VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

I PROMOCIÓN

TESIS DE GRADO DE MAESTRÍA

TEMA: "GUÍA DE EVALUACIÓN DE LA GESTIÓN DE TI CON APLICACIÓN DE COBIT Y COSO EN EL SECTOR PÚBLICO ECUATORIANO"

AUTOR: VILLACÍS LÓPEZ, WILLIAM NAPOLEÓN

DIRECTORA: ING. CECILIA HINOJOSA RAZA

OPONENTE: ING. CARLOS MONTENEGRO

SANGOLQUÍ JULIO 2014

Sangolquí, 30 de junio de 2014

Certificado

Sr. Ing. Rubén Arroyo MSc.
COORDINADOR DE LA MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

ASUNTO: CULMINACIÓN O FINALIZACIÓN DE LA TESIS DE GRADUACIÓN

Por medio de la presente yo, Cecilia Hinojosa MSc., en calidad de Director de la Tesis de Graduación Titulado: “GUIA DE EVALUACIÓN DE LA GESTIÓN DE TI CON APLICACIÓN DE COSO Y COBIT EN EL SECTOR PÚBLICO ECUATORIANO¨, desarrollado por el Sr. Economista William Napoleón Villacís López, egresado de la Maestría en Evaluación y Auditoría de Sistemas Tecnológicos, pongo en conocimiento que la Tesis se encuentra concluida y cumple con todos los parámetros de exigencia, por lo que solicito se digne disponer la evaluación correspondiente.

Solicito además, brindar las facilidades para la Defensa Final ante el Tribunal de Graduación.

Atentamente,

Ing. Cecilia Hinojosa MSc.
DIRECTORA DE LA TESIS

Autoría de responsabilidad

Quien suscribe, declaro que los contenidos y los resultados obtenidos en la presente tesis, como requerimiento para la obtención del Título de Magister en la Maestría de Evaluación y Auditoría de Sistemas Tecnológicos, Primera Promoción, son absolutamente originales, auténticos, personales y de exclusiva responsabilidad legal y académica del autor.

WILLIAM NAPOLEÓN VILLACÍS LÓPEZ

_____

CI: 170655487-8

Autorización (publicación biblioteca virtual)

Yo, William Napoleón Villacís López, C.I. 170655487 – 8, autorizo a la Universidad de Fuerzas Armadas, ESPE, publique en la Biblioteca Virtual la Tesis para la Maestría en Auditoría y Evaluación de Sistemas Tecnológicos, titulada: “GUÍA DE EVALUACIÓN DE LA GESTIÓN DE TI CON APLICACIÓN DE COBIT Y COSO EN EL SECTOR PÚBLICO ECUATORIANO”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Dedicatoria

La consecución de esta tesis, la dedico a mi familia, a mi esposa, a mi hija y a mi nieto, por quienes brindo mis esfuerzos que sirvan de guía y ejemplo para que alcancen sus más caros anhelos y objetivos.

Agradecimiento

A Dios por ser quien me ha dado ánimo y fuerzas para continuar. A mi padre por servirme de ejemplo para seguir adelante, con la finalidad de alcanzar las metas propuestas; a mi madre por seguirme dando ánimo, a mí familia por apoyarme en los momentos que más lo necesité.

Un especial agradecimiento a la Ing. Cecilia Hinojosa Raza y al Ing. Carlos Montenegro por sus valiosos aportes como Directora y Profesor Oponente de la Tesis.

ÍNDICE GENERAL

ÍNDICE DE CUADROS

TABLA DE FIGURAS

RESUMEN

El autor describe la Guía de Evaluación de la Gestión de TI, aplicando COBIT y COSO para el Sector Público Ecuatoriano y se fundamenta como acciones correctivas en las metas de actividad, métricas clave e indicadores de desempeño de COBIT, con aplicación de uno de los componentes de COSO, denominado “Actividades de Control”, desarrollado en el grupo de Normas Técnicas de Control Interno 410 “Tecnologías de la Información”, emitido por la Contraloría General del Estado, para comprobar los medidores de COBIT. Se indica modelos de recomendaciones a la máxima autoridad de TI, basados en los procesos de COBIT. Esta Guía, mediante la aplicación de la matriz propuesta, contribuye a determinar las áreas críticas relacionadas con los objetivos de control descritos en los dominios de COBIT por lo que se facilita la generación de acciones correctivas que encajan en el marco de trabajo propuesto para las TI.

PALABRAS CLAVE: EVALUACIÓN, GESTIÓN DE TI, COBIT, COSO, SECTOR PÚBLICO ECUATORIANO.

ABSTRACT

The author describes as the guide of evaluation of TI, apply COBIT and COSO for the Public Sector of Ecuador, is based corrective actions on the goals of activity, metrics key and indicators of performance of COBIT, with application of one of the components of COSO, called "Control activities", developed in the technical standards of Control internal 410 group "Information technologies" issued by the Controller General of the State to check the meters of COBIT. Models of recommendations to the highest authority, based on the COBIT processes are indicated. This guide, with the application of the proposed matrix, helps to determine the critical areas related to the control objectives described in COBIT domains by allowing the generation of corrective actions for the work proposed for the TI.

KEYWORDS: MANAGEMENT, IT EVALUATION, COBIT, COSO, ECUADORIAN PUBLIC SECTOR.

CAPÍTULO I.- INFORMACIÓN INICIAL

1.1 EVALUACIÓN DE LA GESTIÓN DE TI

Según el artículo 226 de la Constitución Política del Ecuador, en el Sector Público legalmente se debe realizar solamente lo que dispone la Ley, por tanto, en materia de control se cumplirá lo dispuesto en los artículos: 211 y 212 de la Carta Magna, por medio de los cuales la Contraloría General del Estado, como organismo técnico de control de los recursos públicos, dirigirá el sistema de control administrativo que se compone de auditoría interna, auditoría externa y del control interno de las entidades del sector público; determinará las responsabilidades administrativas y civiles culposas e indicios de responsabilidad penal; expedirá la normativa para estas funciones y asesorará a las entidades del Sector Público. (Constitución, 2008).

En cumplimiento de este mandato constitucional, la Contraloría General del Estado, mediante Acuerdo No. 39, publicado en el Registro Oficial Suplemento del 14 de diciembre de 2009, emitió las Normas de Control Interno para fijar parámetros y controles claves en la administración pública, basadas en los componentes de COSO I. (Organizations, Commitee of Sponsoring, 1997).

Incluidas en las Normas de Control Interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado

que dispongan de recursos públicos, se encuentra la Norma 600-02: “Evaluaciones periódicas”, que dispone:

> *“La máxima autoridad y las servidoras y servidores que participan en la conducción de las labores de la institución, promoverán y establecerán una autoevaluación periódica de la gestión y el control interno de la entidad, sobre la base de los planes organizacionales y las disposiciones normativas vigentes, para prevenir y corregir cualquier eventual desviación que ponga en riesgo el cumplimiento de los objetivos institucionales… Las evaluaciones periódicas o puntuales también pueden ser ejecutadas por la Unidad de Auditoría Interna de la entidad, la Contraloría General del Estado y las firmas privadas de auditoría.- En el caso de las disposiciones, recomendaciones y observaciones emitidas por los órganos de control, la unidad a la cual éstas son dirigidas emprenderá de manera efectiva las acciones pertinentes dentro de los plazos establecidos, considerando que éstas son de cumplimiento obligatorio.- La máxima autoridad y los directivos de la entidad, determinarán las acciones preventivas o correctivas que conduzcan a solucionar los problemas detectados e implantarán las recomendaciones de las revisiones y acciones de control realizadas para fortalecer el sistema de control interno, de conformidad con los objetivos y recursos institucionales.”.* (Acuerdo 39, 2009)

La Comisión del Senado de los Estados Unidos, gestionó la formación del Comité de Organizaciones Patrocinadoras (Committee of Sponsoring Organizations) conocido desde entonces por sus siglas en inglés como COSO. Este comité investigó sobre criterios de control interno para

principalmente prevenir o detectar los fraudes. (Organizations, Commitee of Sponsoring, 1997)

Los Objetivos de Control para la Tecnología de la Información que en inglés sería Control Objetives for Information and Related Technology, (COBIT) son prácticas de control en Tecnologías de la Información que van hacia el aseguramiento de la información y el aseguramiento de la calidad de la información. (ISACA Governance Institute, 2005).

En uso de las facultades conferidas en los artículos 12, literal c) y 14 de la Ley Orgánica de la Contraloría General del Estado (LOCGE), las unidades de auditoría interna pueden realizar la evaluación integral del Sistema de Control Interno, sujetándose a la aprobación por parte de la CGE, de su Plan Anual de Control de cada año, concordante con las normas ecuatorianas de auditoría gubernamental, emitidas con acuerdo 019 – CG de 5 de septiembre de 2012. (Acuerdo 19, Contraloría General del Estado, 2002).

Conforme a las disposiciones legales en vigencia, en materia de control interno realizado por auditores gubernamentales, se pueden realizar evaluaciones, exámenes especiales o auditorías de gestión en las Direcciones de Tecnologías de la Información, aplicando los parámetros de medición emitidos por la Contraloría General del Estado. (Contraloría General del Estado, 2002).

1.2 PLANTEAMIENTO DEL PROBLEMA

En el Sector Público Ecuatoriano, en materia de auditoría de Tecnologías de la Información (TI), no existe en el marco legal vigente, disposiciones concretas para realizar evaluaciones de gestión y relacionarlas con los procedimientos de las fases de auditoría gubernamental, esto es la planificación, la ejecución en el campo y la comunicación de resultados. (Acuerdo 19, Contraloría General del Estado, 2002).

Así mismo, según la experiencia del autor como auditor gubernamental, existe confusión entre una intervención de auditoría con auditores gubernamentales y una intervención de personal de controladores, supervisores o verificadores para realizar una evaluación a las áreas de Tecnologías de la Información, debido que a veces estos evaluadores, pertenecen a la misma área de TI, por lo que existe la posibilidad de que sus resultados puedan sesgarse por la falta de independencia, al pertenecerse al área auditada.

Los parámetros de medición comunes para áreas administrativas se aplican independientemente de los parámetros de Tecnologías de la Información; es decir, por un lado, se aplican las Normas Técnicas de Control Interno, emitidas por la Contraloría General del Estado, basadas en COSO I; (Acuerdo 39, 2009) y, por otro, se aplican los parámetros para aspectos netamente técnicos, aplicando los objetivos de control para Tecnologías de la Información COBIT. (ISACA Governance Institute, 2005).

En las evaluaciones de Tecnologías de la Información, realizadas por personal que no es auditor gubernamental, se analizan aspectos netamente técnicos. No se logra una combinación adecuada entre: los controles básicos para la gestión pública como son los derivados de los componentes de COSO I, con los controles básicos de un área de TI como son los descritos en los dominios de COBIT.

Las disposiciones legales en vigencia, brindan parámetros generales de control y no tienen la especialización y profundidad que se requiere y que se lograría al aplicar estándares internacionales descritos en COBIT.

Por lo expuesto, se observa que no existe la obligación legal emitida por la Contraloría General del Estado, mediante un reglamento, manual o guía para realizar evaluaciones de la gestión de TI en el Sector Público, que oriente a cumplir con los estándares nacionales e internacionales de control.

1.3 JUSTIFICACIÓN E IMPORTANCIA

Con una guía metodológica, se lograría una combinación adecuada para evaluar un área de Tecnologías de la Información, utilizando controles básicos para la gestión administrativa como son los componentes de COSO con las Normas Técnicas de Control Interno emitidas por la Contraloría General del Estado (Acuerdo 39, 2009) y los controles básicos de un área de TI como son los dominios de COBIT (ISACA Governance Institute, 2005).

Con esta combinación de procedimientos, se podría estructurar equipos multidisciplinarios con técnicos independientes y auditores gubernamentales que generen resultados y acciones correctivas, llegando incluso al establecimiento de responsabilidades, si es el caso, siguiendo el debido proceso dispuesto en el artículo 76 de la Constitución de la República del Ecuador. (Constitución, 2008).

Al contar con una guía que permita aplicar las fases de la auditoría gubernamental y que garantice la presentación de resultados de manera transparente y con objetividad, se aplicaran los mejores principios y políticas de auditoría y evaluación de TI, generalmente aceptados a nivel internacional.

1.4 OBJETIVOS

OBJETIVO GENERAL

Desarrollar una guía para evaluar la gestión del área de tecnologías de la información en el sector público, aplicando uno de los componentes de COSO denominado “Actividades de control”, desarrollado en el grupo de Normas Técnicas de Control Interno 410 “Tecnologías de la Información”, emitidas por la Contraloría General del Estado, para determinar áreas críticas y relacionarlas con los objetivos de control descritos en los dominios

de COBIT para la generación de acciones correctivas en procura del mejoramiento continuo de los procesos.

OBJETIVOS ESPECÍFICOS

- Guiar paso a paso la evaluación de la gestión en las unidades de tecnologías de la información (TI), mediante la implementación de una matriz, que describe los lineamientos para:

  - Elaborar el Programa de Trabajo y la Planificación Específica.
  - Definir la estructura del equipo de auditoría, responsabilidades y funciones de supervisores y auditores gubernamentales independientes; y/o, personal de controladores o verificadores de la misma área de tecnologías de la información.
  - Distribuir tareas mediante el Programa de Auditoría.

- Orientar la aplicación de pruebas de auditoría a las áreas críticas de TI.
- Diseñar los procedimientos orientados al análisis de la brecha existente, mediante la aplicación de metas y métricas descritas en COBIT, entre lo que se desea en TI y el grado de madurez encontrado,
- Guiar la combinación de procedimientos que ejecuten técnicos y auditores gubernamentales que generen resultados y acciones correctivas, mediante la emisión de un informe con comentarios,

conclusiones y recomendaciones con una seguridad razonable de que se aplicarán los mejores principios y políticas de auditoría y evaluación de TI.

- Demostrar la validez de la Guía, mediante el ejemplo de aplicación en una entidad pública real.

1.5 ALCANCE

La Guía para la evaluación de áreas de Tecnologías de la Información será de aplicación a las instituciones del sector público determinadas en los artículos 225 y 315 de la Constitución de la República (Constitución, 2008). Se desarrollará una evaluación en una institución pública, que se describe en el anexo 2, con una matriz que consta de tres partes: la evaluación al cumplimiento de las normas de control interno vigentes en el sector público ecuatoriano; la calificación del riesgo de auditoría y el enfoque de auditoría basado en los riesgos.

Con la finalidad de validar la presente Guía se aplicó sus procedimientos en la evaluación de la Unidad de TI de la Una entidad pública como parte de la Evaluación Integral del Sistema de Control Interno Institucional. El informe correspondiente se tramitó a la Contraloría General del Estado, la misma que mediante oficio 01825 del 18 de enero de 2013, en base a la supervisión realizada en la Dirección de Auditorías Internas, avocó conocimiento de su contenido para el trámite de comunicación a la máxima autoridad de la institución y exhortar al cumplimiento de sus recomendaciones. Los

documentos y papeles de trabajo relevantes de esta evaluación se encuentran en el anexo 1. En consideración de la confidencialidad de la información referente al control interno de la Dirección de Tecnologías de la Información, se presenta ejemplos de esta evaluación, suficientes para explicar la aplicación de la Guía.

El trabajo desarrollado consistió básicamente en evaluar los controles existentes en la institución, de conformidad con el artículo 9 de la Ley Orgánica de la Contraloría General del Estado (CGE) y las normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos emitidas con Acuerdo 039 – CG, publicado en el Registro Oficial 78 y Suplemento 87 de 1 y 14 de diciembre de 2009 (Acuerdo 39, 2009).

CAPÍTULO II.- MARCO TEÓRICO DE REFERENCIA

En el sector público, según los artículos 20, 21 y 22 de la Ley Orgánica de la Contraloría General del Estado, la auditoría es el examen profesional de la gestión pública y se ejercerá mediante (Ley 73, 2002):

La auditoría financiera que informará sobre la razonabilidad de las cifras presentadas en los estados financieros de una institución pública, mediante un informe profesional.

La auditoría de gestión que es la acción fiscalizadora dirigida a examinar y evaluar el control interno, la gestión y el desempeño de una institución, utilizando recursos humanos de carácter multidisciplinario, evaluará los resultados originalmente esperados y medidos de acuerdo con los indicadores institucionales y de desempeño pertinentes.

La auditoría de aspectos ambientales que auditará los procedimientos de realización y aprobación de los estudios y evaluaciones de impacto ambiental en los términos establecidos en la Ley de Gestión Ambiental, y:

La auditoría de obras públicas que examinará la gestión de la contratación para obras públicas

Como parte de la auditoría gubernamental, según el artículo 19 de la Ley Orgánica de la Contraloría General del Estado (Ley 73, 2002), se debe utilizar el examen especial para verificar, aspectos limitados o de una parte de la gestión financiera, administrativa, operativa y medio ambiental, con

posterioridad a su ejecución, aplicará las técnicas y procedimientos de auditoría, de la ingeniería o afines, o de las disciplinas específicas, de acuerdo con la materia de examen y formulará el correspondiente informe que deberá contener comentarios, conclusiones y recomendaciones.

De lo expuesto en la conceptualización de la auditoría en el sector público la actividad de control en el área de TI, se debe encaminar por una auditoría de gestión si se trata de opinar sobre la totalidad de las actividades en esta área o un examen especial de gestión si se pretende examinar un componente de la misma. Cabe indicar también que como auditoría interna se podría realizar evaluaciones similares a las que realizarían los mismos técnicos encargados de sus procesos de TI, en la aplicación de su control previo o continuo; utilizando estándares internacionales o normas de control interno basados en COSO (Acuerdo 47, GUIA METODOLOGICA CGE, 2011).

Para ejercer el examen especial al área de TI, existen varios organismos especializados en este tipo de control como el Instituto de Auditores Internos, IAI, que confiere el Certified Internal Auditor, CIA; (Certificado de Auditor Interno CIA) y la ISACA (Information Systems Audit and Control Association) que confiere el Certified Information Systems Auditor (CISA).

Estos organismos internacionales recomiendan el uso de las mejores prácticas de auditoría en Tecnologías de la Información que van hacia el

aseguramiento de la información y el aseguramiento de la calidad de la información, como lo son los Objetivos de Control para la Tecnología de la Información que en inglés sería Control Objetives for Information and Related Technology, (COBIT) (ISACA Governance Institute, 2005).

De igual manera que COBIT, existen otros estándares internacionales como el British Standard BS 15000; (Británico Estándar BS 15000), la Information Technology Infraestructure Library, ITIL; (Biblioteca de infraestructura de tecnología de la información ITIL).BS 7799 e ISO 17799, metodología de análisis y gestión de riesgos de los sistemas de información, MAGERIT, Sarbanes-Oxley, SOX (Office of Government Commerce ITIL v3 Ministerio de Hacienda del Reino Unido., 2007)

1.6 DOMINIOS DE COBIT

COBIT (Control Objetives for Information and Related Technology), (ISACA Governance Institute, 2005) tiene los cuatro siguientes dominios, que constituyen un marco de trabajo, creado para control de la tecnología de la información (TI) y de Gobierno de TI:

Planear y organizar (PO)

Este dominio tiene relación con las estrategias y como identificar la manera en que TI contribuye al logro de los objetivos de la entidad. La misión y visión de la entidad requiere ser planeada, comunicada y administrada desde las perspectivas de la TI. Finalmente, se debe

implementar una estructura organizacional y una estructura tecnológica apropiada.

Este dominio cubre los siguientes conceptos:

Adquirir e implementar (AI)

Se relaciona con el cambio y mantenimiento de los sistemas existentes para cumplir la misión de la Unidad de TI, pasa por un proceso de identificación, desarrollo, adquisición e integración a la gestión de la entidad, para satisfacer los objetivos trazados.

En este dominio, se desarrollan temas como:

Entregar y dar soporte (DS)

Manejo y medición del desempeño para implantar acciones correctivas oportunas
Monitoreo y evaluación del control interno
Cumplimiento e involucramiento con la gestión de la entidad
Seguridad razonable de que los controles internos son efectivos y eficientes
Administración de los riesgos.
Entrega de servicios de TI de acuerdo a prioridades
Optimización de costos de TI
Capacitación de los usuarios para producir con seguridad al utilizar los sistemas de TI
Confidencialidad
Integridad; y,
Disponibilidad

Se relaciona con la entrega de los servicios, incluye la prestación y continuidad del mismo, así como con la administración y seguridad de los datos e instalaciones.

Temas desarrollados en este dominio:

Monitorear y evaluar (ME)

Para medir la eficiencia, eficacia y calidad, en cumplimiento de los controles de Tecnologías de la Información. Abarca temas como:

Para cada uno de estos temas desarrollados en los dominios de COBIT, se cuenta con un enlace a las metas de negocio y TI. Se proporciona la información de cómo se pueden medir las metas y cuáles son sus actividades clave o entregables principales, así como quién es el responsable de ellas. (ISACA Governance Institute, 2005).

1.7 CONTROL INTERNO

COSO I (Organizations, Commitee of Sponsoring, 1997)

En la década de los años 80, la Comisión del Senado de los Estados Unidos, ante las dificultades financieras del sistema de ahorro y crédito y varios eventos de corrupción, gestionó la formación del Comité de Organizaciones Patrocinadoras (Commitee of Sponsoring Organizations) conocido desde entonces por sus siglas en inglés como COSO. Este comité

investigó sobre la aplicación y mejora de criterios de control interno en las empresas que sirvieron de guías para la gestión del riesgo corporativo, control interno y prevenir o detectar los fraudes.

El informe COSO, en su primera versión en inglés se publicó en 1992. La misma que la tradujo al español la firma Coopers & Lybrand conjuntamente con el Instituto de Auditores Internos, Capítulo España, en 1997. En el 2004 se publicó el COSO ERM, conocida como "Gestión de Riesgos Corporativos".

Los miembros de COSO son: American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executive Institute (FEI), Institute of Internal Auditors (IIA) y el Institute of Management Accountants (IMA). (Organizations, Commitee of Sponsoring, 1997)

En esta versión de COSO I (1992), toda entidad debió definir y desarrollar los siguientes componentes (Organizations, Commitee of Sponsoring, 1997):

Ambiente de control y trabajo
Evaluación de riesgos
Actividades de control
Sistemas de información y comunicación
Supervisión o monitoreo

COSO II

Para el 2004 se tenían mayores necesidades de control y de prevención de eventos nocivos para la administración de las entidades por lo que se incrementaron componentes orientados a la Administración de Riesgos

Corporativos (Enterprise Risk Management).Por lo que a COSO se le conoce en la actualidad como COSO ERM: (Organizations, Commitee of Sponsoring, 2004)

Normas de Control Interno (Acuerdo 39, 2009)

En el año 1992, la Organización Internacional de Entidades Fiscalizadoras Superiores, INTOSAI, aprobó la guía para las Normas de Control Interno del Sector Público, concebida para visualizar el diseño, implantación y evaluación del control interno en las entidades fiscalizadoras superiores. Esta guía fue actualizada en distintos eventos internacionales, siendo la última reforma en el año 2004, luego del XVII Congreso Internacional de las Entidades Fiscalizadoras Superiores, INCOSAI, realizado en Budapest. (Acuerdo 39, 2009).

Con el propósito de asegurar la correcta y eficiente administración de los recursos y bienes de las entidades y organismos del sector público ecuatoriano, en el 2002, la Contraloría General del Estado emitió las Normas de Control Interno, que constituyen lineamientos orientados al cumplimiento de dichos objetivos.

La última reforma de estas normas se encuentra en el Acuerdo de la Contraloría General del Estado 39, publicado en el Registro Oficial Suplemento 87, del 14 de diciembre de 2009 reformado en diciembre de 2010 y se relacionan con los componentes detallados en COSO I.

Incluidas en la Normas de Control Interno, se encuentra la Norma 600-02 "Evaluaciones periódicas" (Acuerdo 39, 2009), que dispone que:

> *"La máxima autoridad y las servidoras y servidores que participan en la conducción de las labores de la institución, promoverán y establecerán una autoevaluación periódica de la gestión y el control interno de la entidad, sobre la base de los planes organizacionales y las disposiciones normativas vigentes, para prevenir y corregir cualquier eventual desviación que ponga en riesgo el cumplimiento de los objetivos institucionales… Las evaluaciones periódicas o puntuales también pueden ser ejecutadas por la Unidad de Auditoría Interna de la entidad, la Contraloría General del Estado y las firmas privadas de auditoría.- En el caso de las disposiciones, recomendaciones y observaciones emitidas por los órganos de control, la unidad a la cual éstas son dirigidas emprenderá de manera efectiva las acciones pertinentes dentro de los plazos establecidos, considerando que éstas son de cumplimiento obligatorio.- La máxima autoridad y los directivos de la entidad, determinarán las acciones preventivas o correctivas que conduzcan a solucionar los problemas detectados e implantarán las recomendaciones de las revisiones y acciones de control realizadas para fortalecer el sistema de control interno, de conformidad con los objetivos y recursos institucionales.".* (CGE Normas de Control Interno, 2009)

Los grupos de normas: 200, 300, 400, 500 y 600 de las Normas de Control Interno, corresponden a los componentes de COSO I.

Normas de Control Interno basadas en COSO I y su relación con COBIT

Cuadro 1:
Relación COSO I - Normas de control Interno CGE – COBIT

COMPONENTES DE COSO I	NORMAS DE CONTROL INTERNO(CGE)	DOMINIOS DE COBIT
Ambiente de Control y Trabajo	200 Ambiente de Control	
Evaluación de Riesgos	300 Evaluación del Riesgo	
Actividades de Control	400 Actividades de Control	
Actividades de Control	410 Tecnología de la Información	
Actividades de Control	410-01 Organización Informática	PO – PLANEAR Y ORGANIZAR
Actividades de Control	410-02 Segregación de Funciones	PO – PLANEAR Y ORGANIZAR
Actividades de Control	410-03 Plan Informático estratégico de tecnología	PO – PLANEAR Y ORGANIZAR
Actividades de Control	410-04 Políticas y Procedimientos	PO – PLANEAR Y ORGANIZAR
Actividades de Control	410-05 Modelo de Información	PO–PLANEAR Y ORGANIZAR
Actividades de Control	410-06 Administración de Proyectos	PO – PLANEAR Y ORGANIZAR
Actividades de Control	410-07 Desarrollo y adquisición de software	AI – ADQUIRIR E IMPLEMENTAR
Actividades de Control	410-08 Adquisiciones de Infraestructura	AI – ADQUIRIR E IMPLEMENTAR
Actividades de Control	410-09 Mantenimiento y control de la infraestructura tecnológica	DS – ENTREGAR Y DAR SOPORTE

CONTINUA

Actividades de Control	410-10 Seguridad de Tecnología de Información	ME – MONITOREAR Y EVALUAR
Actividades de Control	410-11 Plan de Contingencias	PO – PLANEAR Y ORGANIZAR
Actividades de Control	410-12 Administración de soporte de tecnología de información	DS – ENTREGAR Y DAR SOPORTE
Actividades de Control	410-12 Sitio Web, servicios de internet e intranet	DS – ENTREGAR Y DAR SOPORTE
Actividades de Control	410-15 Capacitación informática	DS – ENTREGAR Y DAR SOPORTE
Actividades de Control	410-16 Comité informático	ME – MONITOREAR Y EVALUAR
Actividades de Control	410-17 Firmas electrónicas	DS – ENTREGAR Y DAR SOPORTE
Sistemas de Información y Comunicación	500 Información y Comunicación	
Supervisión y Monitoreo	600 Seguimiento	

1.8 PLANIFICACIÓN DE AUDITORÍA

Cuadro 2:

Planificación de los exámenes de auditoría;

EVALUACIÓN DEL RIESGO	NIVEL DE RIESGO	PLANIFICACIÓN
1	BAJO	3er. Año
2	MEDIANO	2do. Año
3	ALTO	1er. Año

Según las actividades que se realizan en las auditorías internas del Sector Público y las disposiciones de la Contraloría General del Estado, para cumplir los objetivos de auditoría, se respeta una serie de pasos que se fijan en un marco normativo; lo que implica que en la Auditoría Gubernamental, se utilice una estrategia y un enfoque, productos del análisis de riesgos. A criterio del autor, para dar un orden a la ejecución de los exámenes en la planificación de auditorías, se debe utilizar un indicador de impacto y probabilidad, para destinar su análisis en un período no más allá de tres años (Acuerdo 012 Manual Aud Gub, 2003)

La Planificación en la Auditoría se fundamenta en:

- La Planificación Global de Auditoría que puede ser a 3 años
- La Planificación Operativa Anual considerada para el año actual y,
- La Planificación Individual de Auditoría que considera: (La Planificación Preliminar y la Planificación Específica) como parte de la ejecución de la auditoría o examen especial.

La Planificación Global de Auditoría

Una vez que se realizó el análisis de riesgos se puede determinar una prioridad a base de los indicadores de probabilidad e impacto, según la capacidad y disponibilidad de recursos se puede proyectar la realización de exámenes a tres años. Cabe indicar que todo depende de la complejidad de la gestión de la entidad. Habrán entidades que puedan cubrir sus áreas críticas en un año, en dos o hasta en tres, que es lo prudente para realizar una evaluación de riesgos.

Planificación Operativa Anual

Es la planificación anual de control, considerada como una planificación a corto plazo, de las unidades auditables, comprende el desarrollo de una estrategia, al igual que el establecimiento de un enfoque sobre la naturaleza, oportunidad y alcance de los procedimientos de auditoría que deben aplicarse. Existe normativa y políticas para que la Contraloría General del Estado, apruebe el Plan Operativo Anual de cada entidad, que son emitidas por el Contralor General del Estado a través de la Dirección de Auditorías Internas, mediante Acuerdos anuales de Este Organismo de Control.

Planificación Individual de Auditoría

Es la planificación que se realiza exclusivamente para un área crítica que será auditada conforme al Plan Operativo Anual, se debe traducir los objetivos generales de una auditoría integral en objetivos específicos de

control de TI. (Acuerdo 19, Contraloría General del Estado, 2002). En esta planificación se deben considerar dos tipos de planeación:

Planificación Preliminar

Consiste en la obtención o actualización de la información de la entidad mediante la revisión de archivos, reconocimiento de las instalaciones y entrevistas con funcionarios responsables de las operaciones, tendientes a identificar globalmente las condiciones existentes y obtener el apoyo y facilidades para la ejecución de la auditoría. Comienza con la Visita previa.

Consiste en la obtención o actualización de la información de la entidad mediante la revisión de archivos, reconocimiento de las instalaciones y entrevistas con funcionarios responsables de las operaciones, tendientes a identificar globalmente las condiciones existentes y obtener el apoyo y facilidades para la ejecución de la auditoría.

Se debe obtener un entendimiento de la misión, objetivos, propósito y procesos del negocio Identificar el estado de contenidos específicos (políticas, normas, directrices, procedimientos y estructura organizacional). Realizará un análisis de riesgos y conducirá una revisión de control interno.

Planificación Específica

Según la Norma Ecuatoriana de Auditoría Gubernamental PAG. – 05 (Acuerdo 19, Contraloría General del Estado, 2002) la planificación de la

auditoría incluirá la evaluación de los resultados de la gestión de la entidad a examinar con relación a los objetivos, metas y programas previstos. La evaluación del control interno es obligatoria para obtener información complementaria, evaluar y calificar los riesgos así como seleccionar los procedimientos que se aplicarán. En esta fase se deberá generar los siguientes productos de la planificación específica de auditoría (Acuerdo 19, Contraloría General del Estado, 2002):

- Programas específicos para aplicar las pruebas sustantivas y el alcance previsto.
- Plan de muestreo.
- Requerimientos de personal técnico o especializado, en la ejecución de la auditoría.
- Distribución del trabajo y tiempo estimado para realizar el examen ajustándose a lo establecido en la orden de trabajo.
- Uso de técnicas de auditoría asistidas por computadora.
- Memorando de planeamiento.
- Papeles de trabajo de la fase.
- Informe de evaluación al control interno para conocimiento del titular de la entidad examinada, con comentarios y recomendaciones.

La Planificación Específica es la estrategia a seguir en el trabajo, se fundamenta por la información obtenida en la planificación preliminar y en la evaluación del Control Interno. Sobre la base de la calificación de los

factores de riesgo por cada componente de la auditoría, se determinará la extensión de las pruebas, se preparará el plan de muestreo y los programas específicos a aplicarse en la siguiente fase. Concretamente se establecerá el alcance y los objetivos de la auditoría y se desarrollará el enfoque o la estrategia de auditoría para asignar los recursos de personal a la auditoría y dirigir la logística del trabajo de auditoría para lograr evidencia suficiente y competente que respalden los hallazgos de auditoría, se la obtiene a través de TAAC´s (Técnicas de Auditoría Asistidas por Computador).

Pruebas de cumplimiento.- Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente. Tratan de obtener evidencia de que se están cumpliendo y aplicando correctamente los procedimientos de control interno existentes y los estándares y prácticas sanas aceptadas internacionalmente.

Pruebas sustantivas.-Verifican el grado de confiabilidad de la TI del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información. Las pruebas sustantivas que tratan de obtener esa evidencia referida a la información auditada. Están relacionadas con la integridad, la exactitud y la validez.

Las principales herramientas para aplicar estas pruebas de auditoría son (Acuerdo 47, GUIA METODOLOGICA CGE, 2011):

- Observación
- Realización de cuestionarios
- Entrevistas a auditados y no auditados
- Muestreo estadístico
- Flujo gramas
- Listas de chequeo
- Mapas conceptuales

Los objetivos de la auditoría

A criterio del autor, son los resultados que se espera obtener de la evaluación o auditoría, se enfocan a validar que existen controles para minimizar los riesgos del negocio y que estos funcionan como se espera. En el área de TI, se relacionan con la seguridad de la información, donde se debe verificar: la confidencialidad, Integridad, disponibilidad y confiabilidad en el uso de los recursos (eficiencia) y el alcance de los objetivos institucionales (eficacia).

Respecto de la **confidencialidad** la Organización Internacional de Estandarización (ISO) en la norma ISO-17799 (International Organization for Standardization, 2000) la define como la garantía de que la información es accesible sólo para aquellos autorizados a tener acceso y es una de las

piedras angulares de la seguridad de la información. La confidencialidad es uno de los objetivos de diseño de muchos cripto sistemas, hecha posible en la práctica gracias a las técnicas de criptografía moderna. Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

La confidencialidad también se refiere a un principio ético asociado con varias profesiones (por ejemplo, medicina, derecho, religión, psicología profesional, y el periodismo); en este caso, se habla de secreto profesional. En las jurisdicciones en que la ley prevé la confidencialidad, hay sanciones por su violación.

La confidencialidad en informática se entiende en el ámbito de la seguridad, como la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros. Esto debe hacerse independientemente de la seguridad del sistema de comunicación utilizado: de hecho, un asunto de gran interés es el problema de garantizar la confidencialidad de la comunicación utilizada cuando el sistema es inherentemente insegura como el Internet.

Según los criterios de información de COBIT (ISACA Governance Institute, 2005), para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, como la confidencialidad que se refiere a la protección de la información contra la revelación no

autorizada. La integridad que está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio. La disponibilidad que se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento; y, la confiabilidad se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

Análisis de Riesgos en la Auditoría

La norma ISO / IEC TR 13335 – 1 STANDARD publicada el 26 de marzo de 2001 por Canada National Standard / Canadian Standards – ISO / IEC (Norma ISO / IEC TR 13335 – 1 STANDARD, 2001); define al riesgo como la probabilidad de que una amenaza determinada pueda explotar vulnerabilidades del negocio u organización, causando pérdida o daños no esperados. La amenaza como es un factor externo está fuera de nuestro control, pero la vulnerabilidad es un factor interno susceptible de control y acciones correctivas.

De la experiencia en materia de control del autor, se puede indicar que el análisis de riesgos, es una parte importante de la Planificación Global e Individual de Auditoría, ayuda a identificar amenazas y vulnerabilidades para que el Auditor pueda determinar los controles necesarios para mitigar esos riesgos. Por tanto, el auditor de TI debe utilizar una técnica o enfoque

apropiado de evaluación de riesgos al desarrollar el Plan Global de auditoría de TI y al determinar prioridades para la asignación eficaz de los recursos de auditoría de TI; el auditor de TI identificará y evaluará los riesgos relevantes al área bajo revisión para planear revisiones individuales.

En las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI) que son emitidas por la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), se indica que hay que identificar los eventos que podrían tener impacto negativo o positivo en el logro de los objetivos y que los eventos con impacto negativo representan los riesgos. (INTOSAI, 2004)

En las Normas Ecuatorianas de Auditoría Gubernamental, emitidas mediante Acuerdo de la Contraloría General del Estado 19, el 10 de octubre de 2002, en el Grupo de Normas relacionado con la Planificación de Auditoría Gubernamental PAG – 06, sobre la evaluación del riesgo, determina que para planificar el enfoque de la auditoría y examen especial el auditor debe tener una comprensión suficiente de la entidad y aplicará su criterio profesional para evaluar el riesgo de auditoría, definiéndola como la posibilidad de que la información contenga errores significativos que no sean detectados. Estos riesgos de auditoría pueden ser (Acuerdo 19, Contraloría General del Estado, 2002):

Riesgo inherente

La posibilidad de que existan errores o irregularidades en la gestión administrativa y financiera, antes de verificar la eficiencia del control interno diseñado y aplicado por el ente a ser auditado, este riesgo tiene relación directa con el contexto global de una institución e incluso puede afectar a su desenvolvimiento.

Riesgo de control

Es la posibilidad de que los procedimientos de control interno incluyendo a la unidad de auditoría interna, no puedan prevenir o detectar los errores significativos de manera oportuna. Este riesgo si bien no afecta a la entidad como un todo, incide de manera directa en los componentes.

Riesgo de detección

Se origina al aplicar procedimientos que no son suficientes para lograr descubrir errores o irregularidades que sean significativos, es decir que no detecten una representación errónea que pudiera ser importante.

Como producto del conocimiento de la entidad y la evaluación del control interno, el supervisor y jefe de equipo elaborará un reporte para aprobación del jefe de la unidad de auditoría que emitió la orden de trabajo en el que permita se determine el enfoque final del examen a ejecutar.

Para calificar los riesgos por componentes, se preparará una matriz que contenga, entre otros aspectos los siguientes: componente analizado, riesgos y su calificación (inherente, de control y de detección), enfoque esperado de la auditoría y las instrucciones para la ejecución de la auditoría (Acuerdo 19, Contraloría General del Estado, 2002)

Evidencia en la Auditoría

Conforme a las Normas Ecuatorianas de Auditoría Gubernamental, el auditor obtendrá la certeza suficiente y apropiada a través de la ejecución de sus comprobaciones de procedimientos para permitirle emitir las conclusiones sobre las que fundamentará su informe acerca de la gestión del área de TI. (Acuerdo 19, Contraloría General del Estado, 2002).

En la Norma Ecuatoriana de Auditoría Gubernamental EAG – 05 del Grupo relativo a la ejecución de la Auditoría Gubernamental titulada: evidencia suficiente, competente y relevante manifiesta que: para fundamentar los comentarios, conclusiones y recomendaciones respecto a la administración de un ente, programa u operación significativa, sujetos a la auditoría, el auditor obtendrá evidencia suficiente, competente y pertinente, mediante la aplicación de técnicas de auditoría.

La evidencia de auditoría comprende toda información que provenga de varias fuentes y sirvan de respaldo de las actividades operativas,

administrativas, financieras y de apoyo que desarrolla la entidad auditada, las mismas que deben contener las siguientes características:

a) Suficiente.- Cuando los resultados de una o varias pruebas proporcionan una seguridad razonable para proyectarlos con un mínimo riesgo, al conjunto de actividades de este tipo;

b) Competente.- Para ser competente, la evidencia debe ser válida y confiable, indagándose cuidadosamente si existen circunstancias que puedan afectar estas cualidades; y,

c) Pertinente.- Se refiere a la relación que existe entre la evidencia y su uso.

El auditor necesita apoyarse en evidencias que son más persuasivas que concluyentes; y, con frecuencia, busca evidencias de diferentes fuentes y de distinta naturaleza para sustentar una misma aseveración.

Técnicas y Prácticas de Auditoría

Las técnicas de auditoría constituyen métodos prácticos de investigación y prueba, que el auditor emplea a base de su criterio o juicio según las circunstancias, unas son utilizadas con mayor frecuencia que otras, a fin de obtener la evidencia o información adecuada y suficiente para fundamentar sus opiniones y conclusiones contenidas en el informe

Durante la fase de planeamiento y programación, el auditor determina las técnicas a emplear, cuándo debe hacerlo y de qué manera. Las técnicas seleccionadas para una auditoría al ser aplicadas se convierten en los procedimientos de auditoría.

Algunas de las técnicas para la aplicación de las pruebas en la auditoría en el sector público se clasifican, a base de la acción que se va a efectuar, las que pueden ser: oculares, por escrito, por revisión del contenido de documentos y por constatación física. (Acuerdo 016, 2001).

Acogiendo esta clasificación, las técnicas de auditoría se agrupan de la siguiente manera.

Técnica de verificación verbal - Indagación

Es una conversación que mantiene el auditor con los auditados, con la finalidad de obtener información, que debe respaldarse con un papel de trabajo donde se descrina en forma de narración los resultados de las indagaciones realizadas.

Técnicas de verificación ocular

Comparación

Es la relación que existe entre dos o más aspectos, para observar la similitud o diferencia entre ellos. La forma de comparación más común, constituye la que se efectúa entre los ingresos percibidos o los gastos efectuados, con las estimaciones incluidas en el presupuesto. Así mismo, es frecuente la comparación entre los ingresos mensuales provenientes de una fuente, con meses anteriores o el mismo mes del año precedente.

El auditor, si dispone de normas de calidad, estándares de rendimiento, de productividad, entre otros, puede utilizar estos índices en sus comparaciones. Ciertos procedimientos de auditoría se fundamentan en la comparación de información o realidades, contra criterios aceptables, facilitando la evaluación, la formulación de comentarios y acciones correctivas.

Observación

Es el examen de la forma como se ejecutan las operaciones, es considerada la técnica más general y su aplicación es de utilidad en casi todas las fases de un examen. Por medio de ella, el auditor verifica ciertos hechos y circunstancias, principalmente relacionados con la forma de ejecución de las operaciones, dándose cuenta, de cómo el personal realiza las operaciones.

Esta técnica se utiliza especialmente cuando el auditor observa la aplicación de los procedimientos preparados y la realización efectiva del

levantamiento de inventarios, que efectúan los servidores de la entidad, sin proceder a efectuar las constataciones físicas de las existencias.

Revisión selectiva

Es el examen ocular rápido, con el fin de separar mentalmente asuntos que no son típicos o normales. Constituye una técnica frecuentemente utilizada en áreas que por su volumen u otras circunstancias no están contempladas en la revisión o estudio más profundo. Consiste en pasar revista rápida a datos normalmente presentados por escrito. En la aplicación de esta técnica, el auditor debe prestar atención a la identificación de operaciones fuera de lo común en la materia sujeta a revisión.

Rastreo

El rastreo consiste en seguir la secuencia de una operación, dentro de su procesamiento. El ejemplo típico de esta técnica, es seguir un asiento en el diario hasta su pase a la cuenta del mayor general, a fin de comprobar su corrección.

Al evaluar el control interno, es frecuente que el auditor seleccione algunas operaciones o transacciones representativas y típicas de cada clase o grupo, con el propósito de rastrearlas desde su inicio hasta el fin de los procesos normales.

Técnica de verificación escrita:

Análisis

Analizar es determinar la composición o contenido y verificar las transacciones del período, clasificándolas de manera ordenada y separar en elementos o partes. Se puede analizar tomando de su registro las transacciones en detalle o en forma selectiva. Otra forma consiste en presentar varias clases o grupos de una misma naturaleza.

En la auditoría, con cierta frecuencia, este tipo de análisis se efectúa mediante flujo gramas del proceso, que facilita su comprensión.

Conciliación

Significa poner de acuerdo o establecer la relación exacta entre dos conjuntos de datos relacionados, separados e independientes.

La conciliación bancaria constituye la práctica más común de esta técnica, que implica hacer concordar el saldo de una cuenta auxiliar según el banco, con el saldo según el Mayor General de Bancos. Siempre que existan dos fuentes independientes de datos originados de la misma operación, la técnica de la conciliación es aplicable.

Confirmación

Consiste en cerciorarse de la autenticidad de la información, mediante la afirmación o negación escrita de una persona o institución independiente y que se encuentra en condiciones de conocer y certificar la naturaleza de la operación consultada.

Para que el elemento de juicio obtenido mediante la aplicación de esta técnica tenga valor, es indispensable que el auditor mantenga un control completo y directo sobre los procedimientos para efectuar la confirmación. La confirmación se efectúa a través del correo, pero si el servicio postal no es confiable, se hace necesario utilizar mecanismos alternativos, que pueden incluir servicios de reparto de confirmaciones y recopilación de contestaciones o en casos especiales hasta visitas personales a terceros efectuadas por el auditor.

La confirmación de datos es a veces más compleja y tardía, en ocasiones el beneficiario de servicios públicos no está en condiciones de confirmar los datos requeridos.

Existen dos modalidades para efectuar confirmaciones: positiva o negativa y a su vez, la primera puede ser directa o indirecta.

Técnicas de verificación documental:

Comprobación

La comprobación constituye la verificación de la evidencia que sustenta una transacción u operación, para comprobar la legalidad, propiedad y conformidad con lo propuesto. Así, tenemos que para efectos contables, los documentos de respaldo (facturas, cheques, papeles fiduciarios, contratos, órdenes de compra, informes de recepción,) sirven para el registro original de una operación, constituyendo.

Computación

Como técnica de auditoría permite verificar cálculos y procesos con datos ingresados a un sistema informático.

Técnicas de verificación física

Inspección

La inspección consiste en la constatación o examen físico y ocular de los activos, obras, documentos y valores, con el objeto de satisfacerse de su existencia, autenticidad y propiedad. La aplicación de esta técnica es sumamente útil, en lo relacionado con la constatación de valores en efectivo, documentos que evidencian valores, activos fijos y similares. La verificación de activos, tales como documentos a cobrar o pagar, títulos, acciones y otros similares, se efectúa mediante la técnica de la inspección.

La aplicación del examen físico o inspección, es factible, para los bienes unitarios en un inventario, así como los documentos que representen un título o valor fiduciario.

Es aplicable esta técnica, también en la revisión de contratos para obras públicas, así como la inspección de obras durante y después de su construcción.

Técnicas de Auditoría Asistidas por Computadora o TAAC's (Acuerdo 016, 2001)

Responden a programas de computación que son usadas por el auditor, como parte de sus procedimientos, para procesar la información que es significativa en su trabajo.

Estas técnicas automatizadas permiten desempeñar varios procedimientos de auditoría, tales como:

Muestreo en Auditoría (Acuerdo 016, 2001)

El muestreo puede ser definido como el proceso de inferir conclusiones acerca de un conjunto de elementos denominados universo o población, a base del estudio de una fracción de esos elementos, llamada muestra. Como norma general el muestreo puede aplicarse:

- En pruebas de cumplimiento de controles, que permitan obtener evidencias de auditoría en cuanto al flujo de la documentación y sus controles inherentes.
- En pruebas sustantivas para verificar saldos y operaciones.
- En pruebas de doble propósito que comprueben tanto el cumplimiento de un procedimiento de control que proporcione evidencia documentada de su realización, como la razonabilidad de la cantidad monetaria registrada en las transacciones y saldos.

Por lo tanto el muestreo de auditoría es aplicable: para pruebas de cumplimiento, cuando se utilicen técnicas de muestreo para probar los procedimientos de control interno sobre los cuales el auditor planea confiar, y para pruebas sustantivas, cuando se utilicen técnicas de muestreo para probar detalles de transacciones y saldos.

El muestreo de auditoría puede efectuarse mediante procedimientos estadísticos o no estadísticos, ambos procesos requieren de la selección de una muestra en la cual se encuentren las características representativas del universo.

Los auditores pueden utilizar métodos de muestreo estadístico o no estadístico para pruebas representativas. Los dos métodos se apoyan significativamente en el juicio profesional del auditor y se basan en la

presunción de que una muestra revelará información suficiente acerca del universo en su conjunto. Su diferencia consiste en el grado de formalidad y estructura involucrados en la determinación del tamaño de la muestra, en la selección de la muestra y la evaluación de los resultados. Al realizar la elección del método de muestreo, el auditor debe considerar los objetivos de auditoría y la naturaleza del universo a muestrear, así como también las ventajas y desventajas de cada método. Como el muestreo estadístico proporciona varias ventajas, se prefiere que este método sea utilizado cuando resulte práctico, efectivo y eficiente para el trabajo de auditoría.

Muestreo estadístico (Acuerdo 016, 2001)

Para ejecutar estos procedimientos se dispone de algunas alternativas como:

- Paquetes o programas diseñados y elaborados por la entidad auditada, lo cual involucra una fase previa de definición de los requerimientos por parte del auditor para establecer los datos que necesita obtener (aplicando criterios de selección) según los objetivos de la prueba que va a ejecutar.
- Programas diseñados y elaborados por el auditor, mediante el uso de lenguajes de programación, lo que requiere de un alto nivel de conocimientos técnicos para desarrollar y ejecutar dichos programas, por ejemplo un programa para calcular intereses por mora.

- Software de utilidad y servicio, son programas provistos por los fabricantes de software, como es el caso de hojas electrónicas (Excel, Lotus, Q-Pro), editores de texto, bases de datos (Access), entre otros. y que en muchos casos facilitan ejecutar procedimientos de auditoría, a saber: clasificaciones, extracción de datos (filtros), cálculos matemáticos, totales y subtotales, reportes, etc. con la restricción de que no se pueden especificar más opciones que las propias de cada paquete, y en el caso de las hojas electrónicas el número limitado de filas y columnas que puede manejar.
- Paquetes de auditoría específicos, tales como: IDEA, ACL, FOCAUDIT, EASYTRIEVE, etc. los cuales constituyen herramientas, que independientemente de la plataforma tecnológica utilizada por la entidad auditada, ofrecen opciones específicas para importar y exportar datos, analizar, estratificar, probar cálculos, aplicar muestreo estadístico, establecer rupturas de secuencia, registros duplicados, realizar uniones de archivos que permiten cruzar información desde fuentes diferentes.

Muestreo no Estadístico (Acuerdo 016, 2001)

El muestreo no estadístico no prevé la estimación anticipada y objetiva del tamaño de muestra requerido, ni la proyección o evaluación objetiva de los resultados de la muestra, se basa exclusivamente en el criterio del

auditor, según sus conocimientos, habilidad y experiencia profesional; por lo que, su naturaleza es de carácter subjetivo.

La decisión de utilizar el muestreo en auditoría depende del alcance y naturaleza de la evidencia que se necesita, de las características de la cuenta a examinar, los objetivos de la auditoría, la naturaleza del universo a muestrear y las ventajas y desventajas de cada método. Las evaluaciones del riesgo inherente son fundamentales para determinar el alcance de la evidencia que se requiere.

Para determinar el alcance de la evidencia de auditoría requerida se puede utilizar cuatro niveles de evaluación de riesgo para proponer los posibles enfoques y la aplicación del muestreo de auditoría.

Indicadores

En la Guía Metodológica para la Auditoría de Gestión de la Contraloría, (Acuerdo 47, GUIA METODOLOGICA CGE, 2011) sobre indicadores de gestión determina que:

> *"Los Indicadores de gestión son variables o parámetros que permiten medir de forma cuantitativa y cualitativa, el grado de cumplimiento de un sistema, proyecto, programa, componente, proceso, actividad o de la ejecución de las operaciones, en términos de eficiencia, economía, efectividad e impacto.- Para la construcción del indicador se deberá colocar en el numerador las variables con datos relativos a insumos, procesos o productos y en el denominador se colocarán las variables cronológicas, físicas o económicas de comparación.- Se pueden utilizar datos primarios o indicadores que relacionan dos datos; una vez elegidos los indicadores, se definen los objetivos contra los que se van a comparar, la periodicidad en que se realizarán las mediciones y cuando*

los desvíos se convertirán en alertas, es decir, indicarán los niveles por encima o por debajo de los cuales el indicador es importante.- Características.- - Estarán ligados a la misión, visión, los objetivos estratégicos y las metas trazadas- - Establecerán una periodicidad y un responsable de cálculo.- - Proveerán información útil y confiable para la toma de decisiones.- - El número de indicadores será el necesario para evaluar la gestión, uso de los recursos y grado de satisfacción de los usuarios, evitando los que nos son aplicables.- Se integrarán con los procesos, áreas funcionales y sistemas de evaluación organizacional.- Ficha técnica de indicadores.- Los indicadores se presentarán en una matriz denominada ficha técnica, que contiene la siguiente información: ...- Nombre del indicador.- - Factores críticos de éxito.- - Fórmula de cálculo del índice.- - Unidad de medida.- - Frecuencia.- - Estándar.- - Fuente de información.- - Interpretación.- - Brecha.- … Indicadores cuantitativos.- Son indicadores que miden el rendimiento de una actividad y entre otros pueden ser: Indicadores de volumen de trabajo, de eficiencia, de economía, de efectividad.- … Indicadores Cualitativos:.- Estos no miden numéricamente una actividad, sino que se establecen a partir de los principios generales de una sana administración.- Criterios para identificar un indicador.- - Simples y claros.- - Representativos.- - Investigativos.- - Comparables.- - Estables.- - Relación costo-efectividad.- Criterios para seleccionar indicadores.- - Identificar el proceso.- - Identificar actividades críticas a medir.- - Establecer metas de desempeño o estándares.- - Establecer medición de desempeño.- - Identificar las partes responsables.- - Recopilar los datos.- - Analizar y reportar el actual desempeño.- - Comparar el actual desempeño con las metas o estándares.- - Determinar si las acciones correctivas son necesarias.- Hacer cambios, para que el proceso concuerde con las metas o estándares.- - Determinar si nuevas etapas o nuevas medidas son necesarias.".

MATRIZ DE CONSTRUCCIÓN DE INDICADORES

Como se dijo en el anterior numeral los indicadores se desarrollan para evaluar el uso de los recursos y el cumplimiento de los objetivos, por lo que a criterio del auditor, se pone a consideración el uso de la matriz de construcción de indicadores a partir de los objetivos. Por lo tanto es importante primero desarrollar los objetivos de un proceso, de tal manera que se pueda identificar: la acción a realizar, las metas y las variables.

Seguidamente se identificarán los recursos para el indicador de eficiencia y las metas para el de eficacia

La matriz tiene una columna para identificar:

- El número del objetivo, útil para describir varios objetivos de una misma planificación.

- La acción a tomar, durante el período por analizar.

- Meta planificada, es la base del objetivo que indica que es lo que se quiere alcanzar.

- Plazo previsto, por lo general se trata de períodos anuales para el Planificación Operativa Anual o más de 1 para la PPA (Planificación Pluri Anual).

- Presupuesto o recursos asignados, es el insumo básico para identificar un objetivo relacionado con la eficiencia (recursos).

- Insumo básico para identificar un objetivo relacionado con la eficacia (metas).

- Variables, es la cuantificación de las metas y de los recursos.

Cuadro 3: Construcción de Objetivos

OBJETIVO Nº	OBJETIVOS OPERATIVOS (ESPECÍFICOS)				VARIABLES	
	ACCIÓN A TOMAR (verbo en infinitivo)	META PLANIFICADA	PLAZO PREVISTO	PRESUPUESTO O RECURSOS ASIGNADOS		
	(b)	(c)	(d)	(e)	METAS (f = c)	RECURSOS (g = e)
1	CUMPLIR	6 ACTIVIDADES DEL POA	EN 12 MESES	CON 2´500,000,00 USD	6 ACTIVIDADES DEL POA	2´500,000
2	TRAMITAR	TODAS LAS ÓRDENES DE GASTO A LA DIRECCIÓN FINANCIERA SIN ERRORES	EN 12 MESES	CON 4 PERSONAS	TODAS LAS ÓRDENES DE GASTO A LA DIRECCIÓN FINANCIERA SIN ERRORES	CON 4 PERSONAS

Agregación más preposición (porcentaje de… o cantidad de…); **Sustantivos o variables**, (tareas, actividades, órdenes de gasto, órdenes de pago, proyectos, presupuesto, informes, personas, cursos, productos terminados, meses, etc.), **Verbo en participio pasado** (cumplidas, tramitadas, utilizadas), **adjetivo** (oportunamente, efectivamente, correctamente), **Cumplimiento de circunstancias** (en el 2007, en el plazo de 12 meses, a la Dirección Financiera), **Relación de variables** (lo alcanzado; como numerador sobre las metas o recursos disponibles; como denominador), **Índice** (resultado de la relación de variables), **Estándar** (la línea base o lo esperado); **y, Brechas** (diferencia):

1.9 EJECUCIÓN DEL TRABAJO EN LA AUDITORÍA

Luego de la planificación, donde se determinaron los objetivos y el alcance de la auditoría, a base de sus productos terminados, se procede a la ejecución de un programa de auditoría donde se redactan las pruebas de cumplimiento y pruebas sustantivas, específicas para un área crítica. En esta fase el auditor debe aplicar los procedimientos establecidos en los programas de auditoría supervisados y, aprobados por el Jefe de la Unidad de Auditoría. Además, deberá desarrollar completamente los hallazgos con la evidencia suficiente y pertinente, aplicando la importancia relativa para eventos significativos relacionados con las áreas y componentes considerados como críticos, determinando los atributos de condición, criterio, efecto y causa que motivaron cada desviación o problema identificado.

Todos los hallazgos desarrollados por el auditor, estarán respaldados en papeles de trabajo en donde se concreta la evidencia suficiente, pertinente, competente y adecuada, que respalda la opinión y el informe y que pueda ser sustentada en un posible litigio (Acuerdo 19, Contraloría General del Estado, 2002).

1.10 COMUNICACIÓN DE RESULTADOS

Es de fundamental importancia que el auditor mantenga una comunicación continua y constante con los funcionarios y empleados relacionados con el examen, con el propósito de mantenerles informados sobre las deficiencias y desviaciones detectadas a fin de que en forma

oportuna se presente los justificativos o se tomen las acciones correctivas pertinentes.

La comunicación de resultados es la última fase del proceso de la auditoría, sin embargo ésta se cumple durante la ejecución del examen. Está dirigida a los funcionarios de la entidad examinada con el propósito de que presenten la información verbal o escrita respecto a los asuntos observados.

Esta fase comprende también, la redacción y revisión final del borrador del informe, que será elaborado en el transcurso del examen, con el fin de que al finalizar el trabajo en el campo y previa convocatoria, se comunique los resultados mediante su lectura a las autoridades, funcionarios y ex funcionarios responsables de las operaciones examinadas.

El informe contendrá los comentarios, conclusiones y recomendaciones relativos a los hallazgos de auditoría. Tratándose de auditoría financiera incluirá la carta de dictamen, los estados financieros y las notas aclaratorias correspondientes.

En el área de auditoría de gestión en el sector público ecuatoriano, se ha llegado a establecer que los esfuerzos de auditoría, se deben orientar hacia las áreas críticas.

Sin embargo, la metodología para establecer las áreas críticas difiere desde la aplicación de sencillos cuestionarios de control interno, hasta el uso de sofisticados estudios estadísticos para establecer un mapa de riesgos con medición del impacto y la probabilidad de que ocurran eventos no esperados (Acuerdo 19, Contraloría General del Estado, 2002).

1.11 INVENTARIO DE PROCESOS DE UNA UNIDAD DE AUDITORÍA INTERNA

En base a la experiencia del autor, a continuación se describen los principales procesos que deberían utilizarse para la gestión de una unidad de auditoría:
Cuadro 4:
Procesos de una unidad de auditoría interna

P R O C E S O S	A C T I V I D A D E S	P R O D U C T O S
D I R E C C I O N A R E S T R A T E G I A S P A R A L A G E S T I Ó N D E A U D I T O R Í A	• Elaborar el Plan Estratégico de la Unidad de Auditoría	**Misión, Objetivos, Políticas, Estrategias, Valores. P l a n E s t r a t é g i c o .**
P L A N I F I C A R Y N O R M A R L A G E S T I Ó N D E A U D I T O R Í A	• • Planificar a mediano plazo • Planificar a corto plazo • Elaborar la Proforma Presupuestaria. • Monitorear y Evaluar resultados.	**N o r m a s y p o l í t i c a s . P l a n O p e r a t i v o A n u a l . P l a n A n u a l d e C o n t r o l . Proforma Presupuestaria de Auditoría. Acciones de corrección, mantenimiento o mejoramiento.**
REALIZAR EL CONTROL POSTERIOR EVALUAR LA GESTIÓN DE LAS UNIDADES DE TI	• Estructurar el equipo de trabajo • Verificar la relevancia de la evaluación en la la Planificación Global y en el Plan Operativo de Control • Elaborar la Planificación Preliminar (recopilación de la información) • Elaborar la Planificación Específica • Evaluar el control interno y calificar el riesgo • Comunicar a los auditados • Leer el borrador del Informe en la Conferencia Final de Comunicación de Resultados • Tramitar el Informe de la Evaluación de Áreas de	**O r d e n d e T r a b a j o I n f o r m e d e V i s i t a P r e l i m i n a r . Memorando de Planificación Preliminar Memorando de Planificación Específica P r o g r a m a d e T r a b a j o Matriz sistemática de la evaluación de la g e s t i ó n e n l a s u n i d a d e s d e T I D e t a l l e d e c o m u n i c a c i o n e s e n v i a d a s B o r r a d o r d e l i n f o r m e l e í d o y d i s c u t i d o c o n l o s a u d i t a d o s I n f o r m e d e f i n i t i v o**

CAPÍTULO III.- GUIA DE EVALUACIÓN DE LA GESTIÓN DE TI CON APLICACIÓN DE COBIT Y COSO EN EL SECTOR PÚBLICO ECUATORIANO

Si la Unidad de Auditoría de la entidad, constantemente va a examinar el área de tecnologías de la información, se podría incluir en el personal de auditores gubernamentales a ingenieros informáticos, los cuales reporten a la Contraloría General del Estado como Jefes de Equipo o como miembros de un equipo multidisciplinario.

Por otra parte, es importante diferenciar, quien va a realizar la evaluación o examen al área tecnológica, si son auditores gubernamentales, con nombramiento de la Contraloría General del Estado, necesariamente deben cumplir con la normativa de este Organismo Técnico Superior de Control, incluso en el debido proceso para el establecimiento de responsabilidades. Sin embargo, si el personal que va a realizar la evaluación o examen es de otra área, incluso de la misma Dirección de Tecnologías de la Información, no debe denominarse auditoría o examen especial, se debe denominar “evaluación” y no se vuelve obligatorio utilizar los procedimientos constantes en los manuales y normativa de la CGE, sin embargo es una ayuda eficiente para garantizar óptimos resultados y que se pueda facilitar el proceso de pre establecimiento y establecimiento de responsabilidades, con la intervención de un equipo de auditoría del Organismo Técnico Superior de Control.

Basado en la experiencia de las unidades de auditoría interna en las evaluaciones de control interno integrales, el autor sugiere que la evaluación

al área de TI realizada por auditores gubernamentales, se diferencie de una auditoría o examen especial, en el hecho que no predeterminará responsabilidades y se basará en pruebas de cumplimiento. Por tanto, no se realizará la segunda fase del proceso de auditoría que es la ejecución de pruebas sustantivas, pero sí se realizará la tercera fase que es la comunicación. De creerse necesario y relevante, el informe de evaluación será un insumo de un futuro examen especial para predeterminar formalmente responsabilidades.

1.12 ACTIVIDADES DE LA EVALUACION DE TI

A continuación se detalla las actividades de la evaluación que en sí son similares a las actividades de una auditoría, en las fases 1 (Planificación) y 3 (Comunicación) (Acuerdo 19, Contraloría General del Estado, 2002):

Cuadro 5:
Guía de evaluación de la gestión de TI

ACTIVIDADES DE LA EVALUACIÓN	RESPONSABLE Y PARTICIPANTES	PRODUCTO
Estructurar el equipo de trabajo.	Responsable: Director	Orden de Trabajo
Verificar la relevancia de la evaluación en la Planificación Global y en el Plan Operativo de Control.	Responsable: Jefe de Equipo. Participan: Supervisor y Encargado de la Planificación.	Informe de Visita Preliminar
Elaborar la Planificación Preliminar (recopilación de la información)	Responsable: Jefe de Equipo Participan: Supervisor Colaboran como personal de apoyo: Miembros del equipo multidisciplinario.	Memorando de Planificación Preliminar
Elaborar la Planificación Específica	Responsable: Jefe de Equipo Participan: Supervisor Colaboran como personal de apoyo: Miembros del equipo multidisciplinario.	Memorando de Planificación Específica y el Programa de Trabajo
Evaluar el Control Interno y calificar el riesgo	Responsable: Jefe de Equipo. Participan: Supervisor Colaboran como personal de apoyo: Miembros del equipo multidisciplinario.	Matriz Sistemática de Evaluación de la Gestión en las Unidades de Tecnologías de la Información
Comunicar a los auditados	Responsable: Jefe de Equipo. Colaboran como personal de apoyo: Miembros del equipo multidisciplinario.	Detalle de comunicaciones enviadas
Leer el borrador del Informe en la Conferencia Final de Comunicación de Resultados	Responsable: Jefe de Equipo. Participan: Miembros del equipo. Colaboran como personal de apoyo: Miembros del equipo multidisciplinario.	Acta de Conferencia Final de Comunicación de Resultados
Suscribir y tramitar el Informe.	Director de la Unidad de Auditoría Colaboran como personal de apoyo: Miembros del equipo multidisciplinario.	Borrador de informe revisado y suscrito para trámite

Estructurar el equipo de trabajo

Como se ha manifestado, para realizar labores de auditoría en el área de Tecnologías de la Información del sector público ecuatoriano, se debe emplear un equipo multidisciplinario, cuyos miembros deben ser auditores gubernamentales, acompañados con especialistas o profesionales del área a examinar. Cabe manifestar que si la entidad constantemente debe realizar auditorías al área de tecnologías de la información, se podría tener en la auditoría interna, enrolados como auditores técnicos a profesionales en informática y afines, que según su experiencia podrían actuar como Supervisores, Jefes de Equipo o auditores operativos.

El personal de la Unidad de Auditoría o área de Tecnologías de Información encargada de monitorear y planificar el uso del Talento Humano, deberá sugerir los profesionales adecuados para conformar el equipo de trabajo. Analizará los profesionales disponibles, verificará su formación y capacitación, determinará la compatibilidad de los posibles miembros del equipo y verificará que no existan conflictos de intereses entre los miembros del equipo.

Escogerán candidatos para estructurar el equipo de auditoría de la siguiente manera:

Supervisor: Entre los que tengan el nombramiento de mayor escala, en el Sector Público. Se aplica la escala del Ministerio de Relaciones Laborales, donde esta función es asignada al Servidor Público 7.

Jefe de Equipo: Se debe utilizar para esta función al personal más experimentado que ha demostrado liderazgo y trabajo a presión, puede estar entre el Servidor Público 6 y 5.

Auditores Operativos: Se acostumbra designar para esta función a los profesionales conocedores del área a examinar, en este caso a los Ingenieros expertos del área de TI. Sin embrago no se descarta la posibilidad de que sea uno de estos profesionales que por su experiencia haya obtenido el nombramiento de auditor gubernamental, convirtiéndose en candidato para Supervisor o Jefe de Equipo.

LOGOTIPO DE LA INSTITUCION (1)

OFICIO No. (Número y siglas unidad administrativa de control) (2) (3)
Sección: (UNIDAD ADMINISTRATIVA DE CONTROL) (4)
Asunto: Orden de trabajo para actividad de control planificada

(Ciudad, fecha) (5)

Señor/a
(Nombres y Apellidos) (6)
(Cargo) (7)
(Entidad) (8)
Presente.

En cumplimiento de los artículos 211 de la Constitución de la República del Ecuador y 36 de la Ley Orgánica de la Contraloría General del Estado, autorizo a usted que con cargo al Plan Operativo de Control año (año),(9) de la (unidad de control) (10), en calidad de jefe de equipo, realice (tipo y nombre de la acción de control) (11), en (nombre de la institución), ubicada en (ciudad), (cantón) y (provincia), (12) (por los ejercicios económicos terminados al 31 de diciembre de …) o (por el período comprendido entre el…. y el…..) (años o período) (13).

Los objetivos generales son: (14)
--
--

El equipo de trabajo estará conformado por: (Nombres y Apellidos). (15) y como Supervisor (Nombees y Apellidos) (16), quien en forma periódica informará sobre el avance del trabajo.

El tiempo estimado para la ejecución de esta acción de control es de …. (17) días laborables que incluye la elaboración del borrador del informe y la conferencia final.

Atentamente,
Dios, Patria y Libertad,
(Por el Contralor General del Estado,) (18)

(Nombres y Apellidos) (19)
Del servidor (a) a cargo de la unidad administrativa de control

Figura 1: Orden de Trabajo:
Fuente: Acuerdo CGE 18, RO 481: 30 jun 2011

El Director de Auditoría mediante una comunicación interna denominada: “orden de trabajo” (CGE 18, 2011)conformará el equipo aceptando la sugerencia del personal planificador, mediante comunicaciones individuales para designar un supervisor, un jefe de equipo y el número de auditores operativos necesarios (profesionales en Tecnologías de la Información).

Verificar la relevancia de la evaluación en la Planificación Global y en el Plan Operativo de Control

Cuadro 6:

Priorización de componentes en la planificación de auditoría según el nivel de riesgo

NIVEL DE RIESGO	PRIORIZACIÓN
1 (BAJO)	Se puede auditar hasta en 3 años
2 (MODERADO)	Se puede auditar hasta en 2 años
3 (ALTO)	Se debe auditar en el corto plazo de un año

La Planificación Global o Institucional de Auditoría, es un detalle de posibles exámenes a realizar, puede ser a largo plazo (3 años) y se debe estructurar al identificar las áreas significativas y de riesgo potencial en los procesos institucionales, su relevancia para el presupuesto asignado para

Alcanzar los objetivos de la entidad y la vinculación del área de TI a las políticas establecidas para alcanzar los resultados esperados de la gestión

institucional, a la cual la gestión de TI se debe involucrar para asegurar su continuidad.

Se consideran exámenes para el corto plazo (1 año) y el auditor de TI debe verificar en el Plan Operativo Anual o Plan Operativo de Control, la relevancia de realizar el examen, que se refiere a verificar la importancia de realizar la evaluación, verificando su prioridad en los niveles de planificación de la Unidad de Auditoría. ISACA sugiere que este tipo de planeación se realice después de un análisis de riesgos corporativos en el área de TI, basada en el impacto y la probabilidad. Para la valoración el autor sugiere que se le dé al riesgo inherente que existe en las áreas relevantes de TI una escala de 1, 2 y 3 que significaría niveles de riesgo: bajo, mediano y alto, mediante pruebas de cumplimiento. Según estos niveles se les asignará un orden de prioridad para ser evaluados en no menos de 3 años, dependiendo del tamaño de la entidad.

Para este ejemplo se supone una entidad grande con un grado de madurez 4 “Administrado”, según los modelos de madurez de COBIT, es decir: (ISACA Governance Institute, 2005)

> *“… es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada”.*

Para el ejemplo, la evaluación se realizó a 4 Departamentos de la Dirección de TI, encargados de la ejecución de los 4 Dominios de COBIT,

(Planear y Organizar, Adquirir e implementar, Entregar y dar Soporte y Monitorear y Evaluar); cuyos promedios de riesgo es el resultado de la evaluación del riesgo de los 34 procesos de COBIT, sus resultados finales fueron:

Cuadro 7:
Cuadro resumen del riesgo promedio de cada dominio

DOMINIOS Y PROCESOS DE COBIT	IMPACTO	PROBABILIDAD	RIESGO INHERENTE (PROMEDIO POR DOMINIO)	PRIORIDAD SEGÚN NIVEL DE RIESGO
PO - PLANEAR Y ORGANIZAR	2	2	3	BAJO
AI - ADQUIRIR E IMPLEMENTAR	2	2	4	MODERADO
DS - ENTREGAR Y DAR SOPORTE	1	1	7	ALTO
ME - MONITOREAR Y EVALUAR	1	2	3	BAJO

Para estructurar este cuadro resumen de evaluación del riesgo, se ponderó el impacto y la probabilidad en base a un check list con una escala de 1 a 3, seguidamente se multiplicó el impacto por la probabilidad para determinar la prioridad y aplicar la distribución del control, basados en los siguientes niveles:

De 1 a 3 se considera un nivel de riesgo bajo, por lo que se podría programar un examen al tercer año de la planificación.

De 4 a 6 se considera un nivel de riesgo moderado, por lo que se podría programar un examen al segundo año de la planificación.

De 7 a 9 se considera un nivel de riesgo alto, por lo que se debe programar un examen el primer año de la planificación.

El personal encargado de la Planificación, el Supervisor y el Jefe de Equipo, deberán determinar exámenes especiales en grupo o según los procesos críticos de cada dominio, tomando en cuenta los promedios de evaluación del riesgo, por lo que determinan que el primer dominio tiene un nivel de 3 que corresponde a un riesgo bajo (de 1 a 3), y deciden incluir en la planificación para auditarlo en el tercer año de la Planificación. El segundo dominio de COBIT tiene un nivel de 4 “Moderado”, por lo que se auditará en 2 años, el tercer dominio tiene 7 como promedio de riesgo que equivale a un nivel “alto”, por lo que se decide realizar la acción de control de auditoría en el primer año por considerar un área crítica, enfocando acciones de control a los procesos de: DS3, DS4, DS5, DS6, DS7, DS8 DS9, DS10, DS11 y DS12.

Como se observa, el cuarto dominio ME – Monitorear y Evaluar, tiene una prioridad de 3, que corresponde a un riesgo bajo, por lo que se decide incluir en la planificación para auditarlo en el tercer año de la Planificación.

Cuadro 8:
Cuadro resumen del riesgo promedio del dominio DS – Entregar y dar Soporte

DOMINIOS Y PROCESOS DE COBIT	IMPACTO	PROBABILIDAD	RIESGO INHERENTE (PROMEDIO DEL DOMINIO DS)
DS - ENTREGAR Y DAR SOPORTE	1	1	7
DS1 Definir y Administrar los Niveles de Servicio	1,17	2,67	2,83
DS2 Administrar los Servicios de Terceros	1,75	3,00	5,25
DS3 Administrar el Desempeño y la Capacidad	2,80	3,00	8,40
DS4 Garantizar la Continuidad del Servicio	2,90	3,00	8,70
DS5 Garantizar la Seguridad de los Sistemas	2,82	3,00	8,45
DS6 Identificar y Asignar Costos	2,00	3,00	6,00
DS7 Educar y Entrenar a los Usuarios	2,00	3,00	6,00
DS8 Administrar la Mesa de Servicio y los Incidentes.	2,00	3,00	6,00
DS9 Administrar la Configuración	3,00	3,00	9,00
DS10 Administración de Problemas	2,75	3,00	8,25
DS11 Administración de Datos	2,83	3,00	8,50
DS12 Administración del Ambiente Físico	2,00	3,00	6,00
DS13 Administración de Operaciones	1,20	3,00	3,60

Cuadro 9:
Cuadro resumen del riesgo promedio del sub dominio: DS1-Definir y Administrar los Niveles de Servicio

DOMINIOS Y PROCESOS DE COBIT	IMPACTO	PROBABILIDAD	RIESGO INHERENTE (PROMEDIO POR EL PROCESO DS1 DEL DOMINIO DS)
DS1 Definir y Administrar los Niveles de Servicio	1,17	2,67	2,83
DS1.1 Marco de Trabajo de la Administración de los Niveles de Servicio	1,00	3,00	3,00
DS1.2 Definición de Servicios	1,00	3,00	3,00
DS1.3 Acuerdos de Niveles de Servicio	1,00	3,00	3,00
DS1.4 Acuerdos de Niveles de Operación	1,00	3,00	3,00
DS1.5 Monitoreo y Reporte del Cumplimento de los Niveles de Servicio	2,00	1,00	2,00
DS1.6 Revisión de los Acuerdos de Niveles de Servicio y de los Contratos	1,00	3,00	3,00

De esta manera se, valida y verifica la ejecutabilidad de las ordenes de trabajo para determinar de manera transparente, su importancia relativa y prioridad en el uso de los recursos de auditoría.

Sin embargo, en la planificación de las acciones de control, también tiene relevancia la necesidad de control que tienen los usuarios, por lo general, solicitan intervenciones de auditoría, ante situaciones eventuales, como: cambio de funcionarios claves, resultados no esperados, pérdida de activos, información o recursos.

Ante esta situación los auditores que toman las decisiones, deberán priorizar y considerar la relevancia de realizar una acción de control; muchas veces, con una visita preliminar se puede llegar a la conclusión, si amerita o no destinar los recursos de auditoría, que por lo general son escasos.

Sin embargo, también existe la posibilidad de realizar equipos estructurados con personal auditor y profesionales de otras áreas, siempre y cuando se guarde la independencia de quien conformará el equipo para que no haya conflicto de intereses

Visita Preliminar

Cuadro 10: Estructura del Informe de Visita Preliminar

INFORME DE VISITA PRELIMINAR
Nombre de la entidad. Ubicación. Naturaleza de la entidad. Visión, misión y objetivos. Actividad principal. Ambiente organizacional. Fuentes de financiamiento. Indicadores de gestión. Detección de las fortalezas, debilidades, oportunidades y amenazas, FODA. Estructura de control interno. Definición del objetivo y estrategia de la evaluación. Personal necesario para su ejecución.

La Contraloría General del Estado, dispone que antes de efectuar una acción de control, se deberá realizar una Visita Preliminar, para determinar para determinar la pertinencia de realizar el examen y validar el análisis realizado en la planificación, en el caso de exámenes planificados y para

determinar su relevancia, en el caso de exámenes imprevistos por denuncias o situaciones emergentes. El resultado de esta validación se revela en el informe de visita preliminar que debe tener como mínimo los elementos para establecer el estado de las actividades de la entidad y determinar la oportunidad de realizar la acción de control, como se describe en la tabla 13.

Cabe destacar que cuando la entidad es conocida y se tiene un conocimiento sólido de las actividades del área a evaluar, se puede prescindir de realizar la visita preliminar y realizar directamente la evaluación comenzando por la planificación preliminar con un informe semejante.

Elaborar la Planificación Preliminar (recopilación de la información)

Se recopilará información de la entidad a ser examinada. Se efectuará una evaluación del control interno a fin de determinar el enfoque del trabajo a realizar, permitirá: contar con información del área de TI, misión, visión, metas y objetivos del proyecto o programa a examinar y su naturaleza jurídica. Se contará con información de las actividades principales y planes. Informes de avance o de progreso y las evaluaciones realizadas por la propia entidad, al cumplimiento de los planes estratégicos y operativos. Identificación de las políticas y prácticas administrativas y financieras. Determinación del grado de confiabilidad de la información administrativa y financiera.

Se contará con información global del desarrollo, complejidad y grado de dependencia de los sistemas informáticos y de asuntos de mayor importancia, que orienten al auditor para identificar las fuentes y montos de

financiamiento de sus operaciones, identificación de los funcionarios principales y de los indicadores de gestión preparados por la entidad. (Acuerdo 19, Contraloría General del Estado, 2002).

Con la presentación formal de los profesionales del equipo multidisciplinario, explicarán a los auditados, la metodología, estándares y normativa a aplicarse en la evaluación, que deberá resumirse en verificar lo que hicieron en un período determinado con respecto a lo que debieron hacer para cumplir su misión. Utilizarán las indagaciones en entrevistas programadas con el responsable del área de Tecnologías de la Información y con los directores o autoridades competentes.

Además, en el Sector Público con la finalidad de brindar el derecho a la defensa se debe notificar a los auditados que se va a realizar la evaluación. Inmediatamente después del envío de la notificación a la máxima autoridad y al Director de TI, es importante que mediante otro oficio se le solicite la información general de la entidad o de la Unidad de TI y que se ordene la colaboración al equipo de auditoría.

El Jefe de Equipo con el Supervisor debe identificar los elementos claves de la administración de TI y evaluar la importancia de los objetivos de la auditoría, a fin de obtener el diseño de una estrategia general en el Memorando de Planificación Preliminar dirigido a la máxima autoridad de la Unidad de Auditoría. Al tratarse de entidades pequeñas, no se puede

presentar el informe de planificación preliminar pero, no impide que se realice la visita previa, para establecer el estado en que se encuentra las actividades de la entidad y determinar la oportunidad de efectuar la auditoría. (Acuerdo 19, Contraloría General del Estado, 2002)

Elaborar la Planificación Específica

Utilizando la información obtenida en la planificación preliminar, se examinarán los resultados de la gestión del área de TI con relación a los objetivos, metas y programas previstos.

Se evaluará el control interno y se calificará el riesgo. Se evidenciarán los procedimientos de auditoría aplicados y que deben orientar a conseguir información pertinente para lograr el primer capítulo del informe. Se destacarán las áreas que a criterio del auditor tienen un alto riesgo inherente, es decir aquella probabilidad de que sucedan eventos no deseados propios de cada proceso o actividad, antes de ejecutar cualquier control, por ejemplo cuando existe un constante cambio de servidores, existe el riesgo inherente de que se debilite la seguridad de acceso a los sistemas.

El Memorando o informe de Planificación Específica

El Supervisor y Jefe de Equipo incluirán en este memorando los siguientes subtítulos, tal como dispone la Contraloría General del Estado en el formato 3 del Modelo de informe de examen especial, en su Acuerdo

emitido el 26 de octubre de 2012 y servirán para desarrollar el primer capítulo del informe, (Acuerdo 026 Contraloría General del Estado, 2012)

Misión de la Entidad.- Para identificar la razón de ser de la Institución y si la gestión de Tecnologías de la Información se encuentra alineada.

Motivo del examen.-Se señalará el nombre de la entidad examinada y el número y fecha de la orden de trabajo; además se precisará si el examen se realizará en cumplimiento del plan operativo de control del año…, de la unidad de auditoría… o si obedece a un imprevisto autorizado, citando el número y fecha de tal autorización, así como las modificaciones si las hubiere.

Para el caso de las auditorías internas, en los exámenes imprevistos, se señalará la autorización expresa de la autoridad competente.

Objetivos del examen.-Se indicarán los objetivos generales incluidos en la orden de trabajo, que tendrán relación directa con la naturaleza del examen; así como los objetivos específicos establecidos en la planificación del examen.

Alcance del examen.- Se describirá el trabajo a realizar, con indicación de: componentes, áreas, proyectos, contratos, procesos o actividades examinadas y el período cubierto.

Deberá guardar conformidad con la orden de trabajo y sus modificaciones o ampliaciones debidamente autorizadas.

Se indicará en un párrafo informativo, lo relacionado con exámenes realizados por la Contraloría General del Estado y/o por la unidad de auditoría interna de la entidad examinada y/o por firmas privadas de auditoría, relacionados con alcance del examen que se ejecutó.

Limitación al alcance.- Se señalarán limitaciones únicamente en los casos en que exista imposibilidad práctica de aplicar un procedimiento de auditoría por restricciones o impedimentos impuestos por la administración de la entidad o terceros relacionados.

Base legal.- Se consignará la disposición legal en la cual consta la creación o constitución de la entidad y sus reformas.

Estructura orgánica.- Se señalará la estructura orgánica vigente de la entidad o de la unidad o área examinada, según corresponda, con el propósito de ubicar al lector en el campo de acción del examen, a la fecha de corte de la auditoría.

Objetivos de la entidad.- A fin de dar a conocer los objetivos que la entidad pretende alcanzar a través de sus unidades, áreas o actividades, se revelarán aquellos que constan en la normativa de creación o en el plan estratégico de la misma y que están relacionados con el objeto de la acción de control.

Monto de recursos que se examinarán.- Se consignará el monto de los recursos analizados en el examen especial al rubro, componente, área o proyecto. La información incluirá las fuentes de financiamiento de la entidad, en valores efectivos correspondientes al período examinado. Pudiendo ser "indeterminado", para el caso que involucra aspectos ambientales no susceptibles de una valoración directa.

Servidores relacionados.- Se realizará un detalle de los nombres, apellidos, cargo y período de gestión de los servidores principales, que actuaron durante el período de las operaciones examinadas y se presentará como anexo al informe.

Además de estos aspectos para el capítulo 1 del informe, es necesario plasmar en el memorando de planificación temas como:

Resultados de la evaluación preliminar de control interno.- Sirven para identificar áreas críticas y el riesgo de auditoría.

Inventario de Sistemas de Tecnologías de la Información.-Con la finalidad de comprobar su vigencia y utilidad para la misión de la entidad.

Inventario de activos relacionados con TI.- Importante para evaluar la eficiencia, eficacia y calidad de los servicios que brinda la Unidad de TI.

Otros hechos evidenciados en la Fase de Planificación.- Para orientar la evaluación, examen o auditoría al área de Tecnologías de la Información.

Ejemplo de Programa de Trabajo como otro producto de la Planificación Específica:

Cuadro 11:

Formato para Programa de Auditoría

DIRECCIÓN DE AUDITORÍA				
ENTIDAD: TIPO DE EXAMEN: EVALUACIÓN DE GESTIÓN CONCEPTO: PROGRAMA DE TRABAJO COMPONENTE: DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN ALCANCE: AL 30 DE ABRIL DE 2012				
No.	**DESCRIPCIÓN**	**REF: P/T**	**ELAB. POR**	**FECHA**
	OBJETIVO.- Verificar la implementación de roles y responsabilidades autorizadas y relevantes de acuerdo a cada puesto de los miembros de la Unidad de Tecnologías de la Información (TI).			
	PROCEDIMIENTOS			
1	Aplique el cuestionario de control interno específico al área crítica y analice sus respuestas para evidenciar posibles hallazgos	**F2-1**	**WV,VB**	**30/03/2012**
2	Compruebe que los roles con descripción de puestos y autoridad se encuentren documentados. Prepare y aplique un indicador: Roles documentados / total de roles de TI.	**F2-2**	**WV,VB**	**30/03/2012**
3	Compruebe los procesos de la entidad que no reciben soporte de TI. En varias unidades de la entidad; aplique el indicador: Procesos sin soporte TI Procesos con soporte de TI,	**F2-3**	**WV,VB**	**07/04/2012**

Fuente: **Manual Auditoría Financiera Gubernamental:** Acuerdo 016 - CG - 2001 (27/08/2001) R.O. 407 (07/09/2001).

Un programa de auditoría es un papel de trabajo donde se incluyen los objetivos y los procedimientos. Deberá dejar indicado la distribución de tareas con las siglas de los miembros del equipo que las deben realizar.

Durante su ejecución se completa la información señalando la fecha que se realizó el procedimiento y la referencia de los papeles de trabajo que evidencian su ejecución. Es importante en los procedimientos señalar la técnica de auditoría.

Ejemplos de procedimientos de auditoría al área de TI

Como se observa en el Anexo 4, se adaptaron los procedimientos de ejemplo, en base a los Lineamientos de Sistemas para Intermediarios, emitidas por la Dirección General Adjunta de Sistemas en México, D.F. el 20 de febrero de 2004 (Sociedad Hipotecaria Federal, 2004) .

Evaluar el control interno y calificar el riesgo

Se deberá identificar el grado de aplicación de los elementos del control interno (COSO II ERM). Como se explicó en el capítulo I, las Normas de Control Interno se basan en COSO I, sin embargo para efectos de evaluación del sistema de control interno relacionado con TI, es importante indagar y conocer la aplicación de los elementos de Control Interno basados en COSO II (Organizations, Commitee of Sponsoring, 2004), debido a que en esta versión se incluyen componentes orientados a la administración de riesgos de la entidad. Se debe preparar cuestionarios sencillos con preguntas generales para calificar el grado de cumplimiento y un acercamiento a determinar el riesgo inherente en la aplicación de componentes como:

Ambiente de control

Establecimiento de objetivos

Identificación de eventos

Evaluación de riesgos

Respuesta al riesgo

Actividades de control

Información y comunicación

Supervisión (monitoreo)

En base a la experiencia del autor se observa que la evaluación de control interno se basa en la emisión de una normativa emitida por la Contraloría General del Estado, de cumplimiento obligatorio; sin embargo la aplicación de los procesos de COBIT, actualmente, dependen de la voluntad y el grado de madurez que necesita la entidad pública. Por lo expuesto, las normas de control interno que se califiquen como incumplidas, deberán ser relacionadas con los dominios y procesos de COBIT, para aplicar acciones correctivas que se conviertan de cumplimiento obligatorio al ser emitidas en un informe de auditoría aprobado por la Contraloría General del Estado.

También sugiere el autor que se identifique la relación de los resultados de la evaluación de control interno con los procesos de COBIT, mediante una matriz elaborada en una hoja electrónica de Excel; en su primera columna se describen los 17 numerales de la Norma de Control Interno 410 denominada: Tecnologías de la Información. Cada una debe ser descrita con

preguntas estructuradas por el auditor, orientadas a ubicar el nivel de confianza en 3 rangos que describen igualmente el nivel de riesgo

Los formularios de los cuestionarios de control interno, ver anexo 2; para su valoración contienen dos columnas, una de ponderación (POND) y otra de calificación (CALIF), las cuales se sumarán una vez concluida la evaluación del control interno y aplicadas las pruebas de cumplimiento, obteniendo dos valores, el uno corresponderá a la ponderación total (PT) y el otro a la calificación total (CT).

Evaluación al cumplimiento de las NCI (COSO I)					
NORMA DE CONTROL INTERNO 410 TECNOLOGÍAS DE LA INFORMACIÓN	**PT**	**CT**	**CP**	NIVEL DE CONFIANZA	OBSERVACIONES / FACTORES DE RIESGO DE AUDITORÍA
	PONDERACIÓN (entre 1 y 10)	CALIFICACIÓN (entre 15 y 95)	CALIFICACIÓN PORCENTUAL CP=CT x 100 / PT		
TOTAL NCI 410	**1,0**	**83,8**	**83,1**	**ALTO**	

Figura 2: Cuestionario de Control Interno.

Fuente: (Acuerdo 012 Manual Aud Gub, 2003)

Según el Manual General de Auditoría gubernamental emitido por la Contraloría General del Estado, para obtener la calificación porcentual (CP) se multiplicará la calificación total (CT) por 100 y se dividirá para la ponderación total (PT).

CP = CT x 100 / PT, la calificación porcentual que se obtenga, se interpretará como el Grado de confianza o solidez que deposita el auditor en los controles internos de la entidad determinándose de esta manera el nivel de riesgo que el auditor enfrentará.

Cuadro 12:
Equivalencia de los niveles de confianza y riesgo

EQUIVALENCIA DE LOS NIVELES		
CALIFICACIÓN PORCENTUAL	**GRADO CONFIANZA**	**NIVEL DE RIESGO**
15 - 50 %	1 BAJO	3 ALTO
51 - 75 %	2 MEDIO	2 MODERADO
76 - 95 %	3 ALTO	1 BAJO

Fuente: (Acuerdo 012 Manual Aud Gub, 2003)

Por ejemplo la norma 410 – 01 dice:

> *"Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.".*

Una de las preguntas relacionadas con esta norma 410 – 01 Organización Informática diría:

¿La estructura organizacional de la entidad contiene una unidad de tecnología de información establecida formalmente dentro de los niveles de asesoría o apoyo y que disponga de facultades, atribuciones, roles o competencias?

El auditor, mediante pruebas de cumplimiento deberá obtener evidencias del grado de observancia de la normativa vigente. En el caso analizado, la entidad auditada, si cuenta con una Unidad de Tecnología de la Información, formalmente estructurada con facultades, atribuciones, roles y competencias, por lo que el auditor califica como un grado de confianza de 3 lo que determina una valoración cualitativa de: *"Confianza Alta",* por tanto el riesgo es bajo.

Se han desarrollado 4 preguntas en esta norma, las cuales tienen la misma calificación y valoración de 3, lo que significa igual promedio para calificar a toda la norma 410 – 01. Igualmente se obtiene un promedio del total de la norma aplicada, que resulta un nivel de 1 es decir "Bajo" para el riesgo de auditoría. Como se observa, este nivel de riesgo, permitirá dar el enfoque de la auditoría, es decir la profundidad de las pruebas de auditoría, que podrían ser:

- Pruebas Sustantivas, si el riesgo es moderado o alto
- Pruebas de Cumplimiento si el riesgo es bajo; y,
- Si no tiene relevancia, no ameritaría invertir recursos en pruebas de auditoría, como es el caso de analizado.

Se entiende por pruebas de cumplimiento a una verificación de la normatividad que según el autor, se podría plasmar en un check list, que contesta a la pregunta: ¿cumple o no cumple? con un sí o un no, como también se podría utilizar un 1 o un cero para realizar cálculos, porcentajes o proyecciones.

Seguidamente se realizará una vinculación con COBIT de aquellas preguntas que dan un enfoque hacia pruebas de cumplimiento y sustantivas para la auditoría, es decir las que tienen riesgo moderado y alto. Tomando como aplicación la norma 410 – 02 Segregación de Funciones, dio como resultado un enfoque de auditoría con pruebas de cumplimiento, por lo que relacionando con los controles de COBIT, para mitigar riesgos e implantar acciones correctivas, se debe orientar hacia los dominios: (PO) Planificar y Organizar, (DS) Entregar y dar Soporte y (ME) Monitorear y Evaluar.

Al realizar esta vinculación con COBIT, se estructura el programa de auditoría basándose en los procedimientos de COBIT, para sustentarse en los medidores y procesos. Por ejemplo: el enfoque de la Norma 410 – 02 Segregación de Funciones tiene una calificación de 3 con una valoración cualitativa de la confianza en el control interno de “Alta”, un riesgo de auditoría de 1,6667 “Bajo”, dando un enfoque de auditoría hacia pruebas de cumplimiento.

Del primer dominio relacionado con COBIT (PO) Planificar y Organizar, se desarrolla el proceso PO4.11 Segregación de funciones que manifiesta:

> *"Implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico.- La gerencia también se asegura de que el personal realice sólo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas.".*

Como se explica en el punto 3.3.1, el auditor deberá estructurar su hallazgo, partiendo del cumplimiento de las normas de Control Interno (COSO I) y relacionándolos con COBIT para lograr recomendaciones que generen valor agregado. Es decir, con la finalidad de cumplir con estándares internacionales, se debe orientar las recomendaciones en base a las metas de COBIT, descritas en niveles para:

"…el negocio… TI… el proceso… la actividad.".

Bajo el marco de trabajo de COBIT, las metas del negocio determinan las metas de TI, las que a su vez determinan las metas del proceso de TI que tienen relación con las metas de actividad, lo que quiere decir que si se logran las metas de más bajo nivel, las metas de actividad, se asegura el cumplimiento de las metas del siguiente nivel, metas del proceso y éstas a su vez del siguiente, metas de TI, para así lograr las metas del negocio.

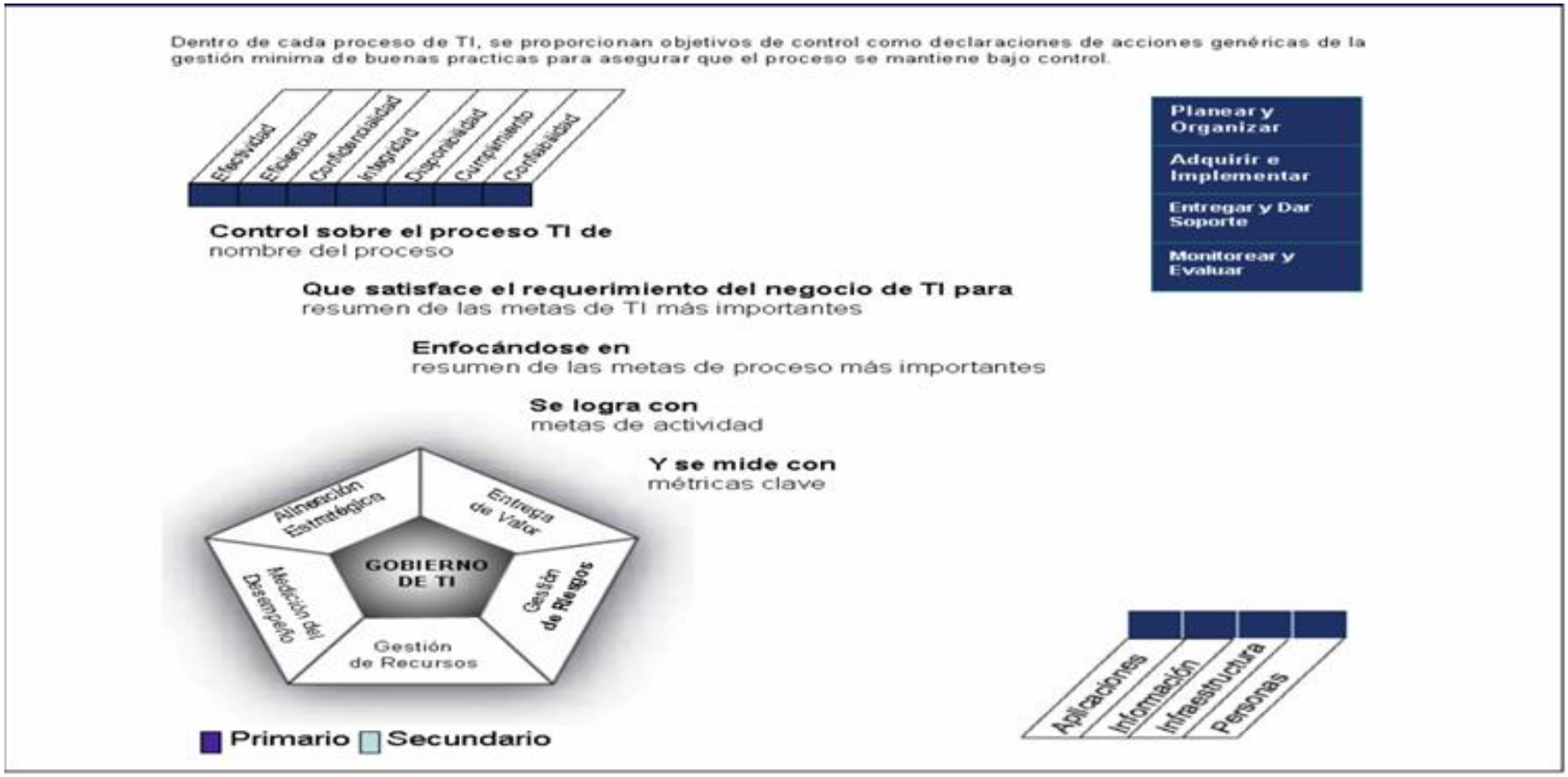

Figura 3: Navegación en COBIT

Fuente: (ISACA Governance Institute, 2005)

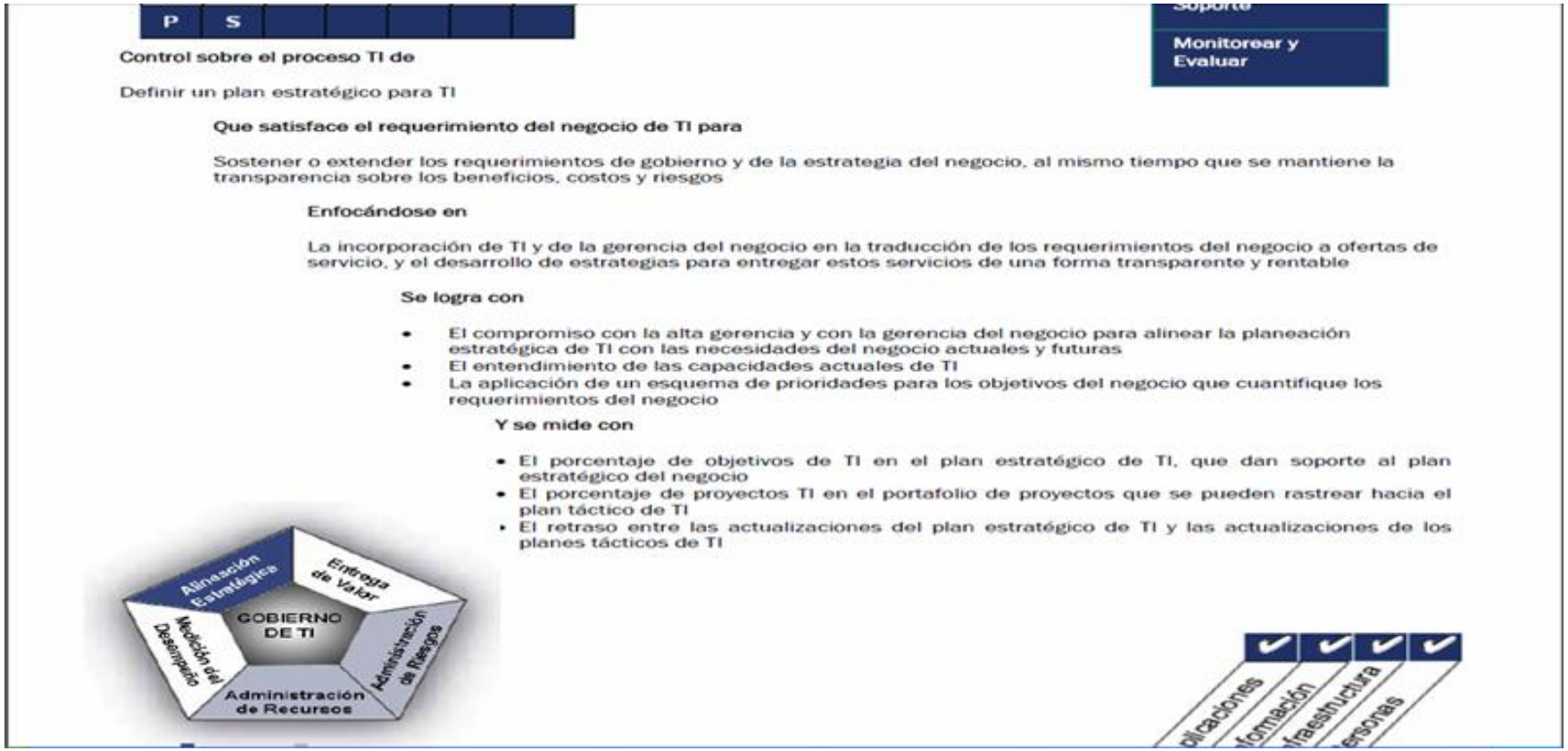

Figura 4: Descripción del Proceso PO4 de COBIT:
Fuente: (ISACA Governance Institute, 2005)

El autor sugiere para la evaluación de TI, hacer la medición de las metas de actividad con las métricas claves que COBIT señala para cada proceso.

COBIT detalla las metas de actividad bajo el subtítulo: "*se logra con"* y las métricas clave, bajo el subtítulo: "*se mide con".*

Para el proceso P04, resulta:

> *"…La definición de un marco de trabajo de procesos de TI.- El establecimiento de un cuerpo y una estructura organizacional apropiada.- La definición de roles y responsabilidades.".*

COBIT señala métricas clave, bajo el subtítulo: "*se mide con"*, donde igualmente, se describen:

> *"…El porcentaje de roles con descripciones de puestos y autoridad documentados.- El número de unidades como numerador y los procesos del negocio que no reciben soporte de TI y que deberían recibirlo, como denominador.- El número de actividades clave de TI fuera de la organización de TI que no son aprobadas y que no están sujetas a los estándares organizacionales de TI.".*

Ejemplo con P04: "Definir los Procesos, Organización y Relaciones de TI":

El control sobre el proceso TI, según COBIT es: "Definir los procesos, organización y relaciones de TI": que satisface el requerimiento del negocio de TI para: "Agilizar la respuesta a las estrategias del negocio mientras se cumplen los requerimientos de gobierno y se establecen puntos de contacto definidos y competentes"; enfocándose en: "El establecimiento de estructuras organizacionales de TI transparentes, flexibles y responsables, y

en la definición e implementación de procesos de TI con dueños, y en la integración de roles y responsabilidades hacia los procesos de negocio y de decisión"; y, Se logra con: "La definición de un marco de trabajo de procesos de TI. El establecimiento de un cuerpo y una estructura organizacional apropiada y la definición de roles y responsabilidades"; finalmente según COBIT, este proceso se mide con: "El porcentaje de roles con descripciones de puestos y autoridad documentados.- El número de unidades/procesos de negocio que no reciben soporte de TI y que deberían recibirlo, de acuerdo con la estrategia.- Número de actividades clave de TI fuera de la organización de TI que no son aprobadas y que no están sujetas a los estándares organizacionales de TI.".

1.13 MATRIZ SISTEMÁTICA DE EVALUACIÓN DE LA GESTIÓN EN LAS UNIDADES DE TECNOLOGÍAS DE LA INFORMACIÓN

El autor propone utilizar lo que denomina la Matriz Sistemática de Evaluación de la Gestión en las Unidades de Tecnologías de la Información, donde el Supervisor y el Jefe de Equipo evidenciarán la evaluación de control interno y la calificación del riesgo, según los siguientes pasos:

1. Evaluación del cumplimiento de la Normas de Control Interno emitidas por la Contraloría General del Estado, fundamentadas en COSO I.
2. Evaluación del riesgo de auditoría; y,
3. El enfoque que se debe dar en un examen especial a las áreas críticas.

Como se describe en el cuadro siguiente, la evaluación de control interno total, calificó a la norma 410 Tecnologías de la Información mediante un nivel de confianza alto, con un puntaje de 3 y un riesgo de auditoría de 2.1 “Moderado”. Lo que permite enfocar los procedimientos sustantivos de auditoría.

Por cuestiones de reserva en la información de la entidad auditada, se visualiza solo la ponderación de la Norma de control Interno 410.4 “Políticas y Procedimientos”.

Para estructurar las recomendaciones, el autor sugiere relacionar las debilidades detectadas al verificar el cumplimiento de las Normas de Control Interno y relacionarlas con las metas de actividad y las métricas claves de cada proceso de COBIT, como se detalla en el siguiente análisis que es parte del anexo 5.

Cuadro 13:
Metas y métricas de COBIT vs. Procedimientos y recomendaciones de auditoría:

RELACIÓN DE LAS DEBILIDADES DETECTADAS AL VERIFICAR EL CUMPLIMIENTO DE LAS NORMAS DE CONTROL INTERNO CON LAS METAS DE ACTIVIDAD Y LAS MÉTRICAS CLAVES DE CADA PROCESO DE COBIT (ANEXO 5).

PROCESO	METAS DE ACTIVIDAD	MÉTRICAS CLAVE INDICADORES DE DESEMPEÑO	PROCEDIMIENTO DE AUDITORIA PARA COMPROBAR LOS MEDIDORES DE COBIT	MODELOS DE RECOMENDACIONES BASADOS EN LOS PROCESOS DE COBIT (A la máxima autoridad de TI)
P01 Definir un Plan Estratégico de TI	• El compromiso con la alta gerencia y la gerencia del negocio para alinear la planeación estratégica de TI con las necesidades del negocio actuales y futuras	• El porcentaje de objetivos de TI en el plan estratégico de TI, que dan soporte al plan estratégico del negocio	Compruebe el porcentaje de objetivos de TI en el plan estratégico de TI, que dan soporte al plan estratégico del negocio.	Informará periódicamente a los niveles de decisión gerencial sobre las capacidades de TI y coordinará su alineamiento a la planificación estratégica, en base a las necesidades para el cumplimiento de objetivos Institucionales a corto, mediano y largo plazo.
	• El entendimiento de las capacidades actuales de TI	• El porcentaje de proyectos TI en el portafolio de proyectos que se pueden rastrear hacia el plan táctico de TI	Analice la incidencia de los proyectos TI en el portafolio de proyectos de la entidad y en el plan táctico de TI	La máxima autoridad de TI mantendrá un esquema de prioridades para el cumplimiento de los objetivos de la entidad, que cuantifique los requerimientos de TI.
	• La aplicación de un esquema de prioridades para los objetivos del negocio que cuantifique los requerimientos del negocio	• El retraso entre las actualizaciones del plan estratégico de TI y las actualizaciones de los planes tácticos de TI	Compruebe la actualización de los planes estratégico y táctico de TI	

Fuente: Metas de Actividad y Métricas de COBIT: (ISACA Governance Institute, 2005): Procedimientos y Recomendaciones de Auditoría,

1.14 COMUNICACIÓN

Durante el transcurso del examen el auditor o evaluadores, deberán constantemente comunicar a los evaluados sobre los posibles hallazgos con la finalidad de brindarle el derecho a la defensa y cumplir el debido proceso.

Se comunica mediante oficios dirigidos a la persona a quien se quiere hacer la solicitud de información adicional o comunicar el posible hallazgo, deberá recabar su firma de recepción en la copia del oficio y cerciorarse que es la misma firma que consta en su cédula de identidad. Esta verificación se hace en las notificaciones de inicio de examen, en las comunicaciones de resultados, en la convocatoria a la Conferencia Final de Comunicación de Resultados y en los oficios que sea necesaria la evidencia de su recepción.

El Jefe de Equipo, deberá manejar una numeración secuencial de los oficios que emite en el detalle de comunicaciones enviadas.

Narración de los hallazgos

El informe contiene comentarios, conclusiones y recomendaciones. En un comentario se narra el hallazgo de auditoría tomando en cuenta los cuatro atributos que son: condición, criterio, causa y efecto. Seguidamente se detalla la parte del comentario que evidencia que se dio a los auditados el derecho a la defensa y consiste en dejar indicado el oficio con el cual se comunicó individualmente a cada posible responsable del hallazgo, para que envíe al equipo de auditoría, información adicional al respecto. Se dejará

constancia en esta parte del comentario, las opiniones remitidas por los auditados.

Si es necesario a continuación se detalla las acciones tomadas por la entidad al respecto del comentario y otras opiniones relevantes.

A continuación, en base al análisis descrito en la Matriz Sistemática de la Evaluación de TI, anexo 2, se desarrolla un comentario, respecto de: “Las políticas y procedimientos para ejecutar el Plan Estratégico de Tecnología de la información”.

Evaluación al cumplimiento de las NCI (COSO I)						RIESGO DE AUDITORÍA					ENFOQUE DE LA AUDITORÍA
NORMA DE CONTROL INTERNO 410 TECNOLOGÍAS DE LA INFORMACIÓN	PT PONDERACIÓN (entre 1 y 10)	CT CALIFICAC (entre 15 y 95)	CP PORC CP=CT x 100	NIVEL DE CONFIANZA	OBSERVACIONES / FACTORES DE RIESGO DE AUDITORÍA	INHERENTE	DE CONTROL	DE DETECCIÓN	RIESGO DE AUDITORÍA	VALORACIÓN CUALITATIVA	
TOTAL NCI 410	1,0	83,8	83,1	ALTO		1,2	2,4	2,5	2,1	MODERADO	SUSTANTIVAS
410-04 Políticas y procedimientos	1,1	32,0	28,0	BAJO	La DIR de TI no cuenta con políticas y procedimientos aprobados.	3,0	1,0	2,7	2,2	MODERADO	SUSTANTIVAS
¿Las políticas y procedimientos que permiten organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria,	2,0	60,0	30,0	BAJO	Tecnologías de la Información no cuenta con políticas y procedimientos aprobados formalmente.	1,0	1,0	1,0	1,0	BAJA	NO AMERITA

CONTINUA

fueron aprobados formalmente por la máxima autoridad?											
¿La Unidad de Tecnología de Información definió, documentó y difundió las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización?	1,0	15,0	15,0	BAJO	Faltan políticas, estándares y procedimientos que regulen las actividades.	3,0	1,0	3,0	2,3	MODERADO	SUSTANTIVAS

Figura 5: Desarrollo de un ejemplo de hallazgo

Título del comentario: La entidad no cuenta con procedimientos aprobados en el área de Tecnologías de la Información

(Solo con fines de aclarar la presente Guía, se incluyen los subtítulos: condición, criterio, causa, efecto, derecho a la defensa).

Condición.-

La Dirección de Tecnologías de la Información de la entidad, no cuenta con políticas y procedimientos aprobados,

Efecto.-

Lo que no le permitió organizar formalmente el área de tecnología, asignar el talento humano calificado según sus competencias, definir los estándares y responsables de su cumplimiento, así como el control permanente de procesos para asegurar el cumplimiento de su gestión.

Causa.-

Este hecho se produce debido a que el Director de TI no coordinó con la Sección Encargada de la Entidad, la definición y aprobación oficial de un marco de trabajo con una estructura organizacional, relaciones de procesos y productos de TI, tales como un modelo de información o un diccionario de datos corporativo.

Criterio.-

Al respecto la Norma de Control Interno 410 – 04 políticas y procedimientos y 410 – 12 Administración de soporte de tecnología de la Información,

disponen la aprobación e implantación de políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información, asignar el talento humano calificado y definir procedimientos de operación y mecanismos para soporte técnico, encriptación y autenticación.

Derecho a la defensa

Mediante oficio PR-0045-WV-2013 de 14 de diciembre de 2012, se comunicó al Director de Tecnologías de la Información sobre la ausencia de políticas y procedimientos aprobados.

Conclusión

La Dirección de Tecnologías de la Información de la Entidad, no cuenta con políticas y procedimientos aprobados, lo que no le permite organizar formalmente el área de tecnología, debido a que el Director de TI no coordinó con la Sección encargada de la Entidad.

Recomendación

Al Director de Tecnología de la Información

Coordinará con la Sección Encargada de la Entidad, la definición de un marco de trabajo para el proceso de TI, que permita definir formalmente las políticas y procedimientos para ejecutar el plan estratégico de TI, con una estructura y relaciones de procesos definidas, con la finalidad de asegurar la medición del desempeño y el cumplimiento de metas, orientadas hacia las políticas de la Entidad.

Leer el borrador del Informe en la Conferencia Final de Comunicación de Resultados

Finalizado el estudio se hará conocer los resultados del examen, mediante una reunión de trabajo. En esta reunión, las discrepancias de criterio se presentarán documentadamente, los que se agregarán al informe si amerita su contenido.

Se enviará la convocatoria para la lectura del borrador del informe, por lo menos con 48 horas de anticipación indicando el lugar, día y hora de la reunión. La conferencia final será presidida por el jefe de equipo o por el funcionario delegado expresamente por el Contralor General del Estado.

En la conferencia final serán convocados y participarán las siguientes personas: La máxima autoridad de la entidad examinada o su delegado, los servidores, y ex servidores y quienes por sus funciones o actividades estén vinculados a la materia objeto del examen, e máximo directivo de la unidad de auditoría responsable del examen, el supervisor que actuó como tal en el examen, el jefe de equipo de auditoría.

Al final de la Conferencia Final se firmará un acta para dejar constancia de lo actuado. En caso que algún funcionario se negare a suscribir el acta, el jefe de equipo dejará constancia del motivo de esta situación. Informe y trámite en la Evaluación de áreas de TI.

Informe y trámite en la Evaluación de Áreas de TI

Luego de cinco días laborables de realizada la conferencia final, el auditor preparará el informe definitivo, para lo cual, toma en cuenta los resultados obtenidos de las justificaciones presentadas oportunamente por los funcionarios de la entidad con la finalidad de dejar constancia de las opiniones presentadas en la lectura del borrador del informe.

En el mencionado Acuerdo 26 de la Contraloría General del Estado se expide el Reglamento para la elaboración trámite y aprobación de informes de auditoría disposiciones que se deben cumplir para emitir los informes de Evaluación de la Gestión de las Áreas de TI.

En el Acuerdo 26, mencionado, se describe la estructura y contenido de los informes que será la siguiente:

Como información anexa a los informes para el trámite se debe adjuntar:

El Director de la Unidad de Auditoría Interna, luego del control de calidad, suscribirá el informe definitivo para su envió a la Contraloría General del Estado, donde se lo aprobará.

Derecho a la Defensa en el proceso de Comunicación

En la Norma Ecuatoriana de Auditoría Gubernamental IAG – 04 relativa a la oportunidad en la comunicación de resultados, se dispone que el informe de auditoría gubernamental debe emitirse en forma oportuna a fin de que permita la toma de las acciones correctivas en forma inmediata y la EAG – 09 relativa a la comunicación de hallazgos de auditoría, dispone que durante el proceso de auditoría, tan pronto como se haya concluido el estudio y análisis de una actividad o componente el supervisor y el jefe de equipo deben comunicar el contenido de los hallazgos a las personas que tengan relación con los mismos, estén o no prestando servicios en la entidad examinada, a fin de que presenten sus aclaraciones o comentarios sustentados documentadamente para su evaluación y consideración en el informe. Se refiere a los hallazgos de auditoría como las posibles deficiencias o irregularidades identificadas como resultado de la aplicación de procedimientos de auditoría. Los resultados de las actividades de control realizadas, serán analizados únicamente con las personas involucradas en los hechos examinados y con las autoridades de la entidad.

En la Ley Orgánica de la Contraloría General del Estado su artículo 90 dispone sobre la notificación inicial y comunicación de resultados, la auditoría gubernamental se realizará de acuerdo con el plan de trabajo anual de la Contraloría General del Estado y previamente a su iniciación se notificará a las autoridades, funcionarios, servidores, ex servidores y demás personas vinculadas con el examen. En el curso del examen los auditores gubernamentales mantendrán comunicación con los servidores de la

entidad, organismo o empresa del sector público auditada y demás personas relacionadas con las actividades examinadas. Al finalizar los trabajos de auditoría de campo, se dejará constancia de que fue cumplida la comunicación de resultados y la conferencia final en los términos previstos por la ley y las normas profesionales sobre la materia. (Contraloría General del Estado, 2002)

En el artículo 24 del Reglamento a la Ley Orgánica de la Contraloría General del Estado se dispone que los resultados obtenidos hasta la conclusión del trabajo en el campo, de toda actividad de control, constarán, en el respectivo borrador de informe que será analizado en la conferencia final, por los auditores gubernamentales actuantes, los representantes de la entidad objeto del examen y todas las personas vinculadas con el mismo y que cualquier información explicativa o documentos justificativos que los asistentes o vinculados con el examen, deseen presentar, lo realizarán durante los 5 días laborables posteriores a la conferencia final y mediante comunicación dirigida al máximo directivo de la unidad de control responsable del trámite del informe definitivo. Así mismo determina que se dejará constancia de la participación y de la asistencia de los convocados a la comunicación de los resultados obtenidos, en la conferencia final, en original y copia, un acta de la conferencia final. (Decreto Ejecutivo 548, 2003)

En el Reglamento de Responsabilidades emitido por la Contraloría General del Estado, mediante Acuerdo de la CGE 26, publicado en el Registro Oficial 386 del 27 de octubre de 2006, en su artículo 10 dispone sobre lo relativo a la comunicación con los auditados que para la ejecución de la auditoría gubernamental se notificará el inicio del examen, se comunicará los resultados parciales y se convocará a la conferencia final, de conformidad con lo estipulado en los artículos 20, 21, 22 y 23 del Reglamento de la Ley Orgánica de la Contraloría General del Estado, a las autoridades, dignatarios, funcionarios y demás servidores de las instituciones del Estado, a los personeros, directivos, empleados, trabajadores y representantes de las personas jurídicas y entidades de derecho privado con participación estatal en funciones y a aquellas que han dejado de desempeñarlas por cesación definitiva de las mismas.

CAPÍTULO IV.- CONCLUSIONES Y RECOMENDACIONES

1.15 CONCLUSIONES

1. Se desarrolló la guía para evaluar la gestión del área de tecnologías de la información en el sector público, con el componente de COSO: “Actividades de control”, que la Contraloría General del Estado desarrolló en el grupo de Normas Técnicas de Control Interno 410 “Tecnologías de la Información”, emitidas, en el Acuerdo 39, publicado en el Registro Oficial 87 del 14 de diciembre de 2009. Esta Guía, mediante la aplicación de la matriz propuesta, contribuye a determinar las áreas críticas relacionadas con los objetivos de control descritos en los dominios de COBIT por lo que se facilita la generación de acciones correctivas que encajan en el marco de trabajo propuesto para las TI.
2. Con una guía metodológica, se logró una combinación adecuada para evaluar un área de Tecnologías de la Información aplicando los componentes de COSO y las Normas Técnicas de Control Interno emitidas por la Contraloría General del Estado con los controles básicos a un área de TI descritos en los cuatro dominios de COBIT.
3. La guía desarrollada se validó mediante su aplicación en una Entidad Pública y los resultados de esta evaluación se describen en el anexo 2, con una matriz que consta de tres partes: la evaluación al cumplimiento de las normas de control interno vigentes en el sector público ecuatoriano; la calificación del riesgo de auditoría y el enfoque de auditoría basado en los riesgos.

4. Se realizó una evaluación del área de TI; y, se ejecutaron los procedimientos que se aplican en la primera y tercera fases de una auditoría o examen especial, es decir en la fase de planificación y comunicación. Como dispone la Contraloría General del Estado, se concluyó la primera fase al identificar áreas críticas por intermedio de la evaluación de control interno, basados en la normativa vigente y en los controles de COBIT. Además se cumplió la tercera fase de comunicación dando énfasis al derecho a la defensa y debido proceso en auditoría.
5. Se implementó una matriz que orienta a estructurar el Programa de Auditoría donde se describen los lineamientos para: distribuir tareas. definir las responsabilidades y funciones de supervisores y auditores gubernamentales independientes; y/o, personal de controladores o verificadores de la misma área de tecnologías de la información, orienta la aplicación de pruebas de auditoría a las áreas críticas de TI.
6. Con esta Guía se contribuyó a evidenciar los hallazgos, basados en la brecha existente, entre lo que se deseó en TI y el grado de madurez encontrado, mediante la aplicación de metas y métricas descritos en COBIT, con la emisión de un informe con comentarios, conclusiones y recomendaciones.
7. La guía orientó el cumplimiento de la fase de Comunicación de Resultados, lo que implicó, asegurar que se brinde el derecho a la defensa de los auditados.

8. Con respecto a la aplicación de COBIT, en las entidades evaluadas, no se alcanzó el grado de madurez necesario, por no existir la obligación legal emitida por la Contraloría General del Estado para implantar el marco de trabajo sugerido en COBIT.
9. Al contar con una guía que permitió cumplir con las exigencias de la auditoría gubernamental y que garantizó la presentación de resultados de manera transparente y con objetividad; se alcanzó la seguridad razonable de que se aplicaron los mejores principios y políticas de auditoría y evaluación de TI, generalmente aceptados a nivel internacional.
10. Se logró la especialización y profundidad que se requiere en materia de control a las Tecnologías de la Información al aplicar estándares internacionales descritos en COBIT.
11. Se cumplió lo dispuesto en los artículos 211 y 212 por medio de los cuales la Contraloría General del Estado, como organismo técnico de control de los recursos públicos, dirige el sistema de control administrativo que se compone de auditoría interna, auditoría externa y del control interno de las entidades del sector público.

1.16 RECOMENDACIONES

1. Se analizó dos de las tres fases de auditoría, esto es la Planificación y la Comunicación, por lo que como complemento a esta Guía de Evaluación de la Gestión de Tecnologías de la Información con aplicación de COBIT y COSO en el Sector Público Ecuatoriano, se debería completar el estudio y estructurar una Guía de Auditoría de Gestión a Tecnologías de

la Información, con las tres fases de la auditoría, utilizando COBIT y COSO, esto es: la planificación, la ejecución y la comunicación, poniendo énfasis en la segunda, (Ejecución), para desarrollar procedimientos técnicos.

2. Se sugiere aplicar estándares internacionales descritos en COBIT y la combinación de procedimientos descritos en las Normas de Auditoría Generalmente Aceptadas, con técnicos independientes y auditores gubernamentales que generen resultados y acciones correctivas, llegando incluso al establecimiento de responsabilidades.
3. Los auditores y evaluadores del área de Tecnologías de la Información, que utilicen esta Guía, se sugiere que comuniqués a los auditados, que la evaluación al área de TI, es el primer paso fundamental para establecer áreas críticas, a las cuales se podría aplicar un examen especial o auditoría de gestión si es del caso, para llegar a establecer posibles responsabilidades, de existir efectos relevantes, perjuicio económico o indicios de responsabilidad penal por el cometimiento de delitos tipificados en la Ley.
4. Se debería comprobar que las preguntas utilizadas en la Matriz de Evaluación Sistemática de la Gestión de TI sean aplicables al grado de madurez del área de TI. Es conveniente que el evaluador analice cuidadosamente cada pregunta y ponderar la relevancia de cada ítem, antes de calificar con el nivel que más se ajuste a la realidad.

5. Es necesario que conforme a la normativa legal vigente, los auditores y evaluadores que usen esta Guía, procuren dar el derecho a la defensa a los auditados, comunicando constantemente los resultados provisionales para tener los elementos de juicio suficientes y hallazgos definitivos. Se les comunicará en una Conferencia Final donde se procederá a leer los resultados provisionales de la evaluación.
6. Se sugiere que los evaluadores realicen recomendaciones a los directamente relacionados con las acciones correctivas mediante reuniones de trabajo previas, sin recomendar el cumplimiento de leyes y reglamentos, que son de cumplimiento obligatorio.
7. Es necesario que realicen el seguimiento de recomendaciones producto de la aplicación de esta Guía y brinden asesoramiento en el cumplimiento de normas legales del país y estándares internacionales aceptados a nivel mundial.

1.17 Bibliografía

Acuerdo 012 Manual Aud Gub, C. G. (6 de junio de 2003). Manual General de Auditoría Gubernamental. *Acuerdo 012 - CG - 2003*. Quito, Pichincha, Ecuador: R.O. 107 (19/06/2003).

Acuerdo 016, C. G. (2001). Manual de Aditoría Financiera Gubernamental. *Acuerdo CGE*. Pichincha, Ecuador: CGE.

Acuerdo 026 Contraloría General del Estado. (2012). *Reglamento para la elaboración, trámite y aprobación de informes de auditoría.* Quito: CGE.

Acuerdo 18 Instructivo Órdenes Trabajo, C. G. (30 de junio de 2011). Instructivo para Órdenes de Trabajo de auditoría en Contraloría. *Acuerdo CGE 18*. Quito, Pichincha, Ecuador: registro Oficial.

Acuerdo 19, Contraloría General del Estado. (10 de octubre de 2002). Normas Ecuatorianas de Auditoría gubernamental. *Norma: Acuerdo de la Contraloría General del Estado 19*. Quito, Pichincha, Ecuador: Registro Oficial.

Acuerdo 19, Contraloría General del Estado. (10 de octubre de 2002). Normas Ecuatorianas de Auditoría Gubernamental. *Registro Oficial Suplemento 6; Acuerdo 19*. Quito, Pichincha, Ecuador: Registro Oficial.

Acuerdo 39, C. G. (14 de DICIEMBRE de 2009). Normas de Control Interno, NCI. *Acuerdo 39; Publicación*. Quito, Pichincha, Ecuador: Registro Oficial suplemento 87, Acuerdo 39.

Acuerdo 47, GUIA METODOLOGICA CGE. (2011). *GUIA METODOLOGICA PARA LA AUDITORIA DE GESTION DE LA CONTRALORIA.* Quito: Registro Oficial Suplemento 600.

CGE 18, C. G. (30 de junio de 2011). Instructivo para Órdenes de Trabajo de auditoría en Contraloría. *Acuerdo CGE 18*. Quito, Pichincha, Ecuador: registro Oficial.

Constitución. (2008). *Constitución de la República del Ecuador.* Montecristi, Manabí, Ecuador.

Contraloría General del Estado. (10 de octubre de 2002). Normas Ecuatorianas de Auditoría gubernamental. *Norma: Acuerdo de la Contraloría General del Estado 19*. Quito, Pichincha, Ecuador: Registro Oficial.

Contraloría General del Estado, R. O. (12 de junio de 2002). Ley Orgánica de la Contraloría General del Estado. *Registro Oficial Suplemento 595*. Quito, Pichincha, Ecuador: Registro Oficial Suplemento.

Decreto Ejecutivo 548, P. d. (07 de julio de 2003). Reglamento de la Ley Orgánica de la Contraloría General. *Decreto Ejecutivo 548*. Quito, Pichincha, Ecuador: Registro Oficial 119.

International Organization for Standardization. (2000). *Information technology.* La Organización Internacional de Normalización (ISO), Ginebra: ISO.

INTOSAI, O. I. (septiembre de 2004). *Guía para las Normas del Control Interno del Sector Público*. Recuperado el 16 de noviembre de 2012, de http://www.intosai.org: http://www.issai.org/media(594,1033)/INTOSAI_GOV_9130_S.pdf

ISACA Governance Institute, I. G. (2005). COBIT. Obtenido de http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf

Ley 73, C. N. (12 de junio de 2002). Ley Orgánica de la Contraloría General del Estado. *Registro Oficial Suplemento 595*. Quito, Pichincha, Ecuador: Registro Oficial Suplemento.

Norma ISO / IEC TR 13335 – 1 STANDARD, C. N. (26 de marzo de 2001). Canada National Standard Norma ISO. *Norma*. Canada, Canada: por – ISO / IEC.

Office of Government Commerce ITIL v3 Ministerio de Hacienda del Reino Unido. (2007). *ITIL v3.* Reino Unido: Ministerio de Hacienda.

Organizations, Commitee of Sponsoring. (1997). COSO I.

Organizations, Commitee of Sponsoring. (2004). COSO II.

Sociedad Hipotecaria Federal, S. D. (20 de febrero de 2004). *Procedimientos.* México, D.F: Sociedad Hipotecaria Federal, S.N.C.

Acuerdo 012 Manual Aud Gub, C. G. (2003, junio 6). Manual General de Auditoría Gubernamental. *Acuerdo 012 - CG - 2003*. Quito, Pichincha, Ecuador: R.O. 107 (19/06/2003).

Acuerdo 016, C. G. (2001). Manual de Aditoría Financiera Gubernamental. *Acuerdo CGE*. Pichincha, Ecuador: CGE.

Acuerdo 026 Contraloría General del Estado. (2012). *Reglamento para la elaboración, trámite y aprobación de informes de auditoría.* Quito: CGE.

Acuerdo 18 Instructivo Órdenes Trabajo, C. G. (2011, junio 30). Instructivo para Órdenes de Trabajo de auditoría en Contraloría. *Acuerdo CGE 18*. Quito, Pichincha, Ecuador: registro Oficial.

Acuerdo 19, Contraloría General del Estado. (2002, octubre 10). Normas Ecuatorianas de Auditoría gubernamental. *Norma: Acuerdo de la Contraloría General del Estado 19*. Quito, Pichincha, Ecuador: Registro Oficial.

Acuerdo 19, Contraloría General del Estado. (2002, octubre 10). Normas Ecuatorianas de Auditoría Gubernamental. *Registro Oficial Suplemento 6; Acuerdo 19*. Quito, Pichincha, Ecuador: Registro Oficial.

Acuerdo 39, C. G. (2009, DICIEMBRE 14). Normas de Control Interno, NCI. *Acuerdo 39; Publicación*. Quito, Pichincha, Ecuador: Registro Oficial suplemento 87, Acuerdo 39.

Acuerdo 47, GUIA METODOLOGICA CGE. (2011). *GUIA METODOLOGICA PARA LA AUDITORIA DE GESTION DE LA CONTRALORIA.* Quito: Registro Oficial Suplemento 600.

CGE 18, C. G. (2011, junio 30). Instructivo para Órdenes de Trabajo de auditoría en Contraloría. *Acuerdo CGE 18*. Quito, Pichincha, Ecuador: registro Oficial.

Constitución. (2008). *Constitución de la República del Ecuador.* Montecristi, Manabí, Ecuador.

Contraloría General del Estado. (2002, octubre 10). Normas Ecuatorianas de Auditoría gubernamental. *Norma: Acuerdo de la Contraloría General del Estado 19*. Quito, Pichincha, Ecuador: Registro Oficial.

Contraloría General del Estado, R. O. (2002, junio 12). Ley Orgánica de la Contraloría General del Estado. *Registro Oficial Suplemento 595*. Quito, Pichincha, Ecuador: Registro Oficial Suplemento.

Decreto Ejecutivo 548, P. d. (2003, julio 07). Reglamento de la Ley Orgánica de la Contraloría General. *Decreto Ejecutivo 548*. Quito, Pichincha, Ecuador: Registro Oficial 119.

International Organization for Standardization. (2000). *Information technology.* La Organización Internacional de Normalización (ISO), Ginebra: ISO.

INTOSAI, O. I. (2004, septiembre). *Guía para las Normas del Control Interno del Sector Público*. Retrieved noviembre 16, 2012, from

http://www.intosai.org: http://www.issai.org/media(594,1033)/INTOSAI_GOV_9130_S.pdf

ISACA Governance Institute, I. G. (2005). COBIT. Retrieved from http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf

Ley 73, C. N. (2002, junio 12). Ley Orgánica de la Contraloría General del Estado. *Registro Oficial Suplemento 595*. Quito, Pichincha, Ecuador: Registro Oficial Suplemento.

Norma ISO / IEC TR 13335 – 1 STANDARD, C. N. (2001, marzo 26). Canada National Standard Norma ISO. *Norma*. Canada, Canada: por – ISO / IEC.

Office of Government Commerce ITIL v3 Ministerio de Hacienda del Reino Unido. (2007). *ITIL v3.* Reino Unido: Ministerio de Hacienda.

Organizations, Commitee of Sponsoring. (1997). COSO I.

Organizations, Commitee of Sponsoring. (2004). COSO II.

Sociedad Hipotecaria Federal, S. D. (2004, febrero 20). *Procedimientos.* México, D.F: Sociedad Hipotecaria Federal, S.N.C.