UNIVERSIDAD MAYOR DE SAN ANDRES
FACULTAD DE CIENCIAS ECONOMICAS Y FINANCIERAS
CARRERA DE AUDITORÍA

TESIS DE GRADO

"UN ENFOQUE METODOLÓGICO PARA AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES CASO: REGISTRO ÚNICO PARA LA ADMINISTRACIÓN TRIBUTARIA MUNICIPAL"

POSTULANTE: Janhett Ramos Maldonado

TUTOR: Dr. Luís Adalid Aparicio Delgado Ph. D.

LA PAZ – BOLIVIA

2012

INDICE

CAPITULO I
INTRODUCCIÓN

1.1 INTRODUCCIÓN

El avance continuo de la tecnología ofrece una gama de herramientas para la administración de los sistemas de información, que posibilita mejorar el servicio tanto en el ámbito privado y gubernamental.

Con relación a la administración pública de nuestro país, se denota que los procesos en áreas críticas están siendo automatizados de manera gradual, a través de recursos tecnológicos, como ser; adquisición de equipos informáticos, infraestructura tecnológica, desarrollo de sistemas de información, construcción de bases de datos, entre otros, este escenario está generando un ambiente propicio para el desarrollo de auditorías a los sistemas de información y las tecnologías que las soportan con el fin de determinar la eficacia y/o eficiencia de tales tecnologías, del control interno asociando a éstas, así como de la consecución de sus objetivos institucionales, de tal forma de promover en el sector público la mejora en la gestión y uso de los recursos públicos.

1.2 ANTECEDENTES DE LA INVESTIGACIÓN

Efectuada la recopilación de los antecedentes sobre el desarrollo de auditorías informáticas en el ámbito gubernamental, desde la promulgación (gestión 2005) de las Normas de Auditoria de Tecnologías de la Información y Comunicación (TIC) emitida por la Contraloría General del Estado (CGE) se tiene 14 auditorías desarrolladas a la fecha[1].

En base a la estadística obtenida de la CGE, se puede inferir que aun las unidades de auditoría interna dependientes del ámbito gubernamental no ejecutaron auditorias TIC, en parte se debe a que no cuentan con procedimientos para la ejecución de auditorías TIC.

[1] Contraloría General del Estado

Revisado los temas relacionados en la Biblioteca de la Facultad de Auditoria, se realizaron los siguientes trabajos:

TITULO	AUTOR	AÑO DE EDICIÓN
Auditoría técnica operativa de sistemas informáticos como un instrumento de control confiable de la facturación telefónica.	Canaviri Limachi Lucio	2002
Metodologías para la auditoria a los sistemas de información y la tecnología que las soporta de las entidades financieras bancarias del país	Landivar Portugal, Freddy	2002
Evaluación de los Sistemas de Información y su Tecnología como base para determinar el grado de confianza en el procesamiento de la Información Financiera	Celis Rioja, José Arturo	2005

FUENTE: BIBLIOTECA UMSA - FACULTAD DE AUDITORIA

1.3 PLANTEAMIENTO DEL PROBLEMA

En el momento actual que vive la humanidad y nuestro país por los efectos de la globalización económica, el avance de las tecnologías de información y las comunicaciones; lenguajes de programación, sistemas operativos, software, hardware y telecomunicaciones para la administración de los sistemas de información, éstos se convirtieron en elementos estratégicos para mejorar los requerimientos de la administración pública y apoyar a la toma de decisiones a nivel ejecutivo.

A fin de afrontar los riesgos y ejercer un mejor control gubernamental en la administración pública, la Contraloría General del Estado, ha emitido entre las normas específicas, **las Normas de Auditoría de Tecnologías de la Información y la Comunicación** a objeto de evaluar la eficacia y/o eficiencia de las tecnologías, del control interno asociado a éstas, así como de la consecución de sus objetivos en relación a los objetivos institucionales para mejorar la gestión y el uso de los recursos tecnológicos del sector público.

Sin embargo, *aún existen vacíos* para la ejecución de auditorías de sistemas de información en la administración pública, en ese entendido si surgiesen aspectos no contemplados en las Normas de Auditoría Gubernamental, deben observarse

las Normas Generales de Auditoría de Sistemas de Información emitidas por la Asociación de Auditoría y Control de Sistemas de Información ISACA[2]. Sus estándares tienen amplio reconocimiento internacional, se caracterizan prácticamente a la par del avance de la tecnología, asimismo desarrollaron un estándar para el control interno de sistemas de información denominado Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT)[3] que la misma norma exige para las unidades de auditoría interna en la administración pública.

1.4 FORMULACIÓN DEL PROBLEMA

¿Es factible proponer un enfoque metodológico que posibilite la ejecución de auditorías de tecnologías de la información y comunicaciones en el marco de las Normas de Auditoria Gubernamental con el apoyo de estándares internacionales que nos permita controlar, evaluar el **gobierno de tecnologías de información**[4] en la administración pública a fin de validar, especializar y jerarquizar la credibilidad en la emisión de *una opinión independiente* sobre los criterios de control de la información llevados a través de medios tecnológicos?

Por tanto, la aplicación de normas y procedimientos adecuados que tenga mayor alcance, que goce de su propia jerarquía y desarrollo harán posibles estos objetivos. Las fuentes para desarrollar los procedimientos estarán en función de:

1. Ley Nº 1178 “Ley de Administración y Control Gubernamental”.
2. Decreto Supremo Nº 23215 “Reglamento para el Ejercicio de atribuciones de la Contraloría General del Estado**”.**
3. Normas de Auditoría Gubernamental emitidas por la Contraloría General del Estado.

[2] ISACA “Information Systems Audit and Control Associaton”, ver: www.isaca.org/cobit
[3] **COBIT** “Control Objetive for Information and related Technology”. Ver pg. web www.isaca.org
[4] **Gobierno de TI (IT Governance)** Governance es un término que representa el sistema de control o administración que establece la alta gerencia para asegurar el logro de los objetivos del negocio. Manual de preparación al examen CISA 2008, Estados Unidos, 2008

4. Normas de Auditoría de Tecnologías de la Información y Comunicación emitidas por la Contraloría General del Estado.
5. Normas de Auditoría de Sistemas de Información y metodología COBIT emitida por ISACA.
6. Otros estándares; ISO 27001 “Sistema de Gestión de Seguridad de la Información – Requisitos”, ISO 27002 “Técnicas de Seguridad – Código de práctica para la gestión de seguridad de la información”.

1.5 OBJETIVOS

a) Objetivo General

Elaboración y sistematización de un enfoque metodológico para la ejecución de auditorías de tecnologías de la información y comunicación en el marco de las Normas de Auditoría Gubernamental de Tecnologías de la Información y Comunicación con el apoyo de estándares internacionales para las entidades públicas y hacer posible la emisión de una opinión independiente.

b) Objetivos Específicos

- Relevar y comprender los conceptos básicos y la importancia de la Norma de Auditoría de Tecnologías de la Información y la Comunicación en los procesos tecnológicos de la administración pública.
- Entender la metodología COBIT, propuesta por ISACA para la evaluación de auditorías de tecnologías de la información y comunicación.
- Elaborar procedimientos que posibiliten el desarrollo de auditorías informáticas.

1.6 HIPÓTESIS

a) Planteamiento de la Hipótesis

“La aplicación de un enfoque metodológico basado en las Normas de Auditoría de Tecnologías de la Información y Comunicación promulgada por la Contraloría General del Estado y con el apoyo de estándares internacionales emitida por ISACA para la ejecución de auditorías de tecnologías de la información y

comunicación en Unidades de Auditoría Interna de la administración pública, por profesionales o firmas de auditoría o consultoría especializada, posibilita *una adecuada evaluación* de las tecnologías de la información a objeto de emitir una opinión independiente sobre el cumplimiento de los criterios de la información, al uso eficaz de los recursos tecnológicos, requerimientos legales y la efectividad del sistema de control interno asociado a las mismas".

b) Comprobación de la hipótesis

i) Variable Independiente (Causa)

Aplicación de metodologías para la ejecución de las Auditorías de Tecnologías de la Información y Comunicación en entidades públicas.

ii) Variable Dependiente (Efecto)

Adecuado control de los sistemas de información y mejor rendimiento de los recursos de la administración pública.

1.7 JUSTIFICACIÓN BASE DEL TEMA

El efecto de la globalización, la nueva economía y la evolución incesante de la ciencia tecnológica y comunicación, están cambiando de manera significativa el ambiente de las organizaciones privadas y públicas a nivel mundial. En esta última década, Bolivia también es participe de estos cambios en especial en el ámbito público, con la finalidad de mejorar la gestión de los sistemas de información la calidad de servicio a la sociedad y estar a la par con el entorno internacional; sin embargo, el uso inadecuado de los recursos tecnológicos y la ausencia de controles implica riesgos de seguridad y de eficiencia que puede afectar el entorno económico, financiero, social, legal y político del Estado.

La incorporación de Tecnologías de Información y Comunicación en el sector público están generado un ambiente propicio para la ejecución de auditorías de esta naturaleza. En ese entendido, es factible la aplicación de criterios que nos permita evaluar y determinar la eficacia y/o eficiencia de uso de las tecnologías a fin de eliminar los riesgos.

a) Justificación Científica

Con la aplicación de las Normas de Auditoría de Tecnologías de la Información y Comunicación en la administración pública y con el apoyo de estándares internacionales, se pretende cubrir vacíos sobre el desconocimiento de metodologías que coadyuvarán a la evaluación de los sistemas de información y de las tecnologías que las soportan.

b) Justificación Económica

El control y la evaluación de los recursos tecnológicos; aplicaciones, información, infraestructura y recursos humanos en la administración pública permitirán evitar costes económicos innecesarios. Estas irregularidades afectan no solo al normal funcionamiento de las entidades auditadas, también afectan a la Cuenta de Pérdidas y Ganancias de los Estados Financieros.

c) Justificación Social

Con el avance continuo de las tecnologías y sus ventajas estratégicas que ofrecen para administrar los sistemas de información, es necesario implantar procedimientos de evaluación y control para los procesos administrativos y operativos de las entidades públicas a fin de minimizar los riesgos (vulnerabilidades y amenazas) y evitar el uso ilícito de las mismas.

El enfoque metodológico pretende obtener una opinión razonable sobre el uso de los recursos tecnológicos del Estado, mejorar la administración del gobierno de tecnologías de información y otorgar fiabilidad al entorno. Con la evaluación e implantación de controles adecuados a los sistemas de información y las tecnologías que las soportan proporcionaran una mejora continua para brindar un servicio de calidad a la sociedad.

d) Justificación Técnica

La aplicación de metodologías y estándares asociados para el desarrollo de las auditorías de tecnologías de información y comunicación nos permitirá elaborar un esquema tentativo para el desarrollo de las fases de una auditoría; relevamiento, planificación, ejecución y comunicación de resultados.

e) Justificación Legal

De acuerdo a las Normas de Auditoría Interna emitida por la Contraloría General de Estado, acápite Alcance de la auditoría interna punto 05 señala: *"La Unidad de Auditoría Interna debe contar con manuales de procedimientos de auditoría interna para el desarrollo de sus actividades."*

En tal sentido, el enfoque metodológico que se propone se plasmará en un conjunto de procedimientos que formarán parte del Manual de Procedimientos de una unidad de auditoría interna, el cual permitirá cumplir lo establecido con la norma.

1.8 ALCANCES Y APORTES DEL TEMA

a) Alcances

Las Normas de Auditoría Gubernamental son de aplicación obligatoria en la práctica de la auditoría realizada en toda entidad pública, por tanto para la aplicabilidad del presente trabajo de investigación se eligió el Registro Único para la Administración Tributaria Municipal (RUAT) ubicado en la ciudad de La Paz cuya misión es: *"Diseñar, desarrollar y administrar sistemas informáticos que permitan a los Gobiernos Municipales, Ministerio de Economía y Finanzas Publicas y Policía Nacional cumplir con las atribuciones conferidas por Ley en lo relativo a tributos e ingresos propios"*.[5]

Las Normas de Auditoría de Tecnologías de la Información y la Comunicación engloban una serie de especialidades, definida principalmente por sus objetivos y el alcance puede ser orientado hacia uno o varios de los siguientes enfoques:

1. Enfoque a las seguridades
2. Enfoque a la información
3. Enfoque a la infraestructura tecnológica
4. Enfoque al software de aplicación
5. Enfoque a las comunicaciones y redes

[5] Ver página web: www.ruat.gob.bo

b) Aportes

1. Proponer y facilitar un enfoque metodológico que coadyuve a la ejecución de las auditorías de tecnologías de información y comunicación en la administración pública.

2. Fortalecer en el ámbito gubernamental la aplicación de la Norma de Auditoría de Tecnologías de Información y Comunicación, acorde a las Normas de Auditoría Gubernamental promulgadas por la Contraloría General del Estado con el apoyo de las Normas de Auditoría de Sistemas de Información emitidas por ISACA.

3. Coadyuvar en la ejecución de auditorías de tecnologías de la información y la comunicación a las:
   - ✓ Unidades de Auditoría Interna de las entidades públicas
   - ✓ Auditorías externas
   - ✓ Consultarías, etc.

4. Impulsar el interés del Auditor Gubernamental a la especialización en el ámbito de la Auditoría de Tecnologías de la Información y Comunicaciones.

5. Incrementar el conocimiento en el área y servir de guía para los docentes, auditores, informáticos, ingenieros de sistemas, universitarios y público en general.

1.9 METODOLOGÍA Y HERRAMIENTAS DE INVESTIGACIÓN

El método es el medio por el cual se establece una relación entre el investigador y el objetivo de estudio.

El presente trabajo se desarrolló utilizando la metodología de la investigación científica que comprenderá el desarrollo de las siguientes etapas:

- ✓ Planteamiento del problema

- ✓ Elaboración del marco teórico
- ✓ Deducción de las consecuencias particulares
- ✓ La prueba de la hipótesis
- ✓ Conclusiones finales

a) Tipo de estudio

El método de investigación utilizado hipotético-deductivo, se basa en la utilización de una hipótesis que sirve de guía para la investigación y al mismo tiempo delimita el problema que se va a investigar.

b) Técnicas e instrumento

Las técnicas e instrumentos utilizadas para el logro de los objetivos de la presente investigación son los siguientes:

- ✓ Observación directa
- ✓ Exámenes de documentos
- ✓ Comparación
- ✓ Encuestas
- ✓ Entrevistas

c) Fuentes de información

Las siguientes son las fuentes de información que se emplearán para obtener información:

Primarias: Corresponde a la información obtenida del personal involucrado del área de sistemas y auditoría interna del Registro Único para la Administración Tributaria Municipal.

Secundaria: Se realizará la consulta a la bibliografía existente sobre la ejecución de auditoría de sistemas de información y normas vigentes en el ámbito gubernamental y páginas web oficiales del internet.

CAPITULO II
MARCO REGULATORIO

2.1 INTRODUCCIÓN

Inicialmente, para el conocimiento y comprensión del presente tema de investigación es muy importante abordar el marco regulatorio en el que se desenvuelve la auditoría gubernamental en la administración pública, asimismo cabe señalar que en la gestión 2009, Bolivia fue sujeta de cambios coyunturales por situaciones políticas, sociales y culturales que consecuentemente afectaron el marco jurídico, en ese entendido se procederá a detallar las Leyes, Normas y Decretos Supremos que regulan el Sistema de Control Gubernamental:

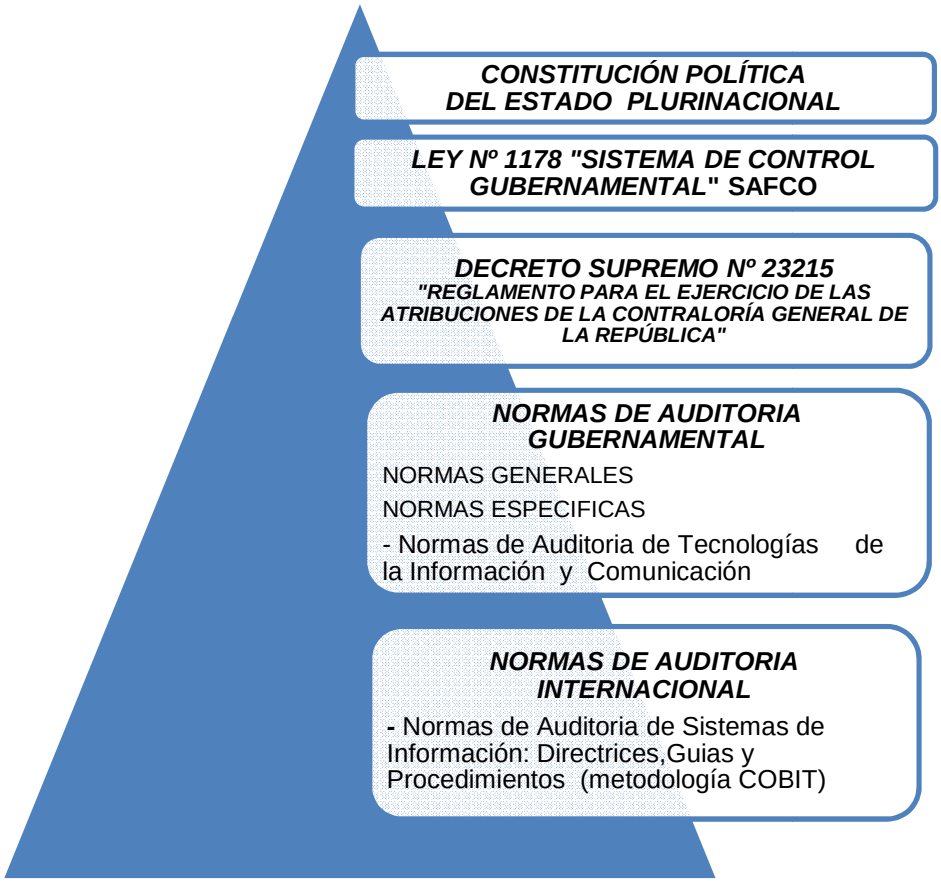
1. Constitución Política del Estado Plurinacional
2. Ley Nº 1178 Sistema de Control Gubernamental – "SAFCO"
3. Decreto Supremo Nº 23215 "Reglamento para el ejercicio de las Atribuciones de la Contraloría General de la República actual Contraloría General del Estado.
4. Normas de Auditoría Gubernamental
    a. Normas Generales
    b. Normas Específicas
        i. Normas de Auditoría de Tecnologías de la Información y la Comunicación
5. Normas Internacionales de Auditoría
    a. Normas Generales de Auditoría de Sistemas de Información

2.2 MARCO JURÍDICO

Para una adecuada comprensión y conocimiento sobre las definiciones del Sistema de Control Gubernamental que se sustenta el Estado Plurinacional de Bolivia, representaremos gráficamente la prelación del marco jurídico del Sistema de Control Gubernamental de la siguiente manera:

GRÁFICO Nº 1

PRELACIÓN DEL MARCO JURÍDICO DEL SISTEMA DE CONTROL GUBERNAMENTAL



FUENTE: ELABORACIÓN PROPIA

2.3 SISTEMA DE CONTROL GUBERNAMENTAL[6]

El Sistema de Control Gubernamental es un conjunto de principios, políticas y normas, procesos y procedimientos cuyo marco legal está constituido en el siguiente orden:

a) Constitución Política del Estado Plurinacional

El 7 de febrero de 2009, se promulgó la Nueva Constitución Política del Estado, a partir de esa fecha cambia de denominación el país de *REPÚBLICA NACIONAL*

[6] Contraloría General del Estado – Centro Nacional de Capacitación, "Fundamentos del Sistema de Control Gubernamental y Aspectos conceptuales de Control Interno", Bolivia, junio/2006

DE BOLIVIA A ESTADO PLURINACIONAL DE BOLIVIA[7]*,* consecuentemente cambiaron las atribuciones de la actual Contraloría General del Estado, de la siguiente manera:

Según el artículo 154º y 155º de la antigua Constitución Política de la República, el Sistema de Control Gubernamental se encontraba bajo tuición de la Contraloría General de la República, cuya función fue la del **CONTROL FISCAL** sobre las operaciones de las entidades públicas y la revisión de la gestión anual de estas entidades a través de auditorías especializadas.

En la nueva Constitución Política del Estado Plurinacional artículo 213º, señala que el Sistema de Control Gubernamental se encuentra bajo tuición de la "*LA CONTRALORÍA GENERAL DEL ESTADO* (denominación que fue adoptada a partir del 1ro de abril de 2009, mediante Resolución Nº CGE 001/2009 el 31 de marzo de 2009)[8]*, institución técnica que ejerce la función de control de la administración de las entidades públicas y de aquellas en los que el Estado tenga participación o interés económico",* y el artículo 217º establece que "LA CONTRALORIA GENERAL DEL ESTADO *será responsable de la* ***SUPERVISIÓN Y DEL CONTROL*** *externo posterior de las entidades públicas y de aquellas en las que tenga participación o interés económico el Estado. La supervisión y el control se realizará asimismo sobre la adquisición, manejo y disposición de bienes y servicios estratégicos para el interés colectivo".* Con relación a las Leyes y Decretos Supremos que regulan el Sistema de Control Gubernamental, no fueron modificados por la promulgación de la Nueva Constitución, éstos aún se encuentran vigentes, se detallan a continuación:

[7] Honorable Congreso Nacional, Constitución Política del Estado, Bolivia, 07/02/2009

[8] Ver página web: www.cge.gob.bo

b) Ley Nº 1178 Sistema de Control Gubernamental "SAFCO"

La Ley Nº 1178 denominada "Sistema de Control Gubernamental" SAFCO, fue promulgada el 20 de julio de 1990, en el cual expresa un modelo de administración para el manejo de los recursos del Estado; establece sistemas de administración financiera y no financiera, que funcionan de manera interrelacionada entre sí y con los Sistemas Nacionales de Planificación e Inversión Pública; establece el régimen de responsabilidad de los servidores públicos por el desempeño de sus funciones.

Consecuentemente, el *artículo 13º señala que el Control Gubernamental se aplicará* sobre el funcionamiento de los Sistemas de Administración de los recursos del Estado y que estará integrado por el Sistema de Control Interno y el Sistema de Control Externo Posterior. Para efectos de cumplimiento el artículo 23º de la misma Ley, define que la Contraloría es el Órgano Rector del Sistema de Control Gubernamental otorgándole las siguientes facultades:

- Emitir las norma básicas del control interno y externo.
- Evaluará la eficacia de los sistemas de control interno.
- Realizará y supervisará el control externo.
- Ejercerá la súper vigilancia normativa de los sistemas contables del Sector Público.
- Promover el establecimiento de los sistemas de contabilidad y control interno.
- Conducir los programas de capacitación y especialización de servidores públicos.

c) Decreto Supremo Nº 23215 "Reglamento para el Ejercicio de las atribuciones de la Contraloría General de la República"

El presente Decreto, regula el ejercicio de las atribuciones conferidas por la Ley Nº 1178 a la Contraloría General de la República actual Contraloría General del Estado como Órgano Rector del Control Gubernamental y autoridad superior de ***Auditoría del Estado***.

Mediante este Decreto Supremo, la Contraloría regula la normatividad del Control Gubernamental emitiendo las *Normas de Auditoría Gubernamental* y las normas básicas y secundarias del Sistema de Control Interno y Control Externo Posterior.

Las ***Normas Básicas*** de control gubernamental interno son ***normas generales de carácter principista*** que definen el nivel mínimo de calidad para desarrollar adecuadamente las políticas, los programas, la organización, la administración y el control de las operaciones de las entidades públicas.

Y las ***Normas Secundarias***[9] de control gubernamental están conformadas por las normas de aplicación general dictadas por la Contraloría, en desarrollo de las normas básicas emitidas por la misma y la normatividad elaborada por cada entidad pública con fundamento en las normas básicas dictadas por los órganos rectores.

d) Normas de Auditoría Gubernamental

Las Normas de Auditoría Gubernamental, constituyen el conjunto de normas y aclaraciones que definen pautas técnicas y metodológicas de la *Auditoría Gubernamental* en Bolivia, los cuales contribuyen al mejoramiento del proceso de la misma, en los entes sujetos a auditoría, por parte de la Contraloría General del Estado, las unidades de auditoría interna de las entidades públicas y los profesionales o firmas de auditoría o consultoría especializada.

Asimismo, constituyen *el instrumento* para fortalecer y estandarizar el ejercicio profesional del auditor gubernamental y permiten la evaluación del desarrollo y resultado de su trabajo, con características técnicas básicas actualizadas, asegurando la calidad requerida por los avances de la profesión de la auditoría.

Las Normas de Auditoría Gubernamental, son de *cumplimiento obligatorio* para todos los *auditores gubernamentales* (de la Contraloría General del Estado y de

[9]Contraloría General del Estado, Manual de Normas de Auditoria Gubernamental, CGE, Bolivia, 2007

las Unidades de Auditoría Interna) que realizan auditorías en las entidades sujetas a fiscalización, contempladas en los artículos 3º y 4º de la Ley Nº 1178, también son de *aplicación obligatoria* para los *auditores independientes*, ya sea que actúen de forma individual o asociada, así como para los profesionales de otras disciplinas y especialidades, que participen en el proceso de la auditoría gubernamental.

i) Cronología de las Normas de Auditoría Gubernamental

La primera versión de las Normas de Auditoría Gubernamental fue aprobada mediante Resolución Nº CGR – 1/017/92 el 30 de septiembre de 1992, bajo la denominación de "Normas de Auditoría Gubernamental para el ejercicio del Control Posterior en Bolivia", vigente hasta el 31 de diciembre de 1996.

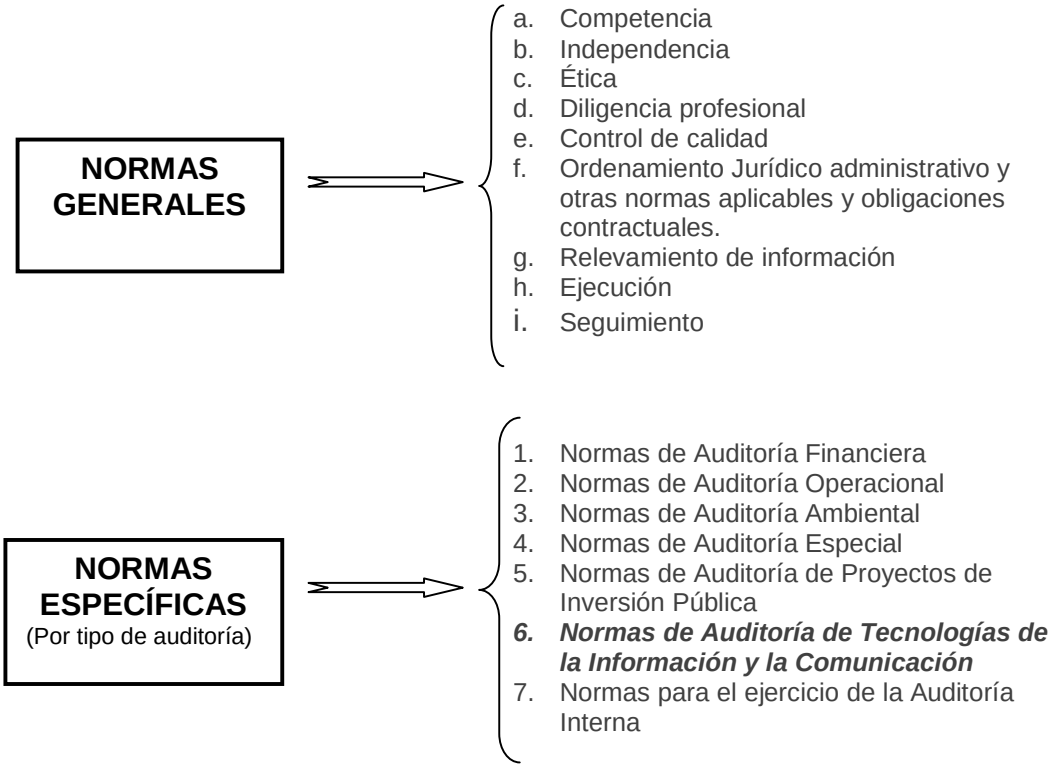
La cuarta versión fue aprobada mediante Resolución Nº CGR/026/2005 el 24 de febrero de 2005, donde se resuelve aprobar el "Manual de Normas de Auditoría Gubernamental" (M/CE/10), que incluye las *NORMAS DE AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN.*

Por último, mediante Resolución Nº CGR/079/2006 de 4 de abril de 2006 se aprueba la división del "Manual de Normas de Auditoría Gubernamental", de la siguiente manera:

DESCRIPCIÓN	SIGLA	VERSIÓN
Normas Generales de Auditoría Gubernamental	M/CE/10-A	4
Normas de Auditoría Financiera	M/CE/10-B	4
Normas de Auditoría Operacional	M/CE/10-C	4
Normas de Auditoría Ambiental	M/CE/10-D	4
Normas de Auditoría Especial	M/CE/10-E	4
Normas de Auditoría de Proyectos de Inversión Pública	M/CE/10-F	3
Normas de Auditoría de Tecnologías de la información Y Comunicación	M/CE/10-G	1
Normas para el Ejercicio de la Auditoría Interna	M/CE/10-H	4

ii) Estructura de las Normas de Auditoría Gubernamental

Las Normas de Auditoría Gubernamental, están definidas bajo la siguiente estructura:



FUENTE: ELABORACION PROPIA

2.4 NORMAS GENERALES DE AUDITORÍA GUBERNAMENTAL

Contemplan los *requisitos personales* que debe reunir el auditor gubernamental o quien ejerza dicha función, éstas se encuentran definidas en el Manual de Normas de Auditoría Gubernamental.

2.5 NORMAS ESPECÍFICAS DE AUDITORÍA GUBERNAMENTAL[10]

Fueron definidas en base a los tipos de auditoría clasificadas en el ámbito gubernamental, la Contraloría emitió las *Normas Específicas* para cada una de ellas con el propósito de *orientar la ejecución de los diferentes* tipos de auditoría, con base en una *planificación* específica y la *evaluación del control interno*, así como una *supervisión* permanente y la obtención de evidencia competente y suficiente, a través de la aplicación adecuada de técnicas y procedimientos de auditoría diseñados para cumplir con los objetivos de cada uno de las auditorías. Asimismo establecen criterios técnicos del contenido, elaboración y presentación

[10] Contraloría General del Estado, Manual de Normas de Auditoria Gubernamental, Bolivia, 2007

del informe de auditoría gubernamental, de acuerdo a cada tipo de auditoría que fueron definidas bajo el siguiente criterio:

1. *Auditoría Financiera***,** es la acumulación y examen sistemático y objetivo de evidencia, con el propósito de:

    a) Emitir una opinión independiente respecto a sí los estados financieros de la entidad auditada presentan razonablemente en todo aspecto significativo, y de acuerdo con las Normas Básicas del Sistema de Contabilidad Gubernamental Integrada, la situación patrimonial y financiera, los resultados de sus operaciones, los flujos de efectivo, la evolución del patrimonio neto, la ejecución presupuestaria de recursos y de gastos, y los cambios en la cuenta de ahorro – inversión financiamiento.

    b) Determinar si: i) la información financiera se encuentra presentada de acuerdo con criterios establecidos o declarados expresamente; ii) la entidad auditada ha cumplido con requisitos financieros específicos, y; iii) el control interno relacionado con la presentación de informes financieros, ha sido diseñado e implantado para lograr los objetivos.

2. *Auditoría Operacional,* es la acumulación y examen sistemático y objetivo de evidencia con el propósito de expresar una opinión independiente sobre: i) la eficacia de los sistemas de administración y de los instrumentos de control interno incorporado a ellos, y; ii) la eficiencia, eficacia y economía de las operaciones.

3. *Auditoría Ambiental*, es la acumulación y examen metodológico y objetivo de evidencia con el propósito de expresar una opinión independiente sobre la eficacia de los sistemas de gestión ambiental y/o el desempeño ambiental y/o los resultados de la gestión ambiental.

4. *Auditoría Especial,* es la acumulación y un examen sistemático y objetivo de evidencia, con el propósito de expresar una opinión independiente sobre el cumplimiento del ordenamiento jurídico administrativo y otras normas legales aplicables, y obligaciones contractuales y, si corresponde, establecer indicios de responsabilidad.

5. *Auditoría de Proyectos de Inversión Pública,* es la acumulación y examen objetivo, sistemático e independiente de evidencia con el propósito de expresar una opinión sobre el desempeño de todo o parte de un proyecto de inversión pública y/o de la entidad gestora del mismo.

6. *Auditoría de Tecnologías de la Información y la Comunicación,* por tratarse del objeto de investigación se describe de manera detallada en el punto 2.6.

7. *Normas para el ejercicio de la Auditoría Interna,* la auditoría interna es una función de control posterior de la organización, que se realiza a través de una unidad especializada, cuyos integrantes no participan en las operaciones y actividades administrativas. Su propósito es contribuir al logro de los objetivos de la entidad mediante la evaluación periódica del control interno.

Para llevar a cabo la ejecución de los diferentes tipos de auditoría definidas en las normas específicas, se establecieron normas relativas a la *Planificación, Supervisión; Control Interno, Evidencia y Comunicación de Resultados* cada una de ellas están estipuladas en base a la esencia de la norma.

2.6 NORMAS DE AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Como se mencionó precedentemente, las *Normas de Auditoría de Tecnologías de la Información y la Comunicación,* fue incluida mediante Resolución Nº CGR/026/2005 el 24 de febrero de 2005, en su cuarta versión en las Normas de Auditoría Gubernamental, con la sigla NAG 270, normas que se definieron para la

aplicación en el ámbito público con el objeto de asegurar la calidad y la uniformidad del trabajo de auditoría.

La presente norma es la base fundamental para el desarrollo del tema de investigación, por tal razón a continuación se describe de manera detallada el contenido de la misma:

Según las Normas de Auditoría Gubernamental de Tecnología de la Información y la Comunicación (NAG - TIC), una auditoría de TIC constituye *el examen objetivo, crítico metodológico y selectivo de evidencia relacionada con políticas, prácticas procesos y procedimientos en materia de Tecnologías de la Información y Comunicación para expresar una opinión independiente respecto:*

i. A la confidencialidad, integridad, disponibilidad y confiabilidad de la información.
ii. Al uso eficaz de los recursos tecnológicos.
iii. A la efectividad del sistema de control interno asociado a las Tecnología de la Información y la Comunicación.

Este tipo de auditoría es definida principalmente por sus objetivos y puede estar orientada hacia uno o varios de los siguientes enfoques:

a) Enfoque a las Seguridades

Consiste en evaluar las seguridades implementadas en los sistemas de información con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información.

b) Enfoque a la Información

Consiste en evaluar la estructura, integridad y confiabilidad de la información gestionada por el sistema de información.

c) Enfoque a la Infraestructura tecnológica

Consiste en evaluar la correspondencia de los recursos tecnológicos en relación a los objetivos previstos.

d) Enfoque de software de Aplicación

Consiste en evaluar la eficacia de los procesos y controles inmersos en el software de aplicación, que el diseño conceptual de éste cumpla con el ordenamiento jurídico administrativo vigente.

e) Enfoque a las Comunicaciones y Redes

Consiste en evaluar la confiabilidad y desempeño del sistema de comunicación para mantener la disponibilidad de la información.

Para la evaluación de los objetos que son parte de las TIC, es preciso realizar su correcta conceptualización, caracterización y delimitación, ya que en diversos casos su abstracción no es una práctica sencilla debido a su naturaleza *virtual,* pero su adecuada abstracción permite un conocimiento y comprensión apropiado de éstos de tal forma de definir tanto los enfoques, objetivos, como el alcance de una auditoría de TIC.

Como se mencionó en el acápite de las normas específicas, la auditoría de tecnologías de la información y la comunicación debe llevarse a cabo de la siguiente manera:

Planificación

Es la primera norma de auditoría de tecnología de la Información y Comunicación, donde señala, que para el desarrollo de la auditoría se debe planificar en forma metodológica, para alcanzar eficientemente los objetivos de la misma, que implica lo siguiente:

- La planificación debe permitir un adecuado desarrollo de las etapas subsecuentes.

- El auditor gubernamental debe comprender del objeto de auditoría, es decir el diseño conceptual, políticas de gestión, formas de registro, niveles de seguridad y uso de las comunicaciones para la gestión de la comunicación.
- En función de la naturaleza, complejidad y modularidad del objeto de auditoría, se determinara las áreas críticas.
- Se diseñaran programas de trabajo que se aplicaran durante la ejecución del trabajo de campo, para el efecto se determinara la naturaleza, oportunidad y extensión de los procedimientos.
- Como resultado del proceso de planificación de la auditoría de Tecnologías de la Información y Comunicación, se debe elaborar un documento resumen, el cual debe contener todos los aspectos detallados en la presente norma.

Supervisión

Corresponde a la segunda norma, el cual señala que la supervisión debe ser realizada por personal competente de manera sistemática y oportuna el trabajo desarrollado por los profesionales que conformen el equipo de auditoría.

La supervisión implica que personal competente y calificado para ejercerla, debe dirigir los esfuerzos del equipo de auditores gubernamentales hacia la consecución de los objetivos de auditoría.

La supervisión efectuada durante el desarrollo de la auditoría, debe ser evidenciada en los papeles de trabajo físicos y si fuera el caso como respaldo en papeles de trabajo electrónicos, acumulados durante la misma.

Control Interno

Comprende la tercera norma de la auditoría, que señala lo siguiente: "*Se debe comprender y evaluar el control interno para identificar las áreas críticas que requieren un examen profundo y determinar su grado de confiabilidad a fin de*

establecer la naturaleza, alcance y oportunidad de los procedimientos de auditoría a aplicar."

Se establecieron dos tipos de controles: el control general y el control detallado de los sistemas de información. El control general involucra a todos los sistemas de información y el control detallado está diseñado para controlar el procesamiento en sí de la información.

Los controles generales son políticas y procedimientos que tienen que ver con el ambiente en el cual se desarrollan, mantienen y operan los sistemas de información y respaldan el funcionamiento efectivo de los controles detallados, en consecuencia involucran a todos los sistemas de información. Se pueden citar por ejemplo, el desarrollo y la implementación de una política de seguridad lógica de los sistemas de información.

Los controles detallados son los aplicables a la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de la información. Se pueden citar por ejemplo, dentro de un software de aplicación parámetros de seguridad de la información, validación de entradas de datos, etc.

El control interno está conformado por cinco componentes que interactúan entre si y se encuentran integrados al proceso de gestión; ambiente de control; evaluación de riesgos; actividades de control; información y comunicación; y supervisión.

Evidencia

Corresponde a la cuarta norma de auditoría de Tecnologías de la Información y la Comunicación, al respecto señala que "*Debe obtenerse evidencia valida, relevante y suficiente como base razonable para sustentar los hallazgos y conclusiones del auditor gubernamental*".

La evidencia es válida, relevante y suficiente.

Las Técnicas de Auditoría Asistidas por Computador (TAAC) pueden producir parte de la evidencia de auditoría, como consecuencia de ello, el auditor debe planificar y ser competente en el uso de las TACC.

La evidencia obtenida por el auditor gubernamental debe conservarse en papeles de trabajo físicos y si fuera el caso como respaldo en papeles de trabajo electrónicos.

Respecto a las características de competencia, suficiencia y clasificación de la evidencia, y a los papeles de trabajo que las contienen, deben considerarse los aspectos mencionados en la NAG 224.02 hasta NAG 224.13.

Comunicación de resultados

Es la quinta norma de auditoría, que señala lo siguiente: "*El informe de auditoría de Tecnologías de la Información y Comunicación debe ser oportuno, objetivo, claro, preciso y será el medio para comunicar los resultados obtenidos durante la misma*".

El informe debe:

- ✓ Ser emitido en forma escrita, lógica y organizada,
- ✓ Debe contener suficiente información para ser entendido por los destinatarios y facilitar la acción correctiva si corresponde.
- ✓ El contenido del informe debe hacer referencia a:
    - o Antecedentes
    - o Objetivos
    - o Alcance referente al sujeto, objeto y periodos examinados, debe especificar que la auditoría se realizó de acuerdo con las normas de auditoría gubernamental.
    - o Limitaciones que permitió el auditor gubernamental cumplir con los objetivos previstos de manera expresa.
    - o Metodología, que explicará las técnicas y procedimientos que fueron empleados para obtener y analizar la evidencia.
    - o Resultado, expondrá:

- Los hallazgos significativos que tengan relación con los objetivos de auditoría, los que incluirán la información suficiente que permita una adecuada comprensión.
- Las recomendaciones que se consideren apropiadas para corregir las causas del problema o hallazgos.

o Las conclusiones que son inferencias lógicas sobre el objeto de auditorías basadas en los hallazgos.

Por tratarse del objeto del presente trabajo, las Normas de Auditoría de Tecnologías de la Información se adjuntan en **ANEXO Nº 1.**

2.7 NORMAS DE AUDITORÍA INTERNACIONAL

Las Normas Internacionales de Auditoría son los requisitos de calidad que deben observarse para el desempeño del trabajo de la auditoría profesional. Por esta razón durante muchos años han constituido y constituyen en la mayoría de los países el soporte obligado de las actividades que conducen los contadores públicos.

Las Normas de Auditoría Gubernamental señalan que si durante el desarrollo de la auditoría se presentan aspectos no contemplados en las Normas de Auditoría Gubernamental, la primera fuente de referencia técnica deben ser las normas emitidas por el Consejo Técnico Nacional de Auditoría y Contabilidad del Colegio de Auditores de Bolivia, si en éstas no se encuentra la referencia técnica necesaria o si la misma fuera insuficiente, se recurrirá a las Normas Internacionales de Auditoría (NIA) y así sucesivamente en el orden de prelación señalado en las mismas Normas de Auditoría Gubernamental.

Para el desarrollo de la Auditoría de Tecnologías de la Información y Comunicación, como se mencionó precedentemente las Normas de Auditoría Gubernamental en su última versión cita como una fuente de referencia técnica a las Normas Generales de Auditoría de Sistemas de Información, emitidas por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) incluido su

modelo de control COBIT (Objetivos de Control de Información y Tecnologías Relacionadas).

Las Normas Generales de Auditoria de Sistemas de Información aun no cuentan con autorización por las vías legales su aplicabilidad en el ámbito gubernamental, sin embargo para fines de conocimiento y efectuar una analogía con las normas nacionales se describen a continuación:

a) Normas Generales de Auditoría de Sistemas de Información[11]

Las Normas Generales de Auditoría de Sistemas de Información, fue emitida por la Asociación de Auditoría y Control de los Sistemas de Información ISACA, por su denominación en inglés "Information System Audit and Control Association", creada el 16 de noviembre de 1969.

En la actualidad cuenta con más de 95.000 miembros en más de 160 países, es un líder mundialmente reconocido, proveedor de conocimiento, certificaciones, comunidad, apoyo y educación en seguridad y aseguramiento de sistemas de información, gobierno empresarial de tecnologías de la información (TI) y riesgos y cumplimiento relacionados con TI.

b) Normas y directrices de ISACA para la auditoría de sistemas de información

El marco general de las Normas de Auditoría de Sistemas de Información de ISACA presenta los siguientes[12] niveles para su aplicabilidad:

- Las Normas definen los requisitos obligatorios para la auditoría y para los reportes de auditoría de SI.
- Los lineamientos (directrices) brindan una guía para aplicar las Normas de Auditoría de SI.
- Los procedimientos ofrecen ejemplos de procedimientos que debe seguir un auditor de SI en una asignación de auditoría. Estos procedimientos brindan información sobre la manera de cumplir con los estándares cuando

[11] Ver página web: www.isaca.org
[12] ISACA, Manual de preparación al examen CISA, Estados Unidos, 2008, página. 18

se está realizando un trabajo de auditoría de sistemas de información pero no establecen requerimientos.

Las normas definidas por ISACA son de cumplimiento obligatorio por el auditor de Sistemas de Información, las directrices proveen una guía de cómo puede el auditor implementar los estándares en diversas tareas de auditoría. Los procedimientos proveen ejemplos de pasos que puede realizar el auditor para implementar los estándares en una tarea específica. Sin embargo el auditor debería hacer uso de su juicio profesional cuando use las directrices y los procedimientos.

El detalle de los estándares, directrices y procedimientos se encuentran descritos en **ANEXO Nº 2.**

CAPITULO III
MARCO CONCEPTUAL

3.1 INTRODUCCIÓN

El capítulo sobre el marco conceptual se ocupa de las definiciones de la auditoría en el ámbito gubernamental y las definiciones de auditoría de sistemas de información emitidas por la Asociación y Control de Sistemas de Información en adelante (ISACA)[13]. Asimismo describe el proceso de ejecución de la auditoría de tecnologías de la información y comunicación, las técnicas y herramientas asistidas por computador (CAATs)[14] como apoyo al desarrollo de la auditoría.

3.2 DEFINICIÓN DE AUDITORÍA

Según la Norma de Auditoría Gubernamental, define a la auditoría como la *"acumulación y evaluación objetiva de evidencia para establecer e informar sobre el grado de correspondencia entre la información examinada y criterios establecidos"*.[15]

3.3 DEFINICIÓN DE AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN O SISTEMAS DE INFORMACIÓN

Desde el punto de vista gubernamental la auditoría de tecnologías de la información y comunicación c*onstituye "Un examen objetivo, crítico metodológico y selectivo de evidencia relacionada con políticas, prácticas, procesos y procedimientos en* ***materia de Tecnologías de la Información y Comunicación,*** *para expresar una opinión independiente respecto a tres aspectos: a la confidencialidad, integridad, disponibilidad y confiabilidad de la información; al uso eficaz de los recursos tecnológicos; y a la efectividad del sistema de control interno asociado a las Tecnologías de la Información y la Comunicación.*

ISACA, define a la auditoría de sistemas de información "*como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (parcial o total) de los*

[13] ISACA "Information System Audit and Control Association", ver página web: www.isaca.org
[14] CAATs " Computer Assisted Audit Techniques"
[15] Contraloría General del Estado, Manual de Normas de Auditoria Gubernamental, Bolivia, 2007

sistemas automáticos de procesamiento de la información incluidos los procedimientos no automatizados relacionados con ellos y las interfaces correspondientes".

De manera más precisa, se puede señalar que la auditoría de sistemas de información es un proceso que recolecta y evalúa la evidencia para determinar si los sistemas de información y los recursos relacionados protegen adecuadamente los activos, mantienen la integridad y la disponibilidad de los datos y del sistema, proveen información relevante y confiable, logran de forma efectiva las metas organizacionales, usan eficientemente los recursos y tienen en efecto controles internos que proveen una certeza razonable que los objetivos de negocio, operacionales y de control serán alcanzados, y que los eventos no deseados serán prevenidos o detectados y corregidos de forma oportuna[16].

3.4 TIPOS DE AUDITORÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Para la ejecución de auditoría de sistemas de información, el auditor gubernamental especializado deberá conocer y entender los diversos tipos de auditoría que pueden efectuarse interna o externamente y los procesos asociados a cada uno de ellos.

En la actualidad existe abundante teoría sobre los tipos de auditoría que se pueden realizar en el ámbito de tecnologías de la información, sin embargo es necesario delimitar el alcance en el presente trabajo de investigación, la clasificación se desarrollará en el marco normativo gubernamental, específicamente bajo los cinco enfoques definidos en las Normas de Auditoría de Tecnologías de la Información y Comunicación[17], que se describen a continuación:

[16] ISACA, Manual de Preparación al examen CISA 2008, Estados Unidos 2009, página 35
[17] Contraloría General del Estado, Manual de Normas de Auditoría de Tecnologías de la Información y Comunicación, CGE, Bolivia, 2007

a) Enfoque a las seguridades

Bajo este enfoque, la evaluación se concentra en las seguridades implementadas en los sistemas de información con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información.

La confidencialidad, integridad y disponibilidad son los tres pilares de la seguridad por tanto los controles van dirigidos a tratar de garantizar algunos de estos criterios que debe cumplir la información.

El criterio de ***confidencialidad*** se cumple cuándo sólo las personas autorizadas (en un sentido amplio podríamos referirnos a sistemas) pueden conocer los datos o la información correspondiente.

El criterio de ***integridad*** se cumple cuando sólo los usuarios autorizados puedan variar (modificar o borrar) los datos. Deben quedar pistas para control posterior y auditoría.

Por último el criterio de ***disponibilidad*** se cumple cuando se alcanza, si las personas autorizadas puedan acceder a tiempo a la información a la que estén autorizadas.

En síntesis, bajo este enfoque se pueden desarrollar auditorías en cuyo objetivo se incluya la revisión de la seguridad, de carácter general podemos mencionar los siguientes:

- Auditoría de la seguridad física
- Auditoría de la seguridad lógica
- Auditoría de la seguridad y el desarrollo de aplicaciones
- Auditoría de la seguridad en el área de producción
- Auditoría en la seguridad de los datos
- Auditoría de la seguridad en comunicación y redes

La seguridad de la información se logra implementando un conjunto adecuado de controles, que incluye políticas, procesos, procedimientos, estructuras organizacionales y funciones de hardware y software. Estos controles deben ser establecidos implementados, monitoreados, revisados y mejorados, donde sean necesarios, para asegurar que se cumplen los objetivos específicos de seguridad y del negocio de la organización. Esto debe hacerse conjuntamente a otros procesos de gestión de negocios.

b) Enfoque a la información

Consiste en evaluar la estructura, integridad y confiabilidad de la información gestionada por el sistema de información. Las posibles auditorías que se pueden ejecutar bajo este enfoque son los siguientes:

- Auditoría al origen, proceso y salida de la información en un sistema de información.
- Auditoría a la distribución, manipulación y almacenamiento externo de la información.
- Auditoría a la información generada por un sistema de gestión de bases de datos.

c) Enfoque a la infraestructura tecnológica

Consiste en evaluar la correspondencia de los recursos tecnológicos en relación a los objetivos previstos.

La cambiante infraestructura tecnológica y la manera de operar han conducido distintas formas evolutivas de realizar auditorías y revisiones específicas de hardware, sistemas operativos, bases de datos, redes de área local, controles operativos de red, operaciones de sistemas de información, reporte de administración de problemas, disponibilidad de hardware y reporte de utilización.
Como ejemplo se cita algunas de las auditorías que se pueden ejecutar:

- Auditoría de gestión de cambios al sistema operativo o Bases de Datos.
- Auditoría de mantenimiento de hardware.

- Auditoría a la configuración y administración de redes.

d) Enfoque al software de aplicación

Consiste en evaluar la eficacia de los procesos y controles inmersos en el software de aplicación, que el diseño conceptual de éste cumpla con el ordenamiento jurídico administrativo vigente.

Bajo este enfoque se evaluará el establecimiento y uso de principios de ingeniería robustos orientados a obtener software económico que sea fiable, cumpla con los requisitos previamente establecidos y funciones de manera eficiente.

La auditoría de software de aplicación evalúa la existencia y aplicación de procedimientos de control adecuados que permitan garantizar que el desarrollo de sistemas de información se ha llevado a cabo según estos principios de o parte por el contrario determinar las deficiencias existentes en este sentido, se cita algunos ejemplos de auditorías que se pueden desarrollar:

- Auditoría a los controles de entrada, proceso y salida de la aplicación.
- Auditoría al ciclo de desarrollo de software (Ingeniería de requerimientos, desarrollo (análisis, codificación y control de calidad), puesta en producción y mantenimiento.

e) Enfoque a las comunicaciones y redes

Consiste en evaluar la confiabilidad y desempeño del sistema de comunicación para mantener la disponibilidad de la información.

Significa que el auditor gubernamental debe revisar los controles sobre las redes de área local (LANs – Local Área Network) para asegurar que existan los estándares para diseñar y seleccionar la arquitectura de un LAN y para asegurar que los costos de obtención y de operación no excedan los beneficios.

Los tipos de auditorías que se pueden efectuar en el área de comunicaciones y redes pueden ser los siguientes:

- Auditoría a la gerencia de comunicaciones.
- Auditoría a la red lógica (tráfico de la información).
- Auditoría a la red física (instalaciones de red).

3.5 DEFINICIÓN DE EVIDENCIA

La evidencia es "*un conjunto de hechos comprobados suficientes componentes y pertinentes que sustentan las conclusiones del auditor. Es la información específica obtenida durante la labor de auditoría a través de la observación, inspección, entrevistas y exámenes de los registros",* la presente definición corresponde a las Normas de Auditoría de Tecnologías de la Información y Comunicación emitida por la Contraloría General del Estado.

Desde el punto de vista de la auditoría en general, la evidencia es toda la documentación elaborada u obtenida por el auditor durante el proceso que respalda sus decisiones y opiniones. El logro de la calidad y volumen suficiente de la evidencia acumulada debe responder a los criterios establecidos que forma parte de toda auditoría.

El auditor gubernamental debe obtener la evidencia necesaria que se ajuste a la naturaleza y objetivos del examen mediante la aplicación de pruebas de cumplimiento y sustantivas que le permitan fundamentar razonablemente los juicios y conclusiones respecto a la entidad auditada.

La evidencia de auditoría queda documentada en los papeles de trabajo los mismos que son organizados en un archivero completo y detallado del trabajo efectuado y de las conclusiones alcanzadas en que se incluyen todos los papeles de trabajo.

3.6 DEFINICIÓN DE PAPELES DE TRABAJO

"Los papeles de trabajo comprenden la totalidad de los documentos preparados recibidos por los auditores gubernamentales, de manera que, en conjunto, constituyan un compendio de las pruebas realizadas durante el proceso de auditoría y de las evidencias obtenidas para llegar a formarse una opinión o abstenerse de ella", definición que corresponde a las Normas de Auditoría de Tecnologías de la Información y Comunicación Nº 274, asimismo deben cumplir los aspectos *mencionados en la NAG 224.02 hasta NAG 224.13",* emitida por la Contraloría General del Estado.

El propósito de los papeles de trabajo es documentar la planificación y realización de la auditoría, en la supervisión y revisión de la misma y de evidencia del trabajo realizado, de tal modo que sirven de soporte a las conclusiones, opiniones, comentarios y recomendaciones incluidas en el informe.

3.7 EJECUCIÓN DE AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Corresponde a la secuencia de pasos que implica llevar a cabo una auditoría que puede variar según las características de cada entidad, proyecto o programa a auditar, fundamentalmente se verifican cuatro etapas esenciales; Actividades previas al trabajo de campo; Planificación de la auditoria; Ejecución del trabajo y conclusión y Comunicación de resultados, En síntesis el objetivo y resultados que se esperan de cada uno de ellos son los siguientes:

CUADRO Nº 1

FASES DE LA AUDITORÍA

ETAPA	OBJETIVO	RESULTADOS
PLANIFICACIÓN PRELIMINAR	Determinar el tipo de auditoría a realizar y planificación administrativa para la ejecución de la auditoría.	Informe de relevamiento
PLANIFICACIÓN	Predeterminar procedimientos	Memorándum de Planificación y programas de trabajo
EJECUCIÓN	Obtener elementos de juicio a través de la aplicación de los procedimientos planificados	Evidencias documentadas en papeles de trabajo
CONCLUSIÓN Y COMUNICACIÓN DE RESULTADOS	Emitir un juicio basado en la evidencia de auditoría obtenida en la etapa de ejecución	Informe del auditor

FUENTE: ELABORACION PROPIA

La clasificación y contenido de las fases de auditoría fueron desarrolladas en base a las Normas de Auditoría de Tecnologías de la Información y Comunicación emitida por la Contraloría General del Estado, tomando como analogía las Normas de Auditoría de Sistemas de Información emitidas por ISACA, que a continuación se detalla:

a) Planificación preliminar

Comprende la ejecución del relevamiento de la información, el cual debe servir de base para determinar el tipo de auditoría a realizar, asimismo, se efectúa el trabajo administrativo relacionado con la planificación de la actividad, como ser; conformar los equipos de trabajo, coordinar con las áreas objeto de la auditoría, cronograma de trabajo y requerimientos de información.

b) Planificación

A través del análisis de la información obtenida en el relevamiento de la información el equipo de auditoría deberá tomar conocimiento y obtener una comprensión del uso de las TIC (NAG 271.02) en los procesos principales de la entidad; lo que implica:

- Entender la naturaleza de la entidad y los procesos relevantes que fueron automatizados; para ello se puede recurrir a las leyes de creación de la entidad y sus regulaciones internas.
- Comprender el objeto de auditoría; el diseño conceptual, políticas de gestión, forma de registro, niveles de seguridad y uso de las comunicaciones para la gestión de la información.
- Identificar las políticas y estrategias institucionales adoptadas, tendientes al logro de los objetivos y metas haciendo uso de las TIC.
- Comprender la relación del área informática respecto a la misión institucional.
- Comprender el diseño organizacional, analizar y registrar la manera en que está organizada el área funcional encargada de la administración y mantenimiento de los sistemas de información automatizados.

➢ ***Identificar y seleccionar los sistemas de información y/o procesos automatizados relevantes***

Habiendo obtenido el conocimiento y la información del objeto del examen, el auditor especializado deberá seleccionar los sistemas de información y/o procesos automatizados más relevantes, lo que implica:

- Estimar en qué medida, los objetivos de cada uno de los sistemas de información y/o procesos automatizados, coadyuvan al logro de los objetivos perseguidos por la entidad.
- En base a lo anterior, definir qué sistemas de información y/o procesos automatizados coadyuvan en mayor grado al logro de los objetivos de la entidad y el tipo de información administrada por éstos.
- Tomar en cuenta en el caso de existir información sobre auditorías anteriores de sistemas de información y/o procesos observados.

- ***Efectuar el análisis de riesgos y establecimiento de áreas críticas***

Para el análisis de riesgos y establecimiento de áreas críticas, es necesario que el control interno proceso que es afectado por la dirección y todo el personal, diseñado con el objeto de proporcionar una seguridad razonable para el logro de los objetivos de la entidad. Además debe comprender el plan de organización y todos los métodos coordinados y procedimientos adoptados en la entidad para promover la eficacia y la eficiencia de las operaciones y la confiabilidad de la información financiera y de gestión, así como el cumplimiento de las políticas gerenciales, el ordenamiento jurídico administrativo y otras normas legales aplicables y las obligaciones contractuales.

Para el análisis, el control interno está conformado por cinco componentes que interactúan entre si y se encuentran integrados al proceso de gestión; ambiente de control; evaluación de riesgos; actividades de control; información y comunicación; y supervisión.

En base al análisis de importancia realizado de los sistemas de información y/o procesos automatizados, se deberá evaluar lo siguiente:

- Comprender y evaluar el control interno, que implica un análisis de riesgos de los controles internos asociados a éstos, para identificar las áreas críticas que pueden ser los sistemas de información y/o procesos automatizados o parte de ellos que requieren un examen profundo y determinar su grado de confiabilidad a fin de establecer la naturaleza, alcance y oportunidad de los procedimientos de auditoría a aplicar.

- ***Definición de objetivos generales y específicos, enfoques y alcances***

La AUTIC[18] está definida principalmente por los objetivos y puede ser orientada hacia uno o varios de los enfoques dependiendo de las circunstancias determinadas en todo el análisis realizado durante esta etapa de planificación,

[18] AUTIC "Auditoría de Tecnologías de la Información y Comunicación"

considerando lo indicado y en función de las áreas críticas, el equipo de auditoría podrá definir los objetivos, enfoques y alcance.

De acuerdo a los objetivos generales y/o el enfoque/s de la auditoría, deberán definirse los objetivos específicos y alcances; que deberán surgir como resultado lógico de todo el trabajo anteriormente desarrollado.

- ***Determinación de metodologías, técnicas y criterios de evaluación***

En función a los objetivos, al enfoque y al alcance previamente definidos, y con el fin de obtener evidencia válida, relevante y suficiente se debe:

- Elegir entre las metodologías y/o técnicas de auditoría generalmente aplicadas en evaluaciones TIC, aquellas que se ajusten a las necesidades particulares de la AUTIC correspondiente.
- Diseñar, cuando corresponda metodologías y técnicas adecuadas.
- Seleccionar, los criterios de TI a aplicar en base a la normativa vigente en el país o recurrir a las fuentes de criterio externos reconocidos internacionalmente (modelo de control COBIT, ISO 27001, etc.).

- ***Elaboración y aprobación del Memorándum de Planificación de Auditoría de Tecnologías de la Información y Comunicación***

Como resultado del proceso de planificación, se obtendrá el documento Memorando de Planificación de Auditoría de Tecnologías de la Información y la Comunicación, el cual incluirá el programa de trabajo que se aplicará durante la ejecución del trabajo de campo, que deberá contener los procedimientos a ser aplicados para el logro de cada objetivo específico. El presente documento deberá ser remitido a las autoridades pertinentes para su aprobación.

Según el documento Nº S5 que corresponde a la Norma de Auditoría de Sistemas de Información – Planeación emitida por ISACA, de manera similar a las normas gubernamentales, define los estándares que debe cumplir el Auditor de Sistemas

de Información (en adelante SI) en la etapa de planificación, que son los siguientes:

- ✓ El Auditor de SI debe planear la cobertura de la auditoría de sistemas de información para cubrir los objetivos de la auditoría y cumplir con las leyes aplicables y las normas profesionales de auditoría.
- ✓ El Auditor de SI debe desarrollar y documentar un enfoque de auditoría basado en riesgos.
- ✓ El Auditor de SI debe desarrollar y documentar un plan de auditoría que detalle la naturaleza y los objetivos de la auditoría, los plazos y alcance, así como los recursos requeridos.
- ✓ El Auditor de SI debe desarrollar un programa y/o plan de auditoría detallando la naturaleza, los plazos y el alcance de los procedimientos requeridos para completar la auditoría.

El desarrollo del programa de auditoría de sistemas de información se basa en los objetivos y alcances definidos en la auditoría. La evaluación de TI estará de acuerdo a las diferentes perspectivas del auditor de SI, tales como la seguridad (confidencialidad, integridad y disponibilidad), la calidad (efectividad, eficiencia), fiduciaria (cumplimiento y confiabilidad), el servicio y la capacidad. El programa de auditoría es la estrategia para cumplir con el plan de auditoría en el cual se identifica el alcance, los objetivos y los procedimientos de auditoría para lograr evidencia suficiente y competente, de esta menara obtener y sustentar las conclusiones y opiniones de auditoría.

ISACA también señala, el auditor de Sistemas de Información además debe entender otras consideraciones para efectuar la planificación, tales como los resultados de la evaluación periódica de riesgos, cambios en la aplicación de tecnologías, y aspectos de privacidad evolucionantes y requisitos regulatorios que pueden afectar el enfoque general de auditoría. También debe considerar las fechas límites establecidas para la implementación y/o actualización de los

sistemas, las tecnológicas actuales y futuras, requerimientos de la entidad (dueños del proceso y las limitaciones de recursos[19] de sistemas de información.

Además debe comprender las diversas prácticas del negocio y de las funciones relativas al sujeto de la auditoría, los tipos de sistemas de información y la tecnología que soportan la actividad. Los pasos a seguir para llevar este tipo de auditorías son los siguientes:

- Lograr un entendimiento de la misión, los objetivos, el propósito y los procesos de negocio, incluyendo los requerimientos de información y procesamiento, tales como la disponibilidad, integridad, seguridad y tecnología del negocio y la confidencialidad de la información.
- Identificar contenidos específicos tales como políticas, estándares y directrices requeridos, procedimientos y estructura de la organización.
- Realizar un análisis de riesgos para ayudar a diseñar el plan de auditoría.
- Llevar a cabo una revisión de los controles internos relacionados con tecnologías de la información.
- Establecer los alcances y los objetivos de la auditoría.
- Desarrollar el enfoque o la estrategia de auditoría.
- Asignar recursos humanos a la auditoría.
- Dirigir la logística del trabajo de auditoría.

c) Ejecución del trabajo de campo

En esta etapa se reúnen los elementos de juicio válidos y suficientes que permitan respaldar el informe a emitir, se aplican todos los procedimientos, metodologías y las técnicas de auditoría descritos en el documento Memorándum de Planificación de Auditoría de Tecnologías de la Información y la Comunicación a objeto de evaluar las distintas evidencias de auditoría obtenidas para concluir sobre la

[19]COBIT: los recursos de TI son: aplicaciones, información, infraestructura y personas. Ver página web: www.isaca.org/cobit

razonabilidad de los mismos. La evidencia debe cumplir con los criterios establecidos en la norma, como se describió en el punto 3.5 del presente capítulo.

i) Elaboración de los papeles de trabajo

La evidencia acumulada durante la ejecución del trabajo de campo deberá ser registrada en papeles de trabajo que respaldan la opinión que se exprese en el informe.

Los papeles de trabajo deben cumplir con las características de: claridad, concisión, pertinencia, objetividad, lógica, orden e integridad, con el propósito de acceder con facilidad a los mismos, estos deben estar referenciados y/o correferenciados; además debe llevar la rúbrica de quién la elaboró, el objetivo de su elaboración, la conclusión a la que arriba y la fuente donde se obtuvo.

ii) Desarrollo de los hallazgos de auditoría

Luego de haber concluido la elaboración de los papeles de trabajo, se deberá desarrollar los atributos correspondientes a los hallazgos detectados, teniendo en cuenta lo siguiente:

- Estructurar los hallazgos redactando respectivamente la condición, criterio, causa, efecto y recomendación.
- Referenciar los hallazgos con las evidencias que soportan las afirmaciones, enunciados, opiniones, etc.

Según el documento S6 “Norma de Auditoría de SI – Realización de labores de auditoría” emitida por ISACA, con relación a la fase de ejecución el Auditor de SI debe cumplir los siguientes estándares:

- Supervisión – El personal de auditoría de SI debe ser supervisado para brindar una garantía razonable de que se lograran los objetivos de la auditoría y que se cumplirán las normas profesionales de auditoría aplicables.
- Evidencia – Durante el transcurso de la auditoría, el Auditor de SI debe obtener evidencia suficiente, confiable y pertinente para

alcanzar los objetivos de auditoría. Los hallazgos y conclusiones de la auditoría deberán ser soportados mediante un apropiado análisis e interpretación de dicha evidencia.

- Documentación – El proceso de auditoría deberá documentarse, describiendo las labores de auditoría realizadas y la evidencia de auditoría que respalda los hallazgos y conclusiones del auditor de SI.

d) Conclusión y comunicación de resultados de la auditoria de tecnologías de la información y la comunicación

La comunicación de resultados se efectuará a través de un informe que debe ser emitido en forma escrita, lógica y organizada en base al desarrollo de hallazgos elaborado, el mencionado informe debe ser oportuno, objetivo, claro, preciso y que sea el medio para comunicar los resultados obtenidos durante la auditoría.

Según las normas gubernamentales, los informes de auditoría son importantes elementos de control y responsabilidad pública y otorga credibilidad a la información generada por los sistemas correspondientes de las entidades públicas, ya que reflejan objetivamente el resultado de las evidencias acumuladas y evaluadas durante la auditoría.

De la misma manera en el documento Nº S7 denominado *"Norma de Auditoría de Sistemas de Información – Reporte"*[20] emitida por ISACA, al respecto define los siguientes estándares:

- El Auditor de SI debe suministrar un informe, al finalizar la auditoría. El informe debe identificar la organización, los destinatarios previstos y respetar cualquier restricción con respecto a su circulación.
- El informe de auditoría debe indicar el alcance, los objetivos, el periodo de cobertura y la naturaleza, plazo y extensión de las labores de auditoría realizada.

[20] Ver página web: www.isaca.org

- El informe debe indicar los hallazgos, conclusiones y recomendaciones, así como cualquier reserva, calificación o limitación que el Auditor de SI tuviese en cuanto al alcance de la auditoría.
- El Auditor de SI debe tener evidencia de auditoría suficiente y apropiada para respaldar los resultados reportados.
- Al emitirse el informe del Auditor de SI debe ser firmado, fechado y distribuido de acuerdo con los términos del estatuto de auditoría o carta de compromiso.

3.8 METODOLOGÍA COBIT

Como se mencionó en el Capítulo II Marco Regulatorio, la Norma de Auditoría de Tecnologías de la Información y Comunicación adoptó la metodología COBIT en caso de existir vacíos técnicos para el desarrollo de este tipo de auditorías, en ese entendido se procederá a describir en qué consiste la presente metodología:

a) ¿Qué es el COBIT?

COBIT[21] "Control Objetives for Information and related Technology" por sus siglas en inglés que significa Objetivos de Control de Información y Tecnologías Relacionadas, fue desarrollado por la organización ISACA y por el IT Governance Institute (ITGI) que se estableció en 1998 para evolucionar el pensamiento y los estándares internacionales respecto a la dirección y control de la tecnología de información de una empresa.

Es una metodología aceptada mundialmente para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que éstas implican, se utiliza para planear, implementar, controlar y evaluar el gobierno sobre tecnologías de la información; incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.

[21] Ver página web: www.isaca.org/cobit

b) ¿Qué ofrece COBIT?

Brinda buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

Permite integrar sistemáticamente la dimensión del negocio (la esencia estratégica de la actividad organizacional), con la dimensión tecnológica (propia de la planeación, implementación, control y evaluación de un proyecto TIC), independientemente de la realidad tecnológica que cada organización haya decidido adoptar.

c) ¿Cuál es su estructura?

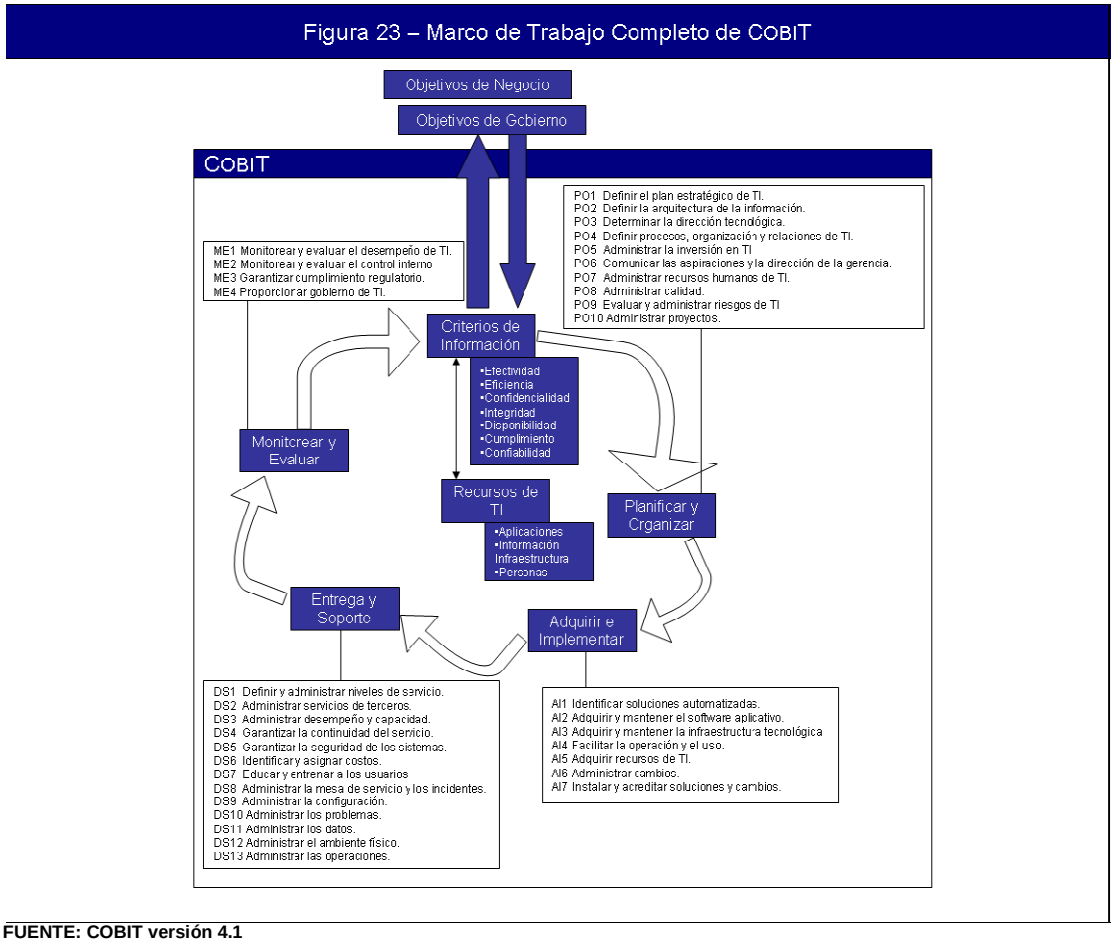
La estructura que adoptó COBIT está orientada bajo el enfoque de procesos, es decir define las actividades de tecnologías de la información en un modelo genérico de procesos organizado en cuatro dominios. Los dominios son los siguientes:

- ✓ Planear y Organizar,
- ✓ Adquirir e Implementar,
- ✓ Entregar y Dar Soporte
- ✓ Monitorear y Evaluar,

En el grafico siguiente se describe la relación que existe entre los dominios y los procedimientos que componen cada uno de ellos:

GRÁFICO Nº 2

ESTRUCTURA DEL COBIT



FUENTE: COBIT versión 4.1

i) Planear y Organizar

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que la tecnología de la información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

ii) Adquirir e Implementar

Para llevar a cabo la estrategia de tecnologías de la información (TI), las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así

como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

iii) Entregar y dar Soporte

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas.

iv) Monitorear y Evaluar

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

Se adjunta en **ANEXO Nº 3** para mayor detalle sobre los dominios, procesos y actividades que contiene la metodología COBIT (Versión 4.1)

3.9 APLICACIÓN DEL COBIT EN LA EJECUCIÓN DE AUDITORÍA – TIC

En cumplimiento a las Normas de Auditoría de Tecnologías de la Información y Comunicación Nº 273, el COBIT y las directrices emitidas por ISACA pueden ser aplicados como criterio para la ejecución de auditoría en función a los cinco enfoques definidos en las NAG - TIC.

Por ejemplo si el enfoque elegido es software de aplicación se puede utilizar como criterio el dominio ADQUIRIR E IMPLEMENTAR descrito en ANEXO Nº 3 y la directriz G23 - Revisión del Ciclo de Vida de Desarrollo de Sistemas (SDLC)[22] emitida por ISACA.

[22] Ver página web: www.isaca.org

Otro ejemplo, en las entidades públicas la evaluación del Control Interno es realizada en base a la metodología COSO[23] (Commette Of Sponsoring Organisation Of The Treadway Commision - Marco de referencia integrado de control interno ampliamente aceptado para gobiernos corporativos y para administración de riesgos), se puede aplicar el siguiente mapeo entre COBIT y COSO:

TABLA Nº 3

MAPEO DE PROCESOS DE COBIT Y COSO

COBIT DOMINIOS Y PROCESOS	**IMPORTANCIA**	**COSO (Cinco componentes del Control Interno)**				
		Entorno de Control	**Evaluación de Riesgos**	**Actividades de Control**	**Información y**	**Monitoreo**
PLANEAR Y ORGANIZAR						
PO1 Definir un plan estratégico de TI	A		P		S	S
PO2 Definir la arquitectura de la información	B			P	P	
PO3 Determinar la dirección tecnológica	M		S	P	S	
PO4 Definir los procesos, organización y relaciones de TI	B	P			S	S
PO5 Administrar la inversión en TI	M		S	P		
PO6 Comunicar las aspiraciones y la dirección de la gerencia	M	P			P	
PO7 Administrar los recursos humanos de TI	B	P			S	
PO8 Administrar la calidad	M	P		P	S	P
PO9 Evaluar y administrar los riesgos de TI	A		P			
PO10 Administrar proyectos	A	S	S	P		S
ADQUIRIR E IMPLEMENTAR						
AI Identificar soluciones automatizadas	M			P		
AI2 Adquirir y mantener software aplicativo	M			P		
AI3 Adquirir y mantener infraestructura tecnológica	B			P		
AI4 Facilitar la operación y el uso	B			P	S	
AI5 Adquirir recursos de TI	M			P		
AI6 Administrar cambios	A		S	P		S
AI7 Instalar y acreditar soluciones y cambios	M			P	S	S
ENTREGAR Y DAR SOPORTE						
DS1 Definir y administrar los niveles de servicio	M	S		P	S	S

[23] COBIT versión 4.1 página 8.

COBIT DOMINIOS Y PROCESOS	**IMPORTANCIA**	**COSO (Cinco componentes del Control Interno)**				
		Entorno de Control	**Evaluación de Riesgos**	**Actividades de Control**	**Información y**	**Monitoreo**
DS2 Administrar los servicios de terceros	B	P	S	P		S
DS3 Administrar el desempeño y la capacidad	B			P		S
DS4 Garantizar la continuidad del servicio	M	S		P	S	
DS5 Garantizar la seguridad de los sistemas	A			P	S	S
DS6 Identificar y asignar costos	B			P		
DS7 Educar y entrenar a los usuarios	B	P			S	
DS8 Administrar la mesa de servicio y los incidentes	B	S			P	P
DS9 Administrar la configuración	M			P		
DS10 Administrar los problemas	M			P	S	S
DS11 Administrar los datos	A			P		
DS12 Administrar el ambiente físico	B		S	P		
DS13 Administrar las operaciones	B			P	S	
MONITOREAR Y EVALUAR						
ME1 Monitorear y evaluar el desempeño de TI	A				S	P
ME2 Monitorear y evaluar el control interno	M					P
ME3 Garantizar el cumplimiento regulatorio	A			P	S	S
ME4 Proporcionar Gobierno de TI	A	P	S		S	P

FUENTE: COBIT versión 4.1 Apéndice II

"Este apéndice proporciona las equivalencias entre los procesos de TI de COBIT y las cinco áreas focales del gobierno de TI, los recursos de TI y los criterios de información. La tabla también contiene un indicador de importancia relativa (alta, media y baja), con base en la evaluación por comparación (benchmarking) vía COBIT ONLINE. Esta matriz en una página, y a alto nivel como el marco de trabajo de COBIT resuelve los requisitos de gobierno de TI y de COSO, y muestra la relación entre los procesos de TI, los recursos y criterios de información de TI. La P se usa cuando hay una relación primaria y la S cuando solamente existe una relación secundaria. El hecho de que no exista una P ni una S no significa que no exista relación, sólo que es menos importante o marginal. Los valores de importancia se basan en la opinión de expertos, y se incluyen sólo como una guía. Los usuarios deben considerar qué procesos son importantes dentro de sus propias organizaciones".

3.10 TÉCNICAS Y HERRAMIENTAS DE AUDITORÍA CON AYUDA DE COMPUTADOR (CAATS)

Las CAATs por su denominación en inglés "Computer Assisted Audit Techniques and Tools" - Técnicas y Herramientas de Auditoría con ayuda del Computador, corresponde al conjunto de herramientas que facilitan al auditor gubernamental en la ejecución de auditorías que abarca desde la planificación, ejecución y reporte de los resultados que puede no ser necesariamente financiera.

En la actualidad, los ambientes de procesamiento de información plantean un duro desafío al auditor gubernamental especializado en sistemas de información, para la recopilación de evidencia suficiente, relevante y útil ya que la evidencia existe en medios magnéticos.

Asimismo, la Norma de Auditoría Gubernamental de Tecnologías de la Información y Comunicación Nº 274 acápite referido a la evidencia punto aclaratorio N 8 autoriza el uso de la siguiente manera: "*Las Técnicas de Auditoría Asistidas por Computador (TAAC) pueden producir parte de la evidencia de auditoría, como consecuencia de ello, el auditor debe planificar y ser competente en el uso de las TAAC".*

3.11 CLASIFICACIÓN DE HERRAMIENTAS ASISTIDAS POR COMPUTADOR

La evolución de los sistemas de información automatizados y no automatizados a forzado que se generen también diferentes técnicas y herramientas automatizadas para su respectiva evaluación tales como; software generalizado de auditoría (Generalized Audit Software - GAS), software utilitario, datos de prueba, rastreo y mapeo de software de aplicación y sistemas expertos.

a) Software generalizado de auditoría

Se refiere al software estándar que tiene la capacidad de leer y acceder a los datos directamente de diversas plataformas de bases de datos, sistemas de archivos planos y formatos ASCII, es un medio independiente para obtener el acceso a datos para su análisis y la habilidad para usar software de alto nivel para resolución de problemas que ejecuta funciones sobre los archivos de datos. Sus características incluyen cálculos matemáticos, estratificación, análisis estadístico, verificación de secuencia, verificación de duplicados y recálculos.

b) Software de utilería

Es el subconjunto de software, como por ejemplo los generadores de informes del sistema de administración de la base de datos que proveen evidencia a los auditores sobre la efectividad de los controles del sistema.

c) La prueba de datos

La prueba de datos involucra que los auditores usen un conjunto de datos como muestra para evaluar si existen errores lógicos en un programa y si el programa satisface sus objetivos.

d) Rastreo y mapeo de software de aplicación

Son herramientas de software que permiten proveer información sobre los controles internos construidos en el sistema.

e) Sistemas expertos de auditoría

Los sistemas expertos proporciona información valiosa para los auditores de todos los niveles mientras ejecutan la auditoría, porque el sistema basado en consultas (SQL – Query Based System) esta creado sobre la base de conocimientos de auditores especializados en el área.

En el siguiente cuadro se describen las herramientas que existen en la actualidad en el mercado tecnológico de software:

CUADRO Nº 2

DETALLE DE HERRAMIENTAS DE SOFTWARE DE AUDITORÌA

BÁSICOS	INTERMEDIOS	COMPLEJOS	ESPECIALES
• Procesadores de textos (MS Word) • Presentaciones (MS Power Point, FlashMX) • Planillas de cálculo (MS Excel) • Programas estadísticos (SPSS) • Software de producción personal	• ACL (Audit Control Langage) • IDEA (Interactive Data Extraction and Analysis) • Monarch • Strata • TopCAATs • Active Data • ProductosMethodware o Ranking Advisor o ProAuditAdvisdor o COBIT Advisor o Audit Builder	• Oracle • SQL Server • Informix • MySQL • MS Access • Toad	• Encase Forensic • Forensic Toolkit • GFiEventsManager • Lumigent Audit BD • In Trust for Active Directory • Hadoop • Weka • Rapidminer • R Project

FUENTE: CURSO CAAT – CONSULTORA YANAPTI.SRL

CAPITULO IV
DIAGNÓSTICO INSTITUCIONAL Y SISTÉMICO

4.1 NATURALEZA Y OBJETIVO

Con la finalidad de cumplir con el objetivo del presente trabajo de investigación, dentro del órgano estatal se eligió al Registro Único para la Administración Tributaria Municipal (en adelante RUAT) debido a su naturaleza, que textualmente la misión de ésta; es la de: ***"Diseñar, desarrollar y administrar sistemas informáticos que permitan a los Gobiernos Municipales, Ministerio de Economía y Finanzas Públicas y Policía Nacional cumplir con las atribuciones conferidas por Ley en lo relativo a tributos e ingresos propios."***[24]

El objetivo del diagnóstico es efectuar el relevamiento de la situación actual en la que se desenvuelve la Dirección de Auditoría Interna dependiente del RUAT frente a las Normas de Auditoría de Tecnologías de la Información y Comunicación emitidas por la Contraloría General del Estado, que es de cumplimiento obligatorio.

4.2 DESARROLLO

Para el efecto aplicaremos dentro de la contextualización descriptiva el empleo de las técnicas de cuestionarios, entrevistas y observaciones *a la situación crítica de su ausencia o insuficiencia* de no contar con una metodología para la ejecución de auditorías de tecnologías de la información y la comunicación en la Dirección de Auditoría Interna de la entidad análogamente se está utilizando las Normas de Auditoría de Tecnologías de la Información y la Comunicación.

4.3 MUESTRA

La aplicación de la técnica de la observación permite una continua interacción realizando pruebas in situ, que significa observar en el propio sitio donde se encuentra el objeto de estudio; que consiste en; la revisión de los documentos que se generan durante el desarrollo de auditorías informáticas, los procesos y/o

[24] Ver: www.ruat.gob.bo

procedimientos que aplica el auditor para el desarrollo de las auditorías informáticas y los recursos tecnológicos que se emplean como herramientas de apoyo.

La aplicación de los cuestionarios en base a preguntas directas, están dirigidas al personal del área informática de la Dirección de Auditoría Interna, que permitirá relevar y evaluar sobre los procedimientos administrativos y operativos que emplean para la ejecución de auditorías informáticas sobre los procesos tecnológicos que desarrolla el RUAT. Se adjunta en **ANEXO Nº 4** el formulario del cuestionario.

Finalmente a objeto de sustentar los resultados producto de la observación y los cuestionarios aplicados al personal, se entrevistó al Director de la Dirección de Auditoría Interna con la finalidad de obtener una reafirmación a los resultados sobre debilidades y amenazas detectadas en la Dirección de Auditoría Interna del RUAT. Se adjunta en **ANEXO Nº 4** el formulario de la entrevista.

4.4 TABULACIÓN DE RESULTADOS

Producto de la observación directa realizada a las actividades de la Dirección de Auditoría Interna, se tiene lo siguiente:

i) Sobre la documentación, se verificó que la ejecución de las auditorías genera la siguiente documentación:

- *Legajo permanente*, que corresponde al compendio de toda la documentación referida a la entidad desde su creación, que es de disponibilidad continua para las labores a realizar en una determinada auditoría, se citan algunos ejemplos:

  - Leyes y normas aplicables
  - Resoluciones administrativas
  - Estados financieros
  - Organigramas
  - Escala salarial

- Nómina de personal
- Otros

o *Legajo de programación*, es la documentación que se genera por cada auditoría ejecutada, contiene información sobre la planificación y programación para llevar a cabo una auditoría:

- Memorándum de programación de auditoría (MPA)
- Programas de trabajo de auditoría
- Cuestionarios si corresponde
- Correspondencia de la auditoría

o *Legajo corriente*, comprende toda la información y documentación obtenida y/o preparada por el auditor gubernamental durante el proceso de ejecución del examen de auditoría, bajo el siguiente detalle:

- Conclusiones y/o informe de auditoría
- Deficiencias
- Papeles de trabajo
- Documentos de respaldo

ii) Sobre los procedimientos y/o procesos, revisada la documentación al respecto, se evidencia que la Dirección no cuenta con un manual y/o procedimiento formalizado para la ejecución de las auditorías informáticas, sin embargo éstas se llevan a cabo de manera similar a las otras auditorías, es decir cumpliendo con las fases de planificación, ejecución, conclusión y comunicación de resultados, en cumplimiento a las Normas de Auditoría de Tecnologías de la Información y Comunicación emitida por la Contraloría General del Estado.

iii) Sobre los recursos tecnológicos, de acuerdo al relevamiento efectuado a la fecha se evidencia que para el desarrollo de las auditorías informáticas,

la Dirección de Auditoría Interna utiliza como herramienta de apoyo el Software WIN IDEA.

El software WIN IDEA[25] es una herramienta para apoyar el trabajo de auditores, contadores, investigadores de fraude y profesionales en sistemas. Permite importar archivos desde diferentes formatos y reportes, leer, visualizar, analizar, procesar, obtener muestras y extraer datos. Provee cinco métodos diferentes de muestreo y funcionalidades para identificar vacíos en secuencia de registros, chequear registros duplicados, comparar, unir y agregar archivos y crear reportes personalizados. Es aplicable a investigaciones sobre fraudes y lavado de activos, tiene la capacidad de efectuar los recálculos en procesos masivos de información.

Como se mencionó en el acápite de la muestra, el cuestionario fue dirigido a los auditores y personal especializado en el área informática dependiente de la Dirección de Auditoría Interna, con la finalidad de obtener información sobre la forma de trabajo y los procedimientos que emplean para la ejecución de auditorías de tecnologías de la información y comunicación, obteniendo los siguientes resultados:

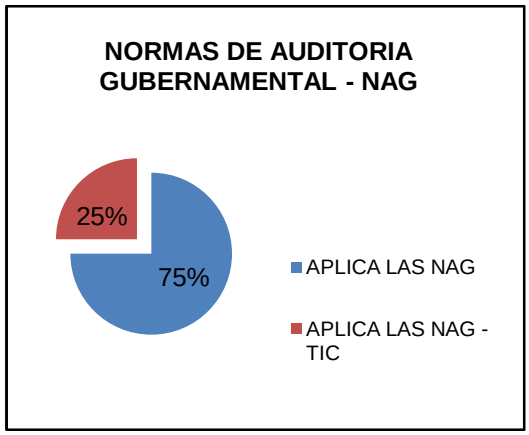
[25]IDEA - Interactive Data Extracción and Análisis - Análisis y Extracción de Datos

PREGUNTA Nº 1

Cuál es el grado de aplicación de las Normas de Auditoría Gubernamental emitidas por la Contraloría General del Estado:

RESULTADO:

Revisado el cuestionario elaborado para el personal del área informática dependiente de la DAI, señala que el grado de aplicación es del 75%, de las NAG, de acuerdo al plan operativo de la DAI, en su mayoría se ejecutan auditorías de confiabilidad y auditoría SAYCO (sistemas de administración según la Ley Nº 1178) y auditorías informáticas en un 25%.

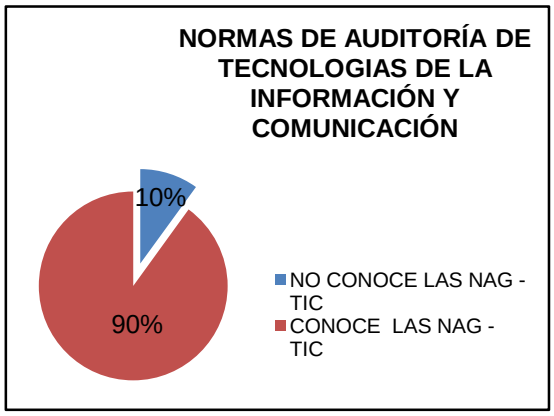


PREGUNTA Nº 2

Cuál es el grado de conocimiento de las Normas de Auditoría de Tecnologías de la Información y la Comunicación (TIC):

RESULTADO:

El resultado del cuestionario realizado al personal del área de sistemas señala que: el grado de conocimiento es del 90% ya que son los responsables en ejecutar las auditorías TIC de acuerdo al Plan Operativo Anual definido por la Dirección de Auditoría Interna.



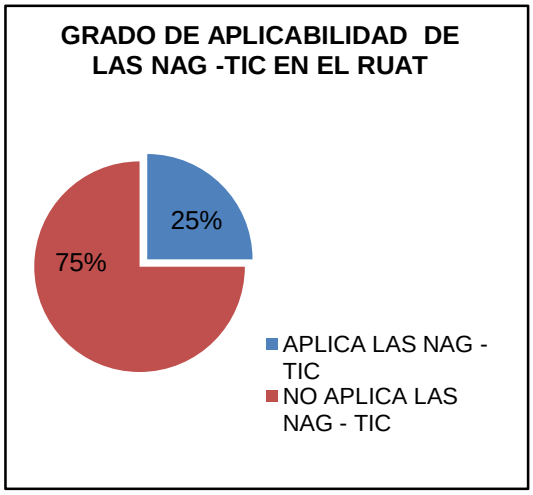
PREGUNTA Nº 3

¿Cuál es el grado de aplicabilidad de la ejecución de auditorías TIC en la entidad?

a) 25%
b) 50%
c) 75%
d) 100%

RESULTADO:

El grado de aplicabilidad es del 25%, según el plan operativo anual de la Dirección de Auditoría Interna, de 15 auditorías programadas en promedio dos corresponden a auditorías de tecnologías de la información, debido a limitaciones de presupuesto asignadas a la DAI no se puede contratar auditores especializados en auditorías de sistemas de información o personal especializado y por otro lado en el mercado laboral existe escases en este tipo de recursos humanos.



PREGUNTA Nº 4

¿Cuenta la Dirección de Auditoría Interna con un enfoque metodológico y/o manual de procedimientos para llevar a cabo las auditorias TIC?

RESULTADO:

En la actualidad la Dirección de Auditoría Interna no cuenta con un enfoque metodológico y/o manual de procedimientos formalizado para llevar a cabo las auditorias de tecnologías de la información y comunicación.

PREGUNTA Nº 5

¿En caso de no existir, explique cómo se llevan a cabo la ejecución de auditorías TIC?

RESULTADO:

Del cuestionario realizado al personal responsable de ejecutar auditorias informáticas, señaló que ésta se ejecuta en base a auditorías realizadas anteriormente y la experiencia laboral adquirida en ese campo y cumpliendo lo estipulado en las NAG – TIC Nº 270.

PREGUNTA Nº 6 ***¿Si los resultados producto de la auditoría de tecnologías de la información y comunicación son implementadas, se efectúa el seguimiento correspondiente?***
RESULTADO: Del resultado obtenido de los cuestionarios, por disposición de la Contraloría General del Estado, el seguimiento a las auditorías es de carácter obligatorio bajo la responsabilidad de la Dirección de Auditoría Interna, por tanto éstos son programados en el plan operativo anual.

PREGUNTA Nº 7 ***¿Mencione las limitaciones y/o dificultades para la ejecución de auditorías TIC?***
RESULTADO: Al no contar con un enfoque metodológico definido y/o procedimientos aprobado para la ejecución de este tipo de auditorías en la Dirección de Auditoría Interna , se presentan las siguientes limitaciones: ➢ No existe uniformidad en los procedimientos a ejecutar durante el desarrollo de las auditorías de tecnologías de la información y la comunicación., ➢ Existe limitada información bibliográfica sobre el tema, ➢ Limitaciones en la forma de aplicar los estándares internacionales, normas y buenas prácticas emitidas en tecnologías de información.

Producto de la observación realizada y el cuestionario aplicado al personal del área informática dependiente de la Dirección de Auditoría Interna, éste fue el resultado de la entrevista realizada al Director de la Dirección de Auditoría Interna de la entidad, formulario de entrevista que se adjunta en **ANEXO Nº 4.**

PREGUNTA Nº 1 ***¿Qué relevancia tiene usted sobre los informes de auditoría de tecnologías de la información y comunicación?***
RESULTADO: La Dirección de Auditoría Interna se encuentra en una fase de madurez inicial en lo que respecta a la ejecución de auditorías informáticas, debido a la reciente aprobación de las Normas de Tecnologías de la Información y Comunicación por la Contraloría General del Estado. En tal sentido, los informes fueron realizados en el marco de las normas gubernamentales, sin embargo para asegurar la uniformidad y calidad de las auditorias se requiere del apoyo de un proceso metodológico. Con el apoyo de esta guía lo que se espera es fortalecer el control interno en procesos tecnológicos que desarrolla la entidad y coadyuvar en el logro de los objetivos institucionales.

PREGUNTA Nº 2 ***¿En qué medida se implementan las recomendaciones?***
RESULTADO: Las recomendaciones que se emitieron fueron recepcionadas de manera favorable por la Máxima Autoridad Ejecutiva y la Dirección de Tecnologías de la Información, por lo que posibilitó su implantación en un 100% otorgando mejora continua en los procesos de tecnologías de la información que ejecuta la entidad.

4.5 ANÁLISIS DE LOS RESULTADOS

En base a las técnicas de observación, cuestionarios y entrevistas realizadas para el desarrollo del presente trabajo aplicadas en la Dirección de Auditoría Interna del Registro Único para la Administración Tributaria Municipal, nos permite arribar a las siguientes conclusiones:

- Los resultados de la aplicación de nuestras técnicas de observación señalan que a la fecha la ejecución de auditorías de tecnologías de la información y comunicación son realizadas de manera similar a las otras auditorías; debido a que la Dirección de Auditoría interna no tiene definido un enfoque metodológico y/o procedimiento formal, donde describa su contenido y desarrollo que se constituya en una guía uniforme para el trabajo de este tipo de auditorías.

- Los resultados de la aplicación de las técnicas del cuestionario y entrevista realizada al personal dependiente de la Dirección de Auditoría Interna, se pudo inferir que existen limitaciones y ausencia de procedimientos formales definidos que dificulta el desarrollo para este tipo de auditorías.

Por lo expuesto en párrafos anteriores, se concluye que la Dirección de Auditoría Interna de la entidad, presenta dificultades en la aplicación de las Normas de Auditoría de Tecnologías de la Información y Comunicación, fundamentalmente porque no se cuenta con un enfoque metodológico base, por lo que nace la necesidad de proponer una metodología integrada a las NAG –TIC y estándares internacionales, herramienta suficiente y necesaria que posibilita la adecuada evaluación de las tecnologías de la información, a objeto de emitir una opinión

independiente sobre el cumplimiento de los criterios de la información, al uso eficaz de los recursos tecnológicos, requerimientos legales, fortalecer el sistema de control interno y coadyuvar en el cumplimiento de la misión que es la razón de existir de la entidad.

Finalmente, de parte de los ejecutivos de la entidad existe una concientización favorable en base a la lectura de las recomendaciones realizadas producto de las auditorías de tecnologías de la información y comunicación que a la fecha fueron aceptadas e implantadas íntegramente, fortaleciendo de esta manera el control interno y coadyuvando en el logro de los objetivos institucionales, como se pudo verificar en los seguimientos de auditoría realizados.

CAPITULO V
PROPUESTA

5.1 INTRODUCCIÓN

Efectuado el relevamiento del marco regulatorio y conceptual sobre el desarrollo de auditorías de tecnologías de la información y comunicación en el ámbito gubernamental y en base al diagnóstico realizado a la Dirección de Auditoría Interna dependiente del Registro Único para la Administración Tributaria Municipal (RUAT), se obtuvo los parámetros necesarios para presentar una propuesta de mejoramiento y coadyuvar en el desarrollo de las auditorías que es de cumplimiento obligatorio para las unidades de auditoría interna.

En la actualidad el ámbito de tecnologías de la información presenta su complejidad en diversos aspectos, por lo que surge la necesidad de contar con una metodología que sirva de guía para obtener uniformidad y calidad en los informes de auditoría

5.2 OBJETIVO GENERAL

Diseñar un enfoque metodológico para evaluar los procesos de tecnologías de la información en las entidades públicas, a través de las unidades de auditoría interna, fundamentada en nuestro diagnóstico institucional y sistémico; con énfasis a los procedimientos y/o procesos administrativo y financiero.

5.3 METODOLOGÍA EMPLEADA PARA EL DESARROLLO DE LA PROPUESTA

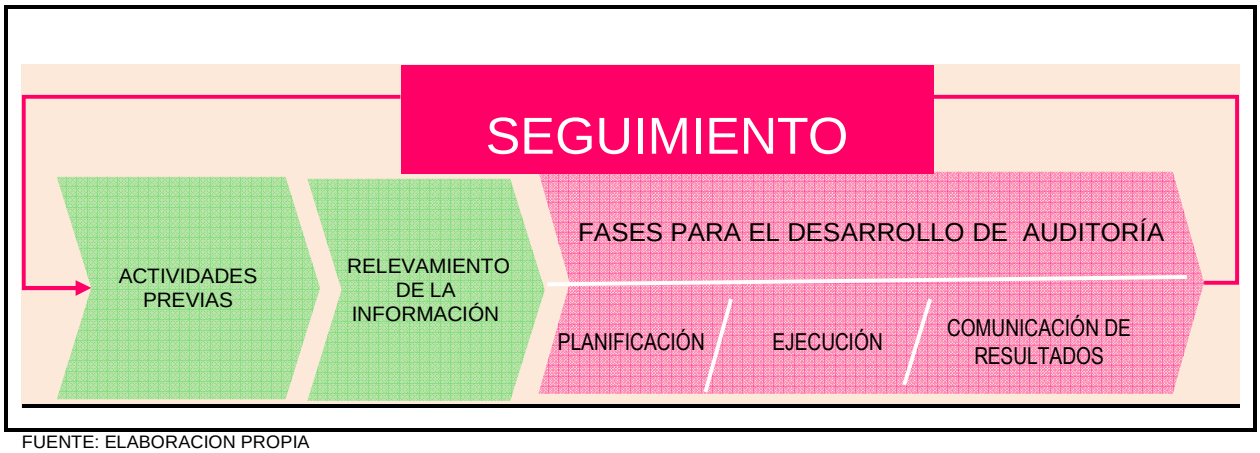
La metodología adoptada para la elaboración de la presente propuesta, está fundamentada en las Normas de Auditoría de Tecnologías de la Información y Comunicación (NAG – TIC) emitida por la Contraloría General de Estado (parte administrativa y de control) con el apoyo de las Normas Internacionales de Sistemas de Información emitida por ISACA y la práctica en el ejercicio de las labores de la Dirección de Auditoría del RUAT (parte técnica) y el cumplimiento de las disposiciones legales vigentes, respecto al ejercicio de las unidades de auditoría interna (parte cumplimiento legal).

5.4 ESTRUCTURA GENERAL DE LA PROPUESTA

Esta metodología será desarrollada bajo el enfoque sistémico considerando cada una de las etapas que intervienen en el proceso de ejecución de la auditoría como se muestra en el **GRÁFICO Nº 3**

GRÁFICO Nº 3

MODELO METODOLÓGICO DE PROPUESTA DE AUDITORÍA DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN



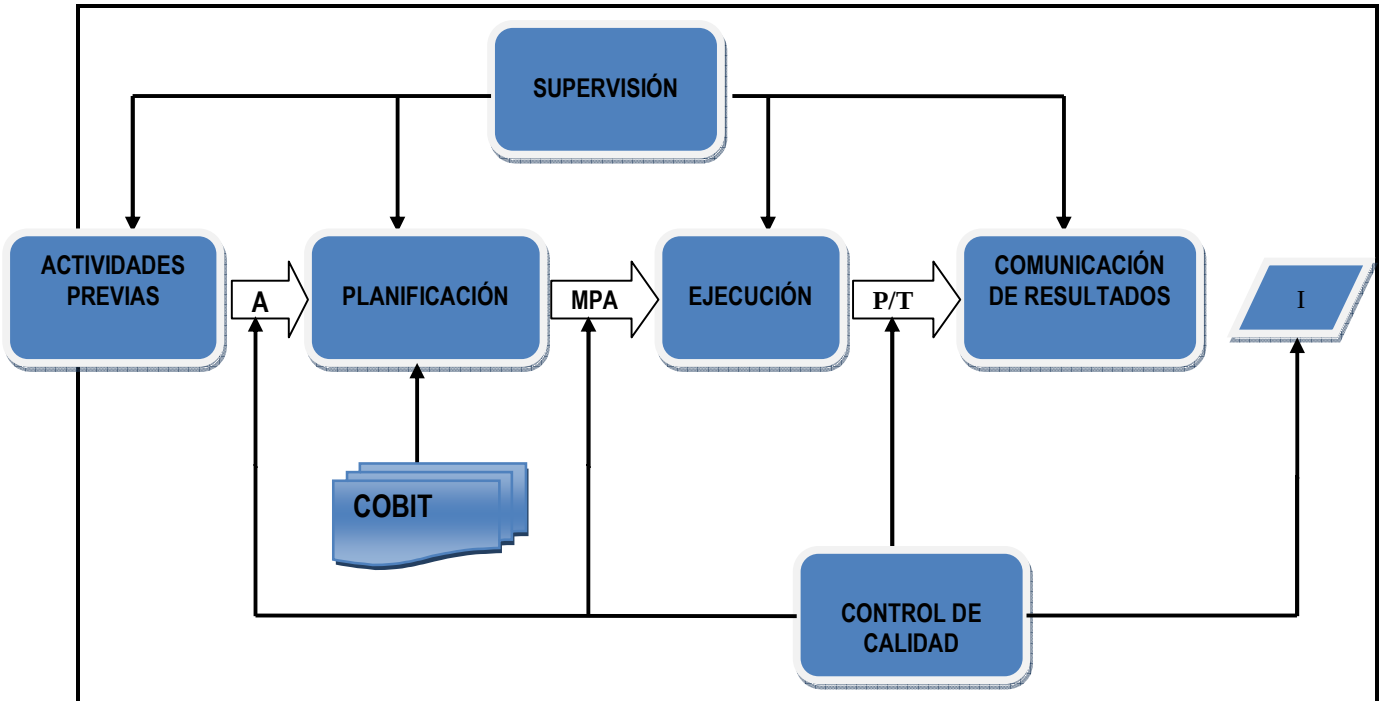
FUENTE: ELABORACION PROPIA

El modelo metodológico para la ejecución de auditorías de tecnologías de la información y comunicación está basado para que los procesos tecnológicos sean evaluados bajo los cinco enfoques definidos en las Normas de Auditoría de Tecnologías de la Información y Comunicación emitidas por la Contraloría General del Estado.

Los recursos de entrada y salida de cada fase de la auditoría de tecnologías de la información y comunicación se presentan en el diseño procedimental del modelo metodológico descrito en el **GRÁFICO Nº 4.**

GRÁFICO Nº 4

FLUJO DEL PROCESO DE AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (ATIC)



PRODUCTOS INTERMEDIOS

A	Aprobación de inicio de auditoría
MPA	Aprobación de Memorándum de Planificación de Auditoría (elaborado en base a la metodología COBIT)
P/T	Control de calidad de papeles de trabajo producto final
B	Control de calidad del informe de razonabilidad
C	Control de calidad de informe de aspectos administrativos y contables

- ✓ Consistencia del MPA y POA
- ✓ Sustento suficiente y competente
- ✓ Verificación de supervisión en todas las etapas de la auditoría

FUENTE: Adecuado según el Compendio para la elaboración de Manual de Procedimiento para el Ejercicio de la Auditoría Interna Gubernamental

5.5 DETALLE DE LA ESTRUCTURA PROPUESTA

La implantación del enfoque metodológico se basa en el *Flujo del Proceso ATIC* descrito en el **GRÁFICO Nº 4,** de los cuales cada fase representa un procedimiento. En los siguientes párrafos se resume los procedimientos definidos necesarios para la ejecución de auditorías de tecnologías de la información y comunicación:

a) Procedimiento - Actividades previas para ATIC

En este procedimiento se describe las actividades administrativas previas necesarias que se requieren para iniciar el trabajo de auditoría, adecuado a las labores que ejerce la Dirección de Auditoría Interna de la entidad.

b) Procedimiento - Relevamiento de la Información para ATIC

Este procedimiento, define los aspectos administrativos que se requieren para efectuar el relevamiento de la información sobre los procesos de tecnologías de la entidad, generalmente se desarrolla para auditorías no recurrentes.

De acuerdo a lo establecido en la Norma de Auditoría Gubernamental 217 Relevamiento de información emitido por la Contraloría General del Estado, en ciertos casos se puede requerir la realización de un relevamiento de información a efectos de establecer el grado de auditabilidad o en la práctica también se lo utiliza para definir el tipo de auditoría a realizar y definir el enfoque.

c) Procedimiento – Planificación de la ATIC

En este procedimiento se define claramente los objetivos, el alcance del trabajo, las técnicas y herramientas a utilizar, los recursos humanos, financieros, técnicos y cronograma de ejecución de la auditoría de tecnologías de la información y comunicación, de acuerdo a lo estipulado en las NAG – TIC 271.

d) Procedimiento – Ejecución de la ATIC

El procedimiento, define los aspectos necesarios para llevar a cabo la ejecución de la auditoría en base a los términos definidos en los Programas de Auditoría que consiste en la obtención y recopilación de la evidencia de auditoría suficiente, pertinente y competente e información adicional para reconsiderar las evaluaciones realizadas con el apoyo de herramientas CAATs.

e) Procedimiento - Comunicación de Resultados de la ATIC

Finalmente, en este procedimiento se define la formalización de la estructura y contenido mínimo de los informes de auditoría de tecnologías de la información y comunicación de acuerdo a lo establecido en la NAG - TIC 275.

5.6 DESARROLLO DEL CONTENIDO DE LA PROPUESTA

Habiendo definido los procedimientos requeridos para la ejecución de auditorías de tecnologías de la información y comunicación, cada procedimiento se desarrolla acorde a los formatos establecidos por el Registro Único para la Administración Tributaria Municipal para posibilitar posteriormente su formalización. El contenido mínimo que debe cumplir cada procedimiento es el siguiente:

1. Objetivos
2. Responsable de su aplicación
3. Aspectos generales (los puntos pueden ser desarrollados acorde a requerimiento del procedimiento ejemplo:)
    - 3.1 Definiciones
    - 3.2 Documentos de referencia
4. Descripción y/o desarrollo del procedimiento
5. Anexos

PROCEDIMIENTO - ACTIVIDADES PREVIAS PARA LAS ATIC

1. Objetivo

Definir los aspectos administrativos previos que se requieren para llevar a cabo la auditoría de tecnologías de la información y comunicación, como ser:

- ✓ Conformar los equipos de trabajo
- ✓ Coordinar con las áreas objeto de la auditoría
- ✓ Cronograma del trabajo a realizar
- ✓ Detalle sobre requerimientos de la información

2. Responsable de su aplicación

El presente procedimiento es de cumplimiento obligatorio por el siguiente personal:

- ✓ Director de Auditoría Interna
- ✓ Profesional y/o auditor Supervisor del área informática
- ✓ Auditores junior y/o personal especializado del área informática

3. Aspectos generales:

3.1 Impedimentos

Señalar las limitaciones y/o impedimentos en cuanto a la independencia del equipo de auditores frente al objeto a auditar.

3.2 Abreviaturas

Definir las abreviaturas a objeto de identificar a los responsables que participaran en la auditoría, por ejemplo:

- ✓ DDAI: Director de la Dirección de Auditoría Interna
- ✓ Pi : Profesional y/o Supervisor del área informática
- ✓ Ai: Auditor junior y/o especializado en informática
- ✓ Pei: Personal especializado en informática

3.3 Documentos de referencia

- ✓ Normas de Auditoría Gubernamental

- ✓ Normas de Auditoría de Tecnologías de la Información y Comunicación
- ✓ Normas de Auditoría de Sistemas de Información emitidas por el organismo internacional de ISACA
- ✓ Políticas, normas y procedimientos que regulan las actividades del ámbito tecnológico de la entidad
- ✓ Otros reglamentos específicos de la entidad

4. Descripción del procedimiento

Para ejecutar las actividades administrativas inherentes a la auditoría, efectuar lo siguiente:

4.1 Actividades previas a la realización de la evaluación

- ➢ Definir la nómina de personal necesario para la evaluación, que conformará el equipo de auditoría
- ➢ Elaborar memorándum de asignación de trabajo de auditoría de acuerdo a la nómina definida

4.2 Comunicación de reunión con el área objeto de la evaluación

- ➢ Definir el flujo de comunicación que se empleará con la parte auditada
- ➢ Elaborar el cronograma de comunicación

4.3 Reunión con los responsables y/o autoridades y visita previa al área objeto de la evaluación.

Especificar que se realizará y/o tratará en la primera reunión, entre los aspectos a considerar, puede ser:

- ✓ Objetivo de la evaluación
- ✓ Presentación del equipo de auditores
- ✓ Quién o quiénes serán los servidores públicos con los cuales se coordinara la solicitud de la información

- ✓ La necesidad de proporcionar el espacio o ambiente para el equipo de auditores, (si corresponde)
- ✓ Visitar el área (as) objeto de la evaluación

4.4 Comunicaciones efectuando el requerimiento de preparación de información y/o documentación y fecha de inicio de la evaluación.

- Definir el flujo de comunicación que se empleará con la parte auditada
- Elaborar el cronograma de comunicación
- La lista de información y/o documentación inicial, necesaria para la fecha de inicio del relevamiento y posterior evaluación
- La preparación del espacio físico para la comisión de auditores (si corresponde)

5. Anexos

La documentación que pueda generarse en esta fase, debe regirse al formato definido por la entidad, por ejemplo las notas internas, memorándums y otros.

PROCEDIMIENTO - RELEVAMIENTO DE LA INFORMACIÓN PARA ATIC

1. Objetivo

Definir los aspectos administrativos que se requieren para efectuar el relevamiento de la información sobre los procesos de tecnologías de información de la entidad.

De acuerdo a lo establecido en la Norma de Auditoría Gubernamental 217 Relevamiento de Información, en ciertos casos se puede requerir la realización de un relevamiento de información a efectos de establecer el grado de auditabilidad o en la práctica también se lo utiliza para definir el tipo de auditoría y el enfoque a realizar. Generalmente la fase de relevamiento es aplicable para auditorias no recurrentes y su documentación es conformada en un legajo apartado.

2. Responsables de su aplicación

El presente procedimiento es de cumplimiento obligatorio por el siguiente personal:

- ✓ Director de Auditoría Interna
- ✓ Profesional y/o auditor Supervisor del área informática
- ✓ Auditores junior y/o personal especializado del área informática

3. Aspectos generales

3.1 Definiciones[26]

Informe de relevamiento: Es el documento mediante el cual el auditor gubernamental comunica por escrito los resultados del relevamiento, cuyo propósito es expresar el grado de auditabilidad del objeto de auditoría.

Objetividad: Los hechos deben ser presentados de manera objetiva y ponderada, es decir con la suficiente información que permita al usuario una adecuada interpretación de los hallazgos expuestos en el informe.

Oportunidad: Los informes deben emitirse oportunamente para que su información pueda ser utilizada por el ejecutivo de la entidad y entidades relacionadas con la misma.

[26] Lic. Eddy M. Salinas Rojas y Coautores, Compendio para la Elaboración de Manual de Procedimientos para el ejercicio de la Auditoría Interna Gubernamental, Simmer, Bolivia – Santa Cruz, 2008

4. Descripción del procedimiento

4.1 Contenido de la primera reunión para iniciar el relevamiento de la información

En la primera reunión se debe explicar lo siguiente:

- El objetivo del relevamiento de información, los objetivos del trabajo, con especial énfasis en que el trabajo está básicamente orientado a mejorar la eficacia y eficiencia de la administración de la entidad con referencia al uso de las tecnologías de la información y comunicación en los procesos automatizados.
- Los resultados que se esperan obtener, aclarando que los mismos serán comunicados mediante informes respectivos.
- Que el trabajo será realizado en constante coordinación con el personal y autoridades de la entidad, para lo cual se solicitará su compromiso y colaboración.

4.2 Elaboración del Programa de Relevamiento de la Información (PRI)

El Profesional y/o auditor Supervisor del área informática preparará el PRI de acuerdo al formato definido, que deberá estar relacionado con los procedimientos específicos directamente vinculados con el objeto del relevamiento, que permitirá concluir sobre la auditabilidad en relación con las condiciones que debe reunir el objeto para ser auditado. Para el logro de cada objetivo el formato del documento PRI deberá considerarse al menos:

- ✓ Nº del procedimiento
- ✓ Descripción de los procedimientos a aplicarse
- ✓ Referencia de papel de trabajo (P/T)
- ✓ Al responsable de realizar el respectivo procedimiento
- ✓ Fecha de inicio y fecha de finalización
- ✓ Horas/hombre presupuestadas.

Los procedimientos que requieran trabajos narrativos para su ejecución, de manera implícita deberán responder las siguientes preguntas:

a) **¿Qué?** Describir el objeto de análisis o relevamiento.
b) **¿Cómo?** Describir la forma como se desarrolla la tarea, actividad y/o procedimiento.
c) **¿Quién?** Señalar el sujeto y/o personas responsables.
d) **¿Por qué?** Describir el objetivo de la tarea, actividad y/o procedimiento.
e) **¿Dónde?** Lugar donde se desarrollo la tarea, actividad y/o procedimiento.
f) **Conclusión** Efectuar el análisis, sobre si el procedimiento cumple con los objetivos establecidos.

4.3 Solicitud de la información

En base a la lista definida acorde al punto 4.4 del PROCEDIMIENTO - ACTIVIDADES PREVIAS PARA LAS ATIC y tomando en cuenta los aspectos establecidos en el PRI, elaborar la nota dirigida a la parte auditada solicitando que la misma sea entregada en un plazo determinado o en su caso se ponga a disponibilidad del equipo de auditores.

4.4 Ejecución del Programa de Relevamiento de la Información

El equipo de auditoría designado, estará bajo la dirección del Supervisor. Esta etapa deberá ser ejecutada de acuerdo a los puntos establecidos en el documento Programa de Relevamiento de la Información, cumpliendo los requerimientos establecidos para la acumulación de la evidencia NAG - TIC 274.

4.5 Estructura y contenido del Informe de Relevamiento de Información de Auditoría de Tecnologías de la Información y Comunicación

El Profesional y/o auditor Supervisor del área informática elaborará el Informe de Relevamiento de la Información de acuerdo al formato definido en este procedimiento. El supervisor conjuntamente con el equipo de trabajo, analizaran los resultados obtenidos, para recomendar los objetivos generales de la auditoría a efectuarse o caso contrario determinará la no auditabilidad del objeto de auditoría, análisis que debe ser expuesto en el informe.

El informe de relevamiento deberá ser remitido a la Máxima Autoridad Ejecutiva de la entidad, en cumplimiento al Decreto Supremo Nº 23215 artículo 35º, que a letra señala: "Los informes de auditoría interna estarán dirigidos al *máximo ejecutivo de la entidad* y los de auditoría externa emitidos por las unidades de auditoría de entidades tutoras, firmas o profesionales calificados e independientes contratados por las entidades públicas, estarán dirigidas a la máxima autoridad, sea colegiada o no, de la entidad pública auditada".

El contenido del Informe debe cubrir el objetivo del relevamiento, considerando como mínimo los siguientes puntos:

ENTIDAD: (Nombre de la entidad)
REFERENCIA: (Titulo del relevamiento de información de ATIC)
DESTINATARIO: (Máxima Autoridad Ejecutiva de la entidad)
FECHA: (Fecha de emisión del Informe de Relevamiento)

ANTECEDENTES:
(Describir la naturaleza del relevamiento)
OBJETIVOS Y ALCANCES DEL RELEVAMIENTO
(Describir el objetivo del relevamiento y el alcance del mismo)
RESULTADOS DEL RELEVAMIENTO

- En este acápite se deberá identificar a las principales autoridades a la fecha de relevamiento: (Nombre del servidor público, cargo, documentación de designación, fecha de designación y antigüedad a la fecha de relevamiento).
- Antecedentes sobre el desarrollo formal de los sistemas operativos relacionados en el ámbito de tecnologías de la información (identificar las unidades de la parte tecnológica de la entidad).
- Objetivos y funciones del área objeto de relevamiento.
- Estructura organizacional del área objeto de relevamiento.

- Grado de implantación de las políticas, normas y procedimientos relacionadas a las tecnologías de la información.
- Reportar áreas de riesgo: información operativa para definir el grado de auditabilidad.

CONCLUSIÓN GENERAL

Este punto deberá ser utilizado cuando los resultados evidencian que el área relevada es auditable, por lo tanto el informe de relevamiento más la documentación que lo sustenta vienen a formar parte de la etapa de planificación de auditoría. Asimismo, señalar el ***enfoque de auditoría sugerido*** de acuerdo a lo establecido en las NAG 270, que pueden ser los siguientes:

- Enfoque a las Seguridades
- Enfoque a la Información
- Enfoque a la Infraestructura Tecnológica
- Enfoque al Software de Aplicación
- Enfoque a las Comunicaciones y Redes

RECOMENDACIONES

Las recomendaciones que se puedan emitir en el informe de relevamiento son utilizados cuando los resultados evidencian que el área relevada no es auditable, por lo tanto se debe informar del hecho y las acciones a seguir.

5. Anexos:

Anexo 1: Modelo del Programa de Relevamiento de Información de ATIC

Anexo 2: Modelo del informe de Relevamiento

Anexo 1: Modelo del Programa de Relevamiento de Información de ATIC

TITULO DEL OBJETO DE RELEVAMIENTO

PERIODO

OBJETIVO:

TIEMPO ASIGNADO:

TIEMPO REAL INCURRIDO:

Nº	PROCEDIMIENTO	REF P/T	HECHO POR (Iníciales y fecha)	REVISADO POR: (Iníciales y fecha)
	(Descripción del procedimiento) Para el caso de trabajo narrativo, seguir el siguiente orden de manera implícita: **¿Qué?** Describir el objeto de análisis o relevamiento. **¿Cómo?** Describir la forma como se desarrolla la tarea, actividad y/o procedimiento. **¿Quién?** Señalar el sujeto y/o personas responsables. **¿Por qué?** Describir el objetivo de la tarea, actividad y/o procedimiento. **¿Dónde?** Lugar donde se desarrolló la tarea, actividad y/o procedimiento. **Conclusión** Efectuar el análisis, sobre si el procedimiento cumple con los objetivos establecidos.			

Anexo 2: Formato del Informe de Relevamiento de Información ATIC

ESTRUCTURA DEL INFORME DE RELEVAMIENTO DE PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Titulo

Destinatario

Fecha

Antecedentes

Objetivos y alcances del relevamiento

Resultados del Relevamiento

a) Disposiciones legales y técnicas aplicadas

- Detalle de políticas, normas, procedimientos y/o buenas practicas
- Detalle de disposiciones técnicas aplicadas en el objeto de relevamiento

b) Estructura orgánica del área informática

- Procedimiento para la definición de la estructura
- Responsables de la definición de la estructura
- Medio de aprobación de la estructura
- Manuales de funciones de los responsables
- Memorándum de nombramiento y designación del cargo
- Niveles de autorización
- Niveles de supervisión
- Canal de comunicación utilizado
- Tipos de documentación que se generan y proceso de archivo
- Tipos de documentación digital y proceso de resguardo de la información
- Medidas de seguridad de la documentación física y digital y responsables de su custodia

c) Recursos humanos

- Responsables del proceso de tecnologías de la información
- Procedimiento de reclutamiento de personal
- Responsables del proceso de contratación del personal
- Términos de referencia o perfil del cargo
- Cantidad de personal
- Perfil del personal contratado

d) Recursos tecnológicos

- Detalle de software adquirido
- Detalle de hardware adquirido
- Grado de utilización de los recursos de software y hardware adquirido

e) Metodología de desarrollo

- Modelo del ciclo de vida utilizado
- Metodología utilizada para el desarrollo de software
- Definición de la estructura aplicada
- Etapas o fases del ciclo de vida aplicados
- Herramienta de desarrollo utilizados en cada fase
- Estándares aplicados en cada fase
- Documentación generada en cada fase (física/digital)
- Responsables de la custodia de la documentación
- Controles incorporados en cada fase
- Plataforma utilizada
- Arquitectura utilizada
- Modelo de Bases de Datos
- Diccionario de Datos
- Riesgos internos y externos identificados durante el desarrollo
- Modelo de codificación aplicada
- Lenguaje de codificación utilizado

f) Áreas críticas según las fases del proceso de TI

- Determinación de áreas críticas (condición, causa) en cada fase del proceso de TI
- Identificación de riesgos por fase

g) Conclusiones

- Sobre el cumplimiento de objetivos del proceso de TI
- Conclusiones sobre la adaptabilidad del proceso de TI
- Conclusiones sobre el grado de auditabilidad y enfoque propuesto

h) Recomendaciones

- En caso de no ser auditable emitir el informe señalando las acciones a seguir

ACLARACION: Este modelo de informe de relevamiento es tentativo, debiendo sujetarse al objetivo del relevamiento a realizar.

PROCEDIMIENTO- PLANIFICACIÓN DE LA ATIC

1. Objetivo

Definir claramente los objetivos y el alcance del trabajo, las técnicas y herramientas a utilizar, los recursos humanos, financieros, técnicos y cronograma de ejecución de la auditoría de tecnologías de la información y comunicación, de acuerdo a lo estipulado en las NAG – TIC 271.

2. Responsabilidad de su aplicación

El presente procedimiento es de cumplimiento obligatorio para el personal dependiente de la Dirección de Auditoría Interna:

- ✓ Director de Auditoría Interna
- ✓ Profesional y/o auditor Supervisor del área informática
- ✓ Auditores junior y/o personal especializado del área informática

3. Aspectos generales

3.1 Definiciones [27]

Datos: Son objetos de información en su sentido más amplio, los cuales pueden ser externos o internos, estructurados y no estructurados del tipo gráfico, sonido, imágenes, números, palabras y de otra índole, etc.

Información: Datos que han sido organizados, sistematizados y presentados de manera que los patrones subyacentes resulten claros.

Tecnología: Es un conjunto ordenado de instrumentos, conocimientos, procedimientos y métodos aplicados a las áreas.

Tecnologías de la Información y la Comunicación (TIC): Se refiere al conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de la información.

Sistema de Información (SI)*:* Se refiere a un conjunto de procesos y recursos de información organizados con el objetivo de proveer la información necesaria (pasada, presente, futura) en forma precisa y oportuna para apoyar la toma de decisiones en una entidad.

[27] Contraloría General de Estado, Nomas de Auditoria de Tecnologías de la Información y Comunicación, CGE, Bolivia, 2007 paginas 81-82

Software de Aplicación: Se refiere a un elemento de los Sistemas de Información, es un conjunto de programas de computador diseñados y escritos para realizar tareas específicas del negocio y que permiten la interacción entre el usuario y el computador.

Sistemas de comunicación: Se refiere a la tecnología que se emplea para el intercambio de información.

Confidencialidad de la información: Se refiere a la protección de la información crítica contra su divulgación no autorizada.

Integridad de la información: Se vincula con la exactitud y la totalidad de la información así como también con su validez de acuerdo con los valores y las expectativas de la entidad.

Confiabilidad de la información: Se vincula con la provisión de la información adecuada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de presentación de reportes financieros y de cumplimiento.

Disponibilidad de la información: Se vincula con el hecho de que la información se encuentre disponible cuando el proceso la requiera. También se asocia con la protección de los recursos necesarios y las capacidades asociadas.

Técnicas de Auditoría Asistidas por Computador (TAAC): Se refiere a las técnicas de auditoría que contemplan herramientas informáticas con el objetivo de realizar más eficazmente, eficientemente y en menor tiempo pruebas de auditoría.

Enfoque a las Seguridades: Consiste en evaluar las seguridades implementadas en los sistemas de información con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información.

Enfoque a la Información: Consiste en evaluar la estructura, integridad y confiabilidad de la información gestionada por el sistema de información.

Enfoque a la Infraestructura tecnológica: Consiste en evaluar la correspondencia de los recursos tecnológicos en relación a los objetivos previstos.

Enfoque al Software de Aplicación: Consiste en evaluar la eficacia de los procesos y controles inmersos en el software de aplicación, que el diseño conceptual de éste cumpla con el ordenamiento jurídico administrativo vigente.

3.2 Abreviaturas

Definir las abreviaturas para identificar los documentos y los responsables que participarán en el proceso de evaluación:

- ✓ DDAI: Director de la Dirección de Auditoría Interna
- ✓ Pi : Profesional y/o Supervisor del área informática
- ✓ Ai: Auditor junior y/o especializado en informática

- ✓ Pei: Personal especializado en informática
- ✓ PA – TIC: Programa de Auditoría de Tecnologías de la Información y Comunicación
- ✓ MPA – TIC: Memorándum de Planificación de Auditoría de Tecnologías de la Información y Comunicación
- ✓ NAG: Normas de Auditoría Gubernamental
- ✓ NAG – TIC: Normas de Auditoría de Tecnologías de la Información y Comunicación

3.3 Documentos de referencia

Debe consultarse la siguiente documentación para obtener más información sobre la planificación de auditoría:

- ✓ Normas de Auditoría de Tecnologías de la Información - Nº 271 Planificación emitida por la Contraloría General del Estado
- ✓ Normas de Auditoria de SI emitidas por ISACA, como ser:
  - Norma de Auditoría de SI – Documento Nº S5 Planeación
  - Guía de Auditoría de SI, G6 - Conceptos de materialidad para la auditoría de SI
  - Guía de Auditoría de SI, G15 – Planeación
  - Guía de Auditoría de SI, G13 - Uso de la evaluación de riesgos en la planeación de la auditoría
  - Guía de Auditoría de SI, G16 - Efecto de terceros en los controles de TI de una organización
  - COBIT versión 4.1
  - Directriz Nº G23"Revisión del Ciclo de Vida de Desarrollo de Sistemas SDLC" (aplicable para el enfoque de software de aplicación)

4. Descripción del procedimiento

4.1 Planificar la cobertura de la auditoría de tecnologías de la información para cubrir los objetivos de la Dirección de Auditoría y cumplir con las aplicables leyes y las normas profesionales de auditoría.

La Dirección de Auditoría Interna debe efectuar la planificación de las auditorías de tecnologías de la información y comunicación a realizar durante la gestión, que deben ser plasmados en el Plan Operativo Anual de la entidad y en el Plan Estratégico de la Dirección de Auditoría Interna, planificación que servirá de marco de referencia para las actividades permanentes de auditoría.

4.2 Desarrollar y documentar la planificación de auditoría que detalle la naturaleza y los objetivos de la auditoría TIC, los plazos y alcance así como los recursos requeridos.

El Auditor Gubernamental debe obtener un entendimiento de la actividad que está siendo auditada. El grado del conocimiento requerido debe ser determinado por la naturaleza de la entidad, su entorno y riesgos, y por los objetivos de la auditoría.

Lo que implica que debe obtener conocimiento general de los procesos sistematizados de la entidad, una evaluación de las fortalezas y debilidades y una lista de materias relacionadas con el área que sea de potencial importancia, en función al objeto de la auditoria, básicamente esta fase comprende:

- Conocimiento general de la entidad con relación al área de tecnologías de la información.
- Conocimiento específico del objeto de auditoría.

Conocimiento general de la entidad

- ✓ **Diagnóstico**

  Efectuar el análisis de la información, en base a la obtención del conocimiento formal general del entorno del objeto de auditoría y los obtenidos durante la fase de relevamiento de la información, misma que se profundizará en la elaboración del MPA – TIC. El diagnóstico debe estar orientado a cumplir lo estipulado por las NAG – TIC 271.02 - 03, lo que implica que se debe analizar:

  - Los sistemas de información y/o procesos automatizados relevantes.

- Efectuar una evaluación de riesgos para brindar una garantía razonable de que todos los elementos materiales serán cubiertos adecuadamente durante la auditoría y para establecer áreas críticas.
- Definir los objetivos y/o enfoques, objetivos específicos y alcances específicos.
- Determinar las metodologías, técnicas y criterios de evaluación.

✓ **Documentos Generales**

Recopilar los documentos para conocer el entorno del objeto de auditoría, como ser:

- Organización, organigrama donde se ubique el área de tecnología dentro de la entidad y el detalle de su estructura, nómina de personal por unidad (nombres y apellidos, cargos) funciones y responsabilidades
- Políticas de seguridad, normas, lineamientos y estándares, procedimientos operativos y administrativos
- Documentación sobre la planificación de desarrollo de software
- Documentación suministrada por proveedores externos de aplicación
- Contratos de nivel de servicios con proveedores externos de TI
- Planes de continuidad del negocio

Conocimiento específico del objeto de auditoría

✓ **Diagnóstico**

Efectuar el análisis de la información, en base a la obtención del conocimiento formal especifico del objeto de evaluación, de acuerdo al enfoque de auditoría recomendado en el informe de relevamiento y/o definido en la planificación. El diagnóstico debe estar orientado a cumplir lo estipulado por las NAG – TIC 271.02 - 03, por ejemplo para el enfoque de software de aplicación, el diagnostico se efectuara a:

- Los sistemas de información y/o procesos automatizados elegidos para el objeto de auditoría.

✓ **Documentos específicos**

Identificar la documentación específica acorde al enfoque de auditoría definido. Por ejemplo si es para el enfoque de software de aplicación se requerirá la siguiente documentación calificando su actualización y vigencia, como ser:

- Políticas, normas y procedimientos de desarrollo de software
- Requisitos funcionales y especificaciones de diseño
- Planes e informes de pruebas
- Programa y documentos de operaciones
- Registros (logs) e historial de cambios a programas
- Manuales de usuario
- Manuales de operación
- Documentos relacionados con la seguridad de los procesos tecnológicos
- Informe de aseguramiento de la calidad de los procesos tecnológicos
- Reportes sobre métricas de seguridad

Toda la información recopilada en esta fase debe ser reflejada en el Memorándum de Programación de Auditoría de Tecnologías de la Información y Comunicación (MPA - TIC), este documento puede ser modificado según las circunstancias que se presenten durante la ejecución de la auditoría, el cual debe ser de conocimiento del equipo de auditoría.

El MPA – TIC, es un documento resumen el cual debe contener todos los aspectos definidos por la NAG - TIC y aquellos que se consideren necesarios incluir y que tengan relación con el objeto del examen, el alcance y la metodología.

La evaluación de los procesos tecnológicos comprenderá los cinco enfoques en su conjunto o uno, o más enfoques individualizados; por lo que el MPA – ATIC deberá identificar los enfoques que serán evaluados.

Los aspectos importantes que debe contener el Memorándum de Planificación de Auditoría se describen en el siguiente acápite.

4.3 Contenido y desarrollo del documento Memorándum de Planificación de Auditoría de Tecnologías de la Información y Comunicación (MPA - TIC)

- **Términos de referencia**

  Se describe todas las características fundamentales para iniciar el trabajo de auditoría.

- **Conocimiento de la entidad y/o área objeto de auditoría**

  Se debe plasmar toda la información obtenida en base al conocimiento general de la entidad con relación al área de tecnologías de la información y conocimiento específico del objeto de auditoría, evaluando y documentando los aspectos definidos en las NAG –TIC 270.01-06.

- **Planificación y metodología adoptada**

  Describir la naturaleza, extensión y oportunidad de los procedimientos y técnicas a ser aplicados para obtener evidencia competente, suficiente y necesaria para alcanzar los objetivos definidos, entre los que se puede mencionar:

  - ✓ Diagnostico (Revisión y análisis de los manuales técnicos diagramas entidad relación, diagrama de flujo de datos, diccionario de datos, etc.)
  - ✓ Pruebas de recorrido
  - ✓ Pruebas de cumplimiento
  - ✓ Cursogramas
  - ✓ Cuestionarios
  - ✓ Observaciones físicas

- ✓ Inspecciones
- ✓ Confirmaciones
- ✓ Otros

Describir las herramientas CAATs (Computer Assisted Audit Techniques and Tools - Técnicas y Herramientas de auditoría con ayuda del computador) que coadyuvará en el análisis de la información técnica necesaria para efectuar el trabajo de auditoría, como ser:

- ✓ Software generalizado,
- ✓ Software de depuración y rastreo,
- ✓ Datos de prueba,
- ✓ Rastreo y correlación de software de aplicación
- ✓ Sistemas expertos.

- **Administración del trabajo**

Definir el equipo de trabajo de auditoría, los costos y el cronograma de ejecución por fases, como por ejemplo:

- ✓ Personal asignado
- ✓ Cargo
- ✓ Horas presupuestadas
- ✓ Fecha de inicio de la evaluación
- ✓ Fecha de entrega del informe en Borrador
- ✓ Fecha de culminación de la evaluación
- ✓ Costo de la evaluación

La elección del criterio fundamentalmente dependerá del juicio profesional del Auditor Gubernamental.

4.4 Desarrollar el Programa de Auditoría de Tecnologías de la Información y Comunicación (PA – TIC) detallando la naturaleza, los plazos y el alcance de los procedimientos requeridos para completar la auditoría.

Los programas y/o cuestionarios deben elaborarse a la medida del objeto de evaluación, los cuales pueden requerir ajustes durante el desarrollo de la auditoría

para abordar las situaciones que surjan (nuevos riesgos, suposiciones incorrectas o hallazgos en los procedimientos ya realizados) durante la auditoría.

Por ejemplo, el criterio para elaborar el programa de auditoría para el ENFOQUE DE SOFTWARE DE APLICACIÓN, puede ser realizado en base a los criterios definidos en la metodología COBIT dominio ADQUIRIR E IMPLEMENTAR, punto AI2 Adquirir y Mantener Software Aplicativo y directriz Nº G23 *"Revisión del Ciclo de Vida de Desarrollo de Sistemas SDLC*" ambos emitidos por ISACA.

5. Anexos

Anexo 1: Formato del Memorándum de Programación de Auditoria

Anexo 2: Modelo del Programa de Auditoría

Anexo 1: Formato del Memorándum de Planificación de Auditoría de Tecnologías de la Información y Comunicación (MPA – TIC)

ESTRUCTURA DEL MEMORANDUM DE PLANIFICACIÓN DE AUDITORÍA – TIC

Términos de referencia

- Naturaleza, objeto, objetivos y enfoque de auditoría
- Alcance del trabajo
- Limitaciones
- Disposiciones legales y profesionales a aplicar
- Emisión de informes
- Actividades y fechas de mayor importancia

Conocimiento de la entidad y/o área objeto de auditoría

- Antecedentes de la entidad, Misión, Visión
- Mandato Legal
- Facultades y Competencias de la entidad
- Actividades principales de la entidad
- Tuición entidad tutora
- Estructura organizativa
    - Organigrama Institucional
    - Organigrama Específico de Puestos de la entidad
    - Organigrama Específico de Puestos de la Dirección de Tecnologías de la Información
- Detalle del personal dependiente de la Dirección de Tecnologías de la Información
- Políticas, normas y procedimientos institucionales con relación a la administración de la información
- Principales sistemas de información
- Uso de las comunicaciones
- Ambiente de Control
- Auditoría interna
- Auditoría Externa

Planificación y metodología a aplicar

- Alcance
- Metodología
- Obtención de la información
- Riesgos de Auditoría

Administración del trabajo

- Personal y tiempo presupuestado

- Uso de especialistas

Programas de trabajo

- El contenido debe reflejar para evaluar el enfoque y/o los enfoques definidos.

Anexo 2: Modelo del Programa de Auditoría

GENERALIDADES DE LA ENTIDAD

PROGRAMA DE AUDITORIA

PERIODO

OBJETIVO:

TIEMPO ASIGNADO:

TIEMPO REAL INCURRIDO:

Nº	PROCEDIMIENTO DESAROOLADO	REF P/T	HECHO POR (Iníciales y fecha)	REVISADO POR: (Iníciales y fecha)
	(Descripción del procedimiento)			

PROCEDIMIENTO – EJECUCIÓN DE LA ATIC

1. Objetivo

Definir los aspectos necesarios para llevar a la práctica los programas de auditoría en base a la obtención de la evidencia de auditoría suficiente, pertinente y competente e información adicional para reconsiderar las evaluaciones realizadas, en base a las Normas de Auditoría Gubernamental 224.02-13, emitida por la Contraloría General del Estado.

2. Responsable de su aplicación

El presente procedimiento es de cumplimiento obligatorio para el personal dependiente de la Dirección de Auditoría Interna:

- ✓ Director de Auditoría Interna
- ✓ Profesional y/o auditor Supervisor del área informática
- ✓ Auditores junior y/o personal especializado del área informática

3. Aspectos generales

3.1 Definiciones[28]

Legajo de Programación: Este legajo debe contener y conservar toda aquella información sobre aspectos inherentes a la programación efectiva de la auditoría, corresponde a la fase de planificación de la auditoria.

Legajo Corriente: En este legajo se mantendrá toda la información y documentación obtenida y/o preparada por el equipo de auditoría durante el proceso de ejecución de la auditoría.

Legajo Permanente: Este legajo deberá conservar información y documentación para consulta continua, la misma que debe ser periódicamente actualizada a fin de proporcionar datos útiles en todas las etapas del proceso de auditoría, facilitando al personal involucrado su familiarización con el área a ser auditada.

[28] Lic. Eddy M. Salinas Rojas y Coautores, Compendio para la Elaboración de Manual de Procedimientos para el ejercicio de la Auditoría Interna Gubernamental, Simmer, Bolivia – Santa Cruz, 2008

3.2 Abreviaturas

Las abreviaturas que se utilizarán y para identificar a los responsables durante la ejecución de la auditoría son las siguientes:

- ✓ DDAI: Director de la Dirección de Auditoría Interna
- ✓ Pi : Profesional y/o Supervisor del área informática
- ✓ Ai: Auditor junior y/o especializado en informática
- ✓ Pei: Personal especializado en informática
- ✓ PA: Programa de Auditoría

3.3 Documentos de referencia

- ✓ Normas de Auditoría Gubernamental emitida por la Contraloría General del Estado.
- ✓ Normas de Auditoría de Tecnologías de la Información y Comunicación NAG –TIC Nº 272 emitida por la Contraloría General del Estado.
- ✓ Norma de Auditoría de Sistemas de Información – S6 Realización de Labores de Auditoría emitida por ISACA
- ✓ Metodología COBIT, compendio de objetivos de control emitida por ISACA.

4. Descripción del procedimiento

4.1 Supervisión - El personal de auditoría debe ser supervisado para brindar una garantía razonable de que se lograrán los objetivos de la auditoría y que se cumplirán las normas profesionales de auditoría aplicables.

Se deben establecer los roles y responsabilidades del equipo de auditoría de tecnologías de la información y comunicación al iniciarse la auditoría, y como mínimo deben definirse los roles de decisión, ejecución y revisión en base a la estructura orgánica establecida para la Dirección de Auditoría Interna de la entidad.

El nivel de supervisión debe ser cubierto por personal competente, el cual pueda ejecutar sistemática y oportunamente el trabajo realizado por los auditores que conforman el equipo de auditoría. Acorde a lo establecido en la NAG TIC Nº 272 las funciones del nivel de supervisión son los siguientes:

- La supervisión implica que personal competente y calificado para ejercerla, debe dirigir los esfuerzos del equipo de auditores gubernamentales hacia la consecución de los objetivos de auditoría.
- La supervisión debe ser realizada en cada una de las etapas de la auditoría, la misma incluye:
    - Examinar la factibilidad y/o razonabilidad técnica de los objetivos y alcances de la auditoria propuestos.
    - Asegurar que los miembros del equipo comprendan los objetivos de la auditoría. En particular se debe asegurar que entiendan claramente el trabajo a realizar, porqué se va efectuar y qué se espera lograr.
    - Guiar a los miembros del equipo de auditoría a lo largo del desarrollo de las tareas asignadas.
    - Revisar oportunamente el trabajo realizado, a través de los respectivos papeles de trabajo físicos y si fuera el caso como respaldo en papeles de trabajo electrónicos.
    - Ayudar a absolver problemas técnicos y administrativos.
    - Detectar debilidades del personal asignado y proporcionar en consecuencia la capacitación necesaria o asegurarse que la misma sea proporcionada por terceros.
    - Asegurar que la evidencia obtenida sea suficiente y competente.

- La supervisión efectuada durante el desarrollo de la auditoría, debe estar evidenciada en los papeles de trabajo físicos y si fuera el caso como respaldo en papeles de trabajo electrónicos, acumulados durante la misma.

4.2 Ejecución - El Auditor Gubernamental de Tecnologías de la Información y Comunicación debe obtener evidencia suficiente, confiable y pertinente para alcanzar los objetivos de auditoría.

El Auditor Gubernamental de Tecnologías de la Información y Comunicación debe obtener toda la evidencia de acuerdo a los términos definidos en el documento Programa de Auditoría de Tecnologías de la Información y Comunicación (definido en el Procedimiento – Planificación de la ATIC) cumpliendo los siguientes requerimientos:

- La evidencia de auditoría debe ser suficiente, confiable y pertinente para formar una opinión o respaldar los hallazgos y conclusiones del Auditor Gubernamental, si en opinión del Auditor Gubernamental, la evidencia de auditoría obtenida no cumple con estos criterios, el Auditor Gubernamental deberá obtener evidencia de auditoría adicional.
- Los hallazgos y conclusiones de la auditoría deberán ser soportados mediante un apropiado análisis e interpretación de dicha evidencia.
- El Auditor Gubernamental para obtener parte de la evidencia, debe planificar y ser competente en el uso de las herramientas CAATs (Técnicas de Auditoría Asistidas por Computador).
- La evidencia obtenida por el Auditor Gubernamental debe conservarse en papeles de trabajo físicos y los obtenidos con las herramientas CAATs en papeles de trabajo digitales, como respaldo del proceso de auditoría.

4.3 Documentación - El proceso de auditoría deberá documentarse, describiendo las labores de auditoría realizadas y la evidencia de auditoría que respalda los hallazgos y conclusiones del Auditor Gubernamental.

El Auditor Gubernamental debe definir la estructura y clasificación de la documentación producto del trabajo realizado desde la fase de actividades previas, relevamiento, planificación, ejecución y comunicación de resultados que formará parte del legajo de programación, legajo corriente y legajo permanente.

La documentación de auditoría debe ser suficiente para permitir que una tercera entidad independiente vuelva a realizar todas las tareas realizadas durante la auditoría para llegar a las mismas conclusiones.

En la elaboración del formato de auditoría debe incluir detalles de quién realizó cada tarea de auditoría y sus funciones. Como regla general, cada tarea, decisión, paso o resultado de la auditoría realizado por un miembro o grupo de miembros del equipo deberá ser revisado por otro auditor del equipo, nombrada de acuerdo con la importancia del elemento considerado.

Los papeles de trabajo[29] que sean generados durante la evaluación deben contener como mínimo la siguiente información:

Encabezamiento*:* incluirá el nombre de la entidad pública, ejercicio económico, tipo de auditoría y área o componente específico, objeto de la auditoría.

Referencias: cada papel de trabajo tendrá su propia referencia, y deberá indicar las hojas de trabajo relacionadas de acuerdo con un sistema de referencias cruzadas o correferencias que permita la revisión.

Fecha e Identificación de quién preparó el papel de trabajo: Mediante rúbrica de la persona que ha contribuido a su elaboración, así como la fecha de realización.

Fecha e Identificación de quién supervisó el trabajo: Mediante iníciales de la persona que revisó el trabajo realizado, como constancia de la supervisión efectuada.

Referencia al paso del programa de trabajo*:* A fin de conocer el objetivo de preparación de la cédula.

El análisis realizado: El mismo estará en función a la ejecución de los procedimientos de auditoría a fin de cumplir con lo definido en los programas de trabajo.

Alcance del trabajo: Relacionando el análisis realizado con el total del rubro, cuenta u operación, objeto del examen, indicando el tamaño de las muestras y la forma de su obtención.

[29] Contraloría General del Estado, Papeles de Trabajo, CGE – CENCAP, Bolivia

Método de muestreo: Cuando sea aplicable será necesario hacer referencia al método de muestreo aplicado.

Fuente de la información obtenida: Se señalará los registros contables o archivo en base al cual fue preparada la cédula, referencia a los documentos base y las personas que la facilitaron.

Explicación de las marcas de auditoría utilizadas: En la parte inferior de la cédula se deberá realizar una descripción del significado de las marcas de auditoría utilizadas en la misma, en el caso de que ésta explicación se encuentre en otra cédula se hará referencia a la misma.

Conclusiones: Cuando corresponda*, se realizará una* exposición sucinta de los resultados logrados con el trabajo, una vez finalizado.

***Documentación preparada o proporcionada por la entidad*:** En el caso de que la cédula haya sido confeccionada y proporcionada por la entidad, en ésta se deberá consignar las iníciales PPE (papel proporcionado por la entidad) y se registrará el trabajo realizado y las referencias y correferencias necesarias, a fin de establecer la utilidad de incluir estas cédulas como parte de los papeles de trabajo.

5. Anexos

Anexo 1: Siglas, estructura y contenido de los legajos de auditoría

Anexo 2: Definición de marcas de auditoría, simbología que se utilizará para marcar las operaciones realizadas en los papeles de trabajo.

Anexo 3: Diseño de los papeles de trabajo, se define el formato de los papeles de trabajo para recopilar las evidencias de auditoría.

Anexo 4: Diseño y contenido de las deficiencias encontradas durante el trabajo de auditoría.

Anexo 1: Siglas, estructura y contenido de los legajos de auditoría

- **Por tipo de auditoría**

SIGLA	DESCRIPCION
ATs	Auditoría de Tecnologías de la Información y Comunicación bajo el enfoque a la Seguridad
ATi	Auditoría de Tecnologías de la Información y Comunicación bajo el enfoque a la información
ATt	Auditoría de Tecnologías de la Información y Comunicación bajo el enfoque a la infraestructura tecnológica
ATw	Auditoría de Tecnologías de la Información y Comunicación bajo el enfoque al software de aplicación
ATc	Auditoría de Tecnologías de la Información y Comunicación bajo el enfoque a las comunicaciones y redes

- **Referencia y contenido de los legajos de auditoría**

REFERENCIA	DESCRIPCIÓN
LPr LPrI/1 … n LPr II/1 … n LPr III/1 … n LPr IV/1 … n	**Legajo de Programación** Memorándum de Planificación de Auditoría TIC Programas de Auditoría o cuestionarios Informe Final Correspondencia
LC LC I/1 a la n LC II/1 a la n LC III/1 a la n LC IV/1 a la n	**Legajo Corriente** Conclusión Deficiencias Programas de Auditoría Papeles de trabajo Documentos de respaldos
LP LP I/1..n	**Legajo Permanente** Antecedentes legales y generales - Legislación vinculada a la institución - Relación de tuición a la vinculación - Estructura organizativa - Principales responsabilidades de la ejecutiva - Rotación del nivel de ejecutivos - Numero de servidores públicos en general y por área - Reglamentos, manuales y normas - Plan estratégico institucional por orden cronológico - Contratos - Propiedades de bienes inmuebles de la entidad

REFERENCIA	DESCRIPCIÓN
LP II/1..n	Naturaleza de las actividades - Naturaleza de las actividades - Detalle de servicios que presta la entidad - Políticas y normas relacionadas a la naturaleza de la actividad
LP II/1..n	Información económica y financiera - Estados financieros en orden cronológico - Principales fuentes de generación de recursos
LP IV/1..n	Control Posterior - Antecedentes y características de la UAI - Manuales y documentos normativos - Detalle de informes de auditoria - Historial de capacidad de la UAI - Flujogramas y/o narrativos de los ciclos transaccionales más importantes
Lr	**Legajo de Relevamiento de Información**
Lr I/1	Informe de relevamiento
Lr II	Programa de Relevamiento de la Información
Lr III	Papeles de trabajo
Lr IV	Documentación de Respaldo

ACLARACION: El legajo de programación y legajo corriente son parte de una auditoria, el legajo permanente es parte de la documentación de la Dirección de Auditoría Interna y el legajo de relevamiento es un legajo separado.

Anexo 2: Definición de marcas de auditoría, simbología que se utilizará para marcar las operaciones realizadas en los papeles de trabajo.

Objetivo:

El uso de las marcas de auditoría es uniformar el criterio de aplicación de marcas de auditoría y su utilización en la elaboración de los papeles de trabajo, a fin de facilitar la lectura e interpretación de éstos, y coadyuvar en las labores de revisión y supervisión de la auditoría.

Reglas para el uso de marcas de auditoría[30]

1. Las marcas deben ser escritas al costado de la partida o saldo trabajado con lápiz o tinta de color rojo, a fin de facilitar su visualización.
2. El significado de la marca utilizada debe ser anotado en forma clara y concisa en la parte inferior del papel de trabajo, o en una hoja separada, si la marca ha sido utilizada en más de un papel de trabajo (resumen de marcas).
3. El Auditor Gubernamental que ha utilizado la marca deberá inicializar (rubricar) el significado de la misma como evidencia de haber realizado satisfactoriamente el procedimiento aplicado.
4. No se debe utilizar una misma marca para explicar la ejecución de procedimientos diferentes dentro de una misma planilla o de un mismo resumen de marcas.
5. Debe evitarse el recargar un papel de trabajo con el uso excesivo de marcas, para no crear confusión y dificultar la revisión de los papeles de trabajo y la supervisión.

Los símbolos que se pueden utilizar en auditorías informáticas dependerá del enfoque de la auditoria, éste podrá ser empleado de acuerdo al criterio del auditor gubernamental

[30] Lic. Eddy M. Salinas Rojas y Coautores, Compendio para la Elaboración de Manual de Procedimientos para el ejercicio de la Auditoría Interna Gubernamental, Simmer, Bolivia – Santa Cruz, 2008
.

Por ejemplo; se propone algunos de los símbolos que podrían ser utilizados en auditoria de tecnologías de la información en general:

MARCAS	DESCRIPCION
T	Cumple con el criterio de confidencialidad
I	Cumple con el criterio de integridad
C	Cumple con el criterio de confiabilidad
BD	Verificado con Bases de Datos
@	Incluir en el informe
FD	Fuente de datos
N/A	No aplicable
S/D	Sin documento de respaldo

Anexo 3: Diseño de los papeles de trabajo, se definirá el formato de los papeles de trabajo para recopilar las evidencias de auditoría

GENERALIDADES DE LA ENTIDAD

TÍTULO DEL OBJETO DE LA AUDITORÍA
PERIODO
Número y nombre del procedimiento

Desarrollo y análisis de las tareas a realizar de acuerdo al programa de auditoría

Objetivo, alcance y método del muestreo
(Describir el objetivo del procedimiento, el alcance y la muestra)

Fuente:
(Describir la fuente y el autor del origen de la información obtenida)

Detalle de marcas de auditoría:
(Describir las marcas de auditoría utilizadas para verificar el procedimiento)

Conclusiones:
(Describir las relaciones y/o diferencias encontradas en el papel de trabajo, cuando corresponda)

REF P/T

ELABORDO POR:……. FECHA:
REVISADO POR:……. FECHA:

Anexo 4: Diseño y contenido de las deficiencias de auditoría, de las deficiencias encontradas durante el trabajo de auditoría

GENERALIDADES DE LA ENTIDAD

TÍTULO DEL OBJETO DE AUDITORÍA
PERIODO
Nº Correlativo por deficiencia
Título de la deficiencia

Ref. P/T	DEFICIENCIA DE AUDITORÍA	HECHO POR (Iníciales y fecha)	REVISADO POR: (Iníciales y fecha)
	Condición (Constituye la situación detectada por el auditor evaluador para validar los resultados logrados en el trabajo de campo, la misma debe ser relatada objetivamente; en sentido amplio, la condición se convierte en una revelación de "lo que es" puede incluir aquellos elementos que el auditor evaluador distingue o reconoce por medio de la aplicación de técnicas y procedimientos de auditoría) **Criterio** (Constituye la manifestación de "lo que debe ser" en el contexto del desarrollo de las operaciones que se examinan, según consta en estándares, leyes, normas, procedimientos internos, políticas contratos etc. los criterios sirven para determinar el cumplimiento a través de procesos comparativos o posibilitan la utilización de parámetros e indicadores cualitativos o cuantitativos que orientan las acciones del auditor evaluador y facultan el logro de los objetivos del examen). (En la medida de lo posible, los criterios deben ser seleccionados por el auditor evaluador en base de su experiencia y conocimientos especializados; para ello, es posible recurrir a la identificación de parámetros de comparación específicos, unidades de medida, indicadores técnicos, metas institucionales de la entidad sujeto de auditoría, normas técnicas internacionalmente aceptadas, registros históricos de la operación que se audita, etc. Es fundamental tener presente que los criterios elegidos deben ser razonables, verificables, relevantes (relación directa con el objeto de auditoría), válidos (consistentes con los hechos) y establecidos en función de las circunstancias reales que rodean el desarrollo del objeto de la auditoría). **Causa** (La causa es la revelación de los motivos o razones del por qué se produjo el efecto, la situación, debilidad o deficiencia detectada). **Efecto** (Constituye el resultado de la comparación practica entre "lo que es" con respecto a "lo que debió ser". Es la consecuencia de la desviación detectada por el auditor evaluador o también el riesgo potencial de mantener inalterada tal condición respecto del logro de los objetivos perseguidos; es decir, la medida del impacto generado por la desviación)		

Ref. P/T	DEFICIENCIA DE AUDITORÍA	HECHO POR (Iníciales y fecha)	REVISADO POR: (Iníciales y fecha)
	Recomendación (La recomendación constituye el criterio del auditor evaluador y debe reflejar el conocimiento y buen juicio con relación a lo que más conviene a la entidad auditada. En general una recomendación se basa en el análisis de los recursos y en la consideración del costo/beneficio de la misma con objeto de disolver o minimizar la causa que originó la deficiencia. La recomendación se la efectúa a la máxima autoridad ejecutiva de la entidad auditada para que este adopte las medidas necesarias para implantar las recomendaciones).		

PROCEDIMIENTO - COMUNICACIÓN DE RESULTADOS DE LA ATIC

1. Objetivo

Formalizar la estructura y contenido mínimo de los informes de auditoría de tecnologías de la información y comunicación, en base a la NAG – TIC 275 01-04.

2. Responsables de su aplicación

El presente procedimiento es de cumplimiento obligatorio para el personal dependiente de la Dirección de Auditoría Interna:

- ✓ Director de Auditoría Interna
- ✓ Profesional y/o auditor Supervisor del área informática
- ✓ Auditores junior y/o personal especializado del área informática

3. Aspectos generales

3.1 Definiciones[31]

Informe de Auditoría: Es el documento mediante el cual el auditor gubernamental comunica por escrito los resultados de la auditoría o evaluación realizada

Utilidad: La utilidad de un informe está representada por el grado de beneficio que se pueda obtener de él para mejorar la probabilidad de lograr los objetivos de la entidad, corrigiendo las deficiencias y desviaciones detectadas.

Oportunidad: Los informes deben emitirse oportunamente para que su información pueda ser utilizada por el ejecutivo de la entidad y entidades gubernamentales relacionadas con la misma.

Objetividad: Los hechos deben ser presentados de manera objetiva y ponderada, es decir con la suficiente información que permita al usuario una adecuada interpretación de los asuntos expuestos en el informe.

Claridad y tono constructivo: El informe debe ser redactado en lenguaje sencillo, entendible y constructivo, tratando los asuntos en forma concreta y

[31]Contraloría General de Estado, Nomas de Auditoria de Tecnologías de la Información y Comunicación, CGE, Bolivia,

concisa, los que deben coincidir de manera exacta y objetiva con los hechos observados.

Veracidad: Requiere que la evidencia presentada sea verdadera y que los hallazgos estén correctamente expuestos. Se basa en la necesidad de asegurar que la información que se presente sea confiable a fin de evitar errores que podrían restar credibilidad y generar el cuestionamiento y validez sustancial del informe.

3.2 Abreviaturas

Definir las abreviaturas que se utilizarán durante el desarrollo de la auditoría, y para identificar a los responsables durante el desarrollo de la evaluación:

- ✓ DDAI: Director de la Dirección de Auditoría Interna
- ✓ Pi : Profesional y/o Supervisor del área informática
- ✓ Ai: Auditor junior y/o especializado en informática
- ✓ Pei: Personal especializado en informática
- ✓ PA: Programa de Auditoría
- ✓ NAG: Normas de Auditoría Gubernamental
- ✓ NAG – TIC: Normas de Auditoría de Tecnologías de la Información y Comunicación.

3.3 Documentos de referencia

- ✓ Normas de Auditoría Gubernamental emitida por la Contraloría General del Estado
- ✓ Normas de Auditoría de Tecnologías de la Información y Comunicación–275 Comunicación de Resultados emitida por la Contraloría General del Estado.
- ✓ Normas de Auditoría de Sistemas de Información – S7Reporte emitido por ISACA.

4. Descripción del procedimiento

4.1 El Auditor Gubernamental debe emitir el informe final de la auditoría en un formato adecuado y establecer el flujo de comunicación con la parte auditada, bajo las siguientes características:

- El informe debe identificar la organización, los destinatarios previstos y respetar cualquier restricción con respecto a su circulación, para el caso de la entidad.
- El informe de auditoría debe indicar el alcance, los objetivos, el enfoque, el período de cobertura y la naturaleza, plazo y extensión de las labores de auditoría realizadas.
- El informe de auditoría debe indicar los hallazgos, conclusiones y recomendaciones, así como cualquier reserva, calificación o limitación que el Auditor Gubernamental tuviese en cuanto al alcance de la auditoría.
- El Auditor Gubernamental debe comentar el contenido del informe en borrador con la jefatura del área bajo revisión antes de la finalización y divulgación, e incluir los comentarios de la jefatura en el informe final cuando corresponda.
- El orden de la redacción del informe debe ir de manera implícita tomando en cuenta la condición, criterio, causa, efecto y recomendación descritos en las deficiencias de auditoría.
- En cumplimiento al Decreto Supremo Nº 23215 artículo 35º emitido por la Contraloría General del Estado, establece que: “Los informes de auditoría interna estarán dirigidos al máximo ejecutivo de la entidad…”. En tal sentido al emitirse el informe de auditoría final, éste debe ser firmado y fechado por el Director de la Dirección de Auditoría Interna de la entidad y remitido a la Máxima Autoridad Ejecutiva, Contraloría General del Estado, Ministerio de Economía y Finanzas (por ser ente tutor) y el Directorio del RUAT (compuesto por los representantes de los Gobiernos Municipales adscritos al RUAT).

4.2 Estructura y contenido del Informe de Auditoría de Tecnologías de la Información y Comunicación

La estructura y contenido del Informe de Auditoría de Tecnología de la Información y Comunicación, debe estar acorde a los puntos establecidos por la NAG –TIC Nº 270.01 al 04:

El informe de auditoría está compuesto por dos partes; la primera corresponde al informe ejecutivo y la segunda al informe analítico en el cual se describen las deficiencias que se reportarán en el informe, el orden es el siguiente:

INFORME EJECUTIVO:

RESUMEN EJECUTIVO

ENTIDAD: (Nombre de la entidad)

REFERENCIA: (Nombre de la auditoria, enfoque y periodo de ejecución)

OBJETIVO: (Descripción del objetivo de la auditoría)

FECHA: (Fecha de emisión del informe)

RESULTADOS: (Nómina de deficiencias)

INFORME ANALITICO:

DESTINATARIO: (Máxima Autoridad Ejecutiva de la entidad)

ANTECEDENTES:

(Resumen del objeto de auditoría)

OBJETO:

(Nombre del objeto de auditoría)

OBJETIVO:

(Mencionar la categoría de objetivos que se cumplirán en la evaluación)

ENFOQUE DE AUDITORIA:

(Mencionar bajo que enfoque se desarrolló la auditoria)

ALCANCE

(Mencionar bajo qué criterios se desarrolló la auditoría)

LIMITACIONES

(Mencionar los impedimentos que se presentaron durante el desarrollo de la auditoria)

METODOLOGÍA

(Describir los principales procedimientos, técnicas y herramientas Catas aplicados para el desarrollo de la auditoría)

RESULTADOS DE LA EVALUACION

Describir las deficiencias en el siguiente orden:

Número y título de la deficiencia

(Enumerar y describir el título de la deficiencia de acuerdo al formato de la deficiencia de auditoría)

Descripción del hallazgo

(Describir el hallazgo considerando de manera implícita el orden definido en las deficiencias (condición, criterio, causa, efecto, recomendación y comentario de la parte auditada si corresponde)

CONCLUSIONES

(Describir las conclusiones en base a las inferencias lógicas sobre el objeto de la auditoría, basadas en los hallazgos expresados explícitamente de manera convincente y persuasiva, evitando el riesgo de interpretaciones por parte de los lectores)

RECOMENDACIÓN

(Parágrafo de carácter obligatorio)

"En aplicación de lo previsto en la Resolución CGR 01/97, emitida por la Contraloría General de la República (actual Contraloría General del Estado), sugerimos a su autoridad instruya a la Dirección de Tecnologías de la Información que dentro los diez días hábiles desde la recepción del presente informe de auditoría, presente por escrito los formatos 1 y 2 de aceptación e implantación de recomendaciones presentadas a la Dirección de Auditoría Interna, caso contrario fundamentar su decisión por la no aceptación de las mismas.

Asimismo, deberá presentar un cronograma de implantación de las recomendaciones aceptadas para su respectivo seguimiento. El mencionado cronograma deberá ser remitido a la Subcontraloría de Control Interno de la Contraloría General del Estado, dentro de los plazos previstos".

Es cuanto informo para los fines consiguientes.

LUGAR Y FECHA
(Describir el lugar y la fecha de emisión del informe)

NOMBRE, APELLIDOS Y RUBRICA DEL AUDITOR GUBERNAMENTAL RESPONSABLE
(Describir nombres y apellido; cargo del Director y/o responsable de la Dirección de Auditoría Interna de la Entidad y rúbrica correspondiente)

5. Anexos

Anexo 1: Estructura del Informe de Auditoria

Anexo 1: Formato del Informe de Auditoría de Tecnologías de la Información y Comunicación

ESTRUCTURA DEL INFORME DE AUDITORÍA – TIC

RESUMEN EJECUTIVO

- Entidad:
- Referencia:
- Objetivo:
- Fecha:
- Resultados

INFORME ANALITICO

- Destinatario
- Antecedentes
- Objeto
- Objetivo
- Enfoque de auditoría
- Alcance
- Limitaciones
- Metodología
- Resultados de los hallazgos de auditoría
- Conclusiones
- Recomendación
- Lugar y Fecha
- Nombres, apellidos y rubrica del auditor gubernamental responsable

CAPITULO VI
CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- ✓ El modelo de propuesta del presente trabajo de investigación fue desarrollado de manera experimental en la Dirección de Auditoría Interna del Registro Único para la Administración Tributaria Municipal, cuyo resultado aportó en la mejora del control interno de los procesos tecnológicos que desarrolla la entidad.

- ✓ La aplicación de auditorías de tecnologías de la información y comunicación son muy poco desarrolladas por las unidades de auditoría interna del ámbito gubernamental, en especial en la entidad objeto de investigación, debido a la carencia de procedimientos formales que posibiliten la uniformidad y calidad de las auditorias.

- ✓ A través del diagnóstico desarrollado se pudo advertir que existen muchas limitaciones para la ejecución de este tipo de auditorías. Estas comienzan, por la ausencia de normas nacionales específicas que permitan evaluar el entorno tecnológico de las entidades estatales, a la fecha nos regimos por normas internacionales basadas en buenas prácticas para la evaluación correspondiente; el avance de las tecnologías de la información ha generado una gama de especialidades y para su respectiva evaluación existe un número reducido de auditores especializados.

- ✓ Es necesario fortalecer el control interno de los procesos tecnológicos en el ámbito gubernamental, de acuerdo a lo estipulado en Ley Nº 1178 “SAFCO” y Decreto Supremo 23215, Reglamento que regula el ejercicio de las atribuciones conferidas por la Ley Nº 1178 a la Contraloría General de la República (actual Contraloría General del Estado) como Órgano Rector del Control Gubernamental y autoridad superior de auditoría del Estado.

- ✓ Es necesario que la Dirección de Auditoría Interna formalice los procedimientos para la ejecución de auditorías de tecnologías de la información y comunicación a objeto de fortalecer el control interno y mejorar los procesos de tecnologías de la información de la Dirección de Tecnologías de la Información y coadyuvar en el logro de los objetivos institucionales del Registro Único para la Administración Tributaria Municipal.

- ✓ El presente enfoque metodológico propuesto para la ejecución de auditorías de tecnologías de la información y comunicación fue desarrollado en base a procedimientos que concilian con las normas estipuladas para el ámbito gubernamental, sin embargo no se considera la evaluación del control interno debido a su amplitud.

6.2 RECOMENDACIONES

- ✓ A fin de garantizar la calidad y uniformidad de las auditorias que desarrolla la Dirección de Auditoría Interna del Registro Único para la Administración Tributaria Municipal, se recomienda viabilizar la formalización de los procedimientos elaborados para la ejecución de auditorías de tecnologías de la información y comunicación mediante los instrumentos legales establecidos por la entidad para que su aplicabilidad sea de carácter obligatorio.

- ✓ A objeto de fortalecer las normas de auditoría que permitan evaluar los procesos tecnológicos, el Consejo Técnico Nacional de Auditoría y Contabilidad del Colegio de Auditores de Bolivia debería homologar y estudiar normas referentes al tema de investigación. Asimismo la Contraloría General del Estado debería elaborar normas de carácter técnico acorde a la realidad nacional para coadyuvar a las Normas de Auditoria de Tecnologías de la Información y Comunicación Nº 270.

- ✓ Según las Normas Gubernamentales y las Normas Internacionales de Sistemas de Información exige que el auditor sea COMPETENTE, en tal sentido la parte ejecutiva de las entidades públicas en especial el Registro

Único para la Administración Tributaria Municipal debería asignar presupuesto para la capacitación continúa de los auditores bajo su dependencia en temas relacionados a la evaluación de procesos tecnológicos.

- ✓ El presente modelo metodológico también podría servir de guía para el desarrollo de procedimientos de auditorías de sistemas de información desarrollados en el ámbito privado.

- ✓ Finalmente podría ser de gran motivación para que otros investigadores desarrollen guías para la evaluación del control interno del ámbito tecnológico y de esta manera completar el proceso de auditoría de tecnologías de la información.

ANEXOS

ANEXO Nº 1

NORMAS DE AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Manual de Normas de Auditoría Gubernamental

Normas de Auditoría de Tecnologías de la Información y la Comunicación

M/CE/10 - G

MANUAL DE NORMAS DE AUDITORÍA GUBERNAMENTAL
INTRODUCCIÓN

Propósito

El presente documento contiene un conjunto de normas y aclaraciones que permiten asegurar la uniformidad y calidad de la auditoría gubernamental en Bolivia. Las normas se presentan bajo el código **01** y las aclaraciones correspondientes bajo los códigos subsiguientes.

Aplicación

Estas normas son de aplicación obligatoria en la práctica de la auditoría realizada en toda entidad pública comprendida en los artículos 3º y 4º de la Ley 1178, de Administración y Control Gubernamentales, promulgada el 20 de julio de 1990, por los auditores gubernamentales de las siguientes organizaciones de auditoría:

- Contraloría General de la República;
- unidades de auditoría interna de las entidades públicas, y
- profesionales o firmas de auditoría o consultoría especializada.

Cuando cualquiera de los miembros de las organizaciones mencionadas ejecuta tareas de auditoría en el Sector Público, se los denomina auditores gubernamentales, para efectos de la aplicación de estas Normas.

Auditoría

Es la acumulación y evaluación objetiva de evidencia para establecer e informar sobre el grado de correspondencia entre la información examinada y criterios establecidos.

Consideraciones básicas

Los servidores públicos deben rendir cuenta de su gestión a la sociedad. En este sentido, los servidores públicos, los legisladores y los ciudadanos en general desean y necesitan saber, no sólo si los recursos públicos han sido administrados correctamente y de conformidad con el ordenamiento jurídico administrativo y otras normas legales aplicables, sino también de la forma y resultado de su aplicación, en términos de eficacia, eficiencia y economía.

El presente documento contribuye al cumplimiento de la obligación que tienen los servidores públicos de responder por su gestión. Incluye conceptos y áreas de auditoría que son vitales para los objetivos de confiabilidad de la información.

Los servidores públicos y otros a los que se les ha confiado la administración de los recursos públicos, deben:

a) Emplear estos recursos con eficacia, eficiencia y economía.
b) Cumplir con el ordenamiento jurídico administrativo y otras normas legales aplicables, implantando sistemas adecuados para promover y lograr su cumplimiento.

c) Establecer y mantener controles efectivos para garantizar la consecución de las metas y objetivos correspondientes, promover la eficiencia de sus operaciones, salvaguardar los recursos contra irregularidades, fraudes y errores, y emitir información operativa y financiera útil, oportuna y confiable.

Los informes de auditoría gubernamental son importantes elementos de control y responsabilidad pública y otorgan credibilidad a la información generada por los sistemas correspondientes de las entidades públicas, ya que reflejan objetivamente el resultado de las evidencias acumuladas y evaluadas durante la auditoría.

Definiciones
Las definiciones presentadas en la Ley 1178 y sus reglamentos deben considerarse en la interpretación y aplicación de estas Normas.

Vacíos técnicos
Si durante el desarrollo de la auditoría gubernamental surgiesen aspectos no contemplados en estas Normas, deben entonces observarse las Normas Generales de Auditoría de Sistemas de Información emitidas por la Asociación de Auditoría y Control de Sistemas de Información ISACA (The Information Systems Audit and Control Association), el modelo de control COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas), las Normas Internacionales de Auditoría (NIA) emitidas por la Federación Internacional de Contadores (IFAC); las Declaraciones sobre Normas de Auditoría (SAS) emitidas por el Instituto Americano de Contadores Públicos (AICPA) y las Normas de Auditoría emitidas por la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI).

Fuentes
Estas Normas incorporan en su contenido los principales criterios de la normatividad emitida al respecto, por:

- La Fundación para la Auditoría y Control de Sistemas de Información (ISACF).
- La Asociación de Auditoría y Control de Sistemas de Información (ISACA).
- La Federación Internacional de Contadores (IFAC).
- El Instituto Americano de Contadores Públicos (AICPA).

Contratación de servicios de auditoría
Aunque no constituye norma de auditoría, es importante aplicar políticas y procedimientos idóneos para la adjudicación u autorización de los contratos de servicios de auditoría y supervisar que las mismas se realicen de acuerdo a las condiciones pactadas. Los objetivos y el alcance de la auditoría tomarán en cuenta la calidad profesional de la propuesta, la experiencia y personal involucrados en la misma, así como el sistema de control de calidad interno de la organización de auditoría y las revisiones externas a las cuales está sujeta.

Registro de firmas y profesionales independientes de auditoría externa y consultoría especializada en auditoría

Para prestar servicios de auditoría en las entidades públicas comprendidas en los artículos 3º y 4º de la Ley 1178 y en aquellas entidades comprendidas en las previsiones del artículo 5º del Decreto Supremo 23215, las firmas y profesionales independientes de auditoría externa y consultoría especializada en auditoría deben inscribirse en el correspondiente Registro que estará a cargo de la Contraloría General de la República. Al respecto, el proceso de inscripción debe sujetarse al Reglamento que el Órgano Rector del Sistema de Control emita a tal efecto.

Ejercicio de la auditoría

Para la aplicación de la presente Norma, en lo que corresponda, necesariamente deberán tomarse en cuenta las Normas Generales de Auditoría Gubernamental (NAG 210)

.

Auditoría de Tecnologías de la Información y la Comunicación

Es el examen objetivo, crítico, metodológico y selectivo de evidencia relacionada con políticas, prácticas, procesos y procedimientos en materia de Tecnologías de la Información y la Comunicación, para expresar una opinión independiente respecto:

i) A la confidencialidad, integridad, disponibilidad y confiabilidad de la información.
ii) Al uso eficaz de los recursos tecnológicos.
iii) A la efectividad del sistema de control interno asociado a las Tecnologías de la Información y la Comunicación.

La auditoria de Tecnologías de la Información y la Comunicación está definida principalmente por sus objetivos y puede ser orientada hacia uno o varios de los siguientes enfoques:

a) **Enfoque a las Seguridades:** Consiste en evaluar las seguridades implementadas en los sistemas de información con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información.

b) **Enfoque a la Información:** Consiste en evaluar la estructura, integridad y confiabilidad de la información gestionada por el sistema de información.

c) **Enfoque a la Infraestructura tecnológica:** Consiste en evaluar la correspondencia de los recursos tecnológicos en relación a los objetivos previstos.

d) **Enfoque al Software de Aplicación**: Consiste en evaluar la eficacia de los procesos y controles inmersos en el software de aplicación, que el diseño conceptual de éste cumpla con el ordenamiento jurídico administrativo vigente.

e) **Enfoque a las Comunicaciones y Redes:** Consiste en evaluar la confiabilidad y desempeño del sistema de comunicación para mantener la disponibilidad de la información. *Para una adecuada comprensión de las normas de auditoría de Tecnologías de la Información y la Comunicación se definen los siguientes conceptos:*

Datos: Son objetos de información en su sentido más amplio, los cuales pueden ser externos o internos, estructurados y no estructurados del tipo gráfico, sonido, imágenes, números, palabras y de otra índole, etc.

Información: Datos que han sido organizados, sistematizados y presentados de manera que los patrones subyacentes resulten claros.

Tecnología: Es un conjunto ordenado de instrumentos, conocimientos, procedimientos y métodos aplicados a las áreas.

Tecnologías de la Información y la Comunicación (TIC): Se refiere al conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de la información.

Sistema de Información (SI): Se refiere a un conjunto de procesos y recursos de información organizados con el objetivo de proveer la información necesaria (pasada, presente, futura) en forma precisa y oportuna para apoyar la toma de decisiones en una entidad.

Software de Aplicación: Se refiere a un elemento de los Sistemas de Información, es un conjunto de programas de computador diseñados y escritos para realizar tareas específicas del negocio y que permiten la interacción entre el usuario y el computador.

Sistemas de comunicación: Se refiere a la tecnología que se emplea para el intercambio de información.

Confidencialidad de la información: Se refiere a la protección de la información crítica contra su divulgación no autorizada.

Integridad de la información: Se vincula con la exactitud y la totalidad de la información así como también con su validez de acuerdo con los valores y las expectativas de la entidad.

Confiabilidad de la información: Se vincula con la provisión de la información adecuada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de presentación de reportes financieros y de cumplimiento.

Disponibilidad de la información: Se vincula con el hecho de que la información se encuentre disponible cuando el proceso la requiera. También se asocia con la protección de los recursos necesarios y las capacidades asociadas.

Técnicas de Auditoría Asistidas por Computador (TAAC): Se refiere a las técnicas de auditoría que contemplan herramientas informáticas con el objetivo de realizar más eficazmente, eficientemente y en menor tiempo pruebas de auditoría.

Ejercicio de la auditoría interna
La auditoría interna es una función de control posterior de la organización, que se realiza a través de una unidad especializada, cuyos integrantes no participan en las operaciones y actividades administrativas. Su propósito es contribuir al logro de los objetivos de la entidad mediante la evaluación periódica del control interno.
Las Normas de Auditoría Gubernamental deben ser aplicadas por el auditor interno gubernamental.

270 NORMAS DE AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

271 Planificación

01. La primera norma de auditoría de Tecnologías de la Información y la Comunicación es:

> **La auditoria de Tecnologías de la Información y la Comunicación se debe planificar en forma metodológica, para alcanzar eficientemente los objetivos de la misma.**

02. La planificación debe permitir un adecuado desarrollo de las etapas subsecuentes; para el efecto, se debe tomar conocimiento del sujeto y del objeto a evaluar. Además, es un proceso continuo y dinámico que puede modificarse o ampliarse durante el desarrollo de la auditoría.

03. El auditor gubernamental debe comprender del objeto de auditoría: el diseño conceptual, políticas de gestión, formas de registro, niveles de seguridad y uso de las comunicaciones para la gestión de la información.

04. En función de la naturaleza, complejidad y modularidad del objeto de auditoría, se determinarán las áreas críticas, dependiendo de éstas se definirán los objetivos o el(los) enfoque(s) y el alcance de la auditoria.

05. Se diseñarán programas de trabajo que se aplicarán durante la ejecución del trabajo de campo, para el efecto se determinará la naturaleza, oportunidad y extensión de los procedimientos que se ejecutarán para obtener evidencia competente y suficiente.

06. Como resultado del proceso de planificación de la auditoría de Tecnologías de la Información y la Comunicación, se debe elaborar un documento resumen, el cual debe contener todos los aspectos detallados en la presente norma y aquellos que se consideren necesarios incluir, y que tengan relación con los objetivos del examen, el alcance y la metodología.

272 Supervisión

01. La segunda norma de auditoría de Tecnologías de la Información y la Comunicación es:

> **Personal competente debe supervisar sistemática y oportunamente el trabajo realizado por los profesionales que conformen el equipo de auditoría.**

02. La supervisión implica que personal competente y calificado para ejercerla, debe dirigir los esfuerzos del equipo de auditores gubernamentales hacia la consecución de los objetivos de auditoría.

03. La supervisión debe ser realizada en cada una de las etapas de la auditoría, la misma incluye:

- Examinar la factibilidad y/o razonabilidad técnica de los objetivos y alcances de la auditoria propuestos.
- Asegurar que los miembros del equipo comprendan los objetivos de la auditoría. En particular se debe asegurar que entiendan claramente el trabajo a realizar, por qué se va efectuar y qué se espera lograr.
- Guiar a los miembros del equipo de auditoría a lo largo del desarrollo de las tareas asignadas.
- Revisar oportunamente el trabajo realizado, a través de los respectivos papeles de trabajo físicos y si fuera el caso como respaldo en papeles de trabajo electrónicos.
- Ayudar a absolver problemas técnicos y administrativos.
- Detectar debilidades del personal asignado y proporcionar en consecuencia la capacitación necesaria o asegurarse que la misma sea proporcionada por terceros.
- Asegurar que la evidencia obtenida sea suficiente y competente.

04. La supervisión efectuada durante el desarrollo de la auditoría, debe estar evidenciada en los papeles de trabajo físicos y si fuera el caso como respaldo en papeles de trabajo electrónicos, acumulados durante la misma.

273 Control interno

01. La tercera norma de auditoría de Tecnologías de la Información y la Comunicación es:

> **Se debe comprender y evaluar el control interno para identificar las áreas críticas que requieren un examen profundo y determinar su grado de confiabilidad a fin de establecer la naturaleza, alcance y oportunidad de los procedimientos de auditoría a aplicar.**

02. Se establecen dos tipos de controles: el control general y el control detallado de los sistemas de información. El control general involucra a todos los sistemas de información y el control detallado está diseñado para controlar el procesamiento en sí de la información.

03. Los controles generales son políticas y procedimientos que tienen que ver con el ambiente en el cual se desarrollan, mantienen y operan los sistemas de información y respaldan el funcionamiento efectivo de los controles detallados, en consecuencia involucran a todos los sistemas de información. Se pueden citar por ejemplo, el desarrollo y la implementación de una política de seguridad lógica de los sistemas de información.

04. Los controles detallados son los aplicables a la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de la información. Se pueden citar por ejemplo, dentro de un software de aplicación parámetros de seguridad de la información, validación de entradas de datos, etc.

05. El control interno es un proceso afectado por la dirección y todo el personal, diseñado con el objeto de proporcionar una seguridad razonable para el logro de los objetivos de la entidad.

Comprende el plan de organización, incluyendo la unidad de auditoría interna, todos los métodos coordinados y procedimientos adoptados en la entidad para promover la eficacia y la eficiencia de las operaciones y la confiabilidad de la información financiera y de gestión, así como el cumplimiento de las políticas gerenciales, el ordenamiento jurídico administrativo y otras normas legales aplicables, y las obligaciones contractuales.

06. El control interno está conformado por cinco componentes que interactúan entre sí y se encuentran integrados al proceso de gestión: ambiente de control; evaluación de riesgos; actividades de control; información y comunicación; y supervisión.

07. El estudio y evaluación del control interno incluye dos fases:
a) Conocimiento y comprensión de los procedimientos establecidos en la entidad referente a los sistemas de información, al término del cual, el auditor gubernamental debe ser capaz de emitir una opinión preliminar presumiendo un satisfactorio cumplimiento del control interno.

b) Comprobación de que los procedimientos relativos a los controles internos están siendo aplicados tal como fueron observados en la primera fase.

274 Evidencia

01. La cuarta norma de auditoría de Tecnologías de la Información y la Comunicación es:

> **Debe obtenerse evidencia válida, relevante y suficiente como base razonable para sustentar los hallazgos y conclusiones del auditor gubernamental.**

02. Se denomina evidencia al conjunto de hechos comprobados, suficientes, competentes y pertinentes que sustentan las conclusiones del auditor. Es la información específica obtenida durante la labor de auditoría a través de observación, inspección, entrevistas y examen de los registros.

03. La acumulación de evidencia es un proceso integrado a toda la ejecución de la auditoría y debe sustentar todos los atributos de los hallazgos de auditoría.

04. La evidencia debe ser acumulada mediante un proceso supervisado de aplicación de metodologías y técnicas de auditoría.

05. La evidencia es válida cuando es consistente con la realidad y los hechos, la misma ha sido obtenida por el auditor en forma directa o se ha asegurado de la confiabilidad de la información generada por la entidad.

06. La evidencia es relevante cuando tiene directa relación con el objeto de la auditoría y contribuye a sustentar al logro de los objetivos.

07. La evidencia es suficiente si basta para sustentar la opinión del auditor gubernamental, para ello debe ejercitar su juicio profesional con el propósito de determinar la cantidad y tipos de evidencia necesarias.

08. Las Técnicas de Auditoría Asistidas por Computador (TAAC) pueden producir parte de la evidencia de auditoría, como consecuencia de ello, el auditor debe planificar y ser competente en el uso de las TAAC.

09. La evidencia obtenida por el auditor gubernamental debe conservarse en papeles de trabajo físicos y si fuera el caso como respaldo en papeles de trabajo electrónicos.

10. Respecto a las características de competencia, suficiencia y clasificación de la evidencia, y a los papeles de trabajo que la contienen, deben considerarse los aspectos mencionados en la NAG 224.02 hasta NAG 224.13.

275 Comunicación de resultados

01. La quinta norma de auditoría de Tecnologías de la Información y la Comunicación es:

> **El informe de auditoría de Tecnologías de la Información y la Comunicación debe ser oportuno, objetivo, claro, preciso y será el medio para comunicar los resultados obtenidos durante la misma.**

02. El informe de auditoría de Tecnologías de la Información y la Comunicación debe ser emitido en forma escrita, lógica y organizada.

03. El informe debe contener suficiente información para ser entendido por los destinatarios y facilitar la acción correctiva si corresponde.

04. El contenido del informe de auditoría de Tecnologías de la Información y la Comunicación deberá hacer referencia a:

- Los antecedentes, acciones o circunstancias que dieron origen a la auditoría.
- Los objetivos, que identificarán los propósitos específicos que se cubrirán durante la misma.
- El alcance, se referirá al sujeto, objeto y periodo examinados; así como a la cobertura del trabajo realizado.
- Se debe especificar en el alcance, que la auditoría se realizó de acuerdo con las normas de auditoría gubernamental.
- Si se presentaron limitaciones que no permitió al auditor gubernamental cumplir con los objetivos previstos, estas deben ser mencionadas en el informe de manera expresa.
- La metodología, explicará las técnicas y procedimientos que fueron empleados para obtener y analizar la evidencia; asimismo, se mencionarán los criterios y normas aplicadas durante el desarrollo del examen.
- El resultado, expondrá:

    • Los hallazgos significativos que tengan relación con los objetivos de auditoría, los que incluirán la información suficiente que permita una adecuada comprensión del asunto que se informa; además, la exposición de la misma debe ser objetiva y convincente.

    • Las recomendaciones que se consideren apropiadas para corregir las causas del problema o hallazgo.

- Las conclusiones, que son inferencias lógicas sobre el objeto de auditorías basadas en los hallazgos, deben ser expresadas explícitamente de manera convincente y persuasiva, evitando el riesgo de interpretaciones por parte de los lectores.

ANEXO Nº 2

NORMAS Y DIRECTRICES DE ISACA PARA LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

NORMAS Y DIRECTRICES DE ISACA PARA LA AUDITORÍA DE SISTEMAS DE INFORMACION[32]

CÓDIGO DE ÉTICA PROFESIONAL DE ISACA

ISACA establece este Código de ética profesional para guiar la conducta profesional y personal de los miembros del a asociación y/o de sus profesionales certificados.

Los miembros y profesionales certificados de ISACA deberán:

1. Apoyar la implementación y fomentar el cumplimiento de las normas, los procedimientos y los controles apropiados en los sistemas de información.
2. Ejecutar sus labores con objetividad, diligencia y cuidado profesional, de conformidad con las normas y mejores prácticas profesionales.
3. Servir en el interés de las partes interesadas en una forma legal y honesta, y al mismo tiempo mantener altos estándares de conducta y de carácter, y no involucrarse en actos que puedan discrepar la profesión.
4. Mantener la privacidad y la confidencialidad de la información obtenida en el curso de su función a menos que la autoridad legal requiera su revelación. Dicha información no será usada para beneficio personal ni será revelada a terceros.
5. Mantener competencia en sus respectivos campos y comprometerse a emprender únicamente las actividades que se espera que puedan realizar con competencia profesional.
6. Informar a las personas adecuadas los resultados del trabajo realizado, revelando todos los hechos significativos de los que tengan conocimiento.
7. Apoyar la formación profesional de las partes interesadas para mejorar su comprensión sobre seguridad y control de SI.

El no cumplir con este Código de Ética Profesional puede tener como resultado una investigación de la conducta de un miembro y/o profesional certificado y, en última instancia, en medidas disciplinarias.

NORMAS DE AUDITORÍA

Las normas de auditoría de SI aplicables a la auditoría de Sistemas de Información son:

S1 Estatuto de Auditoria:

- El propósito, responsabilidad, autoridad y obligación de rendir cuentas de la función de auditoría de SI o tareas de auditoría de SI deberían estar debidamente documentados en un estatuto de auditoría o en una carta compromiso.
- El estatuto de auditoría o contrato debería ser establecido y aprobado por un nivel apropiado dentro de la(s) organización(es).

S1 Independencia:

[32] ISACA, Manual de preparación al examen CISA, Estados Unidos 2008, paginas 17 al 22

- **Independencia profesional -** En todos los asuntos relacionados con la auditoria, el auditor de SI debería ser independiente del auditado tanto en actitud como en apariencia.
- **Independencia organizacional -** La función de auditoría de SI debería ser independiente del área o actividad que se éste revisando para permitir la ejecución objetiva de la tarea de auditoría

S3 Ética y Estándares de Profesionales:
- El auditor de SI debería acatar el Código de Ética Profesional de ISACA.
- El auditor de SI debería ejercer el debido cuidado profesional, incluyendo la observancia de los estándares profesionales de auditoría aplicables.

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

S5 Planeación:
- El auditor de SI debería planear el alcance de la auditoria de sistemas de información tomando en cuenta los objetivos de la auditoria y el cumplimiento con las leyes y los estándares profesionales de auditoría aplicables.
- El auditor de SI debería desarrollar y documentar el enfoque de auditoría basado en riesgos.
- El auditor de SI debería desarrollar y documentar el plan de auditoría detallando la naturaleza, los objetivos, el tiempo el alcance y los recursos requeridos.
- El auditor de SI debería desarrollar el programa y los procedimientos de auditoria

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

S7 Reporte:
- El auditor de SI debería proveer un reporte en un formato apropiado, al terminar la auditoría. El reporte debería identificar la organización, los destinatarios y cualquier restricción sobre su publicación.

- El reporte de auditoría debería establecer el alcance, los objetivos, el periodo cubierto y la naturaleza, el tiempo y la extensión del trabajo de auditoría realizado.
- El reporte debería establecer los hallazgos, las conclusiones y recomendaciones, así como cualquier reserva, restricción o limitación en el alcance que tenga el auditor de SI con respecto a la auditoría.
- El auditor de SI debería tener evidencia de auditoría suficiente y apropiada para respaldar los resultados reportados.
- Cuando de emite, el reporte del auditor de SI debería tener la firma, la fecha y distribuirse de acuerdo con los términos de los estatuto de auditoría o de la carta de cumplimiento.

S8 Actividades de Seguimiento:

- Después de proveer el reporte de hallazgos y recomendaciones, el auditor de SI debería solicitar y evaluar la información relevante para determinar si la gerencia ha tomado las acciones apropiadas de manera oportuna.

S9 Irregularidades y Actos ilegales:

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

  - Revelar al auditor de SI los resultados de la valoración de riesgos de que existan falsas declaraciones importantes como resultado de irregularidades o actos ilícitos.
  - Divulgar al auditor de SI su conocimiento de las irregularidades o actos ilícitos que afectan la organización en lo que se refiere:
    - Gestión
    - Empleados con funciones importantes en controles internos
    - Divulgar al auditor de SI su conocimiento de cualquier alegato de irregularidades o actos ilícitos, o su sospecha, que afectan a la organización según lo comunican los empleados, ex empleados, reguladores y otros.
- Si el auditor de SI identifica una irregularidad o acto ilícito de importancia u obtiene información de que una irregularidad o acto ilícito de importancia material pueda existir, el auditor de SI debería comunicar estos asuntos oportunamente al nivel apropiado de la gerencia de forma oportuna.
- Si el auditor de SI identifica una irregularidad o acto ilícito importante que involucre a la gerencia o a empleados que tengan funciones significativas en el control interno, el auditor de SI debería comunicar estos asuntos de manera oportuna a los encargados del gobierno corporativo.
- El auditor de SI debería aconsejar al nivel apropiado de la gerencia y a los encargados del gobierno corporativo sobre las debilidades importantes en el diseño y la implementación del control interno para prevenir y detectar irregularidades o actos ilícitos que podrían haber sido identificados en el curso de un trabajo de auditoría.
- Si el auditor de SI encuentra circunstancias excepcionales tales como falsas declaraciones o actos ilícitos que afecten su capacidad de continuar con el trabajo de auditoría, el auditor de SI debería considerar sus responsabilidades legales y profesionales aplicables dadas las circunstancias, incluyendo el saber si existe el requerimiento de que el auditor de SI reporte a sus contratantes o en algunos casos a los encargados del gobierno corporativo o las autoridades regulatorias o bien considerar cancelar su contrato.
- El auditor de SI debería documentar todas las comunicaciones, planeación, resultados, evaluaciones y conclusiones relacionadas con irregularidades y actos ilícitos importantes que hayan sido reportados a la gerencia, encargados del gobierno corporativo, reguladores y otros.

S10 Gobierno de TI:

- El auditor de SI debería revisar y valorar si la función de SI está alineada con la visión, misión, valores, objetivos y estrategias de la organización.
- El auditor de SI debería revisar si la función de SI tiene una declaración clara acerca del desempeño esperado por el negocio (efectividad y eficiencia) y valorar si se cumple con el mismo.
- El auditor de SI debe revisar y valorar la efectividad de los procesos de gestión de recursos de SI y de desempeño.
- El auditor de SI debería revisar y valorar el cumplimiento con los requerimientos legales, ambientales, de calidad de la información, fiduciarios y de seguridad.

- El auditor de SI debería usar un enfoque basado en riesgos para evaluar la función de SI.
- El auditor de SI debería revisar y valorar el ambiente de control de la organización.
- El auditor de SI debería revisar y valorar los riesgos que pueden impactar de manera negativa el ambiente de SI.

S11 Uso de la Valoración de Riesgos en la Planeación de Auditoría:

- El auditor de SI debería usar una técnica o enfoque apropiado de valoración de riesgos al desarrollar el plan general de auditoría de SI y determinar las prioridades para una asignación efectiva de recursos de auditoría de SI.
- Al planear las revisiones individuales, el auditor de SI debería identificar y valorar los riesgos relevantes para el área bajo revisión.

S12 Importancia de la Auditoria:

- El auditor de SI debería considerar la importancia de la auditoría y su relación con el riesgo de auditoría mientras determina la naturaleza, el tiempo y la extensión de los procedimientos de auditoría.
- Mientras planea la auditoría, el auditor de SI debería considerar la potencial debilidad o la ausencia de controles y si dicha debilidad o ausencia de controles podría tener como consecuencia deficiencias significativas o una debilidad materialidad en el sistema de información.
- El auditor de SI debería considerar el efecto acumulativo de las deficiencias o debilidades menores de control y la ausencia de controles para traducirlos en deficiencia significativa o debilidad importante en el sistema de información.
- El informe del auditor de SI debería revelar controles ineficaces o ausencia de controles y la significación de las deficiencias de control y la posibilidad de que estas debilidades tengan como consecuencia una deficiencia significativa o una debilidad importante.

S13 Uso de Trabajo de Otros Expertos:

- El auditor de SI debería, donde sea apropiado, considerar usar el trabajo de otros expertos para la auditoría.
- El auditor de SI debería valorar y quedar satisfecho con los procesos de calificaciones profesionales, competencias, experiencia relevante, recursos independencia y control de calidad de otros expertos, antes del compromiso.
- El auditor de SI debería valorar, revisar y evaluar el trabajo de otros expertos como parte de la auditoria y concluir la extensión de uso y confianza en el trabajo de un experto.
- El auditor de SI debería determinar y concluir si el trabajo de otros expertos es adecuado y completo como para permitir que el auditor de SI concluya sobre los actuales objetivos de auditoría. Dicha conclusión debe ser claramente documentada.
- El auditor de SI debe aplicar procedimientos adicionales de prueba para obtener evidencia suficiente y apropiada en circunstancias en las que el trabajo de otros expertos no provee evidencia suficiente y apropiada de auditoría.

- El auditor de SI debería proveer una opinión apropiada de auditoría e incluir limitaciones de alcance donde la evidencia requerida no sea obtenida a través de procedimientos adicionales de prueba.

S14 Evidencia de auditoría:

- El auditor de SI debería obtener evidencia suficiente y apropiada de auditoría para extraer conclusiones sobre las cuales basar los resultados de auditoría.
- El auditor de SI debería evaluar la suficiencia de la evidencia de auditoría obtenida durante la auditoría.

S15 Controles de TI:

- El auditor de SI debe evaluar y monitorear los controles de TI que son parte integral del ambiente de control interno de la organización.
- El auditor de SI debe brindar asistencia a la gerencia por medio de consejos relacionados con el diseño, la implementación, operación y mejoras de los controles de TI.

S16 Comercio Electrónico

- El auditor de SI debe evaluar los controles aplicables y valorar riesgos cuando revisa los ambientes de comercio electrónico para asegurar que las transacciones de comercio electrónico están controladas adecuadamente.

ÍNDICE DE DIRECTRICES

G1 Uso del Trabajo de Otros Auditores, con efecto a partir del 1 de junio de 1998
G2 Requisitos de Evidencia de Auditoría con efecto a partir del 1 de diciembre de 1998
G3 Uso de Técnicas de Auditoría Asistidas por Computadora (CAATS), con efecto a partir de 1 de diciembre de 1998
G4 Contratación de servicios externos de las Actividades de SI para otras Organizaciones, con efecto a partir del 1 de septiembre de 1999
G5 Estatuto de Auditoría, con efecto a partir del 1 de septiembre de 1999
G6 Conceptos de importancia para la Auditoria de Sistemas de Información, con efecto a partir del 1 de septiembre de 1999
G7 Debido Cuidado Profesional, con efecto a partir del 1 de septiembre de 1999
G8 Documentación de la Auditoría, con efecto a partir del 1 de septiembre de 1999
G9 Consideraciones de Auditoría en Casos de Irregularidades, con efecto a partir del 1 de marzo de 2000
G10 Muestreo de Auditoría, con efecto a partir del 1 de marzo de 2000
G11 Efecto de los Controles Generales de SI, con efecto a partir del 1 de marzo de 2000
G12 Relación e Independencia Organizacional, con efecto a partir del 1 de septiembre de 2000
G13 Uso de la Valoración de Riesgos en la Planeación de Auditoría, con efecto a partir del 1 de septiembre de 2000

G14 Revisión de los Sistemas de Aplicación, con efecto a partir del 1 de noviembre de 2001
G15 Planeación Revisada, con efecto a partir del 1 de marzo de 2002
G16 Efecto de Terceros en los Controles de TI de una Organización, con efecto a partir del 1 de marzo de 2002
G17 Efecto del rol de no auditor en la Independencia del Auditor de SI, con efecto a partir del 1 de julio de 2002
G18 Gobierno de TI, con efecto a partir del 1 de julio de 2002
G19 Irregularidades y actos Ilegales, con efecto a partir del 1 de julio de 2002
G20 Reportes, con efecto a partir del 1 de enero de 2003
G21 Revisión de Sistemas de Planeación de Recursos Empresariales (ERP), con efecto a partir del 1 de agosto 2003
G22 Revisión del Comercio Electrónico Negocio a Consumidor (B2C), con efecto a partir del 1 de agosto 2003
G23 Revisión del Ciclo de Vida de Desarrollo de Sistemas (SDLC), con efecto a partir del 1 de agosto 2003
G24 Banca por internet, con efecto a partir del 1 de agosto 2003
G25 Revisión de Redes Privadas Virtuales, con efecto a partir del 1 de julio de 2004
G26 Revisión de Proyectos de Reingeniería de Procesos de Negocio (BPR), con efecto a partir 1 de julio de 2004
G27 Computación Móvil, con efecto a partir del 1 de septiembre de 2004
G28 Informática Forense, con efecto a partir del 1 de septiembre de 2004
G29 Revisión Posterior a la Implementación, con efecto a partir del 1 de enero de 2005
G30 Competencia, con efecto a partir del 1 de junio de 2005
G31 Privacidad, con efecto a partir del 1 de junio de 2005
G32 Revisión de los Planes de Continuidad del Negocio desde una Perspectiva de TI, con efecto a partir del 1 de septiembre de 2005
G33 Consideraciones Generales sobre el uso de Internet, con efecto a partir del 1 de marzo de 2006
G34 Responsabilidad, Autoridad y Registro, con efecto a partir del 1 de marzo de 2005
G35 Actividades de Seguimiento, con efecto a partir del 1 de marzo de 2007
G36 Controles Biométricos, con efecto a partir del 1 de marzo de 2007
G37 Gestión de Configuración, efectivo a partir del 1 de noviembre de 2007
G38 Control de acceso, efectivo a partir del 1 de febrero de 2008
G39 Organizaciones de TI, efectivo a partir del 1 de mayo de 2008

ÍNDICE DE PROCEDIMIENTOS

P1 Valoración de Riesgos de SI, con efecto a partir de 2002
P2 Firmas Digitales, con efecto a partir del 1 de julio de 2002
P3 Detección de Intrusos, con efecto a partir del 1 de agosto de 2003
P4 Virus y Otros Códigos Maliciosos, con efecto a partir del 1 de agosto de 2003

P5 Autoevaluación de Riesgos de Control, con efecto a partir del 1 de agosto de 2003

P6 Firewalls, con efecto a partir del 1 de agosto de 2003

P7 Irregularidades y Actos Ilegales, con efecto a partir del 1 de noviembre de 2003

P8 Valoración de la Seguridad – Prueba de Penetración y Análisis de Vulnerabilidades, con efecto a partir del 1 de septiembre de 2004

P9 Evaluación de Controles de Administración sobre las Metodologías de Encriptación, con efecto a partir del 1 de enero de 2005

P10 Control de Cambios sobre las Aplicaciones de Negocio, con efecto a partir del 1 de octubre de 2006

P11 Transferencia Electrónica de Fondos (EFT), efectivo a partir del 1 de mayo de 2007

ANEXO Nº 3

DOMINIOS Y PROCESOS
COBIT Versión 4.1.

COBIT
OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y LA TECNOLOGÍA RELACIONADA
DOMINIOS Y PROCESOS[33]

PO1 DEFINIR UN PLAN ESTRATÉGICO DE TI

PO1.1 Administración del Valor de TI

Trabajar con el negocio para garantizar que el portafolio de inversiones de TI de la empresa contenga programas con casos de negocio sólidos. Reconocer que existen inversiones obligatorias, de sustento y discrecionales que difieren en complejidad y grado de libertad en cuanto a la asignación de fondos. Los procesos de TI deben proporcionar una entrega efectiva y eficiente de los componentes TI de los programas y advertencias oportunas sobre las desviaciones del plan, incluyendo costo, cronograma o funcionalidad, que pudieran impactar los resultados esperados de los programas. Los servicios de TI se deben ejecutar contra acuerdos de niveles de servicios equitativos y exigibles. La rendición de cuentas del logro de los beneficios y del control de los costos es claramente asignada y monitoreada. Establecer una evaluación de los casos de negocio que sea justa, transparente, repetible y comparable, incluyendo el valor financiero, el riesgo de no cumplir con una capacidad y el riesgo de no materializar los beneficios esperados.

PO1.2 Alineación de TI con el Negocio

Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades. Asegurarse de que el rumbo del negocio al cual está alineado TI está bien entendido. Las estrategias de negocio y de TI deben estar integradas, relacionando de manera clara las metas de la empresa y las metas de TI y reconociendo las oportunidades así como las limitaciones en la capacidad actual, y se deben comunicar de manera amplia. Identificar las áreas en que el negocio (estrategia) depende de forma crítica de TI, y mediar entre los imperativos del negocio y la tecnología, de tal modo que se puedan establecer prioridades concertadas.

PO1.3 Evaluación del Desempeño y la Capacidad Actual

Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.

PO1.4 Plan Estratégico de TI

Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos. Define cómo se cumplirán y medirán los objetivos y recibirán una autorización formal de los interesados. El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de obtención, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI.

PO1.5 Planes Tácticos de TI

Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos deben describir las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados. Los planes tácticos deben tener el detalle suficiente para permitir la definición de planes de proyectos.
Administrar de forma activa los planes tácticos y las iniciativas de TI establecidas por medio del análisis de los portafolios de proyectos y servicios. Esto incluye el equilibrio de los requerimientos y recursos de forma regular, comparándolos con el logro de metas estratégicas y tácticas y con los beneficios esperados, y tomando las medidas necesarias en caso de desviaciones.

[33] Cobit versión 4.1, ver página web ***www.isaca.org/cobit***

PO1.6 Administración del Portafolio de TI
Administrar de forma activa, junto con el negocio, el portafolio de programas de inversión de TI requerido para lograr objetivos de negocio estratégicos específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas. Esto incluye clarificar los resultados de negocio deseados, garantizar que los objetivos de los programas den soporte al logro de los resultados, entender el alcance completo del esfuerzo requerido para lograr los resultados, definir una rendición de cuentas clara con medidas de soporte, definir proyectos dentro del programa, asignar recursos y financiamiento, delegar autoridad, y comisionar los proyectos requeridos al momento de lanzar el programa.

PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN

PO2.1 Modelo de Arquitectura de Información Empresarial
Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI como se describen en P01. El modelo debe facilitar la creación, uso y el compartir en forma óptima la información por parte del negocio de tal manera que se mantenga su integridad, sea flexible, funcional, rentable, oportuna, segura y tolerante a fallos.

PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos
Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización. El diccionario facilita compartir elementos de datos entre las aplicaciones y los sistemas, fomenta un entendimiento común de datos entre los usuarios de TI y del negocio, y previene la creación de elementos de datos incompatibles

PO2.3 Esquema de Clasificación de Datos
Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o cifrado.

PO2.4 Administración de Integridad
Definir e Implementar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato Electrónico, tales como bases de datos, almacenes de datos y archivos.

PO3 DETERMINAR LA DIRECCIÓN TECNOLÓGICA

PO3.1 Planeación de la Dirección Tecnológica
Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiada tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio. También identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.

PO3.2 Plan de Infraestructura Tecnológica
Crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos.
También toma en cuenta los cambios en el ambiente competitivo, las economías de escala para inversiones y personal en sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones.

PO3.3 Monitoreo de Tendencias y Regulaciones Futuras
Establecer un proceso para monitorear las tendencias ambientales del sector / industria, tecnológicas, de infraestructura, legales y regulatorias. Incluir las consecuencias de estas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.

PO3.4 Estándares Tecnológicos
Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección de la tecnología, y medir el cumplimiento de estos estándares y directrices. Este foro impulsa los estándares y las prácticas tecnológicas con base en su importancia y riesgo para el negocio y en el cumplimiento de requerimientos externos.

PO3.5 Consejo de Arquitectura de TI
Establecer un comité de arquitectura de TI que proporcione directrices sobre la arquitectura y asesoría sobre su aplicación, y que verifique el cumplimiento. Esta entidad orienta el diseño de la arquitectura de TI garantizando que facilite la estrategia del negocio y tome en cuenta el cumplimiento regulatorio y los requerimientos de continuidad. Estos aspectos se vinculan con el PO2 *Definir arquitectura de la información*.

PO4 DEFINIR LOS PROCESOS, ORGANIZACIÓN Y RELACIONES DE TI

PO4.1 Marco de Trabajo de Procesos de TI
Definir un marco de trabajo para el proceso de TI para ejecutar el plan estratégico de TI. Este marco incluye estructura y relaciones de procesos de TI (administrando brechas y superposiciones de procesos), propiedad, medición del desempeño, mejoras, cumplimiento, metas de calidad y planes para alcanzarlas. Proporciona integración entre los procesos que son específicos para TI, administración del portafolio de la empresa, procesos de negocio y procesos de cambio del negocio. El marco de trabajo de procesos de TI debe estar integrado en un sistema de administración de calidad y en un marco de trabajo de control interno.

PO4.2 Comité Estratégico de TI
Establecer un comité estratégico de TI a nivel del consejo. Este comité deberá asegurar que el gobierno de TI, como parte del gobierno corporativo, se maneja de forma adecuada, asesora sobre la dirección estratégica y revisa las inversiones principales a nombre del consejo completo.

PO4.3 Comité Directivo de TI
Establecer un comité directivo de TI (o su equivalente) compuesto por la gerencia ejecutiva, del negocio y de TI para:

- Determinar las prioridades de los programas de inversión de TI alineadas con la estrategia y prioridades de negocio de la empresa
- Dar seguimiento al estatus de los proyectos y resolver los conflictos de recursos
- Monitorear los niveles de servicio y las mejoras del servicio.

PO4.4 Ubicación Organizacional de la Función de TI
Ubicar a la función de TI dentro de la estructura organizacional general con un modelo de negocios supeditado a la importancia de TI dentro de la empresa, en especial en función de que tan crítica es para la estrategia del negocio y el nivel de dependencia operativa sobre TI. La línea de reporte del CIO es proporcional con la importancia de TI dentro de la empresa.

PO4.5 Estructura Organizacional
Establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además implementar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos de negocio esperados y las circunstancias cambiantes.

PO4.6 Establecimiento de Roles y Responsabilidades
Definir y comunicar los roles y las responsabilidades para el personal de TI y los usuarios que delimiten la autoridad entre el personal de TI y los usuarios finales y definían las responsabilidades y rendición de cuentas para alcanzar las necesidades del negocio.

PO4.7 Responsabilidad de Aseguramiento de Calidad de TI
Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad (QA) y proporcionar al grupo de QA sistemas de QA, los controles y la experiencia para comunicarlos. Asegurar que la ubicación organizacional, las responsabilidades y el tamaño del grupo de QA satisfacen los requerimientos de la organización.

PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento
Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado. Definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento. Establecer responsabilidad sobre la administración del riesgo y la seguridad a nivel de toda la organización para manejar los problemas a nivel de toda la empresa. Puede ser necesario asignar responsabilidades adicionales de administración de la seguridad a nivel de sistema específico para manejar problemas relacionados con seguridad. Obtener orientación de la alta dirección con respecto al apetito de riesgo de TI y la aprobación de cualquier riesgo residual de TI.

PO4.9 Propiedad de Datos y de Sistemas
Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información. Los dueños toman decisiones sobre la clasificación de la información y de los sistemas y sobre cómo protegerlos de acuerdo a esta clasificación.

PO4.10 Supervisión
Implementar prácticas adecuadas de supervisión dentro de la función de TI para garantizar que los roles y las responsabilidades se ejerzan de forma apropiada, para evaluar si todo el personal cuenta con la suficiente autoridad y recursos para ejecutar sus roles y responsabilidades y para revisar en general los indicadores clave de desempeño.

PO4.11 Segregación de Funciones
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.

PO4.12 Personal de TI
Evaluar los requerimientos de personal de forma regular o cuando existan cambios importantes en el ambiente de negocios, operativo o de TI para garantizar que la función de TI cuente con un número suficiente de recursos para soportar adecuada y apropiadamente a las metas y objetivos del negocio.

PO4.12 Personal Clave de TI
Definir e identificar al personal clave de TI y minimizar la dependencia en un solo individuo desempeñando una función de trabajo crítica.

PO4.14 Políticas y Procedimientos para Personal Contratado
Asegurar que los consultores y el personal contratado que soporta la función de TI cumplan con las políticas organizacionales de protección de los activos de información de la empresa de tal manera que se logren los requerimientos contractuales acordados.

PO4.15 Relaciones
Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre la función de TI y otros interesados dentro y fuera de la función de TI, tales como el consejo directivo,

ejecutivos, unidades de negocio, usuarios individuales, proveedores, oficiales de seguridad, gerentes de riesgo, el grupo de cumplimiento corporativo, los contratistas externos y la gerencia externa (offsite).

PO5 ADMINISTRAR LA INVERSIÓN EN TI

PO5.1 Marco de Trabajo para la Administración Financiera
Establecer y mantener un marco de trabajo financiero para administrar las inversiones y el costo de los activos y servicios de TI a través del portafolio de inversiones habilitadas por TI, casos de negocio y presupuestos de TI.

PO5.2 Prioridades Dentro del Presupuesto de TI
Implementar un proceso de toma de decisiones para dar prioridades a la asignación de recursos a TI para operaciones, proyectos y mantenimiento, para maximizar la contribución de TI a optimizar el retorno del portafolio empresarial de programas de inversión en TI y otros servicios y activos de TI.

PO5.3 Proceso Presupuestal
Establecer un proceso para elaborar y administrar un presupuesto que refleje las prioridades establecidas en el portafolio empresarial de programas de inversión en TI, incluyendo los costos recurrentes de operar y mantener la infraestructura actual. El proceso debe dar soporte al desarrollo de un presupuesto general de TI así como al desarrollo de presupuestos para programas individuales, con énfasis especial en los componentes de TI de esos programas. El proceso debe permitir la revisión, el refinamiento y la aprobación constantes del presupuesto general y de los presupuestos de programas individuales.

PO5.4 Administración de Costos de TI
Implementar un proceso de administración de costos que compare los costos reales con los presupuestados. Los costos se deben monitorear y reportar. Cuando existan desviaciones, éstas se deben identificar de forma oportuna y el impacto de esas desviaciones sobre los programas se debe evaluar y, junto con el patrocinador del negocio para estos programas, se deberán tomar las medidas correctivas apropiadas y, en caso de ser necesario, el caso de negocio del programa de inversión se deberá actualizar.

PO5.5 Administración de Beneficios
Implementar un proceso de monitoreo de beneficios. La contribución esperada de TI a los resultados del negocio, ya sea como un componente de programas de inversión en TI o como parte de un soporte operativo regular, se debe identificar, acordar, monitorear y reportar. Los reportes se deben revisar y, donde existan oportunidades para mejorar la contribución de TI, se deben definir y tomar las medidas apropiadas. Siempre que los cambios en la contribución de TI tengan impacto en el programa, o cuando los cambios a otros proyectos relacionados impacten al programa, el caso de negocio deberá ser actualizado.

PO6 COMUNICAR LAS ASPIRACIONES Y LA DIRECCIÓN DE LA GERENCIA

PO6.1 Ambiente de Políticas y de Control
Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa. Estos elementos incluyen las expectativas / requerimientos respecto a la entrega de valor proveniente de las inversiones en TI, el apetito de riesgo, la integridad, los valores éticos, la competencia del personal, la rendición de cuentas y la responsabilidad. El ambiente de control se basa en una cultura que apoya la entrega de valor, mientras administra riesgos significativos, fomenta la colaboración entre divisiones y el trabajo en equipo, promueve el cumplimiento y la mejora continua de procesos, y maneja las desviaciones (incluyendo las fallas) de forma adecuada.

PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI
Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial general hacia los riesgos y el control que se alinee con la política de TI, el ambiente de control y el marco de trabajo de riesgo y control de la empresa.

PO6.3 Administración de Políticas para TI
Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir su intención, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Su relevancia se debe confirmar y aprobar en forma regular.

PO6.4 Implantación de Políticas de TI
Asegurarse de que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales.

PO6.5 Comunicación de los Objetivos y la Dirección de TI
Asegurarse de que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a los interesados apropiados y a los usuarios de toda la organización.

PO7 ADMINISTRAR RECURSOS HUMANOS DE TI

PO7.1 Reclutamiento y Retención del Personal
Asegurarse que los procesos de reclutamiento del personal de TI estén de acuerdo a las políticas y procedimientos generales de personal de la organización (Ej. contratación, un ambiente positivo de trabajo y orientación). La gerencia implementa procesos para garantizar que la organización cuente con una fuerza de trabajo posicionada de forma apropiada, que tenga las habilidades necesarias para alcanzar las metas organizacionales.

PO7.2 Competencias del Personal
Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso.

PO7.3 Asignación de Roles
Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requerimiento de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales. El nivel de supervisión debe estar de acuerdo con la sensibilidad del puesto y el grado de responsabilidades asignadas.

PO7.4 Entrenamiento del Personal de TI
Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales.

PO7.5 Dependencia Sobre los Individuos
Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal.

PO7.6 Procedimientos de Investigación del Personal
Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI. El grado y la frecuencia de estas verificaciones dependen de que tan delicada ó crítica sea la función y se deben aplicar a los empleados, contratistas y proveedores.

PO7.7 Evaluación del Desempeño del Empleado
Es necesario que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto. Los empleados deben recibir adiestramiento sobre su desempeño y conducta, según sea necesario.

PO7.8 Cambios y Terminación de Trabajo
Tomar medidas expeditas respecto a los cambios en los puestos, en especial las terminaciones. Se debe realizar la transferencia del conocimiento, reasignar responsabilidades y se deben eliminar los privilegios de acceso, de tal modo que los riesgos se minimicen y se garantice la continuidad de la función.

PO8 ADMINISTRAR LA CALIDAD

PO8.1 Sistema de Administración de Calidad
Establecer y mantener un QMS que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad, que esté alineado con los requerimientos del negocio. El QMS identifica los requerimientos y los criterios de calidad, los procesos claves de TI, y su secuencia e interacción, así como las políticas, criterios y métodos para definir, detectar, corregir y prever las no conformidades. El QMS debe definir la estructura organizacional para la administración de la calidad, cubriendo los roles, las tareas y las responsabilidades. Todas las áreas clave desarrollan sus planes de calidad de acuerdo a los criterios y políticas, y registran los datos de calidad. Monitorear y medir la efectividad y aceptación del QMS y mejorarla cuando sea necesario.

PO8.2 Estándares y Prácticas de Calidad
Identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del QMS. Usar las buenas prácticas de la industria como referencia al mejorar y adaptar las prácticas de calidad de la organización.

PO8.3 Estándares de Desarrollo y de Adquisición
Adoptar y mantener estándares para todo desarrollo y adquisición que siga el ciclo de vida, hasta el último entregable e incluir la aprobación en puntos clave con base en criterios de aceptación acordados. Los temas a considerar incluyen estándares de codificación de software, normas de nomenclatura; formatos de archivos, estándares de diseño para esquemas y diccionario de datos; estándares para la interfaz de usuario; interoperabilidad; eficiencia de desempeño de sistemas; escalabilidad; estándares para desarrollo y pruebas; validación contra requerimientos; planes de pruebas; y pruebas unitarias, de regresión y de integración.

PO8.4 Enfoque en el Cliente de TI
Enfocar la administración de calidad en los clientes, determinando sus requerimientos y alineándolos con los estándares y prácticas de TI. Definir roles y responsabilidades respecto a la resolución de conflictos entre el usuario/cliente y la organización de TI.

PO8.5 Mejora Continua
Mantener y comunicar regularmente un plan global de calidad que promueva la mejora continua.
PO8.6 Medición, Monitoreo y Revisión de la Calidad Definir, planear e implementar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que el QMS proporciona. La medición, el monitoreo y el registro de la información deben ser usados por el dueño del proceso para tomar las medidas correctivas y preventivas apropiadas.

PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

PO9.1 Marco de Trabajo de Administración de Riesgos

Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.

PO9.2 Establecimiento del Contexto del Riesgo
Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

PO9.3 Identificación de Eventos
Identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener los riesgos relevantes en un registro de riesgos.

PO9.4 Evaluación de Riesgos de TI
Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

PO9.5 Respuesta a los Riesgos
Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos en costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.

PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos
Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Obtener la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas están a cargo del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

PO10 ADMINISTRAR PROYECTOS
PO10.1 Marco de Trabajo para la Administración de Programas
Mantener el programa de los proyectos, relacionados con el portafolio de programas de inversiones facilitadas por TI, por medio de la identificación, definición, evaluación, otorgamiento de prioridades, selección, inicio, administración y control de los proyectos.
Asegurarse de que los proyectos apoyen los objetivos del programa. Coordinar las actividades e interdependencias de múltiples proyectos, administrar la contribución de todos los proyectos dentro del programa hasta obtener los resultados esperados, y resolver los requerimientos y conflictos de recursos.

PO10.2 Marco de Trabajo para la Administración de Proyectos
Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas en cada proyecto emprendido. El marco de trabajo y los métodos de soporte se deben integrar con los procesos de administración de programas.

PO10.3 Enfoque de Administración de Proyectos
Establecer un enfoque de administración de proyectos que corresponda al tamaño, complejidad y requerimientos regulatorios de cada proyecto. La estructura de gobierno de proyectos puede incluir los roles, las responsabilidades y la rendición de cuentas del patrocinador del programa, patrocinadores de proyectos, comité de dirección, oficina de proyectos, y gerente del proyecto, así como los mecanismos por medio de los cuales pueden satisfacer esas responsabilidades (tales como reportes y revisiones por etapa). Asegurarse que todos los proyectos de TI cuenten con patrocinadores con la suficiente autoridad para apropiarse de la ejecución del proyecto dentro del programa estratégico global.

PO10.4 Compromiso de los Interesados
Obtener el compromiso y la participación de los interesados afectados en la definición y ejecución del proyecto dentro del contexto del programa global de inversiones facilitadas por TI.

PO10.5 Declaración de Alcance del Proyecto
Definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar, entre los interesados, un entendimiento común del alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa global de inversiones facilitadas por TI. La definición se debe aprobar de manera formal por parte de los patrocinadores del programa y del proyecto antes de iniciar el proyecto.

PO10.6 Inicio de las Fases del Proyecto
Aprobar el inicio de las etapas importantes del proyecto y comunicarlo a todos los interesados. La aprobación de la fase inicial se debe basar en las decisiones de gobierno del programa. La aprobación de las fases subsiguientes se debe basar en la revisión y aceptación de los entregables de la fase previa, y la aprobación de un caso de negocio actualizado en la próxima revisión importante del programa. En el caso de fases traslapadas, se debe establecer un punto de aprobación por parte de los patrocinadores del programa y del proyecto, para autorizar así el avance del proyecto.

PO10.7 Plan Integrado del Proyecto
Establecer un plan integrado para el proyecto, aprobado y formal (que cubra los recursos de negocio y de los sistemas de información) para guiar la ejecución y el control del proyecto a lo largo de la vida del éste. Las actividades e interdependencias de múltiples proyectos dentro de un mismo programa se deben entender y documentar. El plan del proyecto se debe mantener a lo largo de la vida del mismo. El plan del proyecto, y las modificaciones a éste, se deben aprobar de acuerdo al marco de trabajo de gobierno del programa y del proyecto.

PO10.8 Recursos del Proyecto
Definir las responsabilidades, relaciones, autoridades y criterios de desempeño de los miembros del equipo del proyecto y especificar las bases para adquirir y asignar a los miembros competentes del equipo y/o a los contratistas al proyecto. La obtención de productos y servicios requeridos para cada proyecto se debe planear y administrar para alcanzar los objetivos del proyecto, usando las prácticas de adquisición de la organización.

PO10.9 Administración de Riesgos del Proyecto
Eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, identificación, análisis, respuesta, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados. Los riesgos afrontados por el proceso de administración de proyectos y el producto entregable del proyecto se deben establecer y registrar de forma central.

PO10.10 Plan de Calidad del Proyecto
Preparar un plan de administración de la calidad que describa el sistema de calidad del proyecto y cómo será implantado. El plan debe ser revisado y acordado de manera formal por todas las partes interesadas para luego ser incorporado en el plan integrado del proyecto.

PO10.11 Control de Cambios del Proyecto
Establecer un sistema de control de cambios para cada proyecto, de tal modo que todos los cambios a la línea base del proyecto (Ej. costos, cronograma, alcance y calidad) se revisen, aprueben e incorporen de manera apropiada al plan integrado del proyecto, de acuerdo al marco de trabajo de gobierno del programa y del proyecto.

PO10.12 Planeación del Proyecto y Métodos de Aseguramiento
Identificar las tares de aseguramiento requeridas para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado. Las tareas deben proporcionar la seguridad de que los controles internos y las características de seguridad satisfagan los requerimientos definidos.

PO10.13 Medición del Desempeño, Reporte y Monitoreo del Proyecto
Medir el desempeño del proyecto contra los criterios clave del proyecto (Ej. alcance, cronograma, calidad, costos y riesgos); identificar las desviaciones con respecto al plan; evaluar su impacto sobre el proyecto y sobre el programa global; reportar los resultados a los interesados clave; y recomendar, Implementar y monitorear las medidas correctivas, según sea requerido, de acuerdo con el marco de trabajo de gobierno del programa y del proyecto.

PO10.14 Cierre del Proyecto
Solicitar que al finalizar cada proyecto, los interesados del proyecto se cercioren de que el proyecto haya proporcionado los resultados y los beneficios esperados. Identificar y comunicar cualquier actividad relevante requerida para alcanzar los resultados planeados del proyecto y los beneficios del programa, e identificar y documentar las lecciones aprendidas a ser usadas en futuros proyectos y programas.

ANEXO Nº 4

FORMULARIO DE CUESTIONARIO Y ENTREVISTA

CUESTIONARIO

DATOS DEL PERSONAL

Nombre y apellido:……
Dirección y Cargo:……
Fecha: ……..
Rubrica: ……..

DETALLE DE PREGUNTAS:

1. ***Cuál es el grado de aplicación de las Normas de Auditoría Gubernamental emitidas por la Contraloría General del Estado:***

COMENTARIO*:……*
……
.....

2. ***Cuál es el grado de conocimiento de las Normas de Auditoría de Tecnologías de la Información y la Comunicación (TIC):***

COMENTARIO*:……*
……
.....

3. ***¿Cuál es el grado de aplicabilidad de la ejecución de auditorías TIC en la entidad? (marcar respuesta)***

e) 25%
f) 50%
g) 75%
h) 100%

COMENTARIO*:……*
……
.....

4. ***¿Cuenta la Dirección de Auditoría Interna con un enfoque metodológico y/o manual de procedimientos para llevar a cabo las auditorias TIC?***

COMENTARIO*:……*
……
.....

5. ***¿En caso de no existir, explique cómo se llevan a cabo la ejecución de auditorías TIC?***

COMENTARIO*:……*
……
.....

6. ¿Si los resultados producto de la auditoría de tecnologías de la información y comunicación son implementadas, se efectúa el seguimiento correspondiente?

COMENTARIO*:……*
……
.....

7. ¿Mencione las limitaciones y/o dificultades para la ejecución de auditorías TIC

COMENTARIO*:……*
……
.....

ACLARACION: Preguntas formuladas para el personal del área informática de la Dirección de Auditoría Interna del RUAT

ENTREVISTA

DATOS DEL PERSONAL

Nombre y apellido:……
Dirección y Cargo:……
Fecha: ……..
Rubrica: ……..

DETALLLE DE PREGUNTAS

1. ***¿Qué relevancia tiene usted sobre los informes de auditoría de tecnologías de la información y la comunicación?***

COMENTARIO*:……*
……
.....

2. ***¿En qué medida se implementan las recomendaciones?***

COMENTARIO*:……*
……
.....

ACLARACION: Preguntas efectuadas durante la entrevista realizada al Director de la Dirección de Auditoría Interna del RUAT.