismo integra a todas las partes interesadas, los directores, gerentes, propietarios de activos y procesos, proveedores de T.I., usuarios y auditores, todo bajo una dirección estratégica para cumplir con los objetivos de una organización.

Uno de los principales beneficios del gobierno de T.I. es que permite maximizar el valor de una organización, con estructuras de interacción entre los procesos, recursos e información de T.I. bajo las mejores prácticas para proyección, planeación, adquisición, implementación, entrega de servicios y soporte,

enfatizando la atención y aseguramiento de la información y la tecnología, dos de los activos más valiosos de una empresa u organización.

Es impórtate señalar que el gobierno de T.I. es responsabilidad de la junta directiva y de la gerencia ejecutiva de una organización, constituido por estructuras de liderazgo y organizacionales, asegurando que la información y la infraestructura tecnológica sean las adecuadas para contribuir a la realización de los objetivos de una organización, basado en un marco de responsabilidades para la toma de decisiones.

**1.6 Responsabilidades.**

El director general de una empresa es la última instancia para el control interno, por lo que los gerentes de T.I. deben asignar responsabilidades para el establecimiento de políticas específicas de control y procedimientos internos para el personal responsable en base a las funciones. El control interno es responsabilidad de todos en una organización y deben formar parte explícita o implícitamente.

En particular, en nuestro país encontramos definido en el manual administrativo de aplicación general en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información (MAAGTICSI) para dependencias y entidades de la administración pública federal, un ejemplo de lo anteriormente mencionado, a través de una gestión integral de procesos para aplicación por unidades administrativas de tecnologías de información y comunicaciones “UTIC”, que son responsables de los servicios de T.I. en una dependencia o entidad, definiendo grupos de trabajos con funciones y objetivos específicos para asegurar las mejores prácticas. Figura 1.3.

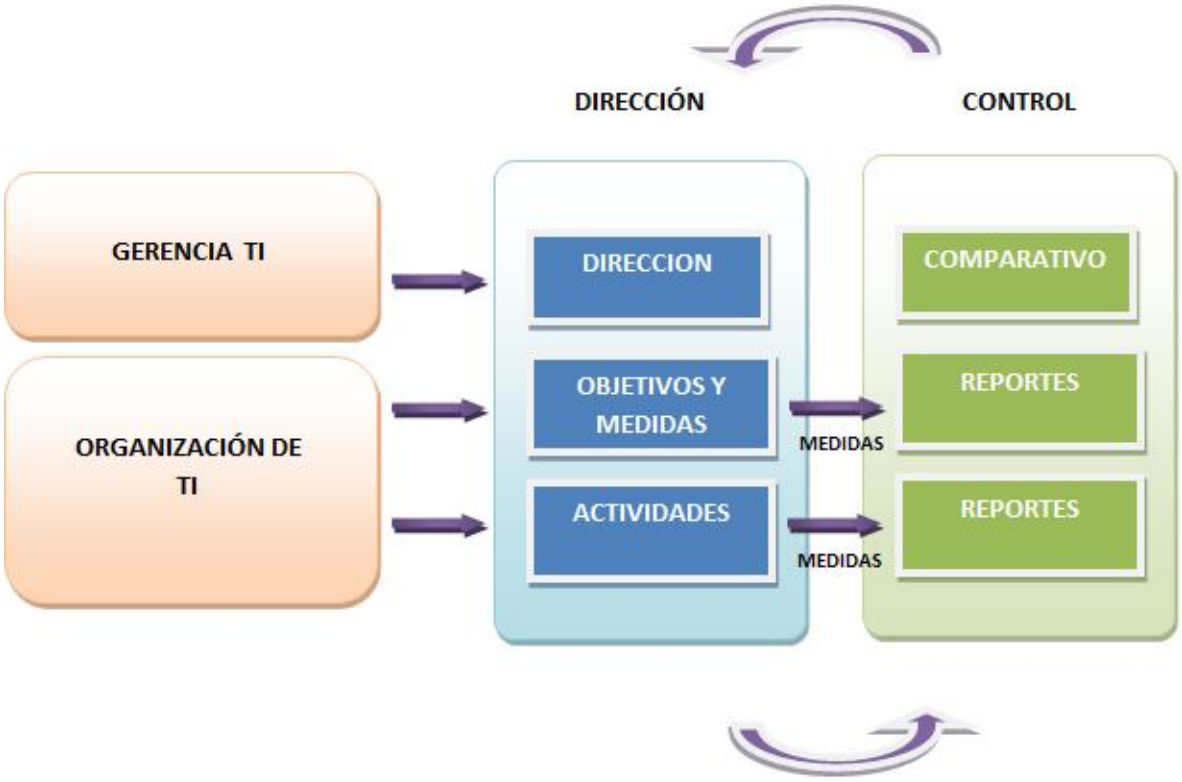


**Figura 1.3 Responsabilidades.**

El gobierno de T.I. es aquel encargado de llenar aquellos espacios vacíos que se forman de manera natural en los dominios técnicos y de administración, no perdiendo de vista los siguientes puntos:

- "brecha de alineación" se presenta cuando las inversiones en T.I. no son trazables a los objetivos de una organización.
- "brecha de ejecución" se presenta cuando los encargados de la entrega de soporte y servicios no tienen una clara "línea de visión" a la estrategia corporativa.
- "brecha de la innovación" se presenta cuando la dirección y el personal no están vinculados a las necesidades del mercado, las tecnologías emergentes y las estrategias de inversión para las necesidades futuras.

## 1.7 Áreas de enfoque del gobierno de T.I.

- **Alineación Estratégica.** Se centra en asegurar el vínculo de la línea de negocios de una empresa con los planes de T.I., manteniendo y validando la parte operativa de T.I.
- **Valor entregado.** Se refiere a la ejecución de tareas a través de un ciclo de entrega, cerciorando que las T.I. ofrecen los beneficios ofertados frente a los objetivos de una organización, asegurando optimizar los gastos, demostrando de esta manera el valor intrínseco de la función de T.I.
- **Administración de riesgos.** Se refiere al conocimiento de los riesgos por parte de los directivos de una empresa, con una clara comprensión de los objetivos y alcances proyectados de la empresa con los riesgos que implican, a fin de tener una visión completa y gestionar los riesgos de la organización.
- **Administración de recursos.** Se refiere a la óptima inversión y gestión de recursos críticos de T.I. tales como aplicaciones, información, infraestructura y personas. Las cuestiones clave se refieren a la optimización de manejo de información e infraestructura.
- **Medición de desempeño**. Se refiere a la implementación de estrategias de seguimiento y monitoreo, uso de recursos, desempeño de procesos y entrega de servicios, medidos en acciones que permitan la mejora continua, así como de conseguir las metas de una organización.

## 1.8 Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, en inglés: Control Objectives for Information and Related Technology).

COBIT (Objetivos de control para la información y tecnologías relacionadas) es una metodología publicada en 1996 por el Instituto de Control de T.I. y la ISACA

(Asociación de Auditoría y Control de Sistemas de Información) que se usa para evaluar el departamento de T.I. de una compañía.

Se basa en un marco de referencia de procesos, indicadores de objetivos clave (KGl, en inglés Key Goal Indicators) e indicadores de rendimiento clave (KPI, en inglés Key Performance Indicators), que se usan para controlar los procesos para recoger datos que la compañía puede usar para alcanzar sus objetivos.
El enfoque COBIT propone 34 procesos, organizados en 4 áreas funcionales más grandes, que abarcan 318 objetivos.
COBIT provee buenas prácticas para la administración de procesos de T.I. en una estructura lógica y manejable. El marco de referencia de COBIT explica cómo los procesos de T.I. entregan la información que la organización necesita para lograr sus objetivos. Esta entrega es controlada a través de “objetivos de control de alto nivel” (dominios) relacionados a la planeación y organización de T.I., adquisición e implementación, administración de la entrega y el soporte al desempeño. Asimismo, COBIT identifica siete criterios de información: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información, así como recursos; personal, sistemas de aplicación, instalaciones, tecnología y datos, que son importantes en cada proceso de T.I. para apoyar los objetivos de negocio de la organización.

En la figura 1.4 se muestran los objetivos del negocio que enmarca el control de objetivos COBIT.

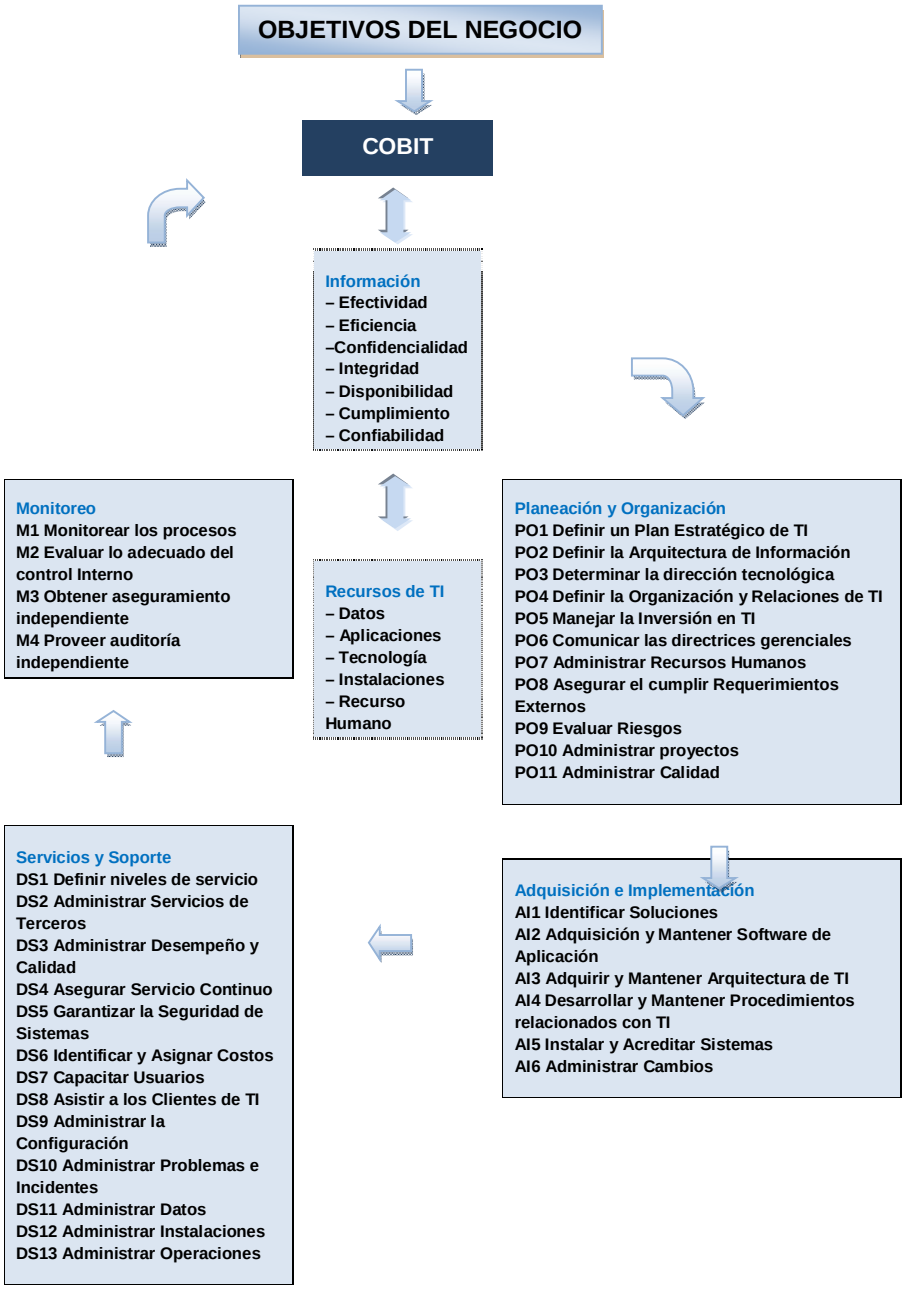


Figura 1.4

### 1.9 Procesos y arquitectura de T.I.

COBIT define en la tabla 1.2 los siguientes procesos, con el fin de mantener la función de T.I. siempre orientada a los objetivos de una organización, mediante cuatro dominios diferentes:

Tabla 1.2.

| Planificación y organización (Plan & Organice) | Adquisición e Implementación (Acquire & Implement) | Entrega y soporte (Deliver &Support) | Monitoreo y Evaluación (Monitor &Evaluate) |
|---|---|---|---|
| **PO1 Definir un Plan Estratégico de T.I.** | AI1 Identificar Soluciones Automatizadas. | DS1 Definir y Administrar Niveles de Servicio. | M1 Monitorear los Procesos. |
| **PO2 Definir la Arquitectura de la Información.** | AI2 Adquirir y Mantener Software de Aplicación. | DS2 Administrar Servicios de Terceros. | M2 Evaluar lo Adecuado del Control Interno. |
| **PO3 Determinar la Dirección Tecnológica.** | AI3 Adquirir y Mantener Infraestructura de Tecnología. | DS3 Administrar el Rendimiento y la Capacidad. | M3 Asegurar el Cumplimiento de los Requisitos Externos. |
| **PO4 Definir la Organización y las Relaciones de T.I.** | AI4 Desarrollar y Mantener Procedimientos. | DS4 Asegurar un Servicio Continuo. | |
| **PO5 Administrar la Inversión de T.I.** | AI5 Adquisición e implementación. | DS5 Asegurar Seguridad de Sistemas. | |
| **PO7 Administrar los Recursos Humanos.** | AI6 Administrar Cambios. | DS6 Identificar y Asignar Costos. | |
| **PO8 Administrar la Calidad.** | AI7 Instalar y Acreditar Sistemas. | DS7 Educar y Capacitar a los Usuarios. | |
| **PO9 Evaluar los Riesgos.** | | DS8 Asistir y Asesorar a los Clientes. | |
| **PO10 Administrar Proyectos.** | | DS9 Administrar la Configuración. | |
| | | DS10 Administrar Problemas e Incidentes. | |
| | | DS11 Administrar Datos. | |
| | | DS12 Administrar Facilidades. | |
| | | DS13 Administrar Operaciones. | |

- **Planificación y Organización (Plan& Organise).**
  - **PO1.** Definir un Plan Estratégico de T.I. Mediante el establecimiento de políticas y procedimientos para la planeación con el objeto de lograr un equilibrio entre las oportunidades de tecnología de la información y de los requerimientos de T.I. de la organización, y asegurar su cumplimiento posterior mediante objetivos y planes a corto y largo plazo de T.I. y organizacionales. Los planes a largo plazo deben ser traducidos periódicamente en planes operativos que fijan metas a corto plazo claros y concretos. Figura 1.5.


**Figura 1.5 Equilibrio en la organización.**

La planificación estratégica de T.I. es necesaria para gestionar y dirigir los recursos de T.I. que deben estar alineados a los objetivos y prioridades de la organización. El plan estratégico debe mejorar la comprensión para las principales partes involucradas en T.I., oportunidades y limitaciones, evaluar el desempeño actual y definir el nivel de inversión requerido. La estrategia de negocio y las prioridades se reflejan en proyectos que establecen objetivos concisos, planes y tareas.

  - **PO2.** Definir la Arquitectura de la Información. La función de los sistemas de información debe de actualizarse periódicamente y definir los sistemas apropiados para optimizar el uso de esta información. Este proceso mejora la calidad de la toma de decisiones administrativas ya que siempre la información es confiable y segura.

Esto se puede llevar a cabo mediante la creación y el mantenimiento de un modelo de información y el desarrollo de un diccionario de datos corporativos, un esquema de clasificación de la información, así como niveles de seguridad.

– **PO3.** Determinar la Dirección Tecnológica. La función de los servicios de información debe determinar la dirección de la tecnología para aprovechar los recursos disponibles y emergentes e impulsar y hacer posible el cumplimiento de la estrategia del negocio. Esto requiere la creación y el seguimiento de un plan de infraestructura técnica que establece y maneja expectativas claras y realistas de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de entrega.

  El plan debe ser actualizado periódicamente y abarca aspectos tales como la arquitectura de sistemas, dirección tecnológica, planes de adquisiciones, normas, estrategias de migración y de contingencia.

– **PO4.** Definir la Organización y las Relaciones de T.I. Una organización de T.I. debe ser definida teniendo en cuenta las necesidades de personal, habilidades, responsabilidad, autoridad, funciones y responsabilidades, y supervisión, elementos que garanticen la transparencia y control, a fin de entregar los servicios correctos de T.I. Es facilitado por una organización adecuada en números y en habilidades con roles y responsabilidades definidos y comunicados, alineados con el negocio y que facilita la estrategia y provee la orientación efectiva y el control adecuado.

– **PO5.** Administrar la Inversión de T.I. Para establecer y mantener un marco de gestión de T.I., mediante programas de inversión que abarquen el costo-beneficio, asignación de prioridades dentro del presupuesto, un proceso de presupuestación y su calendarización para definir la gestión formal del presupuesto. Trabajar con las partes involucradas para identificar y controlar los costos y beneficios totales en el contexto de los planes estratégicos de T.I. e iniciar

acciones correctivas cuando sea necesario, asegurando la inversión y controlar el gasto de recursos financieros. Es reflejado por medio de un análisis para inversión periódico y asignación de un presupuesto operativo establecido y aprobado por la organización.

- **PO6.** Comunicar los Objetivos y la Dirección de la Gerencia. La Gerencia debe desarrollar un marco de control de T.I. empresarial, así como definir y comunicar sus políticas. En este mismo sentido debe ser implementado un programa de comunicación para difundir los objetivos de servicio a través de políticas y procedimientos, aprobados por la dirección. La comunicación asegura la conciencia y la comprensión de los objetivos traduciendo las estrategias en reglas prácticas y utilizables por los usuarios.
- **PO7.** Administrar los Recursos Humanos. Obtener y mantener una fuerza de trabajo motivada y competente y maximizar las contribuciones del personal a los procesos de T.I., para la entrega de servicios de T.I. Esto se consigue haciendo uso de las mejores prácticas de administración de personal para reclutar, contratar, formar, evaluar el desempeño, compensar, entrenar y promover hasta la terminación contractual.
- **PO8.** Gestión de Calidad. Un sistema de gestión de la calidad debe ser desarrollado mediante la planificación, implementación y mantenimiento del sistema independiente que refleje información sobre la calidad de los otros procesos, mediante indicadores cuantificables. La mejora continua se logra mediante el monitoreo permanente: analizar y actuar sobre las desviaciones, y comunicar los resultados para ejecutar las acciones pertinentes. La gestión de calidad es esencial para satisfacer los requerimientos de clientes de T.I. y poder demostrar el valor de T.I. de la empresa, garantizando eficiencia y eficacia en la entrega de servicios.
- **PO9.** Evaluar los Riesgos. Crear y mantener un marco de gestión de riesgos. Para evaluar la situación actual y cualquier impacto

potencial sobre los objetivos de la organización, causado por un acontecimiento imprevisto o de posible ocurrencia, debe ser identificado, analizado y evaluado e implementar estrategias de reducción de los riesgos para reducir al mínimo o a un nivel aceptable. El resultado de la evaluación debe ser expresado en términos financieros, para permitir a los interesados establecer un nivel aceptable de tolerancia y apoyar las decisiones de la Gerencia con el objeto de lograr los objetivos de T.I.

- **PO10.** Administrar Proyectos. Establecer un programa y un marco de gestión para la administración de todos los proyectos de T.I. El marco debe garantizar la correcta asignación de prioridades y la coordinación de los mismos. El marco debe incluir un plan maestro, la asignación de recursos, definición de los resultados, un enfoque por fases para la entrega, garantía de calidad, un plan de protocolos de pruebas. Este enfoque reduce el riesgo de costos inesperados y cancelaciones de proyectos, ya que establece prioridades, tiempos de entrega y estimaciones del presupuesto. Es posibilitado por la organización que identifica y da prioridad a los proyectos que se ajusten con el plan operativo.

- **Adquisición e Implementación (Acquire & Implement).**
  - **AI1.** Identificar Soluciones Automatizadas. Asegurar un enfoque efectivo y eficiente para satisfacer los requerimientos del usuario, posibilitado por una identificación y análisis objetivos y claros de las oportunidades alternativas medidas en contraposición con los requerimientos del usuario.
  - **AI2.** Adquirir y Mantener Software de Aplicación. Proveer funciones automatizadas que soporten efectivamente el proceso del negocio, posibilitado por una definición de declaraciones específicas de requerimientos funcionales y operativos, y una implementación por fase con productos claros.

- **AI3.** Adquirir y Mantener Infraestructura de Tecnología. Proveer las plataformas apropiadas para soportar las aplicaciones del negocio mediante adquisición juiciosa de hardware, estandarización sobre el software, evaluación del rendimiento del hardware y del software, y administración consistente del sistema.
- **AI4.** Desarrollar y Mantener Procedimientos. Asegurar el debido uso de las aplicaciones y de las soluciones tecnológicas establecidas, posibilitados por un enfoque estructurado del desarrollo de manuales de procedimiento de usuario y de operaciones, requerimientos de servicio y materiales de entrenamiento.
- **AI5.** Adquisición e implementación. Proveer recursos de T.I., incluyendo personas, hardware, software y servicios cuando sea necesario, a través de la definición de procesos de aprovisionamiento, la selección adecuada de proveedores y la configuración de condiciones contractuales.
- **AI6.** Administrar Cambios. Minimizar la probabilidad de interrupción, alteraciones no autorizadas y errores, mediante el análisis, la implementación y el seguimiento de todos los cambios solicitados y hechos a la infraestructura existente de T.I.
- **AI7.** Instalar y Acreditar Sistemas. Verificar y confirmar que la solución es adecuada para el propósito que se pretende, mediante una instalación, migración, conversión y plan de aceptación bien formalizados.

- **Entrega y soporte (Deliver & Support).**
  - **DS1.** Definir y Administrar Niveles de Servicio. Establecer un entendimiento común del nivel de servicio requerido, facilitado por el establecimiento de acuerdos de nivel de servicio que formalizan los criterios de rendimiento contra los cuales se medirá la cantidad y la calidad del servicio que será medido.

- **DS2.** Administrar Servicios de Terceros. Asegurar que los roles y responsabilidades de terceros estén claramente definidos, cumplidos y que continúen satisfaciendo los requerimientos, mediante medidas de control dirigidas a la revisión y la monitorización de acuerdos y procedimientos existentes, para su efectividad y cumplimiento con la política de la organización.
- **DS3.** Administrar el Rendimiento y la Capacidad. Asegurar que la capacidad adecuada esté disponible y que se haga el mejor y el óptimo uso de ésta, para satisfacer las necesidades requeridas de rendimiento a través de la recolección de datos, análisis y reporte sobre el rendimiento de los recursos, el dimensionamiento de la aplicación y la demanda de carga de trabajo.
- **DS4.** Asegurar un Servicio Continuo. Asegurar que los servicios de T.I. estén disponibles cuando se requieran y asegurar un impacto mínimo en el negocio en el caso de una interrupción importante. Es factible teniendo un plan operativo y comprobado de continuidad de T.I. que esté en línea con el plan general de continuidad del negocio y con sus requerimientos de negocio relacionados.
- **DS5.** Asegurar Seguridad de Sistemas. Salvaguardar información contra el uso, revelación o modificación no autorizada, daño o pérdida mediante controles de acceso lógico, que aseguran que el acceso a los sistemas, datos y programas esté restringido a los usuarios autorizados.
- **DS6.** Identificar y Asignar Costos. Asegurar un conocimiento correcto de los costos atribuibles a los servicios de T.I., utilizando un sistema de contabilidad de costos que asegura que los costos sean registrados, calculados y asignados al nivel requerido de detalle y a la oferta apropiada de servicio.
- **DS7.** Educar y Capacitar a los Usuarios. Asegurar que los usuarios estén haciendo uso efectivo de la tecnología y que estén conscientes

de los riesgos y responsabilidades involucradas, mediante un extenso plan de entrenamiento y desarrollo.

- **DS8.** Asistir y Asesorar a los Clientes. Asegurar que cualquier problema que experimente el usuario sea resuelto de manera apropiada a través de una facilidad de Help Desk, que provee soporte y asesoramiento de primera línea.
- **DS9.** Administrar la Configuración. Dar cuenta de todos los componentes de T.I., prevenir las alteraciones no autorizadas, verificar la existencia física y proveer una base para una administración sensata de cambios. Es posibilitado por controles que identifican y registran todos los activos de T.I. y su ubicación física, y un programa de verificación regular que confirme su existencia.
- **DS10.** Administrar Problemas e Incidentes. Asegurar que los problemas y los incidentes sean resueltos, y que se investigue la causa para prevenir cualquier recurrencia, usando un sistema de administración de problemas que registra y procesa todos los incidentes.
- **DS11.** Administrar Datos. Asegurar que los datos sigan siendo completos, precisos y válidos durante su ingreso, actualización y almacenamiento, mediante una combinación efectiva de controles generales y de aplicación sobre las operaciones de T.I.
- **DS12.** Administrar Facilidades. Proveer un entorno físico adecuado que proteja el equipo de T.I. y la gente contra riesgos naturales y provocados por el hombre. Es posibilitado por la instalación de controles ambientales y físicos adecuados que sean revisados regularmente en busca de su funcionamiento apropiado.
- **DS13.** Administrar Operaciones. Asegurar que las funciones importantes de soporte de T.I. se realicen regularmente y en la forma debida, mediante un programa de actividades de soporte que es registrado y aprobado para la realización de todas las actividades.

- **Monitoreo y Evaluación (Monitor & Evaluate).**
  - **M1.** Monitorear los Procesos. Asegurar el logro de los objetivos de rendimiento fijados para los procesos de T.I., posibilitado por la definición de indicadores relevantes de rendimiento, el reporte sistemático y oportuno del rendimiento y la pronta acción frente a las desviaciones.
  - **M2.** Evaluar Adecuadamente el Control Interno. Asegurar el logro de los objetivos de control interno fijados para los procesos de T.I., mediante el compromiso de monitorizar el control interno, determinar su efectividad, y reportar sobre ellos regularmente.
  - **M3.** Asegurar el Cumplimiento de los Requisitos Externos. Cumplir con las obligaciones legales, regulatorias y contractuales, identificando y analizando los requerimientos externos para el impacto de su T.I., y tomando las medidas apropiadas para cumplirlas. Lo anterior permite trabajar bajo un modelo sistemático, cuyas ventajas presentan un control elevado de los objetivos, para que la T.I. cumpla satisfactoriamente los requerimientos de negocio, manteniendo esta función siempre enfocada a las metas de una organización. La figura 1.6 muestra el modelo COBIT.

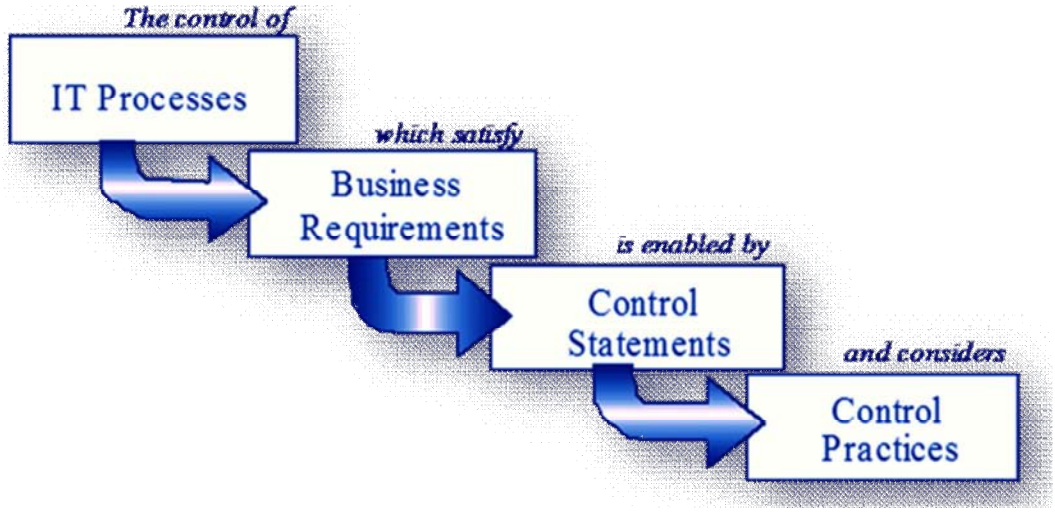


**Figura 1.6 Modelo Framework de COBIT.**

## 1.10 Entrega y soporte de servicios.

Las operaciones de S.I. en las instalaciones en un área de informática son parte de las actividades diarias con el entorno de hardware y software de S.I. de la organización. Esta función es particularmente importante cuando se ejecutan regularmente tareas de cómputo muy grandes y centralizadas para fines del negocio, produciendo resultados y actualizando el estado de situaciones. La organización de las operaciones de S.I. varía dependiendo del tamaño del entorno y de la carga de trabajo de la computadora.

Las operaciones de S.I. incluyen generalmente las áreas de funcionamiento siguientes:

- Administración de Operaciones de S.I.
- Soporte de infraestructura incluyendo operaciones de computadora.
- Soporte Técnico.
- Cronogramas de ejecución de trabajos (Job Scheduling).
- Aseguramiento de la Calidad.
- Control de cambios y administración de publicaciones.
- Administración de la configuración.
- Sistema de administración de biblioteca de programas y software de control.
- Procedimientos de administración de desempeño.
- Monitoreo de la seguridad física y del ambiente.
- Administración de la seguridad de información.
- Monitoreo de la Infraestructura.
- Medición de desempeño.

## 1.11 Administración de servicios de T.I.

La administración de servicios de T.I. (ITSM en inglés Information Technology Service Management) comprende los procesos y procedimientos involucrados en su entrega eficiente y el soporte de diversas funciones de T.I. Se enfoca en afinar los servicios de T.I. para que se ajusten a las cambiantes demandas de la

empresa, y para medir y mostrar mejoras en la calidad del servicio de T.I. ofrecidos, con una reducción en el costo de servicio en el largo plazo.

La administración de servicios de T.I. se encuentra en la perspectiva de negocio y en la administración de infraestructuras de las aplicaciones de T.I. para soporte y entrega de servicios. Un acuerdo de nivel de servicio o ANS (en inglés Service Level Agreement o SLA), Figura 1.7.


**Figura 1.7. SLA (Service Level Agreement) acuerdo de nivel de servicio.**

- **Servicios de soporte de T.I.**
  - Mesas de ayuda.
  - Administración de incidentes.
  - Administración de problemas de configuraciones.
  - Administración de cambios.
  - Administración de activos y recursos.
  - Administración de publicaciones (versiones).

- **Servicios de entrega de T.I.**
  - Administración de nivel de servicios.
  - Administración financiera de T.I.
  - Administración de capacidad.
  - Administración de continuidad de servicios de T.I.
  - Administración de la disponibilidad.

Los servicios de T.I. pueden ser administrados mejor con un contrato de nivel de servicio (SLA, de las siglas en inglés Service Level Agreement) donde los servicios ofrecidos forman una medición de servicio lo cual es la base para dichos contratos. Con esto se trata de subsanar la brecha que se puede generar entre las expectativas de los clientes y los servicios ofrecidos a través del contrato de servicio, definiendo en este la naturaleza, el tipo, el tiempo, entre otros, sobre el servicio que se está ofreciendo.

- **Nivel de Servicio.** El departamento de S.I. es una organización de servicio para los usuarios finales. Como tal, el éxito de este departamento depende de satisfacer los requerimientos de procesamiento y de servicio del usuario final. Estos servicios incluyen exactitud, integridad, oportunidad y distribución apropiada de la salida relacionada con el procesamiento de las aplicaciones.

  A fin de monitorear la eficiencia y efectividad de los servicios brindados por el personal de S.I., se deben aplicar las siguientes herramientas:
  - Reportes de terminación no en tiempo de trabajos.
  - Reportes de problemas del operador.
  - Reportes de distribución de salidas.
  - Registros de la consola.
  - Cronogramas de trabajo del operador.

### 1.11.1 Catálogo de Procesos.

Una forma de simplificar la comunicación con el cliente es la herramienta de catálogo de procesos, en donde se describen los servicios ofrecidos de manera no técnica y comprensible para clientes y personal no experto, que provean los lineamientos de la organización de T.I. para desarrollar las actividades relacionadas con la operación, planeación, evolución y administración.

- **Acuerdo de Nivel de Operación (OLA).** El OLA son documentos de carácter interno de la organización donde se especifican las responsabilidades, compromisos, procesos y procedimientos de los diferentes departamentos de la organización T.I., en la prestación de los niveles de servicio.
- **Contratos de Soporte (UC).** Un UC, de sus siglas en inglés "Underpinning Contract", es un acuerdo con un proveedor externo que soporta los SLA no cubiertos por la propia organización T.I.
- **Programa de Mejora del Servicio (SIP).** El SIP, de sus siglas en inglés "Service Improvement Plan", es un plan para implementar mejoras en los procesos o servicios de T.I. mediante medidas correctivas a fallos detectados en los niveles de servicio, como propuestas de mejora basadas en el avance de la tecnología. El SIP es parte fundamental dentro de la renovación de los SLA.
- **Mesa de Ayuda.** Dentro de este conjunto de procesos es imprescindible la función del servicio de la Mesa de Ayuda, fundamentado en las mejores prácticas según ITIL V3 (Information Technology Infrastructure Library), en virtud que esto nos dará la posibilidad de una interrelación y un conducto de comunicación entre las diferentes funciones de administración de servicios. Siendo el punto de contacto de atención único, con el objetivo de garantizar la calidad y que los tiempos de respuesta de los servicios proporcionados sean adecuados con base en los niveles de servicio establecidos. Así mismo tener un punto de referencia para la mejora continua. Figura 1.8.


**Figura 1.8 Mesa de ayuda**

Como objetivos de la mesa de ayuda se puede mencionar:

- Es el único punto centralizado que permitirá el contacto entre los usuarios y los diferentes departamentos de T.I. en una organización.
- Administrar y controlar los activos compartidos, como proyectores, pantallas, impresoras láser, entre otros. La finalidad es garantizar la mejor calidad en el soporte requerido.
- Soporte de cambios a través de tecnología, procesos y el negocio.
- Mejorar la satisfacción del cliente y reducir tiempos no productivos.
- Identificar oportunidades de negocio adicionales.

Estructura

La estructura de la mesa de ayuda se recomienda en base a un esquema centralizado de atención, como a continuación se presenta en la figura 1.9.

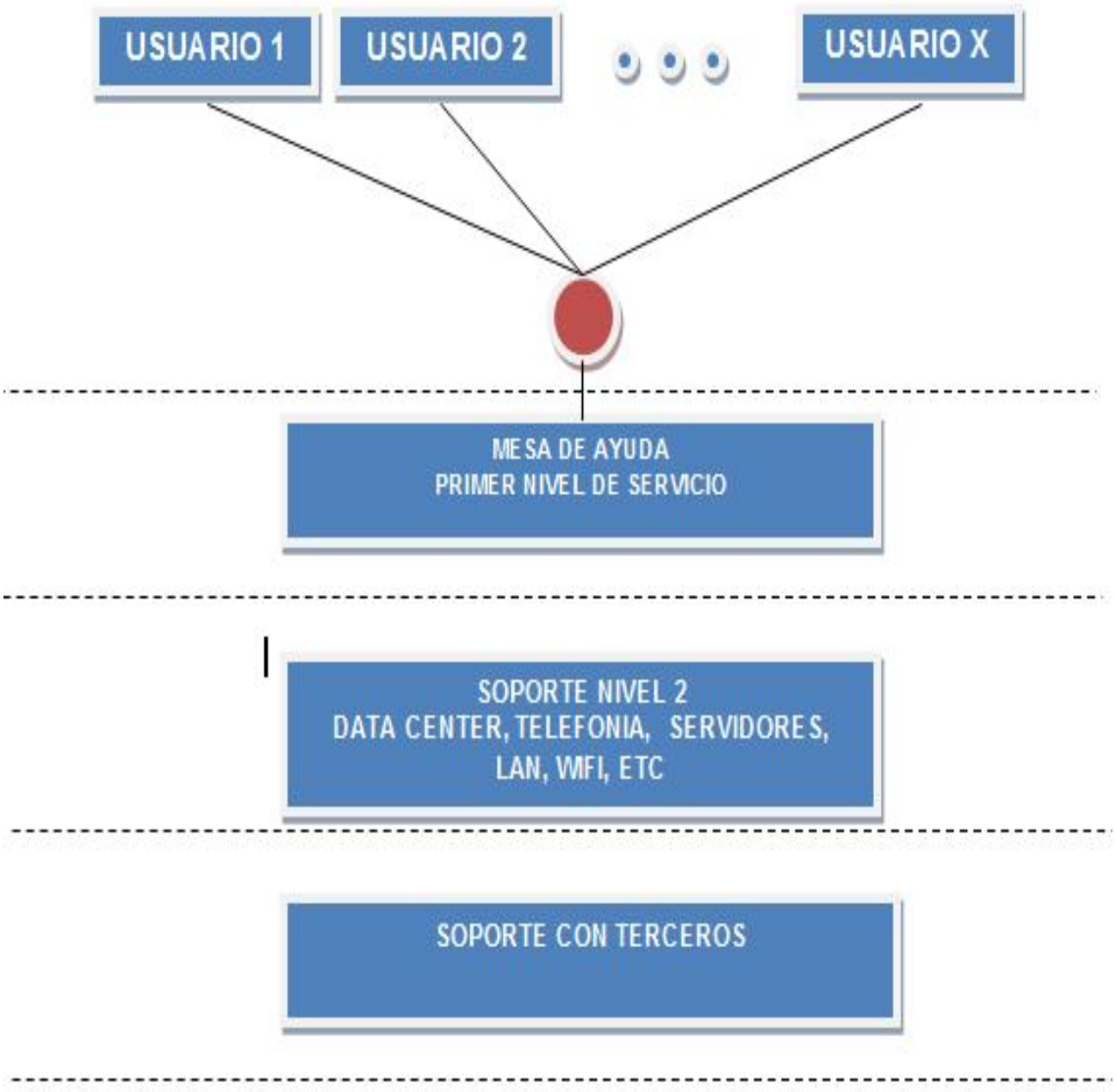


**Figura 1.9 Estructura de la mesa de ayuda.**

En la figura 1.10 se muestra el proceso de operación.

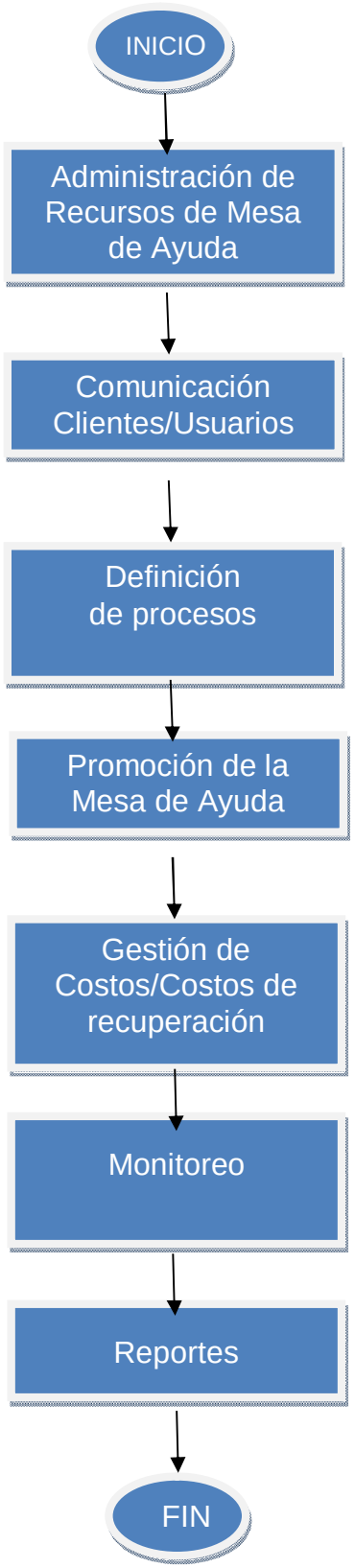


Figura 1.10. Proceso de Operación

### 1.11.2 Programa de Calidad del Servicio (SQP).

El Programa de Calidad del Servicio (SQP, en inglés Service Quality Program) debe incorporar toda la información necesaria para posibilitar una gestión eficiente de los niveles de calidad del servicio

- Objetivos de cada servicio.
- Estimación de recursos.
- Indicadores clave de rendimiento.
- Procedimientos de monitorización de proveedores.

En resumen, el SQP debe contener la información necesaria para que la organización T.I. conozca los procesos y procedimientos involucrados en el suministro de los servicios prestados, asegurando que estos se encuentren alineados con los procesos de negocio y mantengan unos niveles de calidad adecuados.

## Capítulo 2

# Diseño de auditoria para sistemas de información.

La Asociación de Auditoría y Control de Sistemas de Información, define la auditoria de Sistemas de Información S.I. como un proceso que se desarrolla mediante una exhaustiva metodología que permite realizar una verificación sobre cualquier área de Tecnologías de Información T.I., en donde existen cinco tareas dentro del área de proceso de auditoría de S.I., la cuales se presentan a continuación:

- El desarrollo e implementación de estrategias de auditoría de Sistemas de Información fundamentada en los riesgos de la organización en cumplimento con los estándares, directrices y mejores prácticas de auditoría de S.I.
- El planear auditorias específicas para validar que la T.I. y los sistemas de negocio estén protegidos y controlados.
- Llevar a cabo auditorias en conformidad con los estándares, directrices y mejores prácticas de auditoría de S.I. para lograr objetivos planeados de auditoría.
- Comunicar los hallazgos emergentes, los riesgos potenciales y los resultados de la auditoria a los accionistas clave.
- Asesorar sobre la implementación de la información de riesgos y las prácticas de control dentro de la organización, al tiempo que se mantiene la independencia.

Es de señalar que para llevar a cabo las tareas anteriores se deberán poseer los conocimientos definidos por alguna instancia competente y de preferencia con presencia internacional y perfectamente avalada, como ejemplo se encuentra la ISACA (Information System Audit and Control Association por sus siglas en ingles), siendo entre otros los siguientes conocimientos a cubrir:

1) Estándares, directrices y procedimientos de S.I. y código de ética profesional de ISACA, (Normas y estandartes).
2) Prácticas y técnicas de auditoría de S.I.
3) Técnicas para recopilar información y preservar evidencia tales como; ejemplos observación, investigación, entrevista, Técnicas y Herramientas de Auditoría Asistidas por Computadora (CAATTs, en inglés Computer-Assisted Audit Tools and Techniques) y medios electrónicos.
4) Ciclo de vida de la evidencia, es decir todo lo referente a la recopilación, protección y cadena de custodia.
5) Objetivos de control y controles relacionados con S.I.
6) Conocimiento sobre la evaluación de riesgo en un contexto de auditoría.
7) Técnicas de planeación y administración de auditoría.
8) Técnicas de reporte y comunicación, es decir todo lo referente a la facilitación, negociación y resolución de conflictos.
9) Conocimiento de la autoevaluación del control (CSA en inglés, Control Self-Assessment).
10) Técnicas continúas de auditoría.

Con estas herramientas señaladas por la ISACA, la función de auditoría debe ser encaminada de tal forma que se pueda asegurar que las diversas tareas realizadas están alineadas a los objetivos de la función de la auditoria. En este mismo sentido cuidando de conservar la independencia, competencia de la auditoria y el valor agregado a la alta gerencia con el objetivo de lograr los objetivos del negocio.

Es importante mencionar que dentro de cualquier organización, la función de auditoría de S.I., debe estar definida en un estatuto de auditoría. ISACA señala que la parte de auditoría de S.I. puede ser parte de la auditoría interna como un grupo independiente o integrada dentro de las auditorías financieras u operacionales.

Como parte de las recomendaciones se menciona que el estatuto debe establecer claramente las responsabilidades y objetivos de la dirección para la función de auditoría de S.I., así como la delegación de la autoridad para la misma, con respecto a la responsabilidad de Auditoría Interna en funciones distintas de auditoría en el área de T.I.

Frecuentemente los auditores internos deben afrontar la aceptación de responsabilidades por funciones o tareas operativas, distintas de auditoría. La aceptación de tales responsabilidades puede menoscabar la independencia y objetividad, por lo cual, de ser posible, deben ser evitadas.

**2.1 Organización, planeación y recursos de la función de auditoría de S.I.**

La función de auditoría de S.I. puede ser llevada a cabo de manera externa o internamente. La Asociación de Auditoría y Control de Sistemas de Información menciona que la función de auditoría interna de un S.I. debe establecerse mediante un estatuto de auditoría, independiente o integrada a una auditoría financiera u operacional, con el objetivo de garantizar el control relacionado con T.I. frente a los auditores financieros o de la gerencia.

También menciona que en el estatuto se deben definir tres puntos principales, la delegación de autoridad, la responsabilidad y los objetivos específicos (de la dirección) para la auditoría de S.I., por lo tanto en este documento encontramos descrito la autoridad, alcance y responsabilidades generales de la función de auditoría. Es muy importante que todo informe de auditoría debe ser aprobado por el nivel más alto de la dirección y sus modificaciones deben realizarse previa justificación.

Por otra parte, la Asociación de Auditoría y Control de Sistemas de Información requiere la correcta documentación de responsabilidades, autoridad y la obligación

de rendir cuentas de la función de auditoría en el denominado Estatuto de Auditoría de S.I.

Asimismo se hace la diferenciación entre un estatuto de auditoría y una carta compromiso, definiendo el primero como un documento integral que reúne todas las actividades de auditoría en una entidad, y la carta de compromiso como un documento enfocado en un ejercicio particular de auditoría con un objetivo específico.

Otra manera de realizar una auditoría es externa. En este caso el alcance y los objetivos de estos servicios deben ser documentados en un contrato formal o declaración de trabajo entre la organización contratante y el proveedor de servicios. En ambos casos, los resultados y reportes de las auditorias deben dirigirse al nivel más alto de la organización y siempre ser independientes de otros procesos.

Es imprescindible garantizar el nivel de competencia de un auditor, sobre todo tomando en cuenta la vertiginosa evolución de las tecnologías y las técnicas para auditar, acordes a esta tendencia, los planes y programas de capacitación deben ser considerados. Se recomienda una revisión de estos planes y programas de manera semestral, que en función de las necesidades se reflejará en el proyecto presupuestal para este rubro.

Otro punto a contemplarse dentro de la función de auditoría es el relacionado a la planeación de dicha actividad. Esta planeación debe ser administrada en dos vertientes de tiempo ligadas directamente, lo que es referente a la planeación a corto y largo plazo. En este punto es importante señalar que la Asociación de Auditoría y Control de Sistemas de Información menciona lo siguiente:

- Planeación a corto plazo: se considera de un año y durante el transcurso de este lapso de tiempo se deben contemplar los temas, actividades,

estrategias, etc., sustanciales a desarrollar, a fin de cubrir los objetivos propios de esta parte de la planeación de la auditoria.

- Planeación a largo plazo: contempla los riesgos que pudieran presentarse y afectar respecto al desarrollo establecido de la organización.

Cabe hacer mención que, basándose en los estándares de auditoría de S.I. de ISACA, indica que un auditor deberá manejar de manera clara y bien definida la misión, los objetivos, el propósito y los procesos del negocio. Aquí se incluye lo relacionado a los requerimientos de información como tecnología, seguridad, disponibilidad, integridad, confidencialidad de la información y la revisión de controles internos de T.I.

Tener claramente conocimiento de las políticas, estándares y directrices, procedimientos y estructura de la organización, así como la elaboración de un análisis de riesgos para el diseño de la auditoria, estableciendo también el alcance, el o los objetivos, enfoque y asignación de recursos humanos de la misma.

## 2.2 Estándares relativos a la auditoria de un S.I.

En esta sección se mencionará lo relativo a los estándares, lineamientos y procedimientos necesarios que deben reunirse para poder estar en posibilidad de realizar una auditoría, basándose en los estándares de la Asociación de Auditoría y Control de Sistemas de Información. Estos estándares delimitan los requerimientos obligatorios para la auditoría y para los reportes de auditoría de S.I. Tomando como fuente el sitio web de ISACA, a continuación se enlistan los requerimientos para una auditoría de S.I. Tabla 2.1.

**Tabla 2.1 Estándares de Auditoría de S.I.**

| |
|---|
| S1 Estatuto de Auditoría |
| S2 Independencia |
| S3 Ética y Estándares Profesionales |
| S4 Competencia |
| S5 Planeación |
| S6 Realización del Trabajo de Auditoría |
| 57 Reporte |
| S8 Actividades de Seguimiento |
| S9 Irregularidades y Actos Ilegales |
| S10 Gobierno de T.I. |
| S11 Uso de evaluación de Riesgo en la Planeación de Auditoría |
| S12 Materialidad de Auditoría |
| S13 Usar el Trabajo de otros Expertos |
| S14 Evidencia de Auditoría |

Los estándares de la Asociación de Auditoría y Control de Sistemas de Información anteriormente enlistados son parte fundamental de la labor de auditoría, por lo que siendo una herramienta base deben conocerse y ejecutarse. Garantizando las mejores prácticas de la función, a continuación encontramos los estándares de cada uno:

- **S1 Estatuto de Auditoría.** El propósito, responsabilidad, autoridad y rendición de cuentas de la función de auditoría de sistemas de información o tareas de auditoría de sistemas de información deben estar debidamente documentados en un estatuto de auditoría o en un contrato. El estatuto de auditoría o contrato debe ser establecido y aprobado por un nivel apropiado dentro de la organización.

- **S2 Independencia:**
  - Independencia profesional. En todos los aspectos relacionados con la auditoría, el auditor de S.I. debe ser independiente del auditado, tanto en actitud como en apariencia.
  - Independencia organizacional. La función de auditoría de S.I. debe ser independiente del área o actividad que se esté revisando, para permitir la ejecución y conclusión objetiva de la tarea de auditoría.

- **S3 Ética y Estándares Profesionales.** El auditor de S.I. debe cumplir el Código de Ética Profesional en tareas de auditoría.
  El auditor de S.I. debe ejercer el debido cuidado profesional, esto incluye el cumplimiento de los estándares profesionales de auditoría aplicables cuando se realicen tareas de auditoría.

- **S4 Competencia Profesional:**
  - El auditor de S.I. debe ser profesionalmente competente, teniendo las habilidades y los conocimientos para realizar el trabajo de auditoría asignado.
  - El auditor de S.I. debe mantener la competencia profesional a través de una apropiada educación y capacitación profesional continua.

- **S5 Planeación.** El auditor de S.I. debe planear el alcance de la auditoría de sistemas de información, tomando en cuenta los objetivos de la auditoría y el cumplimiento con las leyes y los estándares profesionales de auditoría aplicables.
  - El auditor de S.I. debe desarrollar y documentar el enfoque de auditoría basado en riesgos.
  - El auditor de S.I. debe desarrollar y documentar el plan de auditoría, detallando la naturaleza, los objetivos, el tiempo, el alcance y los recursos requeridos.

- El auditor de S.I. debe desarrollar el programa y los procedimientos de auditoría.

- **S6 Ejecución del Trabajo de Auditoría.** Supervisión. El personal de auditoría de sistemas de información debe ser supervisado para proveer una certeza razonable que los objetivos serán alcanzados y que se observan los estándares profesionales de auditoría aplicables.
  Evidencia. En el curso de la auditoría, el auditor de S.I. debe obtener evidencia suficiente, confiable y relevante para lograr los objetivos de la auditoría. Los hallazgos y las conclusiones deben estar respaldados por un análisis e interpretación apropiados de esta evidencia.
  Documentación. El proceso de auditoría debe estar documentado, describiendo el trabajo de auditoría y la evidencia que respalde los hallazgos y las conclusiones del auditor de S.I.

- **S7 Informe.** El auditor de S.I. debe proveer un informe, en un formato apropiado, al terminar la revisión. El informe debe identificar la organización, los destinatarios, y cualquier restricción sobre su publicación. El informe de auditoría debe establecer el alcance, los objetivos, el período cubierto y la naturaleza, tiempo y extensión del trabajo realizado. El informe debe establecer los hallazgos, conclusiones y recomendaciones, así como cualquier reserva, restricción o limitación en el alcance que tenga el auditor de SI con respecto a la auditoría. El auditor de S.I. debe tener evidencia suficiente y apropiada para respaldar los resultados reportados. El informe debe estar firmado, fechado y ser distribuido de conformidad con los términos del estatuto de auditoría o contrato, cuando se emita.

- **S8 Actividades de Seguimiento.** Después de proveer el informe de los hallazgos y recomendaciones, el auditor de S.I. debe solicitar y evaluar la información relevante, para determinar si la dirección ha tomado las acciones apropiadas de manera oportuna.

- **S9 Irregularidades y Actos Ilícitos.** Al planificar y ejecutar una auditoría para reducir el riesgo a un nivel mínimo, el auditor de S.I. debe considerar el riesgo de irregularidades y actos ilícitos.
  - El auditor de S.I. debe mantener una actitud de escepticismo profesional durante la auditoría, reconociendo la posibilidad de que existan declaraciones erróneas debido a irregularidades y actos ilícitos, independientemente de su evaluación de riesgo.
  - El auditor de S.I. debe obtener un conocimiento de la organización y su ambiente, incluyendo sus controles internos. Cuando se realizan procedimientos de auditoría para obtener un conocimiento de la organización y su ambiente, el auditor de S.I. debe considerar relaciones inusuales o inesperadas que pueden indicar un riesgo de falsas declaraciones materiales debido a irregularidades y actos ilegales.
  - El auditor de S.I. debe obtener evidencia de auditoría suficiente y relevante para determinar si la dirección o alguien más dentro de la organización tienen conocimiento de alguna irregularidad o acto ilícito real, sospechoso o presunto.
  - El auditor de S.I. debe diseñar y ejecutar procedimientos para probar qué tan apropiados son los controles internos y el riesgo de que la dirección no respete los controles.
  - Cuando el auditor de S.I. identifique una declaración errónea, debe evaluar si esto pudiera ser indicativo de irregularidades o actos ilícitos. Si sospecha que así es, debe considerar las implicaciones en relación a otros aspectos de la revisión y en particular a las manifestaciones de la dirección.
  - El auditor de S.I. debería obtener declaraciones escritas de la dirección al menos una vez al año o con más frecuencia, dependiendo del trabajo de auditoría, en las que debería:

- Reconocer su responsabilidad por el diseño e implementación de controles internos para prevenir y detectar irregularidades o actos ilícitos.
- Revelar al auditor de S.I. los resultados de la evaluación del riesgo de que existan declaraciones erróneas como resultado de irregularidades o actos ilícitos.
- Revelar al auditor de S.I. su conocimiento de irregularidades o actos ilícitos que afecten la organización con relación a la dirección y a los empleados que tengan roles significativos en el control interno.

– El auditor de S.I. debe tomar conocimiento de cualquier presunción o sospecha de irregularidades o actos ilícitos que afecten a la organización que hayan sido informados por empleados, ex-empleados, reguladores y otros.
– Si el auditor de S.I. identifica una irregularidad o acto ilícito material u obtiene información de que una irregularidad o acto ilícito material pueda existir, este debe comunicar estos asuntos oportunamente al nivel apropiado de dirección.
– Si el auditor de S.I. identifica una irregularidad o acto ilícito material que involucre a la dirección o a empleados que tengan funciones significativas en el control interno, debe comunicar estos asuntos de manera oportuna a los encargados del gobierno corporativo.
– El auditor de S.I. debe aconsejar al nivel apropiado de dirección y a los encargados del gobierno corporativo sobre las debilidades materiales en el diseño e implementación del control interno, para prevenir y detectar irregularidades o actos ilícitos que podrían haber sido identificados en el curso de un trabajo de auditoría.
– Si el auditor de S.I. encuentra circunstancias excepcionales, tales como falsas declaraciones o actos ilícitos que afecten su capacidad de continuar con el trabajo de auditoría, en ese caso se debe considerar sus responsabilidades legales y profesionales aplicables

dadas las circunstancias, incluyendo el saber si existe el requerimiento de que el auditor de S.I. reporte a sus contratantes, o en algunos casos a los encargados del gobierno corporativo o a las autoridades regulatorias o bien considerar cancelar su contrato.

- El auditor de S.I. debe documentar todas las comunicaciones, planeación, resultados, evaluaciones y conclusiones relacionadas con irregularidades materiales y actos ilícitos que hayan sido reportados a la dirección, encargados del gobierno corporativo, reguladores y otros.

- **S10 Gobierno de T.I.** El auditor de S.I. debe revisar y evaluar si la función de S.I. está alineada con la visión, misión, valores, objetivos y estrategias de la organización. En dicho contexto el auditor debe:
  - Revisar si la función de S.I. tiene una declaración clara acerca del desempeño esperado por el negocio, efectividad, eficiencia y evaluar si se cumple con el mismo.
  - Revisar y evaluar la efectividad en los procesos de administración de recursos de S.I. y de desempeño.
  - Revisar y evaluar el cumplimiento con los requerimientos legales, ambientales, de calidad de la información, fiduciarios y de seguridad.
  - Usar un enfoque basado en riesgos para evaluar la función de S.I.
  - Revisar y evaluar el ambiente de control de la organización.
  - Revisar y evaluar los riesgos que puedan impactar de manera negativa el ambiente de S.I.

- **S11 Uso de la evaluación de riesgos en la planeación de auditoría:**
  - El auditor de S.I. debe usar una técnica o enfoque apropiado de evaluación de riesgos al desarrollar el plan general de auditoría de S.I. y determinar las prioridades para una asignación efectiva de recursos de auditoría.

- Al planear las revisiones individuales, el auditor de SI debe identificar y evaluar los riesgos relevantes para el área bajo revisión.

- **S12 Materialidad de la Auditoría.** El auditor de S.I. debe considerar la materialidad de la auditoría y su relación con el riesgo para determinar la naturaleza, tiempo y extensión de los procedimientos mientras planea la auditoría, por lo que debe considerar:
  - La potencial debilidad o la ausencia de controles y si podría tener como consecuencia deficiencias significativas o una debilidad material en el sistema de información.
  - El efecto acumulativo de las deficiencias o debilidades menores de control y la ausencia de controles, para traducir en deficiencia significativa o debilidad material el sistema de información.
  - El informe del auditor de S.I. debe revelar controles ineficaces o ausencia de controles y lo que representan dichas deficiencias y la posibilidad de que estas debilidades tengan como consecuencia una deficiencia significativa o una debilidad material.

- **S13 Usar el trabajo de otros expertos.** El auditor de S.I. debe, donde sea apropiado, considerar usar el trabajo de otros expertos para la auditoría. En este sentido el auditor de S.I. debe:
  - Evaluar y quedar satisfecho con los procesos de calificaciones profesionales, competencias, experiencia relevante, recursos, independencia y control de calidad de otros expertos, antes del compromiso.
  - Analizar, revisar y evaluar el trabajo de otros expertos como parte de la auditoría y concluir la extensión de uso y confianza en el trabajo de un experto.
  - Determinar y concluir si el trabajo de otros expertos es adecuado y completo, como para permitir que el auditor de S.I. concluya sobre

los actuales objetivos de auditoría. Dicha conclusión debe ser claramente documentada.

- Aplicar procedimientos adicionales de prueba para obtener evidencia suficiente y apropiada de auditoría en circunstancias en las que el trabajo de otros expertos no provee evidencia suficiente y apropiada de auditoría.
- Proveer una opinión apropiada de auditoría e incluir limitación de alcance si la evidencia requerida no se obtuvo a través de procedimientos adicionales de prueba.

- **S14 Evidencia de auditoría.** El auditor de S.I. debe obtener evidencia suficiente y apropiada de auditoría, para extraer conclusiones sobre las cuales basar los resultados de auditoría.
  - El auditor de S.I. debe evaluar la evidencia de auditoría obtenida durante la práctica realizada:
  - La evidencia de auditoría:
    - Los procedimientos que realiza el auditor.
    - Los resultados de procedimientos realizados por el auditor.
    - Los documentos fuente en cualquier formato electrónico o impreso, e información para soportar el informe de auditoría.
    - Los hallazgos y resultados del trabajo de auditoría.
    - El demostrar que el trabajo se realizó y cumple con las leyes, regulaciones y políticas aplicables.

**2.3 Procedimientos para auditoría de S.I.**

En lo referente a los procedimientos de la Asociación de Auditoría y Control de Sistemas de Información, para una auditoria de S.I., se mencionan los que se relacionan en la tabla “índice de procedimientos” Tabla 2.2.

**Tabla 2.2 Índice de procedimientos**

| |
|---|
| P1 Evaluación de Riesgos de S.I. |
| P2 Firmas Digitales |
| P3 Detección de Intrusos |
| P4 Virus y Otros Códigos Maliciosos |
| P5 Autoevaluación de Control de Riesgos |
| P6 Firewalls |
| P7 Irregularidades y Actos Ilegales |
| P8 Evaluación de la Seguridad — Prueba de Penetración y Análisis de Vulnerabilidades, |
| P9 Evaluación de los Controles de la Dirección sobre las Metodologías de Encripción, |
| P10 Control de Cambios de Aplicación del Negocio |

Cabe hacer mención que aunque no son de carácter obligatorio se recomiendan a fin de asegurar que en todo momento se están siguiendo los estándares.

## 2.4 Tipos de auditorías de S.I.

Existen varios tipos de auditorías cuya aplicación puede ser de dos maneras, ya sea interna o externa por lo que el auditor debe conocer los procedimientos asociados con cada tipo según sea el caso. Se define de la siguiente manera algunos ejemplos:

### 2.4.1 Auditorías financieras.

El objetivo de una auditoría financiera es revisar y determinar la exactitud de los estados financieros, con la finalidad de establecer su razonabilidad, dando a conocer los resultados de su examen. La auditoría financiera se relaciona con la integridad y confiabilidad de la información financiera.

### 2.4.2 Auditorías operativas.

Una auditoría operativa evalúa los aspectos de la estructura del control interno en un proceso o área determinada. Mediante esta auditoría se pueden identificar las áreas que requieran mejorar los métodos operativos e incrementar su efectividad. Para este caso, como ejemplos tenemos las auditorías de S.I. de controles de aplicación o de sistemas de seguridad lógica.

### 2.4.3 Auditorías integradas.

Una auditoría integrada es un proceso que une los procedimientos de una auditoría financiera más los de una auditoria operativa. El integrar estos dos aspectos proporciona una herramienta para evaluar los objetivos generales dentro de una organización, relacionados con la información financiera y la salvaguarda de activos, la eficiencia y el cumplimiento.

### 2.4.4 Auditorías administrativas.

Las auditorias administrativas son una evaluación integral o parcial de una organización, con el propósito de identificar el nivel de desempeño mediante la medición de la eficiencia de la productividad operativa dentro de una organización.

### 2.4.5 Auditorías de S.I.

Este proceso se define como la recolección y evaluación de evidencia a fin de establecer si los sistemas de información y los recursos relacionados protegen debidamente los activos, conservan la integridad, disponibilidad de los datos y del sistema. Así mismo, este tipo de auditoría proporciona información relevante y confiable, sobre si se está alcanzando de manera efectiva las metas organizacionales. Proporciona datos sobre el uso de los recursos y la organización cuenta con controles internos que garanticen que los objetivos de negocio, operacionales y de control podrán alcanzarse: En este mismo sentido provee datos acerca de las medidas para prevenir,

detectar y en su caso corregir aquellos posibles eventos no deseados de forma eficaz y eficiente.

### 2.4.6 Auditorías especializadas.

Consiste en auditorias muy especializadas. Como ejemplo tenemos las auditorías basadas en SAS 70 (Statement on Auditing Standards No. 70) el cual es un estándar de auditoría reconocido internacionalmente enfocado a los controles internos y externos que posee una empresa que presta servicios. El reporte consiste en una revisión por parte de una firma auditora independiente certificada.

SAS 70 fue diseñado para proveer información a las organizaciones usuarias y a sus auditores acerca del control interno de la organización de sus servicios y verifica la existencia del control, su documentación, difusión y uso efectivo. Además, analiza su diseño y comprueba su efectividad operativa. Básicamente, es una comunicación "de auditor a auditor".

Este tipo de auditorías se enfoca para evaluar controles internos de una empresa cuando los servicios se realicen por terceros, esto dado las tendencias actuales de subcontratación. Para este caso, el fundamento es la declaración sobre Estándares de Auditoría (SAS) 70, “Informes sobre el Procesamiento de las Transacciones por Organizaciones de Servicio”, que define los estándares que son empleados para evaluar los controles internos de una organización de servicios. Existe una variante más profunda de SAS 70, la tipo 2 SAS 70.

SAS 70 brinda información mediante la cual el auditor puede reportar el estatus que guardan los controles de una organización y la evaluación que indica si son adecuados.

### 2.4.7 Auditorías forenses.

Como parte de las definiciones de una auditoria forense podemos encontrar varias que la refieran como el uso de técnicas de investigación criminalística, integradas con la contabilidad, conocimientos jurídico-procesales, y con habilidades en finanzas y de negocio, como información de carácter jurídico para ser usado como evidencia. Actualmente este tipo de auditoría es útil en investigaciones de cibercrimen. Este tipo de auditoría puede ser aplicado en dispositivos diversos, tales como computadoras personales, portátiles, smartphones, equipamiento de red, dispositivos tecnológicos, etc., que como parte importante de esta auditoría es la obtención completa de la imagen bit-stream del dispositivo y examinar esa imagen, sin alterar los sellos de fecha u otra información atribuible a los archivos examinados.

También se puede recurrir a herramientas para este tipo de auditoría, como el mapeo de datos para la evaluación de riesgos de privacidad y seguridad, y la búsqueda de propiedad intelectual. La Auditoría Forense es una ciencia que permite descubrir, divulgar información financiera, contable, legal, administrativa e impositiva, sobre fraudes y delitos perpetrados en el desarrollo de las funciones públicas y privadas.

La pérdida de los valores morales entre las personas ha ocasionado un aumento en la tramitología de las transacciones y acuerdos que se dan entre personas y sociedades. Antiguamente la tramitología era menor porque se creía en la palabra y la buena fe de las personas. Hoy en cambio, se facilita la corrupción debido las cláusulas excesivas en los contratos por el alto riesgo que se asume, dada la pérdida de confianza en las personas y en los negocios.

Los tiempos han cambiado. Hoy es necesario el ejercicio de la Auditoría Forense para esclarecer posibles fraudes o malos manejos. De ahí que exista la necesidad de preparar personas con visión integral, que faciliten evidenciar especialmente delitos como la corrupción administrativa, el fraude contable, el delito en los seguros, el lavado de dinero, entre otros.

Es importante mencionar que los casos de irregularidades, fraudes o delitos son detectados por denuncias de un empleado o servidor público, por lo que el examinador debe evaluar si la denuncia amerita iniciar una investigación. Cierto número de los casos se originan por venganza, por dinero, por envidia, retribuciones no obtenidas y en un menor caso por preocupaciones genuinas.

La proliferación de los escándalos financieros y fraudes en los últimos años ha hecho de la contabilidad forense una de las áreas de mayor crecimiento, lo que ha exigido la participación frecuente de los contadores en procesos de naturaleza jurídica y en la mayoría de veces en casos de delitos económicos. A causa de los colapsos corporativos y fallas de negocios, las compañías están contratando a auditores forenses para investigar varios tipos de errores, irregularidades y situaciones en las que ya se produjo un daño que tuvo consecuencias graves.

- **Causas de malas prácticas.**

  Las personas se prestan a malas prácticas debido a que presentan alguna o algunas de las siguientes situaciones:

  - Deseo de vivir más allá de sus posibilidades o medios económicos.
  - Deseo extremo de ganancias personales. Deudas personales altas. Relación cercana a los clientes. La compensación no guarda relación con sus responsabilidades.
  - Jugador compulsivo.
  - Presiones familiares o de compañeros de trabajo.

- **Las prácticas que incrementan el riesgo de fraudes en las organizaciones son:**

  - Alteración de documentos.
  - Encubrimiento de ingresos.
  - Endeudamientos ficticios.
  - Manipulación de contratos.
  - Apertura de cuentas de cheques sin autorización.

- Asignación de bienes en comodato.
- Manipulación de registros contables.
- Divulgación de información privilegiada y confidencial a terceros en los procesos de adquisiciones y de obra pública, como concursos, licitaciones públicas, etc.
- Adjudicación con intermediarios.
- Asignación de adquisiciones a parientes y amigos.
- Corrupción de funcionarios y empleados.
- Adjudicación de adquisiciones a sobre precio o en forma directa.

- **El Auditor Forense.**

  El médico legal o patólogo forense es un “Auditor Forense”, pero no es el único profesional que puede acreditarse este título, también lo puede ser el profesional de contaduría que analiza estados financieros fraudulentos, un ingeniero o un arquitecto que investiga las causas de un siniestro.

  La auditoría forense, investiga, analiza, interpreta, y, con base en ello testifica y persuade a jueces, jurados y a otros acerca de la información sobre la que pesa una presunción de delito.

  La sociedad espera de los auditores forenses mayores resultados que minimicen la impunidad, especialmente en estos momentos tan difíciles, en los cuales el crimen organizado utiliza medios más sofisticados para lavar dinero, financiar operaciones ilícitas y ocultar los resultados de sus diversos delitos.

- **Perfil del auditor forense.**

  Es recomendable que un auditor forense cubra el siguiente perfil:

  - Formación académica elevada.
  - Experiencia en auditoría e investigación.
  - Iniciativa y creatividad.
  - Trabajo en equipo.
  - Observador. Mente inquisitiva y abierta. Juicio profesional, maduro y audaz.

- Independencia de criterio.
- Lealtad.
- Análisis de la información en forma exhaustiva.
- Debe poseer un sentido común de los negocios.
- Dominar los elementos básicos del procesamiento electrónico de datos.
- Debe tener completa discreción, amplia experiencia y absoluta confianza.
- Debe contar con conocimientos en temas contables, de auditoría, criminología, de investigación y legales.

- **Diferencias entre el Auditor Financiero y el Auditor Forense.**

  El auditor forense se centra principalmente en excepciones, rarezas, irregularidades, patrones y conductas, mientras que los auditores financieros se centran en errores y omisiones.

  Es más fácil capacitar auditores financieros que auditores forenses, ya que en esta área es más difícil entrenar en la más básica habilidad – PENSAR – como auditores forenses.

- **Peritaje Forense.**

  Incluye la indagación de activos, situaciones de quiebra fraudulentas, análisis de reclamaciones de seguros y averiguaciones de conflictos de interés.

  Los elementos de juicio y evidencia contable constituyen la base fundamental de un peritaje contable, pues a través de su examen crítico y sistemático, el perito contable llegará a conclusiones que serán de ayuda, a quien lo solicite, en la compatibilización y evaluación de evidencias en torno a lo que investiga.

  En la medida que disponga de todos los elementos de juicio relacionados con el peritaje, su opinión tendrá la validez que el caso requiera.

- **La entrevista.**

  No es sino la plática de dos o más personas hacia un determinado tema o suceso.

Es necesario elaborar un plan para cumplir los objetivos propuestos, es escuchar del entrevistado lo que realmente nos interesa.

El auditor forense se puede encontrar con tres tipos de entrevistados: el neutral, que no tiene nada que ganar o perder, el cooperador, dispuesto a ser entrevistado, motivado por variedad de razones, y el hostil, que dice medias verdades por temor a ser descubierto como el autor del fraude.

Las entrevistas deberán comenzar de una manera lógica, comenzando con la persona que cuenta con la menor probabilidad de haber estado involucrado, hacia la persona con mayor probabilidad, neutrales, corroborativos, cooperadores, co-conspiradores, aquellos que se sospecha de haber participado, y los acusados.

Es importante que el entrevistador cuide el enfoque que debe tener el interrogatorio, se recomienda que tenga en mente el orden de las consultas. Deje que el entrevistado hable y mienta y luego lo confronte con la evidencia que se tenga, para hacerlo cambiar de actitud y preste su colaboración.

Para una mejor obtención de información el entrevistador debe ser honesto e íntegro, tener la capacidad de escuchar, mantener el autocontrol, no prejuzgar al entrevistado, no tratar de impresionar, no sea sarcástico, no se enoje, controle sus emociones, sea justo, no haga falsas promesas, no grite, debe ser serio, no rígido y paciente. Las preguntas deben ser claras, concisas, directas, lenguaje simple, etc.

- **Examen de documentos.**

  Para la examinación de los documentos, primero se recaban los documentos originales, se hace la revisión con copias, tratando de tocar lo menos posible los originales, manteniendo un buen sistema de archivo y estableciendo un registro de control y custodia de los documentos.

En conclusión, la responsabilidad por la prevención y detección de fraude y error descansa en la administración por medio de la implementación de sistemas de contabilidad y de control interno adecuados. Los cambios en

las Organizaciones, Dependencias o Entidades de Gobierno deben generar modificaciones o cambios en los Sistemas de Control, ya que los riesgos se incrementan.

La auditoría forense requiere por lo tanto de toda la habilidad técnica, el sano razonamiento, la energía, el valor, la independencia, la imaginación, aspectos éticos y la integridad, que son sellos distintivos.

## Capítulo 3

# Protección y Continuidad de Activos en los Sistemas de Información, Auditoria de un Caso Práctico “Informe de Auditoría”.

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 T.I.

La necesidad del aseguramiento del valor de T.I., la administración de los riesgos asociados, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del Gobierno Corporativo. El valor, el riesgo y el control constituyen la esencia del gobierno de T.I.

El gobierno de T.I. es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que T.I. en la empresa sostiene y extiende las estrategias y objetivos organizacionales. Más aún, el gobierno de T.I. integra e institucionaliza las buenas prácticas para garantizar que T.I. en la empresa soporta los objetivos del negocio. De esta manera, 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 Integrado y de Control Interno, para ello nos basamos en COSO (en inglés Committee Of Sponsoring Organisations Of The Treadway Commission) para controlar la T.I., que se ajuste y sirva como soporte. Este marco de referencia de control es ampliamente aceptado para gobierno corporativo y para la administración de riesgos, así como a marcos compatibles similares.

Las organizaciones deben satisfacer la calidad, los requerimientos y de seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de T.I., 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 T.I. y decidir qué tipo de gobierno y de control debe aplicar.

### 3.1 Protección de activos de la información.

La Asociación de Auditoría y Control de Sistemas de Información, señala dentro del rubro de protección de activos como trascendental la gestión de la seguridad. Esto considerando la convergencia de medios para el intercambio de la información y los potenciales peligros y riesgos que derivan de esta actividad, como lo son la no certeza de la confidencialidad e integridad de la información, ataques con virus, ataques informáticos como denegación de servicios, robo de información personal y accesos no autorizados, sabotaje, afectaciones operativas, entre otros. Por lo cual se debe tomar como fundamento para la gestión de la seguridad la norma ISO 17799, definido por ISACA como la unión de controles que garantizan las mejores prácticas relativas a esta administración. Así mismo, tenemos como referencia de COBIT el denominado “Control Objectives for Information and Related Technology (COBIT 5.0)” con objeto de proteger de forma adecuada la información de una organización. Figura 3.1




**Figura 3.1 Protección de datos.**

En COBIT 5.0 encontramos definidos cuatro dominios, con 220 controles clasificados bajo 34 objetivos de alto nivel. Figura 3.2

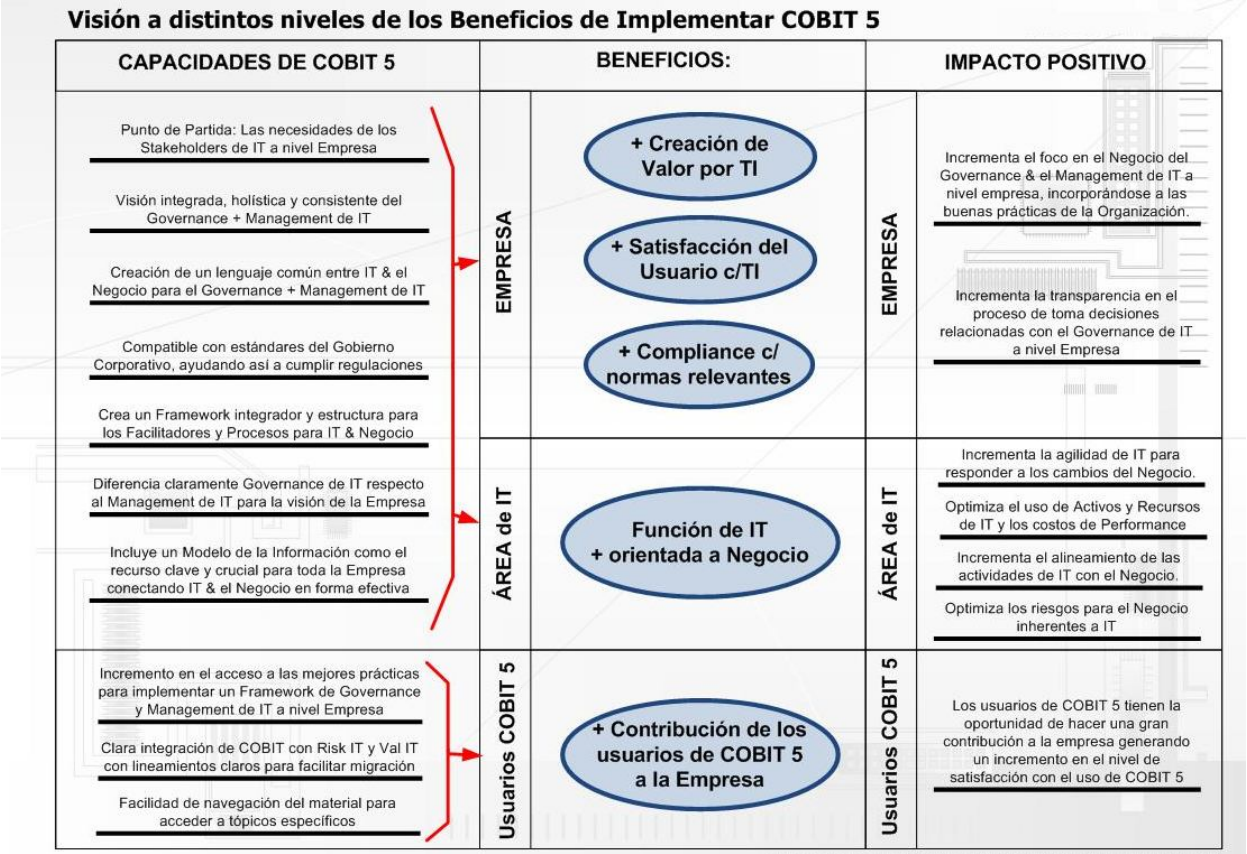


**Figura 3.2 COBIT 5**

La norma ISO 17799, también conocida como ISO 27002, tiene como antecedente el estándar “British Standard BS 7799-1”, mismo que fue publicado primeramente en el año de 1995. Actualmente la ISO 17799 tiene su última revisión en el año 2013. Ese estándar, para la seguridad de la información aplicable a cualquier empresa u organización, básicamente conceptualiza una organización como una totalidad bajo una estructura de diez dominios relacionados a aspectos de seguridad:

- Política de seguridad de la información
- Aspectos organizacionales de la Seguridad de la Información

- Clasificación y control de activos
- Seguridad del recurso humano
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Adquisición, Desarrollo y mantenimiento de sistemas de Información
- Gestión de continuidad del negocio
- Conformidad legal o cumplimiento

Antecedido por estas referencias normativas, la Asociación de Auditoría y Control de Sistemas de Información específica los objetivos que se deben asegurar para satisfacer los requerimientos de un negocio:

- Continúa disponibilidad de sus sistemas de información.
- Integridad de la información en sus sistemas informáticos (almacenada y en tránsito).
- Confidencialidad de los datos sensibles (almacenados y en tránsito).
- Cumplimiento de las leyes, regulaciones y estándares aplicables.
- Cumplimiento con la política de privacidad o leyes y regulaciones de privacidad aplicables.

Lo anterior debe traducirse en buenas prácticas a través de los recursos humanos de una organización, por medio de la definición de roles y responsabilidades para la Gestión de la Seguridad de la Información. En lo particular a este tema se define lo siguiente:

**Responsabilidades a considerar por categoría:**

- **Comité de seguridad de S.I**. Debe establecer y aprobar las políticas, directrices y procedimientos de seguridad de una organización: Así mismo, debe ser establecido formalmente con términos de referencia apropiados y

es conformado por gerencia ejecutiva, la administración de seguridad, el personal de S.I. y un asesor legal.

- **Gerencia ejecutiva/ Dirección General**. El responsable de la protección de los activos de información, y de emitir y mantener el marco de política.
- **Grupo asesor en seguridad:** Este grupo es el responsable de la revisión de los planes de seguridad de la organización, a fin de que estén en apego a los objetivos de la organización.
- **Director de privacidad (Chief Privacy Officer - CPO)**. Es un oficial corporativo responsable de hacer cumplir las políticas de las empresas u organizaciones para proteger los derechos de privacidad de los clientes y empleados.
- **Director de Seguridad de Información (Chief Information Security Officer - CISO)**.- Es un oficial corporativo de alto nivel responsable de hacer cumplir las políticas que las compañías utilizan para proteger sus activos de información. Este es un rol mucho más amplio que el de un Director de Seguridad (CSO), quien normalmente sólo es responsable de la seguridad física dentro de la organización.
- **Propietarios de procesos**. Los propietarios de procesos garantizan que las medidas de seguridad son adecuadas y ligadas con las políticas de la organización, y aseguran su actualización correspondiente.
- **Propietarios de los activos de información y propietarios de los datos**. La responsabilidad de los activos que resguardan.
- **Usuarios/Externos.** Cumplen con los procedimientos establecidos en la política de seguridad de la organización y acatan las regulaciones de privacidad y seguridad.
- **Administrador de seguridad**. Responsable de proveer seguridad física y lógica adecuada para los programas de SI, datos y equipos. Normalmente, la política de seguridad de información proveerá los lineamientos básicos bajo los que operará el administrador de seguridad.

- **Especialistas / asesores de seguridad**. Apoyar en el diseño, implementación, administración, gestión y revisión de las políticas, las normas y los procedimientos de seguridad de la organización.
- **Desarrolladores de T.I**. Implementan la seguridad de la información dentro de sus aplicaciones.
- **Auditores de S.I**. Proporcionan un aseguramiento independiente a la gerencia de T.I. sobre lo apropiado y efectivo de los objetivos y controles relacionados con dichos objetivos de seguridad.

### 3.2 Inventarios y clasificación de los activos de información.

Una vez que hemos señalado los roles y responsabilidades para una apropiada gestión de la seguridad de la información, no se debe perder de vista el control de los activos de la información. A través de un inventario detallado de los activos se logra una clasificación exacta y por ende estaremos en la posibilidad de determinar el nivel de protección para cada uno de estos. Figura 3.3


**Figura 3.3 Clasificación de activos de información**

En este rubro se definen campos específicos que deberá contener dicho inventario, entre los cuales están los siguientes:

- Identificación única del activo.
- Ubicación.

- Clasificación de seguridad.
- Grupo de activos (en caso de ser un elemento de un S.I. más grande).
- Propietario.
- Custodio designado.

Con esta información podremos asignar una clasificación en relación al grado de sensibilidad de cada activo, lo que se refleja en niveles de control de acceso, como anteriormente se mencionaba.

Para determinar cuál es el grado de sensibilidad de cada activo de información, se debe considerar lo que menciona la norma ISO 17799, en lo relativo a la responsabilidad por los activos, donde señala que se debe lograr mantener la protección adecuada de los activos de la organización, por lo que todos los activos se deben incluir y tener un dueño designado. Así mismo, marca que se debe identificar los dueños para todos los activos y asignar la responsabilidad para el mantenimiento de los controles adecuados.

En lo particular en el punto sobre la clasificación de la información, señala que se debe asegurar que la información recibe el nivel de protección adecuado. Así mismo, establece que la información se debe clasificar para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información. Estas son referencias para definir un esquema de clasificación de la información y con ello establecer los niveles de protección y lograr lo que ISACA menciona sobre reducir el riesgo y el costo de sobreproteger o subproteger los recursos de información, al vincular la seguridad con los objetivos del negocio.

En términos prácticos, la clasificación también debe permitir tener claramente la respuesta de las siguientes cuestiones:

- ¿Quién es el dueño del activo de la información?
- ¿Quién tiene permiso de acceso y cuáles son sus privilegios?
- ¿Nivel de acceso a ser otorgado?

- ¿Quién es el responsable de determinar los permisos y los niveles de acceso?
- ¿Qué aprobaciones son requeridas para obtener acceso?
- El grado y profundidad de los controles de seguridad

### 3.3 Permisos de acceso al sistema

Otro de los principales puntos dentro del tema de protección de activos es el relativo al permiso de acceso a un sistema, que en la práctica ha demostrado ser de un alto valor para los administradores de T.I. ya que solo el personal indicado debe acceder a la información y sistemas definidos. En este sentido se define como el privilegio técnico para poder hacer algo con un recurso computarizado o informático, esto se traduce desde la posibilidad para un usuario de acceder a un archivo electrónico hasta leerlo, modificarlo o incluso crear nuevos archivos, entre otras funciones. Figura 3.4.


**Figura 3.4 Seguridad lógica**

ISACA define cuatro grupos sobre la seguridad de activos:

- Redes
- Sistemas operativos
- Bases de datos
- Aplicaciones

Esto permite al propietario de la información, establecer de forma precisa el alcance que debe contener el control de acceso para que sea aplicado de forma adecuada. En este caso, para un auditor de S.I. debe evaluar esta aplicación fundamentándose en los principios de necesidad de saber el menor privilegio y segregación de funciones. El auditor debe tener presente que estas medidas deben ser actualizadas constantemente con base en la situación actual de una empresa u organización.

El acceso no autorizado de información puede tener un alto impacto para una empresa u organización, tales como el robo o pérdida de información financiera, operativa, secreta, entre otros, incluso generar problemas legales para la organización, por lo que se debe considerar dentro de las medidas de seguridad lógica desde la instalación de equipos, como firewalls hasta un programa de sensibilización y entrenamiento para todo el personal, con el fin de englobar al soporte lógico –software-, el soporte físico –Hardware-, el entorno sobre el que se labora el personal y en donde se encuentran físicamente el hardware de un sistema y el elemento humano, el más importante de todos.

### 3.4 Identificación y administración de riesgos.

La identificación de los riesgos para la información y las instalaciones de procesamiento de información es una actividad sumamente relevante en cuestión de seguridad de la información, ya que será la base de una adecuada aplicación de prácticas para la administración de cada uno, teniendo en consideración las diversas implicaciones potenciales en un sistema vulnerable dentro de una organización, desde el punto de vista  informático, hasta sus diversos efectos legales.

Existen diversos modelos de gestión de riesgos, nos basaremos en la propuesta de ISACA denominada Risk I.T. Figura 3.5. Principios de Risk IT

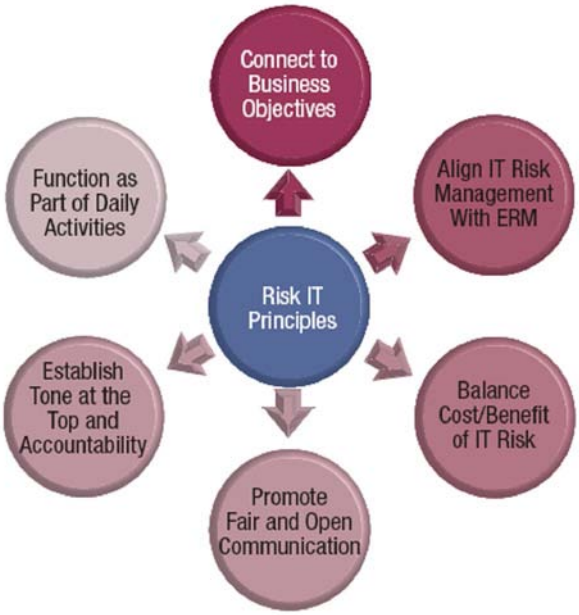


**Figura 3.5 Principios de Risk IT**

Debido a que se focaliza en el cumplimento de los objetivos de una organización y se fundamenta en conceptos de valor y beneficios que la organización obtiene a través de las tecnologías de la información T.I.

Una de las principales características de este modelo que lo convierten en una herramienta útil para una organización son sus principios de mantener siempre su conexión con los objetivos de la organización, la alineación de riesgos relacionados con la gestión de T.I. con los riesgos de toda la organización, un balance de costos y beneficios en la gestión de riesgos y promover una comunicación abierta de los riesgos de T.I., por lo que se consideró incluir en este documento como fundamento de buenas prácticas para la gestión de riesgos.

Como punto de referencia usaremos las definiciones de riesgo y amenaza, en donde se señala lo siguiente:

- **Riesgo.** El potencial de que una amenaza determinada explote las vulnerabilidades de un activo o de un grupo de activos y que ocasione su

pérdida o daños a los mismos. Usualmente se mide la combinación de impacto y la probabilidad de que ocurra.

- **Amenaza**. Es la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización". *Referencia: norma ISO/IEC 13335-1:2004*.

Para el análisis de los riesgos se debe contar con una identificación de activos, como se mencionó anteriormente, contar un inventario de los activos (hardware, software, instalaciones y sus respectivos dueños), para posteriormente poder evaluar las amenazas, según su tipo, causas y la probabilidad de ocurrencia. Como resultado de esto tendremos un listado de activos, amenazas y la probabilidad de que ocurran. Figura 3.6.


**Figura 3.6 Escenarios de riesgo**

Con base en lo anterior, se debe definir una matriz de riesgos con dos ejes: la posibilidad de ocurrencia y el impacto, en donde el impacto es siempre más importante que la posibilidad de ocurrencia, esto para la definición de prioridades.

Con dicha matriz establecida se debe implementar un esquema de tratamiento de los riesgos, tratando de crear un balance entre el nivel de seguridad y su costo, así mismo establecer los niveles de riesgo y de protección de activos desde la alta dirección, mientras se define y refuerza la responsabilidad del personal interno y de terceros para operar en niveles de tolerancia aceptables. Figura 3.7.

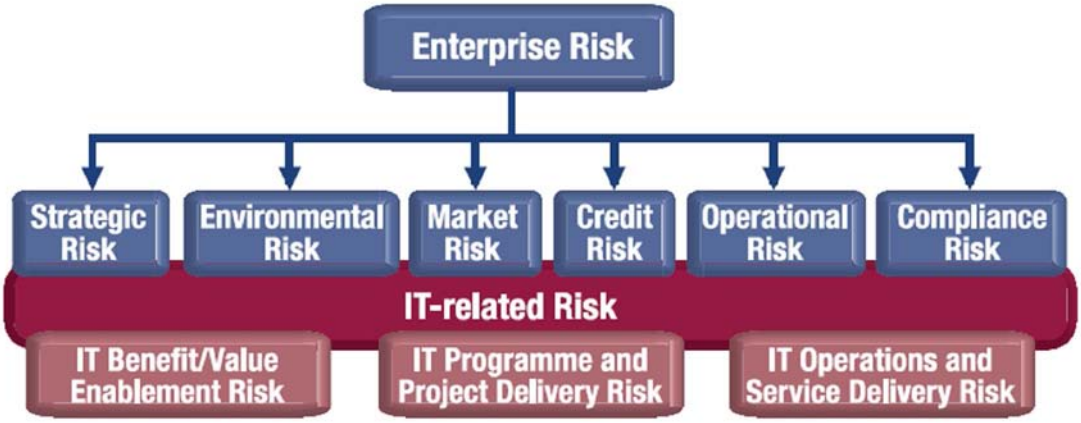


**Figura 3.7 Jerarquía de riesgos**

### 3.5 Continuidad de negocio y recuperación de desastres.

La metodología de planes logísticos enfocado a la recuperación de funciones y procesos críticos después de una posible interrupción no esperada en una organización es el denominado BCP, de sus siglas en ingles Business Continuity Planning o Planeación de continuidad del negocio, Figura 3.8.


**Figura 3.8 BCP, de sus siglas en ingles Business Continuity Planning o Planeación de continuidad del negocio**

Para esta recuperación y continuidad se debe incluir todos los elementos relacionados a dichas funciones como recursos humanos y recursos materiales, a fin de que se garantice la supervivencia de la organización, logrando que se continúe proveyendo los servicios a sus clientes.

Para la implementación del BCP en una organización primero debemos identificar los procesos de negocio de importancia estratégica. En otras palabras aquellos procesos que permitan cumplir los objetivos de la organización en sus diversas líneas de negocio y posteriormente se deberá realizar una evaluación de riesgos. En este punto en particular se define lo siguiente “El riesgo es directamente proporcional al valor de los activos y a la probabilidad de que ocurra la amenaza percibida”, por lo que basándonos en esto la evaluación del riesgo debe indicarnos los siguientes elementos; primero cuales son los recursos humanos y materiales necesarios para llevar a cabo los procesos de importancia estratégica. Como segundo, la identificación de las posibles vulnerabilidades, amenazas y peligros para la organización. Tercero, una relación de posible ocurrencia de cada amenaza. Así mismo se debe incluir en lo relativo a la parte de operaciones, a fin de tener la certeza de continuar brindando los servicios de forma viable.

Esta planeación y la responsabilidad de implementar el BCP es competencia de la alta gerencia con el fin de asegurar los activos clave y de igual manera garantizar la funcionalidad, incluso a nivel mínimo de las operaciones posterior a la ocurrencia de una interrupción y de esta forma minimizar los efectos de dicha interrupción.

Como parte de la planeación para la continuidad del negocio, se debe tener lo siguiente:

- Identificación de aquellas operaciones clave o críticas imprescindibles para la viabilidad de supervivencia de una organización.
- Identificación de todos los recursos humanos y materiales que soportan las operaciones clave.

- Dentro del plan de continuidad del negocio, considerar contar con un plan:
  - Para continuidad de las operaciones.
  - De recuperación de desastres.
  - De restauración.

Cabe hacer mención que con el análisis de riesgos y su debida gestión nos permitirá tener una herramienta para mejorar la seguridad y nos proporcionará una mejor preparación ante las posibles eventualidades que se presenten en un sistema, incluso durante las operaciones normales. Lo anterior a fin de dar cumplimiento de las metas del negocio mediante diversas medidas. Como se puede notar, el Business Continuity Planning es la integración de la planificación de recuperación de desastres con las operaciones del negocio, esto adecuado a las necesidades particulares de cada organización.

ISACA define ciclos de vida para el proceso de BCP, que son los siguientes:

- Creación de una política de continuidad del negocio.
- Análisis del impacto al negocio.
- Clasificación de las operaciones y análisis de criticidad.
- Identificación de los procesos de S.I. que soportan funciones organizacionales críticas.
- Desarrollo de un plan de continuidad del negocio y procedimientos de recuperación de desastre de S.I.
- Desarrollo de procedimientos de reanudación.
- Programa de entrenamiento y de toma de conciencia.
- Prueba e implementación del plan.
- Monitoreo.

Así mismo, un punto importante dentro del BCP es la administración de incidentes. Pero antes de hablar de su administración, se definirá el concepto de incidente:

- **Incidente.** Es cualquier evento no esperado, incluso si éste no causara daños significativos”

Con base en lo anterior debemos considerar que dicha administración debe ser constantemente actualizada, debido a la naturaleza de los incidentes y así mismo estar debidamente documentada.

En este mismo sentido, a fin de tener un control sobre la administración de incidentes debemos clasificarlos con base en el posible impacto de daños para una organización en:

- **Incidentes sin importancia.** Son los que no causan daños perceptibles o significativos, como por ejemplo, caídas del sistema operativo (OS) muy breves con recuperación total de la información o cortes de energía momentáneos con respaldo de suministro de energía ininterrumpible.
- **Eventos menores.** Son los que, aunque no insignificantes, no producen un impacto material (de relativa importancia) o financiero negativo.
- **Los incidentes mayores.** Causan un impactó material negativo sobre los procesos de negocios y pueden afectar otros sistemas, departamentos o incluso clientes externos.
- **La crisis.** Es un incidente mayor que puede tener un impacto material, de relativa importancia, pero serio sobre el funcionamiento continuo del negocio y que puede también tener un impacto adverso sobre otros sistemas o terceros. La seriedad de ellos depende de la industria y de las circunstancias, pero la severidad es por lo general directamente proporcional al tiempo transcurrido desde el inicio del incidente hasta su resolución”.

### 3.6 Recuperación en sistemas de información.

La aplicación del BCP en un sistema de información básicamente es en el mismo sentido de lo anteriormente expuesto, solo que en este caso en particular la amenaza se focaliza sobre los sistemas de procesamiento de un sistema de

información, debido a que claramente es un elemento crítico para los procesos de T.I. en una organización. Esto se traduce que todo el software, hardware, el personal y las instalaciones deben estar preparados para su posible aplicación por causa de una interrupción no esperada, incluso la organización debe contar con instalaciones de respaldo, nunca olvidando que el negocio no debe interrumpir el procesamiento continuo de información y que esto incluye realizar todas las tareas criticas considerando a los empleados, su lugar de trabajo durante el desastre, la ubicación y utilización del equipo, la comunicación entre empleados, terceros y proveedores, etc.

El plan de continuidad del negocio debe fundamentarse en la estrategia de la organización, esto permitirá una adecuada clasificación de criticidad de los diversos sistemas de aplicación con base al valor que estos representan para una organización. Los planes de recuperación de desastre pueden estar incluidos en el plan de continuidad del negocio o como un documento completamente separado, dependiendo de las necesidades del negocio.

Un aspecto importante para el desarrollo del plan de continuidad es el análisis del impacto al negocio (BIA en inglés Business Impact Analisis). Para poder llevar a cabo este análisis debemos tener claramente definido los procesos críticos de la organización y, como se mencionó anteriormente, de los recursos necesarios para soportarlos.

Dentro de los diversos métodos para realizar el análisis del impacto sobre el negocio (BIA) el método de cuestionario, este se conforma de preguntas dirigidas desde personal de T.I., hasta los usuarios finales. Con la información obtenida se realiza una matriz que servirá para realizar el análisis detallado, en este mismo análisis ISACA recomienda a los auditores examinar el volumen de transacciones pasadas. Con esto se puede establecer cuál es el posible impacto en el supuesto que el sistema quedara no disponible por tiempo prolongado.

A continuación se enlistan las principales preguntas que ISACA considera durante la evaluación de BIA:

1) ¿Cuáles son los diferentes procesos de negocio?
2) ¿Cuáles son los recursos de información crítica relacionados con los procesos críticos de negocio de la organización?
3) ¿Cuál es el período crítico de tiempo de recuperación para los recursos de información en el cual se debe restablecer el procesamiento del negocio antes de que se experimenten pérdidas significativas o inaceptables?

## 3.7 Caso práctico.

## Reporte de Auditoría sobre el Sistema de Información en el Sistema de Transporte Colectivo.

### 3.7.1 Situación actual.

El Sistema de Transporte Colectivo (STC) “Metro” no cuenta hoy en día con una plataforma operativa que le permita realizar actividades de seguridad para las aplicaciones productivas y en desarrollo. Debido a esto, los sistemas están expuestos y pueden ser atacados por fines económicos, robo de información, saboteo de las operaciones del negocio, daño en el prestigio del negocio, revanchismo o simplemente por curiosidad, entre otras muchas causas. En cualquier caso, el riesgo e impacto son altos para el STC. La divulgación o pérdida de información sensitiva, el fraude, paro de las operaciones, y las pérdidas en imagen por el impacto publicitario que genere el ataque, representan altos costos de imagen, legales y económicos, además de generar que los tiempos de respuesta y solución a incidentes relacionados con la seguridad de las aplicaciones sea significativo, tal como se detalla más adelante.

Esta aseveración y diagnóstico se basa en que el STC no contó desde su origen con un plan de sistemas que le permitiera atender de manera organizada y con capacidades de procesamiento y almacenamiento, el desarrollo y liberación de los

sistemas a producción. Desde el inicio se adquirieron los primeros servidores del tipo torre 486, Pentium, después otros más robustos del tipo Compaq Proliant, HP, Dell con sistemas operativos Unix SCO, Windows Server, Linux, SMBD Informix, Oracle y diversos lenguajes de programación y desarrollo, todo en ambientes stand alone y cliente servidor. Al ir transcurriendo el tiempo, se fueron "parchando" versiones y ajustando los sistemas y aplicaciones a los nuevos ambientes de programación y desarrollo, sin que existiera una norma y metodología para el análisis, diseño, desarrollo y liberación de los sistemas de información. Se carece de documentación y el soporte técnico se realiza por el expertiz del trabajador, en cuyo caso si el sistema falla y no está el programador original, el sistema o aplicación se vuelve a hacer.

Aunado a lo anterior, no se cuenta con políticas tales como: organización de la seguridad, clasificación y control de los datos, seguridad física, ambiental y de las personas, plan de contingencia, prevención y detección de virus y administración de las computadoras.

Como ejemplo se tienen las veces en que el sistema deja de funcionar aparentemente sin motivo alguno, y es necesario el reinicio de servidores para el restablecimiento de los servicios, tardando hasta horas en restablecerlos, poniendo en riesgo la operación de los sistemas que atienden entre otras cosas las transacciones financieras.

Las áreas que existieron y existen actualmente solo se dedican a programar y dar soporte técnico a computadoras; el área de mantenimiento evolutivo a redes y sistemas no existe. La seguridad informática física y lógica es nula y se tiene un enorme grado de vulnerabilidad a todo (redes, sistemas, bases de datos. aplicaciones etc.). La seguridad informática es de vital importancia para esta administración por lo que se recomienda efectuar un análisis de factores de riesgo, para evitar que ante cualquier contingencia no se cuente con las herramientas y conocimientos correctos.

En las tablas 3.1, 3.2 y 3.3 que a continuación se muestran, se enumera los aspectos técnicos:

**Tabla 3.1 Características técnicas de los servidores y sistemas**

| Servidor | Descripción | Ubicación | Sw Instalado |
|---|---|---|---|
| **Servidor marca Compaq, modelo Proliant ML-570.** | Contiene las bases de datos de los sistemas de SIRM, Contabilidad, Presupuesto. | Centro de Cómputo. | UNÍX SCO OPENSERVER 5.05. INFORMIX IDS 7.30. INFORMIX 4GL. |
| **Servidor marca Compaq, modelo Proliant ML-570.** | Utilizado para los desarrollos y pruebas. | Centro de Cómputo. | UNÍX SCO OPENSERVER 5.05. INFORMIX IDS 7.30. INFORMIX 4GL. |
| **Dell.** | Pruebas | Centro de Cómputo. | Linux Dist. CENTOS v. 6 |
| **Hp (.41) Proliant ML 370.** | Contiene información consolidada de las transacciones de tarjetas de cortesía y venta. Contiene los procesos de consolidación de datos en los registros que vienen en los archivos de actividad y que son insertados en la base de datos. Contiene el inventario del equipamiento de la red. | Centro de Cómputo. | Windows Server 2003 Standard Ed. Oracle v.10g Aplicaciones de Tarjeta Inteligente |
| **HP (.48) Proliant ML370 G5.** | Contiene información detallada de las transacciones de las tarjetas de cortesía y venta. Esta información se almacena un lapso de 100 días. | Centro de Cómputo. | Windows Server 2003 Standard Ed. Oracle v.10g,Aplicaciones de Tarjeta Inteligente |
| **HP (.47) Proliant ML370 G5.** | Contiene los clientes, contratos y tarjetas de la base de datos | Centro de Cómputo. | Windows Server 2003 Standard Ed. Oracle v.10g Aplicaciones de Tarjeta Inteligente |
| **HP (.36) Proliant ML110.** | Se encarga de la gestión de la comunicación de datos entre los servers (.41),(.48),(.47). | Centro de Cómputo. | Windows Server 2003 Standard Ed. Aplicaciones de Tarjeta Inteligente. |
| **Dell Power Edge R900** | Contiene la base de datos del SISEM | Centro de Cómputo. | LINUX MANDRIVA, MYSQL 2009.JAVA |
| **Dell Power Edge R900** | Contiene la base de datos del contabilidad, SIRM, presupuestos, recursos financieros | Centro de Cómputo. | Linux red hat Informix 11.5 |
| **Dell Power Edge R900** | Sin configurar. | Centro de Cómputo. | No Aplica |

**Tabla 3.2 Sistemas y aplicaciones**

| Inventario | Sistema operativo |
|---|---|
| Sistema de Contabilidad Financiera | UNIX SCO OPENSERVER 5.05 |
| Cuentas por pagar | UNIX SCO OPENSERVER 5.05 |
| Egresos | UNIX SCO OPENSERVER 5.05 |
| Sistema de Ingresos | UNIX SCO OPENSERVER 5.05 |
| Sistema de Ingresos por Caja | UNIX SCO OPENSERVER 5.05 |
| Sistema de Tarjeta Inteligente (CET) | WINDOWS 2003 SERVER |
| Sistema Integral de Recursos Materiales (SIRM) | UNIX SCO OPENSERVER 5.05 |
| Sistema de Presupuesto | UNIX SCO OPENSERVER 5.05 |
| Sistema de Conciliación Contable-Presupuestal de Egresos | UNIX SCO OPENSERVER 5.05 |
| Sistema de Inventarios de Bienes Muebles | Windows XP/Vista |
| Sistema de Rol de Taquilla | Windows XP/Vista |
| Sistema de Rol de Supervisoras | Windows XP/Vista |
| Sistema de Inventarios de Taquilla | Windows XP/Vista |
| Incidencias | Windows XP/Vista |

**Tabla 3.3 Matriz de equipos de comunicaciones**

| Dispositivo | Fabricante/Modelo | Tecnología | Ubicación |
|---|---|---|---|
| Switch | etxtreme networks/summit 48 | Switch capa3 | PCC II PISO 2 |
| Switch | etxtreme networks/summit 48 | Switch capa3 | ADMINISTRATIVO PISO 4 |
| Switch | etxtreme networks/summit 24 | Switch capa3 | ADMIISTRATIVO PISO 3 |
| Switch | etxtreme networks/summit 48 | Switch capa3 | ISABEL LA CATOLICA LADO SUR<br>PLANTA BAJA |
| Switch | etxtreme networks/summit 48 | Switch capa3 | JUAREZ PONIENTE PISO 3 |
| Switch | etxtreme networks/summit 24 | Switch capa3 | JUAREZ ORIENTE PISO 1 |
| Switch | etxtreme networks/summit 24 | Switch capa3 | PCC II PLANTA BAJA |
| Switch | etxtreme networks/summit 48 | Switch capa3 | PCC I PISO 6 |
| Switch | etxtreme networks/summit 48 | Switch capa3 | CHABACANO LOCAL TELECOM |
| Switch | etxtreme networks/summit 24 | Switch capa3 | CASONA PLANTA ALTA (VIGILANCIA) |
| Switch | etxtreme networks/summit 48 | Switch capa3 | ADMINISTRATIVO PISO 2 |
| Switch | etxtreme networks/Alpine 3804 | Switch capa3 | ADMINISTRATIVO PISO 1 |
| Switch | etxtreme networks/summit 24 | Switch capa3 | SALTO DEL AGUA PISO1 |

Históricamente se han registrado “caídas” en:

- Sistemas y aplicaciones, por ejemplo: nómina, contabilidad, facturación.
- Redes LAN.
- Internet.
- SITE.
- Hackeos a diversas aplicaciones, página web institucional, y redes sociales.

Los tiempos de respuesta para la atención a dichas caídas son demasiado lentos, la organización de atención de las áreas responsables está mal planeada. Por ejemplo, el área de comunicaciones y peaje se encarga del servicio de redes e internet, las oficinas se encuentran ubicadas en el sitio de Delicias y el personal de dicha área se encuentran en el sitio denominado metro Juárez. Si hay una caída del servicio de bases de datos (nómina, contabilidad, facturación) por falla eléctrica en fin de semana, no se tiene un procedimiento de recuperación y se tiene que esperar hasta el primer día hábil. Es común que el departamento de Energía “baje” el switch para mantenimiento sin avisar a ningún área, incluyendo el departamento de sistemas, solo por citar otro ejemplo. Lo mismo pasa para problemas de mantenimiento evolutivo a los sistemas en producción. En cada caída de la base de datos, es muy lento el proceso de recuperación por la falta de un sistema de respaldo adecuado. Los sistemas contemplados para la aplicación de las pruebas de vulnerabilidad se muestran en las tablas 3.4, 3.5, 3.6 y 3.7, de acuerdo al área (Gerencia) que pertenecen:

**Tabla 3.4 Gerencia de presupuesto.**

| No. | Sistema | Ambiente HW | Ambiente de SW | SMBD |
|---|---|---|---|---|
| 1 | Presupuestos | Cliente / Servidor | Unix | Informix |

**Gerencia de Presupuesto**

- Sistema de Presupuesto
  - Se encuentra en producción
  - Implementado en 2001
  - Linux CENTOS 6.0
  - INFORMIX 4GL
  - Se controla en dos servidores:
    - SERVIDOR DELL (Linux)
    - COMPAQ PROLIANT (Unix)
  - No requiere antivirus
  - Usuarios: Coordinación de Integración Presupuestal y Coordinación de Registro y Control Presupuestal.

La Gerencia de Presupuesto dentro de su estructura cuenta con 3 coordinaciones y son:

- Integración Presupuestal
- Registro y Control Presupuestal
- Programación

El Sistema de Presupuesto va dirigido hacia las dos primeras coordinaciones arriba mencionadas, por requerimientos de la misma Gerencia.

- **Integración Presupuestal.** Su función es integrar las partidas presupuestales, sus montos correspondientes y la asignación a las áreas del organismo en sus programas convenientes.
- **Registro y Control Presupuestal.** Es el registro de los documentos de compromisos ejercidos en sus partidas correspondientes.

  Con base a las actividades que desarrollan dichas Coordinaciones de Presupuesto, se conformó el Sistema de Presupuesto en ocho módulos:

  - Catálogo.
  - Integración Presupuestal.
  - Registro y Control.

- Información General.
- Nómina.
- Ingresos.
- Utilerías.
- Salida.

- **Catálogos.** Involucra los códigos y conceptos requeridos:
  - Partidas códigos de gasto.
  - Ramos o áreas en el organismo.
  - Equivalencias con una correspondencia de códigos internos del STC con los códigos del G.D.F. a los que llama acciones adicionales.
  - Proveedores códigos para identificar a las personas físicas o morales que tienen alguna relación mercantil o de servicio con el STC.
  - Monedas códigos de divisas usadas en los convenios mercantiles.
  - Autorización códigos para los permisos en transferencias de asignaciones.
  - Conceptos contra Partidas, son las equivalencias de códigos de nómina con presupuesto.
  - Salir.

- **Apertura de código Presupuestal.** Se generan las claves presupuestales con la concatenación de función + ramo + partida + subpartida por fuente de financiamiento y dejando un registro con asignación cero. Validando cada uno de los campos en sus respectivos catálogos según corresponda.

- **Transferencias Internas.** Se hacen transferencias de recursos o asignaciones de una clave origen a un destino, llamadas reducción y ampliación, respectivamente, para llevar a cabo los movimientos de asignación de recursos.
  - **Ampliaciones / Reducciones.** Se hacen transferencias de recursos o asignaciones a una clave presupuestal en forma directa sin compensarlo. Está sujeto a la autorización de la Secretaria de Finanzas.
  - **Captura de compromiso y ejercicio para pedidos (nacionales e importación), para contratos (obras y servicios).** Se capturan los datos de los documentos haciendo las afectaciones en la clave presupuestal y fuente de financiamiento al cual se clasificó el movimiento.
  - **Pagos directos.** Se capturan los datos de los documentos de cuenta por pagar y se lleva a cabo las afectaciones en la clave presupuestal y fuente de financiamiento al cual se clasificó el movimiento.
  - **Cargos directos.** Se capturan los datos de los documentos de transferencias bancarias o compensación de adeudos, haciendo las afectaciones en la clave presupuestal y fuente de financiamiento al cual se clasificó el movimiento.
  - **Registro de Cuenta por Liquidar Certificada CLC.** Se capturan el número de identificación CLC proporcionado por Recursos Financieros y afectan a aquellos movimientos, según datos de aplicación, que tengan fuente de aportaciones para pedidos, contratos, pagos directos y cargos directos.
  - **Consultas y reportes de producción por fuente de financiamiento y condensada.**
    - **Códigos.** En los formatos de calendario, anuales, acumuladas de enero al mes de ejercicio y mensual.
    - **Rubros.** En los formatos de acumuladas de enero al mes de ejercicio y mensual con la característica de lista.
    - **Afectación.** Se muestra la clave presupuestal y su fuente de financiamiento, así como los movimientos de compromiso ejercido que soportan a las cifras de la clave presupuestal.

- **Estructura interna.** Es la estructura programática en el STC haciendo las agrupaciones jerárquicas (programa, subprograma, proyecto, capitulo, concepto, partida y subpartida).
- **Códigos registrados.** Es la impresión de las claves presupuestales e importes en sus rubros, incluyen la función, ramo, partida y subpartida de uso interno.
- **Códigos G.D.F.** Son claves utilizados en el Gobierno del Distrito Federal, conocidos como Acciones Adicionales, haciendo las agrupaciones jerárquicas (programa, subprograma, acciones adicionales, capitulo, concepto, partida y subpartida).
- **Cuentas de ejercicio.** De todas las cuentas de ejercido en formato ordenado, estructura interna y CLC. En el caso de aportaciones con o sin identificación de las Cuentas por Liquidar Certificadas.
- **Global.** Es un reporte por capítulos, partidas y subpartidas que el área usuaria denomina GLOBAL. Este reporte se entrega a las áreas del organismo después de los cierres de cada mes.
- **Ramos.** Es un reporte por ramos, capítulos, partidas y subpartidas que el área usuaria denomina RAMOS. Este reporte se entrega a las áreas del organismo después de los cierres de cada mes.

- **Nómina, con las calificaciones e integraciones.** Se reciben los movimientos de Recursos Humanos, a través de correo electrónico, que afectarán presupuestalmente; para obtener las partidas y áreas se realizan las equivalencias.
- **Utilería** Serán opciones para el monitoreo de la integridad de la base de datos, de sus tablas y de datos capturados.

**Tabla 3.5 Gerencia de contabilidad**

| No. | Sistema | Ambiente HW | Ambiente de SW | SMBD |
|---|---|---|---|---|
| **2** | Presupuestos | Cliente / Servidor | Unix | Informix |

**Gerencia de Contabilidad**

- Sistema de Contabilidad Financiera
  - Se encuentra en producción
  - Implementado en 1999
  - Linux CENTOS 6.0
  - INFORMIX 4GL
  - Se controla en dos servidores:
    - ✓ SERVIDOR DELL (Linux):
    - ✓ Dell Power Edge R710, Procesador: Intel Xeon – 8 núcleos, RAM: 32 GB, Disco Duro: 640 GB
    - ✓ COMPAQ PROLIANT (Unix) Procesador: 700 – 2 núcleos, RAM: 1 GB, Disco Duro: 3 de 30 GB
  - No requiere antivirus
  - Usuarios: Coordinación de Registro

El paquete de Contabilidad Financiera ayuda al contador en la obtención de los reportes, controlando los registros de todas las transacciones para que estén completos y correctos. El paquete está enfocado a generar los Estados Financieros, en especial el Balance General y el Estado de Resultados.

La acción de transferir transacciones al Diario Mayor es conocida como Asentar o Actualizar. Cada transacción registrada en el Diario afecta dos ó más cuentas, de manera que en cualquier momento el Balance General debe estar cuadrado.

En un sistema de Contabilidad computarizado, los registros no se hacen en libros, sino en archivos de transacciones. Los datos pueden ser transferidos (asentados) por la computadora al archivo de transacciones del mayor, lo que equivale a registrar diariamente las transacciones en un sistema manual.

- **Descripcion del sistema.** El Sistema de Contabilidad cuenta con los módulos de Actualización, Procesos, Menusec y Procesos Diarios.
- **Actualización.** Realiza Altas, Bajas, Cambios y Reportes de Pólizas Generales, Cuentas, Autorizaciones, Tipos, Origen, Área de Ingeniería Origen, Claves, Monedas y Cuenta Monedas, Claves Conciliación.
- **Procesos.** Se generarán reportes del diario, impresión de Pólizas seguidas o separadas, las Balanzas de Comprobación de 1er, 2do, 3er Nivel ó Libro mayor y Balanzas Consolidadas así como también Consultas de Cuentas.
- **Menusec.** Se generarán los reportes diversos de estados financieros, balances generales, generación de saldos, reportes a COCOE, transacciones, conciliaciones, reporte de analíticas, etc.
- **Procesos Diarios.** Será la generación de los cierres diarios y procesos que se requieran al día, como cálculo de saldos, generación de balance general, estado de resultados, balanzas, analíticas y costos.

**Sistema de Cuentas por Pagar**

El Sistema de cuentas por pagar es una herramienta que permite llevar el registro completo de las Cuentas por Pagar, desde su captura hasta la generación de Pólizas. El sistema cuenta con catálogos, la captura de contratos, contra-recibos, la generación de pólizas, entre otros aspectos.

- Objetivos:
  - Facilitar al usuario la captura de las Cuentas.
  - Llevar un control y registro de las cuentas evitando generar errores.
- Beneficios:
  - Cuenta con varios módulos y validaciones para no generar errores.
  - Cuenta con un Catálogo para un mayor control de la información.
  - Consta de un código de acceso para mayor control de los usuarios.

- **Sistema de Cuentas por Pagar:**
  - Se encuentra en producción
  - Implementado en 2011
  - Linux CENTOS 6.0
  - Visual Basic 6.0
  - Se controla en dos servidores:
    - Servidor marca Dell (con Sistema Operativo Linux).
    - Servidor Dell Power Edge R710, Procesador: Intel Xeon – 8 núcleos, RAM: 32 GB, Disco Duro: 640 GB.
  - Requiere antivirus sólo en máquina de cliente.
  - Usuarios: Coordinación de Trámite y Expedición de Pólizas.

**Tabla 3.6 Gerencia de Adquisiciones y Contratación de Servicios y Gerencia de Almacenes y Suministros**

| **No.** | Sistema | Ambiente HW | Ambiente de SW | SMBD |
|---|---|---|---|---|
| **3** | Presupuestos | Cliente / Servidor | Unix | Informix |

**Gerencia de Adquisiciones y Contratación de Servicios y Gerencia de Almacenes y Suministros**

- Sistema Informático de Recursos Materiales
  - ✓Se encuentra en producción
  - ✓Implementado en 1999
  - ✓Linux CENTOS 6.0
  - ✓INFORMIX IDS 11.05
  - ✓Aplicaciones con SCO-OPENSERVER 5.0.5
  - ✓Se controla en dos servidores:
  - ✓SERVIDOR DELL (Linux):
    Dell Power Edge R710, Procesador: Intel Xeon – 8 núcleos, RAM: 32 GB, Disco Duro: 640 GB
    COMPAQ PROLIANT (Unix) Procesador: 700 – 2 núcleos, RAM: 1 GB, Disco Duro: 3 de 30 GB
  - ✓No requiere antivirus
    Usuarios: Gerencia de Adquisiciones y Contratación de Servicios y Gerencia de Almacenes y Suministros

El Sistema de Transporte Colectivo contempla en su estructura orgánica a la Gerencia de Recursos Materiales, la cual se encarga de manera general del abastecimiento y control de los diferentes artículos y servicios que necesitan cada una de las áreas que conforman a la institución, para laborar y ofrecer un mejor

desempeño. Dada la complejidad de las operaciones del área mencionada y con el objetivo de apoyarlos a realizarlas más eficaz y eficientemente, se implantó el Sistema Informático de Recursos Materiales (SIRM). El SIRM pretende mejorar las funciones que se llevan a cabo en las distintas áreas de Recursos Materiales, así también, permite tener conectividad con otros sistemas informáticos de la institución, mediante la generación de archivos con información para fines específicos.

El SIRM fue diseñado para proporcionar asistencia a:

- Usuarios de cualquier área en la elaboración, actualización y demás operaciones relacionadas a Requisiciones.
- Usuarios del área de Almacenes
- Usuarios del área de Compras Nacionales y Compras al Extranjero.

Por lo anterior, el SIRM está integrado por tres módulos:

- Programa anual
- Almacenes
- Requisiciones

Particularmente en este Manual de Usuario nos enfocaremos al módulo de Programa Anual de Adquisiciones. Este módulo es usado anualmente por las áreas del organismo, las cuales capturan sus requerimientos programados para el año siguiente.

El objetivo fundamental de este manual es que sirva como guía de referencia en las operaciones concernientes a la captura y actualización de requisiciones, así como la generación de reportes y consultas varias entre otras funciones que realiza dicho modulo.

**Tabla 3.7 Gerencia de Salud**

| No. | Sistema | Ambiente HW | Ambiente de SW | SMBD |
|---|---|---|---|---|
| **4** | Servicios médicos | Web | Linux/Windows | Oracle |

**Gerencia de Salud**

- Sistema de Servicio Médico
  - ✓ Se encuentra en producción
  - ✓ Implementado en 2009
  - ✓ JAVA Versión JDK 6u34
  - ✓ Linux Mandriva
  - ✓ Aplicación WEB
  - ✓ Base de datos del Sistema de Servicio Médico en Servidor
  - ✓ SERVIDOR DELL (Linux):
    Dell Power Edge R710, Procesador: Intel Xeon – 8 núcleos, RAM: 32 GB, Disco Duro: 640 GB
  - ✓ No requiere antivirus
  - ✓ Usuarios: Clínicas del STC, Gerencia de Salud

- **Sistema de Servicio Médico SISEM.** El Sistema de Información de Servicio Médico es una herramienta web que permite llevar la administración completa de la clínica de una manera sencilla y eficaz. El SISEM cuenta con el registro de la consulta médica, incapacidades, recetas y pases así como la generación de reportes y estadísticas. Al mismo tiempo se tiene la información de sus pacientes organizada y disponible en segundos.

  **Objetivos***:*

  - Brindar un servicio ágil en la atención médica que requieren los trabajadores y derechohabientes del Sistema de Transporte Colectivo
  - Llevar un control y registro de la atención médica, logrando así la obtención de información real y confiable en un tiempo mínimo.
  - Controlar el gasto asociado que representa cada trabajador y sus derechohabientes en el Sistema de Transporte Colectivo.

**Beneficios:**

- Contar con información oportuna e íntegra de los servicios médicos otorgados a los derechohabientes del Sistema de Transporte Colectivo METRO para la toma de decisiones.
- Proporciona privacidad con los usuarios y niveles de acceso para proteger los datos clínicos o administrativos

Las Pruebas de Vulnerabilidad a estos sistemas deberán realizarse en las instalaciones de la Gerencia de Organización y Sistemas del STC, ubicadas en la calle Delicias No. 87, Segundo Piso, Col. Centro Delegación Cuauhtémoc, C.P. 06070. Distrito Federal

### 3.7.2 Necesidades.

El STC "Metro" requiere de Servicios Profesionales de Auditoría de S.I. para desarrollar un análisis de vulnerabilidades en sus sistemas y aplicaciones que incluyan recomendaciones, soluciones o herramientas que contengan las siguientes capacidades:

- Evitar riesgos de pérdidas de información sensible, tales como Información financiera y contable, de licitaciones, e información de datos personales en el caso del software de servicios médicos, además de:
  - Sistemas de misión crítica
    - Operación de trenes
    - Monitoreo de la ubicación de trenes a través de mando centralizado
- Base de datos
  - Nómina de Empleados
  - Transacciones diarias de usuarios de la tarjeta inteligente
  - Datos clínicos del personal

En estos últimos casos el principal punto es la criticidad de la información; la dificultad para recuperarla en caso de pérdida; o bien, a que se trata en algunos

casos de información confidencial de individuos, información médica, de patologías individuales, diagnósticos, tratamientos médicos, así como datos personales e incluso información de sus domicilios.

Aunque los criterios de la Ley de Datos Personales aplican prácticamente a todos los sistemas, es necesario señalar el Artículo 11, que a la letra refiere *"Los archivos o sistemas creados con fines administrativos por las dependencias, instituciones o cuerpos de seguridad pública, en los que se contengan datos de carácter personal, quedarán sujetos al régimen general de protección previsto en la presente Ley. Los datos de carácter personal obtenidos para fines policiales, podrán ser recabados sin consentimiento de las personas a las que se refieren, pero estarán limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la prevención o persecución de delitos, debiendo ser almacenados en sistemas específicos, establecidos al efecto, que deberán clasificarse por categorías en función de su grado de confiabilidad. La obtención y tratamiento de los datos a los que se refiere el presente artículo, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas por los interesados ante los órganos jurisdiccionales."*

Es por ello que para la protección a usuarios internos y público en general se considera necesario dar cumplimiento a las medidas generales en cuanto a Seguridad de la Información en la Administración Pública del Distrito Federal, como lo son:

- Acceso y uso de los sistemas de información cuando se les requiera, capaces de resistir intrusiones y recuperarse de fallas (disponibilidad).
- Utilización y difusión solo entre y por aquellos que tienen derecho de hacerlo (confidencialidad).

- Protección contra modificaciones no autorizadas, errores e inexactitudes (integridad).
- Intercambio de información y transacciones entre organizaciones e individuos confiable (autenticación y no-repudio).

En lo particular la protección a usuarios internos en cuanto a la certeza del manejo de información generada y procesada en los sistemas señalados, así como en lo que respecta a responsabilidades administrativas de las funciones del personal relacionadas con el manejo de información además de la protección de datos personales e información de los usuarios y público en general.

A nivel de lo establecido en materia de Seguridad de la Información en la Administración Pública del Distrito Federal, como son:

- Cumplir con normatividades gubernamentales y estándares internacionales si es necesario.

En este caso, no están implementadas las normas generales que deben observarse en materia de Seguridad de la Información en la Administración Pública del Distrito Federal, publicado en la GODF el 9 de Julio del 2007, por lo que se considera necesario realizar un diagnóstico situacional mediante el análisis de riesgos y vulnerabilidad, y las pruebas correspondientes. Además de cumplir con otras normas gubernamentales y estándares internacionales se desea cumplir como son PCI Data Security Standard, ISO 17799 and ISO 27001, HIPAA, GLBA and Basel II.

Para tal efecto es necesario que se realicen pruebas de penetración, “PenTest", que es un método de evaluación de seguridad informática y de la red mediante la simulación de un ataque a los sistemas informáticos o redes de amenazas externas e internas.

El proceso implica un análisis activo del sistema que busque posibles vulnerabilidades, mala configuración del sistema, fallas de hardware o software, tanto conocido como desconocido, o debilidades operativas en proceso o contramedidas técnicas. Este análisis se realiza desde la posición de un atacante potencial y puede implicar la explotación activa de vulnerabilidades de seguridad.

#### 3.7.2.1 Descripción de las Pruebas de Penetración

El principal objetivo de las pruebas de penetración será identificar las debilidades para evitar:

- Accesos no autorizados.
- Robo de información propietaria.
- Ataque de negación de servicio (DoS).
- Abuso Interno.
- Mal uso de las aplicaciones.
- Web Penetración de Sistemas.
- Desfiguración del Sitio Web.

Las pruebas de penetración son una simulación controlada del ataque de la red que proporcionará un análisis de la seguridad de los sistemas del alcance.

Se emularán escenarios de ataque del mundo real, para identificar y documentar vulnerabilidades específicas dentro de los sistemas del alcance. Este resultado proporciona un entendimiento de los riesgos de seguridad que sirve para elaborar el plan de trabajo para priorizar las necesidades.

Se identificarán vulnerabilidades en los sistemas del alcance y dispositivos accesibles desde dentro y fuera de la red. A partir de esto, se intentarán explotar las vulnerabilidades que los podrán llevar a extender el acceso a las aplicaciones y dispositivos del cliente (a los ingenieros del proveedor), utilizando el proceso de

‘in-depth análisis’ para explotar las vulnerabilidades conocidas y obtener acceso privilegiado, esto incluye pruebas y sondeos manuales.

La prueba de penetración evaluará las medidas de la seguridad de información de los sistemas del alcance e identificará los diferentes riesgos asociados con estas vulnerabilidades, incluyendo equipamiento y control de acceso. La prueba de penetración evalúa la seguridad de los sistemas del alcance y dispositivos en el sitio y activamente analiza las debilidades del diseño, imperfecciones técnicas y configuraciones inseguras contra los criterios de mejores prácticas.

Las tareas específicas que se realizan durante las pruebas de penetración son:

- Sondear el perímetro de los sistemas del alcance para desarrollar el mapeo de la presencia en la red, incluyendo topología, dispositivos y servicios.
- Escaneos de vulnerabilidad de red para identificar vectores potenciales de ataque; se simulan ataques en una forma controlada y segura.
- Sondeo manual para descartar falsos positivos y descubrir nuevas vulnerabilidades.
- Revisión de la infraestructura de control de acceso y la configuración de dispositivos (listas de acceso, reglas, etc.), para mejorarlas.
- Probar sobre equipos de Red como Firewalls, NIDS, Routers, Switches, VPN, concentradores, etc.
- Se pueden probar Servicios de red como DNS, SMPT, http, HTTPS, FTP, etc.
- Identificar y comunicar al cliente las recomendaciones para atacar los problemas de seguridad de consecuencias críticas.
- Desarrollar recomendaciones para cada debilidad encontrada para ayudar al cliente a priorizar la implementación de las soluciones basadas en los riesgos y nivel de esfuerzo.

El servicio está limitado a realizar la prueba de penetración en hasta 4 direcciones IP que corresponden a los 4 servidores que se mencionan a continuación:

- Servidor de Presupuestos, Cliente / Servidor, Unix, Informix
- Servidor de Contabilidad, Cliente / Servidor, Unix, Informix
- Servidor de Finanzas, Cliente / Servidor, Unix, Informix
- Servidor de Servicio Médico, Web, Linux / Windows, Oracle

A continuación se listan los beneficios obtenidos con la realización de este ejercicio:

- Identificar los diferentes riesgos asociados con vulnerabilidades en los sistemas del alcance y causa raíz de las vulnerabilidades recurrentes.
- Un documento de hallazgos detallado con la lista de recomendaciones de las vulnerabilidades descubiertas y plan de remediación.
- Contar con suficiente conocimiento para mantener un alto nivel de seguridad en la red y de los sistemas del alcance.

Las pruebas de penetración son necesarias por lo siguiente:

1. La determinación de la viabilidad de un conjunto particular de vectores de ataque
2. Identificar las vulnerabilidades de alto riesgo que resultan de una combinación de vulnerabilidades de menor riesgo explotados en una secuencia particular
3. Identificar las vulnerabilidades que pueden ser difíciles o imposibles de detectar con la red automatizado o software de exploración de vulnerabilidades de aplicaciones
4. La evaluación de la magnitud del potencial de las empresas y los impactos operacionales de ataques con éxito
5. Prueba de la capacidad de los defensores de la red para detectar con éxito y responder a los ataques
6. Proporcionar evidencia para apoyar el aumento de las inversiones en personal de seguridad y tecnología

Las pruebas de penetración son un componente de una auditoría de seguridad completa. Por ejemplo, la Industria de Tarjetas de Pago Estándar de Seguridad de

Datos (PCI DSS), y el nivel de seguridad y auditoría, requieren tanto de las pruebas de penetración y permanente después de los cambios del sistema.

### 3.7.3 Alcance.

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica, que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo. Existe un viejo dicho en la seguridad informática que dicta: “lo que no está permitido debe estar prohibido y esto es lo que debe hacer ésta seguridad lógica.

**Premisas**

- Restringir el acceso de personas del STC “Metro” y de las que no lo son a los programas y archivos.
- Asegurar que los usuarios puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan sin una supervisión minuciosa.
- Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
- Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
- Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o software empleado.

La ejecución del análisis de vulnerabilidades y riesgos informáticos deberá de revisar las prácticas, controles e indicadores de los procesos que actualmente

soportan los sistemas críticos. Se identificarán las vulnerabilidades y áreas de mejora, procesos y prácticas que no están formalizadas o no se tienen implementadas. Se determinará también el grado de madurez de los procesos y prácticas, y se generarán las recomendaciones orientadas a eliminar las vulnerabilidades y disminuir los riesgos.

### 3.7.3.1 Modelo General del Diagnóstico.

Basado en lo establecido en el “Information Technology Infrastructure Library” ITIL por sus siglas en inglés, que aportan un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma. Este modelo de mejores prácticas describe a detalle los procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de T.I. de acuerdo a los siguientes estándares:

- ISO/IEC 27000; Conjunto de estándares desarrollados o en fase de desarrollo por ISO (International Organization for Standardization).
- IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización.

### 3.7.3.2 Áreas de Evaluación.

Las áreas a evaluar como parte del análisis de vulnerabilidades y riesgos informáticos deberán ser:

1. Política de Seguridad en la Información.
2. Clasificación y Control de Activos.
3. El rol de Recursos Humanos.
4. Seguridad Física.
5. Administración de los Servicios.

6. Controles de Acceso.
7. Desarrollo y Mantenimiento de Aplicaciones.
8. Administración de Incidentes.
9. Planeación de la Continuidad del Negocio.

### 3.7.4 Justificación del proyecto

Detectar vulnerabilidades en los sistemas o aplicaciones y que se generen soluciones que permitan al STC “Metro” tener control sobre la seguridad de las aplicaciones para su óptimo funcionamiento, con el propósito de evitar ataques, robos o modificación de información, además a tener un programa proactivo, el cual dará seguimiento en tiempo real a los sistemas propuestos para llevar a cabo las pruebas, con lo que se pretende minimizar este tipo de incidentes.

Un análisis de vulnerabilidades y riesgos es el proceso mediante el cual se realiza un estudio físico y lógico exhaustivo, a través de la minuciosa inspección de componentes generales y particulares de un activo, así como de los procedimientos y procesos existentes enfocados a su protección, con la finalidad de identificar las condiciones de funcionalidad, operación y seguridad, localizar las debilidades y su nivel de exposición o vulnerabilidad. Una vez conociendo los aspectos señalados, el compromiso y criticidad de cada activo, se puede identificar el nivel de protección necesaria, y efectuar recomendaciones para fortalecer la seguridad del activo, y garantizar la funcionalidad y operación del activo en caso de materialización de un riesgo.

- **Activos:** Es un recurso de valor que requiere protección; se considera que un activo es cualquier elemento que debido a su valor requiere ser protegido. La necesidad de que el activo sea protegido se debe a su criticidad para mantener la continuidad del negocio, o bien a la dificultad para reemplazarlo en un tiempo determinado. Los activos son:

- **Tangibles.** Empleados, que son el activo más importante de la empresa; edificios, instalaciones, equipos, software, hardware, producción, etc.
- **Intangibles.** Procesos, información, reputación e imagen de la empresa.

En términos generales, en el valor del activo se debe considerar el costo del reemplazo económico, de infraestructura y/o de equipo.

- **Amenazas:** Es un peligro que puede provocar daño parcial o total a la integridad de un activo; Es un "peligro potencial":
  - **Accidentes y/o incidentes**
    - De materiales peligrosos.
    - Incendio.
    - Plagas.
    - De avión.
    - Robo de información.
    - Hundimiento.
    - De transportes.
    - Drogadicción.
    - Anegación.
    - Amenaza de bomba.
    - Intoxicación.
    - Caída.
    - Robo.
    - Abuso de confianza.
    - Precipitación.
    - Robo con violencia.
    - Fraude.
    - Lesiones.
    - Sismo.

- Lluvias fuertes.
- Fatalidades.
- Huracán.
- Vientos fuertes.
- Intrusión delictiva.

- **Vulnerabilidad.** Es la debilidad que presenta un activo ante las amenazas existentes. Las debilidades pueden ser factores detonantes para la afectación de peligros activos o pasivos y provocar daño parcial o total a un activo.
- **Evaluación de vulnerabilidades.** Se determina si un activo es o no vulnerable mediante los siguientes factores:
  - Falta de redundancia o soporte para funciones críticas de activos o sistemas.
  - Identificar los puntos únicos de falla.
  - Componentes críticos.
  - Capacidad de respuesta.
  - Medidas de seguridad.
  - Presencia de materiales peligrosos.
  - Posibilidad de daños consecuenciales.
- **Riesgos:** Es el grado de probabilidad de que una amenaza se materialice; es la exposición a una posible pérdida. Por tanto, las amenazas son el factor cualitativo y los riesgos el factor cuantitativo.

  Mediante el análisis de vulnerabilidades y de riesgos se estudian las causas de las amenazas y eventos no deseados, el nivel de vulnerabilidad o exposición a la materialización de riesgos, así como los daños y efectos consecuenciales que puedan producir. Aunado a lo anterior, para fines de identificar los riesgos específicos y generar el catalogo correspondiente, debe realizarse la ponderación de cada uno de ellos, tomando en cuenta tanto el impacto como la frecuencia, lo que a su vez otorga un valor cuantitativo a cada uno de los riesgos.

Una vez que se cuenta con la ponderación y clasificación de riesgo se pueden desarrollar procedimientos enfocados a la prevención, reacción, y/o restablecimiento de la operación y funciones críticas, en caso de materialización de riesgos, así como las acciones o tareas para minimizar los efectos nocivos de cada riesgo.

### 3.7.5 Beneficios.

- Reducción en costos relacionados a los tiempos de entrega de aplicaciones a producción.
- Incremento de productividad gracias a mayor transparencia y automatización.
- Cumplimiento con estándares internacionales, PCI Data Security Standard, ISO 17799 e ISO 27001, HIPAA, GLBA y Basel II.
- Explorar varias aplicaciones simultáneamente.
- Control centralizado de las pruebas de seguridad de las aplicaciones WEB en todo al STC “Metro”.
- Recomendaciones de reparación inteligente para facilitar el proceso de remediación una vez identificadas y validadas las vulnerabilidades.
- Supervisión ininterrumpida y agregación de métricas para asegurar la remediación y la tendencia a la mejora con el tiempo.
- Paneles de instrumentos sofisticados y vistas de informes flexibles para proporcionar visibilidad de los riesgos y el progreso de remediación en toda la Institución.
- Acceso a los informes y a los permisos de exploración, basado en roles para facilitar la aplicación de las políticas de prueba y centralizar las exploraciones de vulnerabilidad.

## 3.8 Plan de Trabajo

En la tabla 3.8 se muestra el plan general con su respectivo entregable:

**Tabla 3.8 Plan General**

| Fases | Entregable |
|---|---|
| a) Kick-off del Diagnóstico | Presentación de objetivos y cronograma |
| b) Definición del alcance | • Estrategia de ejecución<br>• Documento con el alcance acordado |
| c) Ejecución del Diagnóstico | • Hoja de avance en entrevistas<br>• Comentarios referentes a las entrevistas |
| d) Análisis de resultados | Análisis de procesos y nivel de riesgo |
| e) Presentación de resultados | Resultados del análisis de vulnerabilidades y riesgos informáticos:<br>• Reporte Ejecutivo en formato libre<br>• Reporte detallado en formato libre |

En la tabla 3.9 se muestra el plan de trabajo detallado con sus diferentes tareas y tiempos a considerar.

**Tabla 3.9 Plan de trabajo detallado**

| | Semanas | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Plan de trabajo** | **S1** | | | **S2** | | | **S3** | | | **S4** |
| **1.** Recopilación de la información | | | | | | | | | | |
| **2.** Análisis de las arquitecturas de SW. | | | | | | | | | | |
| **3.** Selección de la herramienta de testeo. | | | | | | | | | | |
| **4.** Implementación de las pruebas. | | | | | | | | | | |
| **5.** Iinstalación y configuración del equipo en el cual se montará la máquina virtual de Check Point. | | | | | | | | | | |
| **6.** Pruebas. | | | | | | | | | | |
| **7.** Puesta en marcha. | | | | | | | | | | |
| **8.** Tareas que implican entregables. | | | | | | | | | | |
| **9.** Evaluación. | | | | | | | | | | |
| **10.** Reportes. | | | | | | | | | | |
| **11.** Recomendaciones. | | | | | | | | | | |
| **12.** Normas. | | | | | | | | | | |
| **13.** Capacitación. | | | | | | | | | | |

### 3.9 Entregables.

**Informe y entrega de resultados.**

Después de finalizar el análisis, los ingenieros de la empresa contratada, valorarán toda la información derivada del procedimiento de las pruebas de penetración. Entonces se enumerarán las vulnerabilidades y se establecerá la prioridad entre las mismas, clasificando los riesgos como altos, medios o bajos y se recibirán las recomendaciones para solucionar las vulnerabilidades.

El informe definitivo de las pruebas de penetración serán presentadas en medio electrónico e impresos y deberá contener:

- En formato de lista; las vulnerabilidades; resultado de la búsqueda, recolección e identificación de información orientada a vulnerabilidades de cada sistema, basado en los estándares citados en el modelo diagnóstico.
- En formato libre; el análisis de vulnerabilidades y riesgos informáticos, así como catálogo de riesgos con apego a los estándares de clasificación de riesgos hidro-meteorológicos, geológicos, químicos, sanitarios y/o socio-organizativos.
- En formato libre la detección de áreas de mejora.
- En formato libre; la propuesta de mejoras para cumplimiento legal reglamentario y normativo, así como de las Mejores Prácticas de seguridad informática, basado en los estándares citados en el modelo diagnóstico.
- En formato libre; el informe de documentación de los procesos de cada sistema.
- En formato libre; el resultado del análisis de los procesos existentes de cada sistema.
- En formato libre; las entrevistas con los usuarios de los sistemas.
- En formato libre; las entrevistas con los administradores de los sistemas.
- En formato libre; las observaciones de cada sistema.
- En formato libre; de las recomendaciones a cada sistema.

El resultado del análisis de riesgos y vulnerabilidad deberá ser entregado en un reporte ejecutivo con los soportes correspondientes y con las recomendaciones para el cumplimiento legal, normativo y reglamentario, así como de mejores prácticas, todos estos en formato libre.

La información proporcionada, antes y durante la realización de las pruebas de vulnerabilidad, así como la contenida dentro del presente anexo, es de carácter confidencial, por lo que se solicita se adopten las medidas legales para garantizar la confidencialidad de la información.

Asimismo se solicita que el pago correspondiente al servicio sea cubierto únicamente hasta la finalización de las pruebas, y la Gerencia de Organización y Sistemas haya recibido toda la información y entregables acordados.

**Conclusiones.**

Una auditoria no fue concebida para un tema en particular, simplemente tiene un campo muy grande de aplicación. El mundo en general se puede auditar y cuando pienso en auditoria visualizo en todo lo que una organización hace desde que se constituye hasta el día a día en su operación, cuando nace hasta que muere, todo lo que una organización hace y lo que es. Partiendo de ese panorama todo es auditable y tiene la manera de ser auditado. Por lo anterior lo que se audita se puede medir y controlar y lo que se mide se puede mejorar.

Hoy en día es fundamental contar con controles y procesos auditables y sobre todo auditados, sin ello no podremos conocer la salud y estado en el que se encuentra cualquier organización independiente del ramo del que se trate. Anteriormente se estilaba o se inclinaba esta práctica a organizaciones del ramo financiero, administrativo y en algunos casos tecnológico, hoy en día aplica a todo tipo de organización tanto pública como privada. Incluso actualmente existen corporaciones dedicadas a esta práctica y con ello cualquier organización puede contratar el servicio de forma externa, la cual tiene por función principal llevar a cabo el trabajo de auditoria sin formar parte de la organización y con enfoques distintos a los que cualquier personal interno de las organizaciones tengan para llevar a cabo esta labor.

Ahora bien, esta tesis constituye un enfoque que busca la obtención de resultados completos, eficientes y sobre todo eficaces en todas las evaluaciones efectuadas a los sistemas de información de cualquier organización, basada en las mejores prácticas. Con ello pretende, de manera puntual y completa, presentar los resultados al personal clave (llámese alta dirección de cualquier organización) para la toma oportuna de decisiones.

La definición de la auditoria de sistemas de información de este trabajo es la *evaluación de riesgos y análisis de procesos y controles para verificar el cumplimiento de lineamientos, normas y procedimientos, evaluando la calidad de la información y analizando el resultado de la gestión, para el cumplimiento de objetivos clave*, tales como:

- Validar y verificar que la plataforma tecnológica con todo lo que ella engloba, sea la adecuada para el cumplimiento de la misión, visión y objetivos de cualquier Organización.
- Conocer, comprender y alinear el Plan Estratégico de la Organización y su normatividad.
- Contar con una perspectiva sistemática de todas las operaciones, clasificándolas de acuerdo a un análisis de riesgo.
- Cubrir todos los aspectos relacionados con el comportamiento de cualquier Organización, particularmente los controles internos, financieros, operativos, administrativos y legales.
- Contar con soporte necesario que permita un Plan de Contingencia ante un evento extraordinario.
- Evaluar la capacidad de la organización para proteger sus activos sensibles tales como la información y debidamente prescindir de la información a personas no autorizadas.

En otras palabras y de manera resumida la auditoria es conocer el estado en el que se encuentra la gestión, procesos y manejo de la información, que permita evaluar todos los riesgos para tomar acciones preventivas y controles que permitan soportar la operación de cualquier organización, basado en las mejores prácticas internacionalmente conocidas.

Desde el enfoque de la organización, la Auditoria es el examen objetivo, crítico, sistemático, posterior y selectivo que se hace a la administración informática, con el fin de emitir una opinión acerca de:

- La eficiencia en la adquisición y utilización de los recursos informáticos.
- La confiabilidad, la integridad, la seguridad y oportunidad de información.
- La efectividad de los controles en los sistemas de información.

Una auditoria de S.I. es diferente a una encargada de los estados financieros. Mientras que una auditoría financiera su propósito es evaluar si una organización está cumpliendo con las prácticas contables habituales, los efectos de una auditoria de S.I. deben evaluar el diseño del sistema de control interno y la eficacia de todo lo referente a las TIC dentro de cualquier Organización. Esto incluye pero no se limita a la eficiencia y protocolos de seguridad, los procesos de desarrollo o de supervisión de S.I.

Este trabajo tiene la virtud de facilitar a los lectores la comprensión del porqué es necesario integrar las auditorías de sistemas de información entre las técnicas utilizadas por los auditores.

Actualmente las organizaciones operan en entornos tecnológicamente complejos, que son la mayoría de los entes públicos y privados hoy en día, por lo que es necesario introducir en el conjunto de procedimientos y herramientas que utilizan nuestros auditores las relacionadas con la auditoría informática.

El trabajo de un auditor de S.I. siempre debe estar presente en los procedimientos de una auditoría en cualquier Organización. Es precisamente este factor (trabajar integrados) un aspecto fundamental para que el trabajo de auditoría en su conjunto, el de los auditores «tradicionales» y los auditores de S.I., alcance su máxima eficacia y eficiencia. Obteniendo con lo anterior un conocimiento valioso

para contribuir en la implementación y aseguramiento de las mejores prácticas en materia de T.I., y la importancia de la auditoría como herramienta de control y auto ayuda, abundado en los temas fundamentales como la estructura de un Departamento de T.I., roles y responsabilidades y controles inherentes a cada función.

Como se pudo apreciar en el caso práctico, el informe de auditoría engloba diversos puntos contenidos en este trabajo, desde los conceptos de auditoria y seguridad, normas y estándares pasando por el Gobierno de T.I. hasta el nivel técnico del auditor y/o equipo de auditores. La calidad de cualquier informe de auditoría en muchas ocasiones se determina con base en las buenas prácticas utilizadas y no se tiene establecido un formato o plantilla a seguir, quedando a criterio del Auditor dicho formato a utilizar. Lo esencial siempre será el contenido del informe el cual debe estar debidamente soportado. Asimismo se pretende resaltar que un área de T.I. en cualquier organización es estratégica e importante como cualquier otra dentro de una organización y que esta debe estar siempre alineada a la estrategia general de cualquier corporación. Para visualizar esto de mejor manera y como se describió en el capítulo 1, la importancia del Gobierno de T.I. y los beneficios que esto trae, dependerán en gran medida de que tan bien se encuentre estructurado y sobre todo de que cuente con los recursos suficientes que le permitan agregarle valor en todos los sentidos a la Organización. La evolución de las tecnologías de la información T.I. demandan recursos y cualquier Organización debe concebirse bajo una cultura y proyección especializada que este adecuada a las evoluciones tecnológicas. Cuando esto no sea así, se padecerá de una gran cantidad de situaciones no deseadas tal y como se pudo plasmar en el trabajo de auditoria mencionado en el caso práctico.

Por último, es importante mencionar que un Auditor de S.I. lleva años de preparación en este campo, no se hace de la noche a la mañana. Incluso ya existen instituciones que se especializan en el tema de la Auditoria de sistemas de la información, con el objeto de preparar profesionales que se encarguen de esta complicada labor. Por ello este trabajo pretende dar un panorama que todo auditor de S.I. debe contemplar.

**Recomendaciones.**

Con base en lo expresado en el capítulo 3, todas las auditorias en cualquier organización deben adoptar la aplicación de la Auditoria de S.I. en la realización de su proceso de gestión.

Es importante que todos los departamentos o gerencias de Auditoría Interna dependan o reporten a la máxima autoridad, por ejemplo la alta dirección.

En caso de la no existencia de un comité de seguridad, es necesario conformar uno que esté integrado por funcionarios de alto nivel de las distintas áreas operativas, incluyendo la de auditoría interna, a fin de recoger todas las necesidades en materias de Seguridad, Informáticas y/o de índole operativa de cada organización, con el objeto de formular, aprobar y/o actualizar el Plan Estratégico Institucional en materia de T.I., en el corto, mediano o largo plazo.

Para la realización de las auditorías de S.I. es necesario se asignen los recursos suficientes y la tecnología necesaria, de lo contrario no se puede asegurar el objetivo y la calidad del trabajo de auditoría.

Una Auditoría de S.I. siempre debe aplicarse cuando:

- Se lleve a cabo la adquisición de tecnologías y contratación de servicios de tecnología informática (outsourcing).
- Siempre que se desarrolle, implemente y/o se aplique mantenimiento de sistemas de información.
- En todo lo referente a la seguridad informática: ya sea física y lógica sobre los datos, hardware, software, comunicaciones, redes y programas de aplicación, entre otros, solo por mencionar los más importantes.

- En toda la administración, configuración y uso de infraestructura de telecomunicaciones.
- Siempre que se realice una sistematización y automatización de procesos.
- Para todo tipo de administración y operación de centros de cómputo.

El auditor de S.I. necesita un buen conocimiento general de la tecnología de información, también debe conocer las bases de la auditoria en general así como las normas y estándares de la industria tecnológica.

Todo auditor de S.I. debe incluir profesionales con formación puntual en sistemas de información, preferiblemente con conocimientos en las diferentes especialidades en tecnologías de información: telecomunicaciones, desarrollo de sistemas, sistemas operativos, bases de datos, etc.

Se reitera la necesidad de la existencia del plan de continuidad operacional y de contingencia en cualquier organización, y realizar la evaluación de su cumplimiento. En caso de no existir es necesario desarrollarlo.

La auditoría de S.I. debe ampliar su enfoque no solo a la evaluación de controles sino también a la evaluación de riesgos y de esta manera avanzar hacia una auditoria preventiva.

El personal de auditoria interna siempre deberá recibir capacitación continua en la materia. Deberá estar capacitado a un nivel que le permita cumplir eficientemente sus tareas y contar con apoyo tecnológico e información actualizada.

## Bibliografia


1. **Arens**, Randal J. Elder, Mark S. Beasley, (2006). Auditoria un enfoque integral, 11ma Edición. México. Pearson Educación.
2. **Cohen y Asin**. (2000), Sistemas de Información un enfoque de toma de decisiones. 3ª Edición. México. Mc Graw Hill.
3. **Kaplan R. y Norton**, D. (1997).Cuadro de mando integral. Editorial Gestión 2000: Barcelona, España.
4. **Norma UNE-EN ISO 19011:** 2012, Directrices para la auditoría de los sistemas de Gestión.
5. **O´Brien, J.** (2003). Sistemas de información gerencial. Cuarta Edición. México. McGraw Hill.


## Referencias electrónicas


1. http://www.itil-officialsite.com/, Página recuperada, Octubre 15 2014
2. http://www.cyclopaedia.es/wiki/Indicadores-Clave-de-Desempeno-1 Página recuperada, Noviembre 20 2014
3. https://www.isaca.org/Pages/default.aspx?cid=1002083&Appeal=SEM&gclid=CPuPqrOokcACFSsV7AodMSwAAA, Página recuperada, enero15 2014.
4. http://sas70.com/ Página recuperada, febrero 8 2015
5. http://www.ssgt.com.mx/pdf/elcontapuntocom-auditoriaforense.pdf Página recuperada, Octubre 15 2014
6. http://codigoverde.com/consultoria-especializada/prueba-de-penetracion-pentest/, Página recuperada, Marzo 11 2015