Universidad de Costa Rica

Sistema de Estudios de Postrado

Auditoría de la seguridad de las Tecnologías de Información del Instituto Costarricense de Acueductos y Alcantarillados, (AyA)

Trabajo Final de Graduación aceptado por la Comisión del Programa de Postgrado en Administración y Dirección de Empresas, de la Universidad de Costa Rica, como requisito parcial para optar por el grado de Magíster en Administración y Dirección de Empresas con énfasis en Auditoría de Tecnologías y Sistemas de Información.

Óscar Gerardo Guzmán Aguilar
Carné 861714

Ciudad Universitaria “Rodrigo Facio”, Costa Rica 2007.

DEDICATORIA

A Gaby y nuestros Gemelos, a mi madresita bella, mis hermanos y sobrino, quienes son la inspiración de mi vida; pilares en la consecución de ésta nueva meta!!!

AGRADECIMIENTOS

Quisiera, primeramente, dar gracias a Dios Todopoderoso por haberme permitido vivir y llevar a cabo este proyecto tan importante en mi vida profesional.

A mi esposa Gabriela por su amor, paciencia y apoyo incondicional...

Al Instituto Costarricense de Acueductos y Alcantarillados, por permitirme trabajar y realizar esta Maestría con su patrocinio.

A la Dirección de Tecnologías de Información por su tiempo y colaboración en especial al Ing. Luis Ulate V.

Al Auditor Interno Don Alcides Vargas y a Doña Mary, por creer en mí, apoyarme y suministrarme tantas facilidades. No puedo dejar de lado a mis compañeros de la Auditoría Interna, quienes recargaron su trabajo para alivianar el mío, y particularmente a Don Efra.

Agradezco a mis tutores y amigos: Don Sergio y Don Xiomar, ambos ejemplo de tenacidad y conocimiento, porque inculcaron en mí ésta inclinación por la Auditoría de Sistemas y me guiaron en este proyecto.

Asimismo, deseo agradecer a todos los compañeros de esta primera generación de la Maestría en Auditoría de Tecnologías y Sistemas de Información de la UCR, por su amistad y camaradería, por las discrepancias y discusiones, pero sobre todo por las ideas, las enseñanzas y conocimientos que se permitieron compartir conmigo.

Finalmente a toda mi familia y a los amigos de siempre; por su voz de aliento y solidaridad.

¡Muchas Gracias!

Óscar Gdo.

HOJA DE APROBACIÓN

Este Trabajo Final de Graduación fue aceptado por la Comisión del Programa de Postgrado en Administración y Dirección de Empresas, de la Universidad de Costa Rica, como requisito parcial para optar al grado de Magister con énfasis en Auditoría de Tecnologías y Sistemas de Información.

_____	_____
MBA, Aníbal Barquero Chacón	MAI, Sergio Espinoza Guido
Director Programa de Maestría	Profesor Coordinador
_____	_____
M Sc., Xiomar Delgado Rojas	Lic., Alcides Vargas Pacheco
Profesor Guía	Supervisor Laboral

_____

Lic. Óscar Gerardo Guzmán Aguilar

Estudiante

CONTENIDO

AUDITORÍA DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN DEL INSTITUTO COSTARRICENSE DE ACUEDUCTOS Y ALCANTARILLADOS (AyA)

	Dedicatoria	**ii**
	Agradecimientos	**iii**
	Hoja de Aprobación	**iv**
	Contenido	**v**
	Índice de Anexos Complementarios	**ix**
	Índice de Siglas y Abreviaturas	**x**
	Resumen	**xii**
	Introducción	**14**
I	**Aspectos Generales del Instituto Costarricense de Acueductos y Alcantarillados (AyA), de la Auditoría Interna, de la Dirección de Tecnologías de Información del AyA.**	**19**
1.1	Aspectos Generales del Instituto Costarricense de Acueductos y Alcantarillados (AyA).	20
1.1.1	Reseña Histórica del Instituto Costarricense de Acueductos y Alcantarillados (AyA).	20
1.1.2	Misión del Instituto Costarricense de Acueductos y Alcantarillados, (AyA).	23
1.1.3	Visión del Instituto Costarricense de Acueductos y Alcantarillados, (AyA).	23

1.1.4	Valores del Instituto Costarricense de Acueductos y Alcantarillados, (AyA).	24
1.1.5	Servicios del Instituto Costarricense de Acueductos y Alcantarillados, (AyA).	24
1.1.6	Estructura organizacional del Instituto Costarricense de Acueductos y Alcantarillados, (AyA).	24
1.1.7	Leyes y reglamentos.	26
1.2	Aspectos Generales de la Auditoría Interna del Instituto Costarricense de Acueductos y Alcantarillados, (AyA).	27
1.2.1	Objetivos de la Auditoría Interna del AyA.	33
1.2.2	Estructura de la Auditoría Interna del AyA.	34
1.2.3	Análisis de la Auditoría Interna del AyA.	34
1.2.3.1	Fortalezas	35
1.2.3.2	Oportunidades	35
1.2.3.3	Debilidades	36
1.2.3.4	Amenazas	38
1.3	Aspectos Generales de la Dirección de Tecnologías de Información del Instituto Costarricense de Acueductos y Alcantarillados (AyA).	38
1.3.1	Objetivos de la Dirección de Tecnologías de Información del AyA.	38
1.3.2	Estructura de la Dirección de Tecnologías de Información del AyA.	39
1.3.3	Análisis de la Dirección de Tecnologías de Información del AyA.	40

1.3.3.1 Fortalezas 40

1.3.3.2 Oportunidades 41

1.3.3.3 Debilidades 42

1.3.3.4 Amenazas 44

1.4 Configuración Computacional del AyA. 45

1.5 Situación de la Seguridad de las Tecnologías de Información en AyA. 47

1.5.1 Sistema de Seguridad Física y Lógica del AyA. 47

1.5.1.1 Seguridad Física 47

1.5.1.2 Seguridad Lógica 48

II Herramientas Teóricas de Auditoría y Tecnologías de Información. 50

2.1 Algunas definiciones y conceptos para el desarrollo del proyecto. 50

2.1.1 Términos y definiciones de Auditoría 50

2.1.2 Términos y definiciones de Tecnologías de Información 60

2.1.3 Términos y definiciones de Seguridad en Tecnología de Información 70

III Análisis de la Situación Actual de la Seguridad de la Información en AyA. 75

3.1 Planeación de la Auditoría 75

3.1.1 Origen del Estudio 76

3.1.2 Área a Auditar 76
3.1.3 Alcance 77
3.1.4 Objetivos 78
3.1.4.1 Objetivo General 78
3.1.4.2 Objetivo Específicos 78
3.1.5 Marco Legal 79
3.1.6 Recursos Requeridos 80
3.1.6.1 Personal 80
3.1.6.2 Materiales 80
3.1.6.3 Tiempo Estimado 80
3.2 Análisis del Riesgo 81
3.2.1 Nuevo personal 82
3.2.2 Sistemas de Información Nuevos o Reorganizados 82
3.2.3 Nuevas Tecnologías 82
3.3 Determinación de Areas Críticas 82
3.4 Evaluación del Control Interno 83
3.5 Elaboración del Programa de Auditoría 83
3.5.1 Pruebas Sustantivas 84
3.5.2 Pruebas de Cumplimiento 84
3.6 Preparación de la Auditoría 85

3.6.1	Elaboración de los Papeles de Trabajo	85
3.7	Aplicación de las Pruebas de Auditoría	85
3.8	Recolección de Hallazgos (Oportunidades de Mejora)	86
3.9	Preparación del Informe	86
IV	**Resultados de la Evaluación**	**88**
4.1	Presentación de Hallazgos u Oportunidades de Mejora	88
4.2	Elaboración del Informe Final de Auditoría	101
4.3	Conferencia Final o Discusión del Informe	101
4.4	Presentación del Informe Final de Auditoría	102
4.5	Seguimiento del Informe Final de Auditoría	103
V	**Conclusiones y Recomendaciones Generales**	**105**
5.1	Conclusiones Generales	105
4.2	Recomendaciones Generales	106
	Bibliografía	**109**
	Anexos Complementarios	**115**

Índice de Anexos Complementarios

Nº 1 Cuestionario de Control Interno.

Nº 2 Plan de Auditoría

Nº 3 Programa de Auditoría.

Nº 4 Organigrama Institucional.

Nº 5 Organigrama de la Dirección de Tecnologías de Sistemas.

Nº 6 Organigrama de la Auditoría Interna.

Nº 7 Centro de Servicios Corporativos.

Nº 8 Elementos de los Servicios de Internet Corporativos.

Nº 9 Informe de Auditoría.

Índice de Siglas y Abreviaturas

Administrador de Bases de Datos	DBA
Asociación de Auditoría y Control de Sistemas de Información	ISACA
Asociación Costarricense de Auditores en Informática	ACAI
Asociaciones Administradoras de servicios de Acueducto y Alcantarillado Comunales	ASADA
Autoridad Reguladora de los Servicios Públicos	ARESEP
Bases de Datos	BD
Compañía Nacional de Fuerza y Luz	CNFL
Contraloría General de la República	CGR
Empresa de Servicios Públicos de Heredia	E.S.P.H
Estándar Británico	B.S.
Estándar de Calidad / Instituto de Regulación de Calidad	ISO
Factores Críticos del Éxito	FCE
Identificación	IDS
Instituto Costarricense de Acueductos y Alcantarillados	AyA
Instituto Costarricense de Electricidad	ICE
Junta de Administración de los Servicios Eléctricos Municipales de Cartago	JASEC
Lenguaje de Consulta de Bases de Datos	SQL
Ley General de Control Interno	LGCI
Licenciatura	Lic.
Maestría en Administración de Empresas	MBA
Maestría en Auditoría Informática	MAI
Maestría en Ciencias Sociales	MSc
Manual sobre Normas Técnicas de Control Interno relativas a los Sistemas de Información Computadorizados	SIC
Objetivos de Control para Información y Tecnologías Relacionadas	Cobit
Préstamos y Proyectos con un Banco Alemán	KFW
Préstamos y Proyectos con un Banco Japonés	JBIC
Préstamos y Proyectos del Banco Interamericano de Desarrollo	BID
Radiográfica Costarricense Sociedad Anónima	RACSA
Red de Área Ancha o Ensanchada	WAN
Red Local	LAN
Red Metropolitana	MAN
Servicio Nacional de Acueductos y Alcantarillados	SNAA
Sistemas, Aplicaciones y Productos (Sistema Financiero Contable	SAP
Sistema Comercial	OPEN
Sistema de Evaluación del riesgo	SEVRI
Sistema Gerencial de Comunicación	SEG

Sistema Integrado Financiero Suministros	SIFS
Sistemas de Información	SI
Tecnologías de Información	TI
Universidad de Costa Rica	UCR

Resumen

Guzmán Aguilar, Oscar Gerardo

Auditoría de la Seguridad de las Tecnologías de Información del Instituto Costarricense de Acueductos y Alcantarillados

Programa de Postgrado en Dirección de Empresas con Énfasis en Auditoría de Tecnologías de Información

El objetivo general del trabajo es realizar una Auditoría de la Seguridad de las Tecnologías de Información del Instituto Costarricense de Acueductos y Alcantarillados (AyA), con el propósito de evaluar los aspectos que intervienen en el proceso de la Seguridad de las Tecnologías de Información, para detectar aspectos potenciales de mejora, mediante la implementación metodológica de una Auditoría basada en los conocimientos adquiridos durante el plan de estudios de la Maestría en Auditoría de Tecnologías de Información.

El Instituto Costarricense de Acueductos y Alcantarillados brinda los servicios de agua potable y alcantarillado sanitario a gran parte del territorio nacional. Tiene, además, la rectoría de esas áreas para todo el país y lo realiza integrando actividades de financiamiento, de protección ambiental y de construcción, con las de operación y mantenimiento de ambos servicios, financiándose con tarifas y tasas bajo el principio de servicio al costo, más un rédito de capitalización para desarrollo, como soporte a esto, las Tecnologías de Información tienen una incuestionable importancia para el logro de los objetivos Institucionales.

Para ello el proyecto desarrolla una investigación de tipo práctica profesional, mediante una Auditoría de la Seguridad de las Tecnologías de Información.

Dentro de sus principales conclusiones se encuentra que en el Instituto existe un ambiente físico y lógico, seguro y controlado, con medidas de protección fundamentadas en las políticas vigentes y en análisis de riesgos, hecho que satisface enormemente.

Con base en todo lo anterior, se recomienda que se siga por esa línea de evaluación de riesgos y de fortalecimiento del ambiente y estructura de seguridad controlada y fundamentada.

Palabras clave:

Auditoría, Tecnologías, Agua, Alcantarillado, Instituto, Servicios Públicos, Controles, Evaluación, Riesgos, Programas de Trabajo, Cuestionario de Control interno.

Director de la investigación:
MAI Sergio Espinoza Guido.
Unidad Académica: Maestría en Auditoría de Tecnologías y Sistemas de Información.
Programa de Postgrado en Administración y Dirección de Empresas.
Sistema de Estudios de Postgrado.

Introducción

Hoy día la incorporación de Tecnologías de Información y Comunicación (TIC) como un elemento más, y de mucha importancia, en el manejo de las empresas es uno de los principales temas que conciernen e inquietan a altos ejecutivos y las organizaciones. Las empresas, tanto privadas como del sector público, han generalizado su utilización con el fin de fortalecer los procesos claves de sus entidades y negocios, todo en procura de mejorar los servicios a los usuarios y al logro de los objetivos propuestos.

Cada día crece más la tendencia de las empresas por adherirse a los avances tecnológicos, llevándolas a efectuar inversiones de recursos económicos muy significativos, muchas veces sin un plan estratégico informático que les ordene, establezca prioridades, les dé seguimiento y sobre todo les asegure el éxito en la consecución de los objetivos que como empresa tienen, lo anterior sin importar la seguridad de la información que manejan.

El sector público costarricense no ha escapado a esta tendencia, en los últimos años se ha evidenciado un importante crecimiento en inversiones de Tecnologías de Información y Comunicación (TIC), por lo que debe convertirse en un elemento de atención de la administración y particularmente de las Auditorías Internas, con el fin de asegurar que éstas se efectúen bajo principios de eficiencia y eficacia, y que la utilización de esas tecnologías efectivamente conlleven un valor agregado a los servicios que se prestan a los usuarios y para asegurarse que cumplen, al menos, con aspectos mínimos de seguridad.

El Instituto Costarricense de Acueductos y Alcantarillados, no ajeno a esta corriente tecnológica procura un uso eficiente y seguro de los recursos invertidos en esta área. La Administración se apoya en un marco estratégico que coadyuve a la mejor gestión de las tecnologías de información y comunicación, y a brindarle la seguridad que estas requieren. De esta manera, la Administración debe velar por el establecimiento de políticas, normas, procedimientos y directrices que regulen la gestión; la administración y la seguridad de esas tecnologías deben ser parte de la cultura organizacional, misma que debe implementar los mecanismos de aseguramiento de la calidad en el tiempo.

En procura de mejorar los controles y niveles de seguridad en esa materia, y a fin de colaborar con el uso más eficiente y eficaz de los recursos invertidos en ese campo y, en general, aportar un valor agregado a las actividades que desarrolla una entidad pública, la Auditoría Interna vela por la salvaguarda de los activos de la organización, al fiscalizar, asesorar y advertir a la Administración para que ésta dé y haga el mejor aprovechamiento de los recursos informáticos y de su alineación con los objetivos institucionales.

En el presente trabajo se realiza una evaluación de la Seguridad de las Tecnologías de Información en el Instituto Costarricense de Acueductos y Alcantarillados (AyA) de conformidad con lo establecido en el “Manual sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computadorizados”, emitido por la Contraloría General de la República.

Asimismo se complementa con las mejores prácticas de aplicación en materia de Seguridad de Tecnología de Información y Comunicación, emitidas por organizaciones internacionales reconocidas, que se han especializado en la materia, tales como: la Asociación de Auditoría y Control de Sistemas de Información (ISACA), con su documento "Objetivos de control para la información y tecnologías relacionadas" (COBIT por su acrónimo en inglés), así como las normas ISO-17799:2000, relativas a seguridad, y la ISO-9001:2000, de gestión de calidad, ambas emitidas por la International Organization for Standarization (ISO).

En cuanto a las limitaciones que en cualquier labor de investigación se presentan, es importante destacar que desde el principio se contó con el apoyo y permiso del Auditor General del AyA, pero la inexperiencia en esta área de la auditoría, el poco tiempo para la ejecución de esta práctica profesional, el no contar con las herramientas tecnológicas necesarias, ni con los antecedentes de auditorías anteriores se convirtieron en las mayores limitantes.

Con este tema, como estudiante de la Maestría en Auditoría de Tecnologías y Sistemas de Información, se tiene la oportunidad de realizar la práctica profesional e implementar integralmente los conocimientos adquiridos estos dos años de compartir y adquirir conocimientos de una serie de profesores y compañeros de mucha experiencia en el área de tecnologías de información.

Se estima que la Auditoría Interna del Instituto Costarricense de Acueductos y Alcantarillados (AyA) se ve beneficiada con este estudio por que la papelería, guías de trabajo, criterios importantes, planes, programas de trabajo, evidencia del trabajo quedan al servicio de ésta, los conocimientos y experiencias de ésta práctica serán plasmados en un documento serio y de enorme cuantía para posteriores evaluaciones y, el Instituto obtiene así una opinión objetiva e independiente de la situación de la seguridad de los sistemas de información que le permitiría, como un valor agregado, para que pueda tomar las precauciones y acciones necesarias para alinear, controlar y ejecutar los mecanismos de aseguramiento de la información en general, que le asegure a la sociedad, tanto interna como externa, que la información personal de sus clientes y funciones está debidamente segura y protegida.

CAPÍTULO 1

1 *Aspectos Generales del Instituto Costarricense de Acueductos y Alcantarillados (AyA), de la Auditoría Interna, de la Dirección de Tecnologías de la Información del AyA.*

Este capítulo introduce de manera general, la historia de la organización en que se realiza la auditoría – el Instituto Costarricense de Acueductos y Alcantarillados (AyA)– algunos aspectos de la Auditoría Interna y de la Dirección de Tecnologías de Información del Instituto, ya que, como parte de toda auditoría, se debe realizar una revisión preliminar, y parte de esta fase es el obtener el conocimiento suficiente de la organización por auditar y de los sistemas que le conforman. En este sentido se analizan aspectos históricos, de conformación y de servicio de la organización y de las unidades citadas.

AyA es una Institución creada para brindar el servicio de agua potable en forma continua, asimismo el de disposición de aguas servidas, o sea, es responsable de proporcionar vida y salud a todos los habitantes de Costa Rica.

Para comprender y conocer mejor la organización en estudio a continuación, en forma muy resumida, un vistazo al pasado del AyA, en él se destacan algunos de los pasos históricos que hicieron grande a ésta noble Institución.

1.1 Aspectos Generales del Instituto Costarricense de Acueductos y Alcantarillados (AyA)

1.1.1 Reseña histórica del Instituto Costarricense de Acueductos y Alcantarillados

En la década de los cincuentas, la población del Área Metropolitana de San José ejercía fuerte presión sobre el gobierno, en procura de una solución al problema de falta de agua potable para consumo básico. Era obvio que a partir de 1950, con la población del país duplicada y con el surgimiento de patrones de consumo diferentes a los acostumbrados, hasta esta fecha la cantidad de agua producida y distribuida en esa área era totalmente insuficiente.

Con el propósito de responder a estas demandas, el gobierno inicio un proyecto de instalación de redes en los barrios del sur de San José, así como la construcción de los actuales Tanques del Sur, cuya inauguración tuvo lugar en 1955.

Al acercarse el final de la década de los cincuentas, ya era evidente el hecho de que, el creciente problema que generaba el abastecimiento de agua no podía resolverse mediante la gestión municipal. Es así como surge la necesidad de crear un organismo independiente que se responsabilizara de la situación y la abordara en términos globales.

Durante la presidencia del Lic. Mario Echando Jiménez, hubo dos proyectos que se presentaron a consideración de la Asamblea Legislativa, con el fin de constituir el nuevo organismo que rigiera las funciones alrededor de la necesidad existente, uno propuesto por el entonces diputado, Lic. Daniel Oduber Quirós, en el cual se planteaba la conveniencia de crear la Dirección de Obras Sanitarias del Área Metropolitana, como organismo semiautónomo adscrito al Ministerio de Obras Públicas y Transportes, con personería jurídica y patrimonio propio; y otro, elaborado por el Poder Ejecutivo en el que se creaba la Dirección de Aguas, Tarifas y Alcantarillados.

Este último fue utilizado como base para discusión y dio origen a la Ley No. 2726 del 04 de abril de 1961, de creación de un organismo con el nombre de Servicio Nacional de Acueductos y Alcantarillados (S.N.A.A.), cuyo propósito primordial era proveer a los habitantes de la República de servicios adecuados de agua potable y de disposición de aguas negras, además de que diera al ámbito nacional un enfoque global y altamente técnico de los problemas en estos campos.

La nueva institución comenzó sus labores el 08 de junio de 1961, con la primera sesión realizada por la Junta Directiva en el despacho del Ministerio de Salubridad Pública el Dr. José Manuel Quince Morales, fue quien asumió el cargo de Presidente de esa Junta. En esta primera reunión se nombró como Gerente al Ing. Jorge Carballo Wedel.

Las oficinas fueron inicialmente instaladas en el edificio Autofores, en avenida 10 calle 9, y el primer personal a su cargo fue trasladado de los Departamentos de Obras Hidráulicas del Ministerio de Obras Públicas, Departamento de Ingeniería Sanitaria del Ministerio de Salubridad Publica y de

cada sistema municipal que adquiría bajo su responsabilidad. La organización de la nueva entidad se diseñó con miras a lograr la consecución de sus dos grandes finalidades: financiación, construcción de obras, así como operación y mantenimiento de todos los sistemas bajo la administración del S.N.A.A.

Como consecuencia del lógico crecimiento institucional la organización experimentó diversas modificaciones tendientes a adecuar permanentemente el funcionamiento del organismo a las necesidades del momento, en procura de las soluciones más adecuadas a los problemas enfrentados. Por iniciativa de la Institución, la Asamblea Legislativa promulgó la Ley No.5915 del 12 de julio de 1976, en virtud de la cual se le introdujeron importantes reformas a su ley constitutiva. Dichas reformas significaron las siguientes modificaciones en el funcionamiento del S.N.A.A.

a) Cambio de nombre a Instituto Costarricense de Acueductos y Alcantarillados, la nueva sigla a partir de este momento sería AyA (abreviaturas de Acueductos y Alcantarillados.)

b) Autonomía: Se le dio a la Institución el carácter de ente autónomo, con lo cual se favoreció su especialidad orgánica en el campo del abastecimiento de agua potable y provisión de sistemas de alcantarillado sanitario.

c) Administración: Sin perjuicio de su función rectora desde el punto de vista técnico, que conserva, se le confirieron a la Institución facultades para dar mayor participación a las comunidades y organismos locales en la administración y operación de los servicios de agua potable y alcantarillado sanitario.

1.1.2 Misión del Instituto Costarricense de Acueductos y Alcantarillados:

El Instituto Costarricense de Acueductos y Alcantarillados tiene la siguiente misión:

> *"Suplir y normar todos los aspectos relacionados con los servicios públicos de agua potable y alcantarillado sanitario para toda la población dentro del territorio nacional, por medio de la integración de las actividades de financiamiento, protección ambiental y construcción, con las de operación y mantenimiento de ambos servicios, financiados por medio de tarifas y tasas que se ajusten al principio de servicio al costo, más un rédito de capitalización para desarrollo."*

1.1.3 Visión del Instituto Costarricense de Acueductos y Alcantarillados:

La visión del Instituto Costarricense de Acueductos y Alcantarillados dice:

> *"AyA será una Institución, que mediante el fortalecimiento de sus potestades de rectoría y operación, se posicione entre las organizaciones líderes a nivel latinoamericano en materia de agua potable y alcantarillado sanitario; mediante el desarrollo de proyectos, donde prevalezca el sentido social, y en armonía con el ambiente"*

1.1.4 Valores del Instituto Costarricense de Acueductos y Alcantarillados:

Los valores del Instituto Costarricense de Acueductos y Alcantarillados son tres: Excelencia, Espíritu de Servicio, Ética.

1.1.5 Servicios del Instituto Costarricense de Acueductos y Alcantarillados:

Los servicios que brinda el Instituto Costarricense de Acueductos y Alcantarillados (AyA) son: los de agua potable y el de disposición de aguas servidas, esto para todo el territorio nacional, en calidad de ello puede y ha recurrido a la delegación de la prestación de esos servicios a Municipios, Asociaciones, y a empresas como la Junta Administrativa de los Servicios Eléctricos Municipales de Cartago (JASEC) y la Empresa de Servicio Públicos de Heredia (ESPH).

1.1.6 La estructura organizacional del Instituto Costarricense de Acueductos y Alcantarillados:

El Instituto Costarricense de Acueductos y Alcantarillados tiene como más alta dependencia a la Junta Directiva que tiene un órgano asesor como lo es la Auditoría Interna.

Cuenta con una Presidencia Ejecutiva, que se relaciona directamente a nivel de staff con una Asesoría Jurídica, una Contraloría de Servicios, un

departamento de Planificación y otro de Prensa y Relaciones Públicas. Aquí se encuentra adscrito también un departamento de Salud Ocupacional.

Luego se encuentran la Gerencia y la Subgerencia, quien cuenta a nivel de staff con el Departamento de Organización y Desarrollo, el Laboratorio Nacional de Aguas y la Dirección de Tecnología Informática.

En el siguiente nivel se encuentran las Direcciones de Gestión Ambiental, con los Departamentos de Cuencas Hidrográficas, Estudios Básicos y Control Ambiental; la Dirección de Construcción de Obras con los Departamentos de Obras por Contrato y Obras por Administración; la Dirección de Agua Potable con los Departamentos de Operación y Mantenimiento y Optimización de Sistemas; la Dirección de Aguas Residuales con los Departamentos de Operación y Mantenimiento y Optimización de Sistemas; la Dirección de AyA Comunales que ya fue relanzada como la Dirección de Acueductos Rurales; la Dirección de Estudios y Proyectos con los Departamentos de Topografía, Diseño y Desarrollo Físico; la Dirección de Servicio al Cliente, con los Departamentos de Mercadeo, Comercial y Medición; la Dirección de Apoyo Logístico con los Departamentos de Proveeduría, Servicios Generales, Gestión de Documentación y Archivo (GEDI) y Gestión del Riesgo; la Dirección de Recursos Humanos con los Departamentos de Gestión del Capital Humano y Desarrollo del Capital Humano; la Dirección Financiera con los Departamentos de Contabilidad, Presupuesto y Tesorería.

Esta estructura se encuentra en cada una de las Regiones que se enumeran a continuación: Huetar Atlántica, Brunca, Central Oeste, Cartago, Chorotega, Heredia, Huetar Norte, Metropolitana y Pacifico Central, todas con una área de Administrativo financiero, de Operación y Mantenimiento, de

Servicio al Cliente, Gestión Ambiental y Recurso Hídrico y Comunales divididas a su vez en Cantonales. Todo lo anterior se puede apreciar más gráficamente en el Organigrama aprobado por MIDEPLAN con el Oficio DM-1780-2005- del 21 de noviembre del año 2005, y que aparece en los anexos.

1.1.7 Leyes y reglamentos

Entre las Leyes y Reglamentos que debe observar Instituto Costarricense de Acueductos y Alcantarillados se encuentran:

- Constitución Política de la República de Costa Rica.
- Ley 7494: Ley de la Contratación Administrativa y su Reglamento
- Ley 2726: Ley Constitutiva de AyA y sus reformas
- Ley 7600: Ley de Igualdad de Oportunidades para las Personas Discapacitadas.
- Ley 8292: Ley General de Control Interno
- Ley Recurso Hídrico
- Ley 5395: Ley General de la Salud
- Ley 8422: Ley contra la corrupción y el enriquecimiento ilícito en la función pública
- Ley 7794: Código Municipal
- Ley Reguladora del Fumado y Decreto 25462-5
- Ley Contra Hostigamiento y Acoso Sexual
- Ley 276: Ley de Aguas
- Ley 218: Ley de Asociaciones
- Ley 7495: Ley de expropiaciones
- Ley 4240: Ley de Planificación Urbana
- Ley 7202: Ley del Sistema Nacional de Archivos

- Ley 1634: Ley General de Agua Potable
- Ley 7010: Aprobación de Créditos
- Ley 7914: Nacional de Emergencia
- Ley 5525: Planificación Nacional
- Ley 8131: Adm Financiera y de Presupuestos Públicos
- Ley 6727: Ley General de la Administración Pública
- Ley 7554: Orgánica del Ambiente
- Ley 8220: Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos
- Ley Nacional del Sistema Bancario
- Ley Riesgos del Trabajo
- Reglamentos Internos.
- Otras Leyes, decretos, resoluciones presidenciales, ministeriales y de la Contraloría General de la República.

1.2 Aspectos Generales de la Auditoría Interna del Instituto Costarricense de Acueductos y Alcantarillados (AyA).

La Auditoría Interna del Instituto Costarricense de Acueductos y Alcantarillados, actúa de acuerdo con las directrices de la Contraloría General de la República en el ámbito de las Auditorías Internas, impartidas mediante el Manual de normas generales de control interno para la Contraloría General de la República y las entidades y Órganos sujetos a su fiscalización, Ley General del Control Interno, Manual de Normas Técnicas de Auditoría, Manual para el ejercicio de la Auditoría Interna y el Manual de Lineamientos en la Promulgación de los Reglamentos de las Auditorías Internas, Ley Orgánica de la Contraloría General de la República.

Se conceptúa a la Auditoría Interna, como la actividad encargada de evaluar en forma independiente dentro de una organización, las operaciones contables, financieras, administrativas y de otra naturaleza, como base para prestar un servicio constructivo y de protección a la Administración. Es un control que funciona al medir y valorizar en forma posterior la eficiencia y la eficacia de todos los otros controles establecidos en el ente.

La Auditoría Interna es función asesora y fiscalizadora no de línea. Sobre esta base no ejerce acción ejecutiva dentro de las labores corrientes administrativas y actúa, como lo ha hecho hasta la fecha, con la información y la comunicación de sus observaciones y recomendaciones, para que la administración tome las medidas correctivas. Compete a la auditoría interna, primordialmente lo siguiente:

a) Realizar auditorías o estudios especiales semestralmente, en relación con los fondos públicos sujetos a su competencia institucional, incluidos fideicomisos, fondos especiales y otros de naturaleza similar. Asimismo, efectuar semestralmente auditorías o estudios especiales sobre fondos y actividades privadas, de acuerdo con los artículos 5 y 6 de la Ley Orgánica de la Contraloría General de la República, en el tanto estos se originen en transferencias efectuadas por componentes de su competencia institucional.
b) Verificar el cumplimiento, la validez y la suficiencia del sistema de control interno de su competencia institucional, informar de ello y proponer las medidas correctivas que sean pertinentes.
c) Verificar que la administración activa tome las medidas de control interno señaladas en esta Ley, en los casos de desconcentración de

competencias, o bien la contratación de servicios de apoyo con terceros; asimismo, examinar regularmente la operación efectiva de los controles críticos, en esas unidades desconcentradas o en la prestación de tales servicios.

d) Asesorar, en materia de su competencia, al jerarca del cual depende; además, advertir a los órganos pasivos que fiscaliza sobre las posibles consecuencias de determinadas conductas o decisiones, cuando sean de su conocimiento.

e) Autorizar, mediante razón de apertura, los libros de contabilidad y de actas que deban llevar los órganos sujetos a su competencia institucional y otros libros que, a criterio del auditor interno, sean necesarios para el fortalecimiento del sistema de control interno.

f) Preparar los planes de trabajo, por lo menos en conformidad con los lineamientos que establece la Contraloría General de la República.

g) Elaborar un informe anual de la ejecución del plan de trabajo y del estado de las recomendaciones de la auditoría interna, de la Contraloría General de la República y de los despachos de contadores públicos; en los últimos dos casos, cuando sean de su conocimiento, sin perjuicio de que se elaboren informes y se presenten al jerarca cuando las circunstancias lo ameriten.

h) Mantener debidamente actualizado el reglamento de organización y funcionamiento de la auditoría interna.

i) Practicar auditorías o estudios especiales de auditoría en cualesquiera unidades administrativas u operativas del Instituto, en el momento que lo considere oportuno, con base en su plan de auditoría o de acuerdo con las prioridades del caso cuando medie petición de la Gerencia o Junta Directiva.

j) Comunicar por escrito a la Gerencia los resultados de cada auditoría o estudio especial de auditoría que se lleve a cabo, por medio de memorandos e informes, con comentarios, conclusiones y recomendaciones, como medio de brindar la asesoría pertinente para mejorar la eficiencia y la eficacia en el sistema de control interno y en la gestión financiera y administrativa de la Institución.
k) Ejecutar sus funciones con libertad e independencia de criterio respecto de las demás unidades administrativas u operativas.
l) Preparar un plan de auditoría que contemple las auditorías o estudios especiales por ejecutarse durante el año.
m) Preparar y remitir a la Junta Directiva un informe anual de labores y de otros aspectos de importancia.
n) Otros que le sean asignados atinentes a su objeto.

Alguna normativa importante de mencionar para asegurar el cumplimiento de las competencias del Auditor en AyA son:

El artículo 11 inciso j) de la Ley Constitutiva de AyA[1] establece la facultad de la Junta Directiva de nombrar el Auditor del Instituto.

El artículo 14 de dicha Ley expresa lo siguiente:

"La Auditoría funcionará bajo la responsabilidad y dirección del Auditor, quien será nombrado por la Junta Directiva con el voto favorable de no menos de cinco de sus miembros. El Auditor deberá ser Licenciado en Ciencias Económicas y Sociales, debidamente autorizado para ejercer la profesión en Costa Rica, y reunir, además, las mismas condiciones exigidas para el cargo de Gerente.

[1] Ley Nº2726 del 14 de abril de 1961 y sus reformas.

Será inamovible salvo que, a juicio de la Junta Directiva y previa información, se demuestre que no cumple debidamente las funciones y deberes inherentes a su cargo y quedará, en todo caso, sujeto a las disposiciones que para los miembros de la Junta Directiva establece la presente ley, en cuanto le fueren aplicables, dada la naturaleza de su cargo y el origen de su nombramiento".

El artículo 15 de la Ley Constitutiva define claramente la dependencia del Auditor, al establecer:

"El Auditor dependerá directamente de la Junta Directiva, ante la cual serán apelables sus decisiones".

Además la Ley General de Control Interno[2], indica en su artículo 23- Organización lo siguiente:

"La auditoría interna se organizará y funcionará conforme lo disponga el auditor interno, de conformidad con las disposiciones, normas, políticas y directrices que emita la Contraloría General de la República, las cuales serán de acatamiento obligatorio.

Cada auditoría interna dispondrá de un reglamento de organización y funcionamiento, acorde con la normativa que rige su actividad. Dicho reglamento deberá ser aprobado por la Contraloría General de la República, publicarse en el diario oficial y divulgarse en el ámbito institucional".

[2]Ley 8292; Ley de Control Interno del 31 de julio del 2002.

También esta misma Ley, indica en su artículo 24- Dependencia orgánica y regulaciones administrativas aplicables:

> "El Auditor y el subauditor internos de los entes y órganos sujetos a esta Ley dependerán orgánicamente del máximo jerarca, quien los nombrará y establecerá las regulaciones de tipo administrativo que le serán aplicables a dichos funcionarios".

Otros aspectos que el funcionario de la Auditoría Interna de AyA debe dominar, son los contemplados en los diversos reglamentos y procedimientos aprobados en la institución, como por ejemplo:

- Reglamento de Organización y funciones de la Auditoría Interna de AyA.
- Manual sobre Normas Generales de Auditoria
- Manual para el Ejercicio de la Auditoria Interna
- Manual de Normas Generales de Control Interno para la Contraloría General de la República y las entidades y órganos sujetos a su Fiscalización.
- Manual de normas técnicas de control interno relativas a los sistemas de información computadorizados.
- Manual de Procedimientos de Auditoría Interna
- Manual de Organización de la Auditoría Interna
- Reglamentos Internos.
- Manuales Internos
- Programas de Auditoría Interna
- Manual de Clasificación de Cuentas
- Manual de Procedimientos de los diferentes Departamentos

- Circulares, instrucciones y otras disposiciones oficiales del Instituto.
- Leyes, decretos, resoluciones presidenciales, ministeriales y de la Contraloría General de la República, y cualesquiera otros que tengan relación con las tareas que cada funcionario desempeña.

1.2.1 Objetivos de la Auditoría Interna del AyA.

La Auditoría Interna del Instituto Costarricense de Acueductos y Alcantarillados busca los siguientes objetivos:

a) Prestar un servicio de asesoría constructiva y de protección a la administración, proporcionándole en forma oportuna, información análisis, evaluación, comentarios y recomendaciones pertinentes, sobre las operaciones que examina en forma posterior.
b) Llevar a cabo las actividades de auditoría financiera, que tienen como propósito el proteger los recursos de la entidad contra errores o posibles irregularidades; verificar las operaciones contables, financieras y de otra naturaleza del Instituto y el cumplimiento de las disposiciones legales, políticas y reglamentaciones internas.
c) Realizar las actividades de auditoría de pagos y contratos, con el propósito de proteger los recursos de la entidad contra errores o posibles irregularidades y velar porque las transacciones se ajusten a las disposiciones legales y reglamentarias vigentes.
d) Coadyuvar con la eficiencia y eficacia de los sistemas de información y el procesamiento de datos, mediante la identificación de los posibles errores que se generen en éste, buscar el camino para corregirlos y los procedimientos adecuados para evitarlos.

e) Examinar las operaciones de la entidad, con la finalidad de evaluarlas y verificarlas, determinando si estas se han logrado en conformidad con las atribuciones asignadas y con la mayor eficacia posible.
f) Evaluar desde el punto de vista de auditoría, en forma oportuna, independiente y a posteriori, las operaciones de la actividad del Sistema Comercial del Instituto, con el propósito de verificar la efectividad de los procesos, la legitimidad de las operaciones y el adecuado cumplimiento de la normativa vigente.

1.2.2 Estructura de la Auditoría Interna del AyA.

Para desarrollar sus funciones básicas la Auditoría Interna se ha dividido en seis actividades o áreas de acción, a saber: Jefatura General de Auditoría, Departamento de Auditoría Financiera, Departamento de Auditoría de Pagos y Contratos, Departamento de Auditoría Informática, Departamento de Auditoría Operacional, Departamento de Auditoría en Región Metropolitana, Departamento de Auditoría Estudios Especiales, Departamento de Auditoría Regional, en los que se dividen sus 32 funcionarios.

1.2.3 Análisis de la Auditoría Interna del AyA.

El siguiente análisis de diagnóstico mediante el uso de la técnica FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) en la Auditoría Interna del Instituto Costarricense de Acueductos y Alcantarillados es el resultado de un ejercicio minucioso, y para la consecución del objetivo fue necesaria la discusión y análisis de todo el grupo. En este sentido la aplicación de esta técnica se realizó para toda la Auditora Interna, con los siguientes resultados:

1.2.3.1 Fortalezas

a) La Auditoría Interna está creada por Ley y su funcionamiento se sustenta en la aplicación de Leyes, reglamentos, manuales, procedimientos y directrices.
b) Posee independencia funcional y de criterio respecto del jerarca (art.21, 24 y 25 LGCI) y de los demás órganos de la administración activa. Además, se encuentra ubicada a nivel Staff de la estructura orgánica de la Institución.
c) En la ejecución de sus funciones cuenta con Recursos Humanos (alta escolaridad), recursos materiales, financieros, tecnología informática (acceso Internet, correo electrónico).

1.2.3.2. Oportunidades

a) La Auditoría se organizará y funcionará conforme lo disponga el Auditor interno (art. 23 LGCI)
b) Participación en la evaluación, control y fiscalización de los proyectos de la Institución (actuales y futuros: JBIC, KFW, BID, etc.)
c) Instaurar en el Manual de Puestos de AyA, los perfiles del funcionario de la Auditoría Interna definidos por la Contraloría General de la República y adaptarlos al escalafón respectivo.
d) Presentación ante la Junta Directiva de los informes realizados por la Auditoría durante el mes, trimestre, semestre etc., para hacer del conocimiento los estudios en los diferentes períodos realizados.

1.2.3.3. Debilidades

a) La Auditoría Interna carece de un plan estratégico que oriente su accionar a mediano o largo plazo (3 a 5 años) en concordancia con el plan estratégico institucional (2003-2020), con el propósito de enfocar sus esfuerzos a los aspectos relevantes, que proporcionen un valor agregado a la Organización y que tome en cuenta la valoración del riesgo y sus objetivos.
b) Ausencia de un programa de valoración del riesgo, que permita identificar las áreas de mayor riesgo y las acciones de auditoría propicias a la evaluación respectiva.
c) Ausencia de un programa de aseguramiento de la calidad que le permita a este Órgano Fiscalizador mejorar los procesos y estudios a efectos de brindar un valor agregado en su gestión.
d) Ausencia de un programa de capacitación continua acorde con las nuevas y sanas prácticas de la auditoría, que contemple normas, directrices y metodologías de acatamiento obligatorio por las auditorías internas.
e) Existencia de reglamentos, manuales y procedimientos no actualizados con los últimos lineamientos, directrices y variaciones de la normativa aplicable a la administración y a las auditorías internas.
f) Ausencia de una base de datos integral y automatizada, de los diferentes estudios por área auditada.
g) Falta de políticas y procedimientos relativos al diseño, revisión, codificación, marcas, manejo, custodia y conservación de los papeles de trabajo (documentales, digitales u otro medio electrónico).

h) Falta de análisis y adecuada interpretación de la normativa vigente, en la aplicación de los diferentes estudios de auditoría.

i) Carencia de un código de ética aplicable a los funcionarios de la Auditoría Interna.

j) No se efectúa una evaluación del personal de acuerdo con su rendimiento que permita valorar elementos y definir aquellos temas en los que se debe dar énfasis en actividades de actualización y desarrollo profesional. Además, en lo que se requiera una supervisión personalizada.

k) Falta definición de las competencias (habilidades, aptitudes y conocimiento) requeridas para la selección y reclutamiento de candidatos idóneos para la Auditoria. Interna.

l) Inopia de profesionales especializados en temáticas de relevancia, en aspectos propios de la operación y mantenimiento de sistemas de agua y alcantarillado sanitario, que permitan efectuar evaluaciones técnicas. De igual forma inexistencia de conocimiento especializado para la tramitación de consultorías en estas áreas.

m) La evaluación de las Asociaciones Administradoras de Sistemas de Acueductos y Alcantarillados Comunales (ASADAS) es insuficiente, por cuanto ésta obedece a la atención de excesivas denuncias que no permiten una evaluación objetiva relacionado con el cumplimiento de la normativa vigente de parte de estas organizaciones.

n) Insuficientes computadores portátiles que permitan el desarrollo de las funciones atinentes a esta Unidad cuando se deben ejecutar estudios fuera de su sede.

o) El vehículo asignado al transporte de los funcionarios de esta auditoría para su gestión es insuficiente.

1.2.3.4. Amenazas

a) La percepción de la Junta Directiva, la Administración respecto a las funciones de la Auditoría Interna.
b) Falta de atención y compromiso por parte de la Administración Superior en relación con algunas recomendaciones emitidas en informes tanto de la Auditoría Interna como de otros Entes externos (CGR, ARESEP, Procuraduría, etc.).
c) Desatención de la Administración respecto al control que debe ejercer sobre las ASADAS (definición y aplicación de roles).
d) La gestión gerencial institucional es insuficiente. (deterioro institucional).
e) La falta de una planificación sustentada en la evaluación de riesgos y debidamente actualizada puede conllevar al desarrollo de estudios de poco impacto.

1.3 Aspectos Generales de la Dirección de Tecnologías de Información del Instituto Costarricense de Acueductos y Alcantarillados, (AyA).

1.3.1 Objetivos de la Dirección de Tecnologías de información del AyA.

La Dirección de Tecnologías de Información del Instituto Costarricense de Acueductos y Alcantarillados busca los siguientes objetivos:

a) Contar con un conjunto de soluciones innovadoras, basadas en tecnologías de información y telecomunicaciones, para apoyar una

efectiva y eficiente gestión institucional en los diferentes niveles del AYA.

b) Contar con una infraestructura de tecnologías de información y telecomunicaciones con alta seguridad y alta disponibilidad en función de los requerimientos técnicos de las soluciones que ésta soporta.
c) Incrementar la cultura informática organizacional en materia de tecnologías de información y telecomunicaciones, que promueva:
   - Su uso efectivo y eficiente.
   - La participación real en los proyectos asociados.
   - La identificación y el entendimiento de su potencial como un medio para mejorar la gestión institucional.
d) Consolidar la organización de Tecnologías de Información del AYA en un área orientada al servicio al cliente que permita altos niveles de desempeño.

1.3.2 Estructura de Dirección de Tecnologías de información del AyA.

Para desarrollar sus funciones básicas la Dirección de Tecnologías de Información del Instituto Costarricense de Acueductos y Alcantarillados, (AyA) se ha dividido en cuatro departamentos: Desarrollo Informático (Proyectos), Soporte, Sistemas (subdividido en Desarrollo y Mantenimiento) y Operación, asimismo cuenta con unidades de Gestión Desconcentradas para la atención de las regionales y cantonales en todo el territorio nacional. En los anexos se presenta un organigrama de la Dirección.

1.3.3 Análisis de la Dirección de Tecnologías de Información del AyA.

El siguiente análisis de diagnóstico, realizado mediante el uso de la técnica FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) en la Dirección de Tecnologías de Información es el resultado de un ejercicio minucioso, para la consecución del objetivo, fue necesaria la discusión y análisis con algunos miembros del equipo de TI. En este sentido la aplicación de esta técnica se realizó por parte de este funcionario de la Auditora Interna, con los siguientes resultados:

1.3.3.1 Fortalezas

Seguidamente se enumeran las fortalezas de TI que fueron identificadas por esta Auditoría Interna:

a) Reglamento Informático que establece la normativa para la adquisición y administración de los recursos informáticos de AYA (se entiende por recurso informático hardware, software y telecomunicaciones)
b) Personal técnicamente calificado en términos de hardware, software y telecomunicaciones actuales y de amplia trayectoria institucional.
c) Conocimiento funcional en materia de comercialización de aguas y finanzas-suministros en empresas de aguas, al haber participado en la implementación de las soluciones informáticas del Open-SGC y el SIFS.
d) Capacidad de reacción frente a imprevistos de acuerdo con las condiciones institucionales vigentes.
e) Administración, mejoramiento y mantenimiento de soluciones estratégicas de nivel institucional basadas en tecnología como lo son: Open SGC, SIFS, Internet y Correo Electrónico.

f) Compromiso aceptable de las áreas para cumplir el rol asignado y un clima organizacional adecuado.

1.3.3.2. Oportunidades

Entre las oportunidades que se reconocen se enumeran las siguientes:

a) Demanda creciente de servicios y soluciones basadas en tecnología informática dentro de la institución, aprovechando la plataforma actual de soluciones y la ejecución de nuevos proyectos.
b) Alta disponibilidad en el mercado de tecnología y soluciones basadas en tecnología para incrementar la eficiencia y efectividad de la Institución.
c) Iniciativas gubernamentales que fortalecen el desarrollo institucional en materia de tecnología informática.
d) Hacer uso de la contratación externa como mecanismo para:
e) Obtener conocimiento y experiencia en nuevas tecnologías y soluciones basadas en tecnología,
f) Para aumentar la productividad de servicios y soluciones basadas en tecnología y telecomunicaciones.
g) Tratado de libre comercio (Apertura de Telecomunicaciones).
h) Institucionalización de política de desconcentración.
i) Búsqueda de financiamiento externo para ejecutar proyectos estratégicos y de alto impacto en materia informática.
j) Los estudios en los diferentes periodos realizados.

1.3.3.3. Debilidades

Seguidamente se enumeran las debilidades que fueron identificadas por consenso:

a) No existe un proceso formal de Servicio al cliente ni procedimientos que aseguren el nivel de calidad esperado por los usuarios y las métricas necesarias para medirlo y evaluarlo.
b) Ausencia de un Plan de Capacitación formal y continuo para el personal técnico en la tecnología existente acorde con los avances tecnológicos y formas innovadoras de hacer negocios en la industria de aguas.
c) Carencia de planificación, acuerdos de nivel de servicio y control adecuados para asegurar el desempeño y los resultados de las contrataciones a terceros.
d) Ausencia de procedimientos formales y periódicos para comunicar resultados y logros de la unidad de Tecnologías de Información a la institución.
e) Débil estructura organizativa y técnica para gestionar las actividades de soporte técnico de forma desconcentrada.
f) Inadecuada preparación para la gestión de cambio promovido por la tecnología.
g) Ausencia de métricas para conocer el desempeño de toda la labor informática.
h) No existe una cultura a lo interno de la importancia del trabajo realizado y su impacto hacia el cliente de la unidad de Tecnologías de Información.
i) No hay imagen de liderazgo consolidada a nivel institucional en relación con la función que desempeña la unidad de Tecnologías de Información.

j) La demanda de soluciones informáticas basadas en tecnología dentro de la institución es superior a la capacidad de los recursos con que cuenta la unidad de Tecnologías de Información.
k) Las actividades operativas y de mantenimiento consumen el mayor porcentaje de la actividad productiva de la unidad de Tecnologías de Información.
l) No existe una estrategia de actualización sostenible en el tiempo de la plataforma tecnológica, que considere la actividad de investigación para la renovación tecnológica y nuevas formas de hacer negocios basadas en tecnología.
m) Falta de planificación de la función informática dentro de la Institución y una vinculación real a la planificación estratégica institucional.
n) Carencia de expertisia en aplicaciones informáticas y conocimiento funcional propios de la producción y comercialización de agua.
o) Falta de procedimientos administrativos internos en la unidad de Tecnologías de Información.
p) No existen lineamientos, normas y estándares referentes a la función informática.
q) Dificultad de trabajo en equipo entre las áreas de la unidad de Tecnologías de Información, que se refleja como decisiones unilaterales que pueden afectar el servicio institucional.
r) Presupuesto insuficiente y subejecución presupuestaria, para cumplir las necesidades y expectativas de los clientes.
s) Alta dependencia del personal en las funciones actuales, debido a la poca disponibilidad de éste.

1.3.3.4. Amenazas

Seguidamente se enumeran las amenazas que fueron identificadas:

a) Percepción negativa de las áreas usuarias sobre la labor de la unidad de Tecnología Informática.
b) Restricción del Gasto Público y recortes presupuestarios por disposiciones gubernamentales.
c) Falta cultura informática a nivel ejecutivo que facilite la ejecución de proyectos institucionales que impliquen grandes inversiones.
d) Cambios políticos que impactan la dirección estratégica en materia informática en diferentes ámbitos de su accionar.
e) Dificultad de disponibilidad de recursos y complejo trámite de contratación para la adopción, actualización y mantenimiento de las nuevas tecnologías y soluciones basadas en tecnología informática que el mercado pone a disposición para mejorar el desempeño y efectividad de la Institución.
f) Mala calidad y disponibilidad de servicios de entes externos que influyen en los servicios que brinda a nivel institucional la unidad de Tecnologías de Información (por ejemplo ICE, CNFL, Racsa).
g) Desarrollo de soluciones informáticas en otras instancias administrativas diferentes a la unidad de Tecnologías de Información, que no están alineadas a la estrategia institucional y de informática.
h) Oportunismo de los proveedores inadecuados para introducir tecnologías y soluciones en diferentes áreas de la Institución ante la falta de Plan Informático y el reconocimiento real de que la función informática es un eje estratégico y rector en esta materia.
i) Incertidumbre ante el proceso de reorganización a nivel institucional que se está dando.

1.4 Configuración computacional de AyA

El AyA cuenta con una plataforma tecnológica moderna y con capacidad de crecimiento en términos de hardware, software y telecomunicaciones, además de soluciones estratégicas de nivel institucional basadas en tecnología como lo son: Open SGC, SIFS, Internet y Correo Electrónico.

Solo en su sede central la configuración computacional de la red consta de los siguientes recursos de hardware: 25 servidores marca Fujitsu, Dell Son y Compaq, clasificados como se define seguidamente: 12 servidores de red, 9 servidores de bases de datos, 1 servidor de página Web, 2 servidores correo electrónico y 1 servidor de archivo.

Área de granja de servidores:

Servidor	Aplicación	Producto
Bases de datos	Sistema Operativo	UNIX-SOLARIS
Redes de área Local	Plataforma operativa	Windows 2000
Comunicaciones	Conexión de redes	TCP/IP otras
Antivirus	Utilitarios	Mcaffe
SW de creación de página Web	Programa	Html
Servidor de correo electrónico	e-mail	Microsoft Outlook

Sistemas operativos:

Cantidad	Sistema operativo	Usado en aplicación
17	Windows NT	Base Datos
8	Unix , Linux	Software y aplicaciones
1	Otros	

Bases de datos: Se utilizan Oracle, SQL, Sybase

Área de comunicaciones:

Se utiliza una red LAN, para efectos internos, la cual se encuentra enlazada con la red WAN a nivel nacional, integrando un total de 64 sucursales en todo el país, las que van aumentando con cada acueducto que asume la Institución o bien cuando por razones de política administrativa se crea una nueva Región u oficina. (Jacó, Orotina, Papagayo, Cartago, etc.)

Características del cableado de red:

Las líneas de comunicación operan a través de una combinación de red de cableado estructurado, sistema digital, conmutada, inalámbrico, de cobre y fibra óptica, todo de acuerdo con la disponibilidad, y las características propias de los lugares por comunicar.

Equipos de comunicación:

La Institución cuenta con 40 concentradores, 36 switches, 5 enrutadores, 2 firewalls (como equipos de seguridad para Internet) y 15 líneas Dedicadas con 1024 megabits de ancho de banda cada una).

Tipo de red utilizada:

Se utiliza una red LAN, para efectos internos, la cual se encuentra enlazada con la red WAN a nivel nacional, integrando un total de 64 sucursales en todo el país.

1.5 Situación de la Seguridad de las Tecnologías de Información en AyA.

1.5.1 Sistema de Seguridad Físico-Lógica.

La Institución cuenta con una serie de elementos de seguridad que van desde sistemas básicos como guardas de seguridad, identificación de personal, hasta elementos de alto grado de tecnología aplicada como el circuito cerrado de televisión, tarjetas de proximidad y dispositivos de identificación biométrica.

1.5.1.1 Seguridad Física.

Los principales mecanismos de seguridad física utilizados son los siguientes:

a) Tarjetas de Proximidad: Es un mecanismo en desarrollo que funciona con tarjetas, que se presentan a los dispositivos para abrir puertas y será asignado a los funcionarios de acuerdo con sus funciones
b) Circuito Cerrado: Funciona con cámara y grabaciones que se soportan en un sistema de identificación el cual se respalda al igual que el resto de la información diaria

c) Identificador biométrico. Mecanismo cuya aplicación es mediante la mano y una clave que se digita, es únicamente en el centro de cómputo para los encargados de éste que están autorizados para su uso
d) También cuenta con una serie de mecanismos de seguridad como lo es un sistema de alarma contra Incendio, sistema detector de humo y sistema de extinción de incendios que funciona con base en gas

1.5.1.2 Seguridad Lógica

a) Se utiliza un sistema por medio de dos Firewalls que funcionan por medio de Hardware.
b) También se utilizan mecanismos IDS identificación de proximidad, especial de Código y password, de software, antivirus de Macaffe, como el Stinger, Antivirus de Microsof mecanismos de filtrado de contenido y sistema de password para los usuarios, el cual debe ser actualizado cada 3 meses previa solicitud del sistema.

CAPÍTULO 2

Capítulo II: Herramientas Teóricas de Auditoría y Tecnologías de Información.

2.1 Algunas definiciones y conceptos para el desarrollo del proyecto.

2.1.1 Términos y definiciones de auditoría.

Administración de riesgos: Gestión que se efectúa para limitar y reducir el riesgo asociado con todas las actividades de la organización en diferentes niveles. Incluye actividades que identifican, miden, valoran, limitan y reducen el riesgo. De esas actividades, el control interno contempla la identificación y la valoración de los riesgos. (Manual CI) / Proceso de identificación, valoración y ejecución de acciones para enfrentar los riesgos. (SEVRI) / La aplicación sistémica de las políticas, procedimientos y prácticas administrativas relacionadas con las tareas de identificar, analizar, valorar, tratar, vigilar y comunicar sobre aspectos de riesgo. / Proceso para identificar, controlar y minimizar o eliminar, a un costo razonable, los riesgos de seguridad que puedan afectar los sistemas de información.

Ambiente de control: Uno de los cinco componentes funcionales del control interno. Comprende el conjunto de factores del ambiente organizacional que el jerarca, los titulares subordinados y demás funcionarios deben establecer y mantener, para permitir el desarrollo de una actitud positiva y de apoyo para el control interno y para una administración escrupulosa del patrimonio público.

Ambiente de Control: Proceso que le permite al auditor independiente conocer los controles que ha implantado la gerencia, en los que se refiere a la existencia de sistemas, personal competente para operarlos y documentación en que consten las operaciones:

> "Representa el efecto colectivo de varios factores en establecer, realizar o mitigar la efectividad de procedimientos y políticas específicos, tales como filosofía y estilo de operación gerencia, estructura organizacional, métodos de control administrativo e influencias externas".

Cuando el auditor se entrevista con el área administrativa (gerente y mandos medios) obtiene compresión de las actitudes, capacidades, percepciones y acciones del personal de una empresa, especialmente por su dirección, el cual debe considerarse al planear el alcance de su trabajo.

Amenaza: Factor físico o lógico capaz de producir daños.

Análisis de riesgos: Proceso de determinar el nivel de riesgo a partir de la posibilidad y consecuencia de los eventos identificados.

Auditoría: Análisis de un componente o proceso organizacional para medir el cumplimiento de criterios establecidos o la efectividad y eficiencia de las operaciones.

Auditoría interna: Uno de los dos componentes orgánicos del sistema de control interno. Es la actividad independiente, objetiva, asesora y que proporciona seguridad al ente u órgano, que se crea para agregar valor y

mejorar sus operaciones. Contribuye a que se alcancen los objetivos institucionales mediante la práctica de un enfoque sistémico y profesional para evaluar y mejorar la efectividad de la administración del riesgo, del control y de los procesos de dirección en las instituciones y órganos. Debe proporcionar a la ciudadanía una garantía razonable de que la actuación del jerarca y demás servidores de la Institución se realiza con apego a sanas prácticas y al marco jurídico y técnico aplicable.

Carta a la gerencia: Philip L. Defliese, define la carta a la gerencia o carta de observaciones como:

> "Un documento con un enfoque constructivo de las fallas y problemas y de cooperación para explorar posibles soluciones que contribuyen al fortalecimiento de la empresa y al mejoramiento de sus operaciones".[3]

Contenido de la Carta de Gerencia: De acuerdo con las declaraciones sobre normas de auditoria:

> "El informe de contador que expresa una opinión sobre el sistema de control interno contable de la entidad debe contener:
>
> - Una descripción del alcance de trabajo.
> - La fecha a la cual se refiere la opinión.
> - Una declaración de que el establecimiento y mantenimiento del sistema es responsabilidad de la administración.
> - Una breve explicación de los objetivos generales y las limitaciones inherentes al control interno contable.
> - La opinión del contador sobre el sistema tomado en conjunto fue suficiente para alcanzar los objetivos generales de control

[3] Defliese y otros. (1991), p.72

interno contable en la medida que esos objetivos permiten la prevención o detección de errores o irregularidades en cantidades que podrían ser importantes..."

Luego de evaluar la estructura de control interno el auditor debe preparar un documento en el que incluya las observaciones de los controles establecidos y las recomendaciones que considere necesarias para fortalecer dichos procedimientos. Además se acostumbra revisar el contenido de la carta con la gerencia antes de que el documento quede terminado.

Conocimiento del cliente: Son todo el procedimiento utilizados por el auditor independiente para obtener información de carácter general relativa al cliente y sus operaciones en la amplitud y profundidad requeridas para lograr una relación ideal. En la auditoría de Montgomery se define como:

"Obtener (o actualizar) y documentar información y considerar la manera en que esa información puede afectar la estrategia de auditoria"[4]

El auditor independiente efectúa una visita preliminar con el objeto de conocer los planes, políticas y prácticas del negocio para establecer claramente el alcance de la auditoría. Se realiza un recorrido por la planta y las oficinas para obtener un juicio inicial acerca de los sistemas de control, además realiza una lectura y extracto de actas y acuerdos para conocer los acuerdos más importantes relacionados con el área por auditar.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizacionales concebidas para brindar una garantía razonable de que los

[4] Defliese y otros, (1991), p.206

objetivos de negocios se lograrán y que los eventos no deseados se impedirán o detectarán y corregirán.

Control interno: También denominado "sistema de control interno". Comprende la serie de acciones diseñadas y ejecutadas por la administración activa para proporcionar una seguridad razonable en torno a la consecución de los objetivos de la organización, fundamentalmente en las siguientes categorías: a) proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal; b) confiabilidad y oportunidad de la información; c) eficiencia y eficacia de las operaciones; y d) cumplir con el ordenamiento jurídico y técnico.

De acuerdo con las Normas y Procedimientos de Auditoria del Instituto Mexicano de Contadores Públicos:

> "El sistema de control interno de una entidad consiste en las políticas y procedimiento establecidos para proporcionar una seguridad razonable de poder lograr los objetivos específicos de la entidad "[5]

Como lo afirman Defliese y otros:

> "El control interno comprende el plan de organización, los procedimientos y registros que se relacionan con la protección de los activos y la confiabilidad de los registros financieros"[6]

---

[5] Instituto Mexicano de Contadores Públicos A.C. Normas y Procedimientos de Auditoria. México, 1995

[6] P. Defliese, K. Jonson R. Macleod. Auditoria Montgomery. México: Prentice-Hall Hispanoamericana S.A. 1991, p.268

Criterios: Los criterios son normas razonables contra las cuales los controles, ya sean, financieros, administrativos o los sistemas de información pueden ser evaluados[7].

Son políticas o lineamientos generales dictados por una autoridad superior, que tienen como propósito orientar la acción, en este caso, de la seguridad de los sistemas de información computadorizados como componentes, para el cumplimiento de los objetivos y metas de una organización. Las políticas que se dicten deberán ser documentadas y divulgadas en los niveles pertinentes de la organización y objeto de actualización permanente.

Los objetivos, metas y acciones constituyen los criterios orientadores para dirigir el desarrollo informático y su administración en todos sus aspectos, los cuales deberán ser concordantes y derivados de los objetivos, estrategias y metas organizacionales.

Estructura Organizacional: Según James A.F. Stoner y Charles Wankel:

"La estructura de una organización especifica su división de las actividades y muestra como están relacionadas las diferentes funciones o actividades; en cierta medida también muestra el grado de especialización del trabajo. Indica además su estructura jerárquica y de autoridad así como sus relaciones de subordinación"[8]

---

[7] Curso Proceso de Auditoría de TI/SI, UCR, Maestría en Auditoría de Tecnologías de Información

[8] Stoner James A: Charles Wankel. Administración. 3º ed. México: Prentice-Hall Hispanoamericana S.A., 1989. p.25

En la visita preliminar que le auditor independiente solicita el organigrama de la entidad, así como cualquier otra información como la centralización y descentralización de la toma de decisiones, el tamaño de la unidad de trabajo y coordinación de las actividades, además, se informa sobre el funcionamiento de los niveles “staff” dentro de la organización de la empresa.

Evento: Incidente o situación, que ocurre en un lugar específico en un intervalo de tiempo particular.

Evaluación de riesgos: Proceso de determinar las prioridades para la administración de riesgos.

Factores críticos de éxito: Hechos que inciden directamente en los procesos y en el logro de los objetivos organizacionales. Constituyen guías que permiten identificar las acciones más relevantes que deben acometerse en términos estratégicos, técnicos, organizacionales o procesales.

FODA: Herramienta de análisis situacional que facilita la determinación de las fortalezas, oportunidades, debilidades y amenazas que experimenta una entidad en el tiempo y espacio.

Gestión de calidad: Proceso gerencial para lograr el mejoramiento continuo de todo lo relacionado con la organización. Se asocia también con los requerimientos de las normas ISO.

Hallazgos: Los hallazgos en una carta de gerencia, están construidos por todas aquellas deficiencias de control de interno que satisfacen los limites de importancia relativa, así como las deficiencias de controles administrativos y controles contables internos; sin embargo, según Defliese, Jaenicke, Sullivan y Gnospeluis:

> "Los auditores deben ampliar esa comunicación a fin de incluir las deficiencias que satisfagan los limites de importación relativa"[9]

Durante la evaluación de la estructura de control interno, el auditor detecta debilidades reportables y debilidades no reportables, las cuales analiza junto con la gerencia de la empresa antes de emitir el documento o carta final de gerencia**.** En lo personal prefiero llamarlos "Oportunidades de Mejora, especialmente al exponerlos al auditado.

Identificación de riesgos: Proceso de determinar los eventos que pueden afectar los objetivos propuestos, sus causas, formas de ocurrencia, oportunidad y posibles consecuencias.

Impacto: Consecuencia o producto de la ocurrencia de un evento expresado cualitativa o cuantitativamente, sea una pérdida, perjuicio, desventaja o el desaprovechamiento de una ganancia o un ahorro.

Implementación: Etapa del proceso de construcción de sistemas de información que comprende la adquisición de hardware y software, el desarrollo de software, la prueba de programas y procedimientos, el desarrollo de la

[9] Defliese. Op Cit. p.65

documentación y una variedad de actividades de instalación, así como la educación y capacitación de usuarios finales y especialistas que operarán el nuevo sistema.

Informe de auditores independientes: El auditor independiente debe dirigir el informe a la compañía bajo auditoría, al consejo de administración, a sus accionistas o bien a una combinación de los tres. Si bien el informe llamado dictamen ha sido una práctica seguida únicamente en la Auditoría de Estados Financieros, y al respecto solo se habla de dictamen del auditor de estados financieros, el auditor de sistemas una vez que el auditor ha terminado su examen y con su juicio profesional determina la clase de opinión que expresa y prepara el dictamen.

Nivel de riesgo: Medida que se determina al combinar la probabilidad de ocurrencia de un evento y su consecuencia potencial sobre el cumplimiento de los objetivos propuestos.

Nivel de riesgo aceptable: El nivel de riesgo que la institución está dispuesta y en capacidad de asumir para poder cumplir con sus objetivos sin incurrir en costos excesivos en relación con sus beneficios, inhibir el aprovechamiento de oportunidades o ser incompatible con las expectativas de los sujetos interesados.

Monitoreo: Uno de los cinco componentes funcionales del sistema de control interno. Incluye las actividades que se realizan para valorar la calidad del funcionamiento del sistema de control interno —y, por ende, el logro de los

objetivos institucionales— a través del tiempo, y asegurar que el sistema pueda reaccionar de manera dinámica según requieran las condiciones imperantes y, más específicamente, la evolución del riesgo.

Procedimiento de Control de Interno: Definido de manera clara, sencilla y contundente los procedimientos de Control Interno como:

> "Aquellos procedimientos y políticos adicionales al ambiente de control y el sistema contable, establecidos por la gerencia para proporcionar una seguridad razonable de poder lograr los objetivos específicos de la entidad."

Durante el desarrollo de la evaluación de control interno, el auditor debe solicitar información sobre la autorización de las transacciones y actividades, segregación de funciones, diseño y uso de documentos y registros, así como los dispositivos de seguridad.

Programas de auditoría: Es una lista detallada de los pasos por seguir en el curso de un examen de Auditoría, indica su naturaleza y extensión ayuda, a distribuir y determinar la oportunidad de trabajo, evita omisiones y duplicaciones y muestra el trabajo que se ha hecho cuando se usa para ese tipo de control. Es necesario para ejercer una adecuada planeación y supervisión del trabajo. Según el texto Auditoria de Montgomery, los programas son procedimientos de auditoria que se organizan:

> "En tal forma que permita la aplicación eficiente de los procedimientos señalados. Mas específicamente se debe organizar de manera que, cuando se examine un documento determinado, se le apliquen tantos procedimientos de auditoria como sea posible.[10]

[10] Defliese y otros. Auditoria de Montgomery. 2º Edición México: Editorial LIMUSA, 1991, p-254

Los programas de auditoria son instrumentos utilizados por el auditor que contienen pruebas analíticas y sustantivas que le permiten obtener una seguridad razonable de su estudio.

2.1.2 Términos y definiciones de Tecnología de Información.

Adquisición e implementación: Para realizar la estrategia de TI, deben identificarse, desarrollarse o adquirirse soluciones de TI y luego implementarse e integrarse en el proceso de la organización. La adquisición e implementación abarcan los cambios y el mantenimiento de los sistemas existentes para garantizar que el ciclo de vida perdure para estos sistemas.

Arquitectura: Diseño de los componentes del software y de hardware, es el conjunto integrado de recursos de TI: instalaciones, hardware, software y tecnología de comunicaciones.

Auditoría de Servicios de Información: Es una instancia que se crea o se separa a partir del personal de auditoría interna de la empresa (en los casos en que exista todo un departamento como tal). Normalmente en algunas organizaciones no existe una estructura operativa muy grande, ni una clara división de funciones, razón por la que la estructura no refleja el área de TI, menos aún un nivel jerárquico acorde con las aspiraciones de los estándares, por la razón de que dichos estándares les afecta la estructura y les impacta en los costos.

Ambiente de desarrollo: Conjunto de componentes de hardware y software donde se efectúan los procesos de construcción, mantenimiento (v.gr. ajustes, cambios y correcciones) y pruebas de sistemas de información.

Base de datos: Colección de datos almacenados en un computador, los cuales pueden ser accedidos de diversas formas para apoyar los sistemas de información de la organización.

Bitácora: Registro manual o automatizado de los diversos eventos producidos por los componentes de un sistema de información**.**

Canales seguros de comunicación: Conducto físico o lógico que incorpora criterios para garantizar la seguridad de la transmisión de datos.

Comité de riesgos de tecnología de información: El comité de riesgos de TI es una instancia especializada y de alto dominio del tema que normalmente esta constituida por personal remunerado de la organización (la gerencia general, el gerente de servicios de información y el gerente financiero), dedicado a la gestión de la norma (o sea los riesgos) y la rendición de cuentas ante terceros, con sanciones claramente expresas si se da la circunstancia de que fallen. En algunos casos es también llamado comité de sistemas.

Comité gerencial de informática: Comité gerencial de informática El Comité Gerencial de Informática constituye la instancia técnica entre el máximo jerarca y la Unidad de Informática, que brinda una asesoría al primero en lo relativo a la administración de TI y de los recursos humanos, materiales y financieros que se destinen para su desarrollo. Le corresponde asesorar al nivel jerárquico superior en cuanto a la gestión de las TI. Se conformará por acuerdo del máximo jerarca, unipersonal o colegiado, y estará presidido por un representante de éste. Usualmente lo integran, además, un representante de las unidades de Planificación Institucional, Financiera e Informática (como secretaría técnica), así como representantes de las unidades usuarias. Eventualmente el Comité podrá convocar a otros representantes de otras unidades, en consideración de los asuntos por tratar.

Contingencia: Riesgo relacionado con la continuidad de los servicios y operaciones.

Continuidad de los servicios: Prevención, mitigación y recuperación de las interrupciones operacionales.

Contraseñas "password": Palabra clave necesaria para tener acceso a un servicio u opción. / Código secreto utilizado para verificar la identidad de una persona y que en general es requerida antes de que ésta utilice un sistema de cómputo. / Hilera de caracteres protegidos, generalmente encriptados por computadora que autentican a un usuario ante el sistema de información.

Conversión: Proceso mediante el cual se cambia el formato de los datos.

Cuentas de usuario: Recurso lógico para facilitar el control de acceso a un sistema computadorizado.

Datos: Objetos en su sentido más amplio (es decir, internos y externos), estructurados y no estructurados, gráficos, sonido, entre otros.

DBA (Data Base Administrator): Persona responsable de la administración de las bases de datos.

Escalamiento: Se refiere a la forma en que el hardware o software se pueden adaptar ante demandas crecientes.

Firewall: Tecnología de software y hardware diseñada para proteger la información almacenada en cualquiera de los componentes tecnológicos de una organización. Usualmente el *firewall* está compuesto por elementos físicos de control de acceso a servicios y puertos de un servidor, sensores de detección de intrusos, tecnología de acceso encriptado a servidores, programas de control de virus informáticos, *firewalls* personales instalados en las estaciones de trabajo, etc.

Firma: Traducción del inglés “signature”. Añadido en un mensaje de correo electrónico o en un mensaje enviado por Internet, que indica quién ha enviado el mensaje y desde dónde.

Firma digital: Una pieza de información, en una forma de firma digitalizada que provee al remitente autenticidad, integridad de mensaje y no rechazo. Una firma digital es generada usando la clave privada del remitente o aplicando una función “*hash*”en un solo sentido.

Función de TI o Función informática: Conjunto de componentes organizacionales y de procesos informáticos que apoyan la gestión organizacional.

Gerencia de servicios de información: La gerencia de servicios de información aparece como la culminación o maduración en una organización de los servicios de información. Se supone que el área de TI debe tener el rango suficiente para evolucionar de manera adecuada, tanto en lo operativo como en lo estratégico, contando con presupuestos adecuados y con una adecuada inserción en las actividades.

Se aspira con la definición de la gerencia de información a que se modifiquen los patrones tradicionales de gestión de la organización que le dan o daban un espacio altamente protagónico a las finanzas, las operaciones y el mercadeo versus un espacio más que secundario a las tecnologías de información.

Gobernabilidad de TI Conjunto de acciones fundamentadas en políticas institucionales que, de una manera global, intentan dirigir la gestión de las TI hacia el logro de los objetivos de la organización. Para ello se procura, en principio, la alineación entre los objetivos de TI y los de la organización, el balance óptimo entre las necesidades de TI de la organización y las oportunidades que sobre ello existen, la maximización de los beneficios y el uso responsable de los recursos, la administración adecuada de los riesgos y el valor agregado en la implementación de dichas TI. Tales acciones se relacionan con los procesos (planificación y organización, adquisición e implementación, entrega y soporte, y seguimiento), y recursos (personas, sistemas, tecnologías, instalaciones y datos) tecnológicos, y con el logro de los criterios fiduciarios, de calidad y de seguridad de la información.

Hardware: Todos los componentes electrónicos, eléctricos y mecánicos que integran una computadora, en oposición a los programas que se escriben para ella y la controlan (software).

Indicadores de desempeño: Constituyen medidas para determinar cuán satisfactorio es el desempeño de un proceso de TI en permitir que se logre la meta. Son indicadores de la probabilidad de que se alcance la meta, y son buenos indicadores de las capacidades, prácticas y habilidades.

Información: Conjunto de datos que han sido capturados y procesados por una computadora, que se encuentran organizados y que tienen el potencial de confirmar o cambiar el entendimiento sobre algo**.**

Información y comunicación: Uno de los cinco componentes funcionales del sistema de control interno. Se refiere al proceso mediante el cual la administración activa, identifica, registra y comunica en la forma, el tiempo y las condiciones precisas, la información financiera, administrativa o de otra naturaleza, relacionada con actividades y eventos internos y externos relevantes para la organización y para otras instancias interesadas.

Infraestructura tecnológica: Conjunto de componentes de hardware e instalaciones en los que se soportan los sistemas de información de la organización.

Internet: Apócope de International Net. Red internacional que conecta miles de redes enlazadas y que utiliza el grupo de protocolos TCP/IP, y que constituye la red de información más grande del mundo gracias a la inmensa maraña de computadores y redes a los que el usuario puede tener acceso.

Intranet: Red basada en el protocolo TCP/IP desarrollado para Internet, que pertenece a una organización y que es accesible solamente por empleados o miembros de la organización debidamente autorizados.

Librería de medios: Se refiere al lugar donde se ubican y custodian los dispositivos de almacenamiento de datos.

Licenciamiento: Proceso mediante el cual la organización se abastece de las autorizaciones o licencias de software necesarias para hacer un uso legal del software sujeto a derechos de autor y otros cargos.

Pistas de auditoría: Información que se registra como parte de la ejecución de una aplicación o sistema de información y que puede ser utilizada posteriormente para detectar incidencias o fallos. Esta información puede estar constituida por atributos como: la fecha de creación, última modificación o eliminación de un registro, los datos del responsable de dichos cambios o cualquier otro dato relevante que permita dar seguimiento a las transacciones u operaciones efectuadas.

Plan de contingencia, Plan de recuperación para casos de desastre Plan de continuidad de TI: Documento que contiene en forma ordenada y coherente las acciones que se ejecutarán, y los responsables de dicha ejecución, para dar continuidad a los objetivos de la entidad en caso de que se produzca un riesgo o evento que interrumpa los procesos o sistemas de la organización.

Plan estratégico de TI (PETI): Documento que contiene los aspectos fundamentales para orientar la gestión de las TI en la organización, entre ellos: marco estratégico, visión, misión, objetivos estratégicos, modelo de información e infraestructura tecnológica, cartera de proyectos, lineamientos sobre gestión de riesgos y calidad y otros de orden general. Dicho documento es el producto de un proceso de planificación estratégica.

Plataforma tecnológica: Término que resume los componentes de hardware y software (software de base, utilitarios y software de aplicación) utilizados en la organización. Refiérase a “recursos informáticos”.

Proceso: Conjunto de las fases sucesivas de una operación.

Programa fuente: Instrucciones de un programa en su estado original o código fuente. Para procesar un programa fuente se debe compilar su contenido para que se convierta en código de máquina (v.gr código objeto).

Recursos informáticos: Personas, sistemas de aplicación, tecnología, instalaciones y datos de una organización.

Riesgo: Probabilidad de que un factor, acontecimiento o acción sea de origen interno o externo, afecte de manera adversa a la organización, área, proyecto o programa y perjudique el logro de sus objetivos. Contingencia de que suceda un evento que tendrá consecuencias sobre el cumplimiento de los objetivos propuestos.

Servicios prestados por terceros, Outsourcing: Servicios recibidos de una empresa externa a la organización. Por lo general, requiere de una contraparte interna de la organización que garantice que el producto desarrollado cumple con los estándares establecidos por ésta.

Software: Los programas y documentación que los soporta que permiten y que facilitan el uso de la computadora. El software controla la operación del hardware.

Software de aplicación: Programa de computadora con el que se automatiza un proceso de la organización y que principalmente está diseñado para usuarios finales.

Software de base (software del sistema): Colección de programas de computadora usados en el diseño, procesamiento y control de todas las aplicaciones, los programas y rutinas de procesamiento que controlan el hardware de computadora. Incluye el sistema operativo y los programas utilitarios.

Soporte técnico para microcomputadoras: Actividades de apoyo para las operaciones realizadas en ambiente de microcomputadores.

Tecnología: Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico. La tecnología, para efectos de este documento, se refiere al hardware, los sistemas operativos, los sistemas de administración de bases de datos, las redes, los multimedios y el software de aplicación, entre otros.

Tecnologías de información (TI): Conjunto de tecnologías dedicadas al manejo de la información organizacional.

2.1.3 Términos y definiciones de Seguridad en Tecnología de Información.

Acceso privilegiado: El acceso a un sistema operativo mediante un código de usuario y una contraseña secreta podrá tener diferentes niveles, según el usuario con que se ingresa al sistema. Existen accesos conocidos como privilegiados o “superusuarios”, los cuales prácticamente poseen el derecho absoluto sobre los recursos internos del sistema. El manejo adecuado de estos usuarios es de suma importancia en el campo de la seguridad tecnológica.

Cifrado: Proceso mediante el cual se aplica un algoritmo determinado a un grupo de datos, y su contenido queda almacenado en forma ininteligible, a no ser que se aplique el proceso de descifrar. / La codificación de la información de acuerdo con reglas predefinidas de tal forma que no pueda ser comprendida sin el conocimiento de tales reglas.

Seguridad: Conjunto de controles para promover la confidencialidad, integridad y disponibilidad de la información.

Seguridad física: Protección física del hardware, software, instalaciones y personal relacionado con los sistemas de información.

Seguridad razonable: Concepto de que el control interno, sin importar cuán bien esté diseñado y sea operado, no puede garantizar que una institución alcance sus objetivos, en virtud de las limitaciones inherentes a todos los sistemas de control interno, tales como los errores de juicio, las limitaciones de recursos, la necesidad de considerar el costo de los controles frente a sus beneficios potenciales, la eventualidad de violaciones del control, la posibilidad de colusión y de infracciones por parte de la administración, y el impacto de otras actuaciones que no son elementos del control interno, entre otros, la determinación de la misión, visión e ideas rectoras.

Seguridad de correo electrónico: Garantía de que un mensaje de correo electrónico no ha sido visto o alterado por personas no autorizadas, de que ha sido efectivamente recibido y que su origen es cierto.

Software malicioso: Programas que atentan contra la integridad de los sistemas de información.

Virus: Programas maliciosos diseñados para diseminarse y replicarse de una computadora a otra a través de enlaces de telecomunicaciones o al compartir información o medios de almacenamiento de información.

Vulnerabilidad: Problema de seguridad debidamente documentado, relacionado con algún componente (hardware o software) de los sistemas informáticos. Se utiliza por terceras personas para dañar los sistemas

Definición de Seguridad de las Tecnologías de Sistemas: Se considera la seguridad informática como aquella “característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos de que dicha información cumpla criterios de confidencialidad, integridad y disponibilidad”. La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica.

Seguridad Física: Está asociada con procedimientos para el desarrollo de infraestructura y acceso a los centros de cómputo y comunicaciones. La seguridad física a su vez tiene que ver con la continuidad de los procesos y servicios, y con el reestablecimiento de éstos cuando por factores internos o externos los mismos han sido suspendidos.

La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

Seguridad Lógica y acceso a los datos: Considera el sistema de seguridad para la confiabilidad de los datos, proceso de otorgamiento de claves de usuarios, los estándares de acceso a la red, controles para evitar el ingreso externo (paredes de fuego) y la regulación del uso de software no autorizado y el correo electrónico.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información. Además, se consideran procesos para la puesta en marcha de programas y aplicaciones y las medidas para la separación de las áreas de desarrollo de las de producción.

CAPÍTULO 3

Capítulo III: Análisis de la Situación Actual de la Seguridad de tecnologías de información en el AyA.

3.1 Planeación de la Auditoría.

Esta fase lo que busca es definir las estrategias por seguir durante el trabajo, mediante una guía elaborada que logre culminar con la Auditoría propuesta, un ejemplo de este documento se puede apreciar en el Anexo Nº 2 donde se ubica el paln de Auditoria de este proyecto.

Con este plan se inicia el proceso evaluativo de la unidad en estudio, proceso que se dividirá en las siguientes cuatro fases:

a. **Planificación Preliminar:** Incluye las siguientes actividades:
   - Un conocimiento de la entidad con énfasis en la seguridad de las tecnologías y sistemas de información.
   - Identificación y selección de las áreas de seguridad que constituyen elementos significativos de TI, con base en criterios preestablecidos.
   - Elaborar un Programa de Planificación Detallada.

b. **Planificación Detallada:** Involucra entre sus actividades:
   - Llevar a cabo la indagación de las áreas de TI sensibles, para el planeamiento detallado de la auditoría;
   - Identificar las áreas de potencial importancia o factores críticos de éxito (FCE) para la seguridad de TI.

- Preparar un plan de Auditoría con los proyectos de auditoría.

c. Examen o Verificación: Consta de las siguientes actividades:

- Preparar detalladamente los programas de auditoría para examinar las áreas de seguridad de potencial importancia.
- Conducir las pruebas de auditoría y obtener de la evidencia de auditoría.
- Desarrollar hallazgos de auditoría.
- Preparar el borrador de informe.

d. Comunicación de Resultados: Consiste en la realización de las siguientes actividades:

- Discutir el informe con la administración para obtener su reacción.
- Realizar correcciones, ajustes e incluir la reacción de la administración.
- Informar al nivel correspondiente.

3.1.1 Origen de Estudio.

Este proyecto se origina en la necesidad de realizar una práctica profesional como requisito de graduación para optar al grado de Magíster en Administración y Dirección de Empresas con énfasis en Auditoría de Tecnologías y Sistemas de Información.

3.1.2 Área a Auditar.

El estudio se realiza en la sede Central del Instituto Costarricense de Acueductos y Alcantarillados, ubicada en Rohomoser, Pavas, San José; particularmente en el Centro de Computo de la Dirección de Tecnologías de Información del AyA.

3.1.3 Alcance.

El estudio considera lo relativo a la seguridad física y lógica de Tecnologías de Información y Comunicación del Instituto Costarricense de Acueductos y Alcantarillados. La parte de seguridad física se evalúa en diferentes sectores de toda la sede, mientras que en lo que respecta a la seguridad lógica el análisis se realiza propiamente en el centro de cómputo. La revisión se desarrolla en el primer trimestre del 2007 y se avoca a una revisión de la misma con fecha de corte al 30 de marzo del 2007; en conformidad con lo establecido en el "Manual sobre normas técnicas de control interno relativas a los sistemas de información computadorizados", emitido por la Contraloría General de la República y que actualmente se encuentra en una etapa de actualización.

Estas normas se complementan con las mejores prácticas de aplicación en materia de seguridad de tecnología de información y comunicación, emitidas por algunas organizaciones internacionales que se han especializado en esa materia, tales como la Asociación de Auditoría y Control de Sistemas de Información (ISACA por sus siglas en inglés), con su documento "Objetivos de control para la información y tecnologías relacionadas" (COBIT por su acrónimo en inglés), así como las normas ISO-17799:2000, relativa a seguridad, y la ISO-9001:2000, sobre gestión de calidad, ambas emitidas por la International Organization for Standarization (ISO).

Algunos rubros de estas normativas no se aplicarían por diversas razones, como por ejemplo:

- Tamaño de la organización.
- Restricciones de acceso a la información.
- Por no pertinencia de acuerdo con la labor que ejecuta el Instituto.
- Por disponibilidad de horarios.
- Por estar en proceso la implementación de nuevos sistemas.
- Por cláusulas de confidencialidad en ciertos contratos.

3.1.4 Objetivos.

3.1.4.1 Objetivo General

Evaluar la Seguridad de las Tecnologías de Información en el Centro de Informática del Instituto Costarricense de Acueductos y Alcantarillados, para comprobar la existencia y cumplimiento de procedimientos y políticas organizacionales que sirvan de apoyo a las prácticas de seguridad física y lógica relacionadas con los sistemas de información en conformidad con la normativa vigente.

3.1.4.2 Objetivos Específicos

a) Determinar la situación actual de la Administración de la Seguridad de las tecnologías de Información en el Centro de Informática del Instituto Costarricense de Acueductos y Alcantarillados con el propósito de valorar aspectos claves que permitan determinar la criticidad del área.

b) Comprobar si la Administración del AyA formula y mantiene políticas de seguridad razonables para los sistemas de información, al verificar las políticas relacionadas con los controles de acceso, de autorización y la difusión que se manejan.

c) Verificar la pertinencia del mantenimiento de la seguridad física de las instalaciones de la Sede del Instituto.

d) Revisar si existe una adecuada administración de los incidentes y anomalías en materia de seguridad de los sistemas de información.

e) Indagar si la organización cuenta con un plan de continuidad de los negocios, que contemple la reducción de riesgos y consecuencias de los incidentes perjudiciales.

f) Obtener mediante los resultados del trabajo de auditoría las conclusiones y brindar las recomendaciones pertinentes.

3.1.5 Marco Legal.

Para realizar las actividades y diseñar los papeles de trabajo se tomó como marco de referencia las siguientes normativas:

- "Manual sobre normas técnicas de control interno relativas a los sistemas de información computadorizados", emitido por la Contraloría General de la República y que actualmente se encuentra en una etapa de actualización.
- Norma ISO 17799.

- Norma BS 7799 : 2002.
- Políticas Institucionales.
- Ley General de Control Interno No 8292.
- Reglamento de Normas y Políticas de Informática Decreto Ejecutivo No 28921-SP.
- Manual de Normas Generales de Control Interno Computadorizados.

3.1.6 Recursos Requeridos.

3.1.6.1 Personal:

Para la ejecución del estudio se requiere contar con los servicios profesionales de los siguientes funcionarios:

Coordinador: Lic. Alcides Vargas Pacheco

Auditor de Sistemas: Lic. Óscar Gerardo Guzmán Aguilar

3.1.6.2 Materiales:

Se requiere la utilización de recursos propios asignados a la Auditoría Interna del Instituto Costarricense de Acueductos y Alcantarillados, lo cual implica material de oficina, carpeta, fotocopias y uso de equipo de cómputo como Pc`s, servidores y scaners. Se utilizará también recursos personales del auditor de sistemas como lo son su cámara digital, la de video, su computador portátil y otros.

3.1.6.3 Tiempo estimado:

La elaboración de un cronograma que sirve como referencia para valorar los avances del trabajo, así como para medir constantemente el tiempo estimado inicialmente para cumplir los objetivos. El cronograma brinda el esquema general de tiempos por emplear en cada una de las partes de la auditoría. Ya se tenía un cronograma para el proyecto total según el documento escrito, requisito indispensable para el cumplimiento del origen mencionado en el respectivo aparte, y para cubrir los objetivos, tanto general como específicos propuestos, el trabajo por desarrollar, propiamente la auditoría, con la aplicación de ejercicios y técnicas de Auditoría, así como el confrontar la situación actual de la seguridad de las tecnologías de AyA con lo establecido por la contraloría General de la República y la normativa vigente; asimismo con los que dictan los estándares internacionales de seguridad mediante la evaluación en la que se aplican los cuestionarios, guías de trabajo, listas de verificación y demás papeles de trabajo, que se necesiten para documentar el ejercicio, se estima el siguiente dato de horas de trabajo:

1 Auditor de sistemas	400 horas
1 Supervisor	50 horas
TOTAL	450 horas.

3.2 Análisis de Riesgos

El análisis de riesgos realizado para la determinación de esta auditoría fue un ejercicio muy subjetivo, fue un tema que le interesó evaluar al redactor de este trabajo, en otras palabras, no fue analizado bajo ningún criterio científico ni matemático, no medio ninguna técnica en la que se utilizaron criterios o pesos

para su determinación. Ya en el análisis de la seguridad propiamente, al evaluar aspectos importantes, se va realizando una valoración del riesgo de cada uno de esos aspectos para determinar la profundidad de las pruebas sustantivas.

Los elementos a los que se le pusieron mayor atención son los siguientes:

3.2.1 Nuevo Personal

Un nuevo personal puede tener un diferente enfoque o entendimiento del control interno.

3.2.2. Sistemas de información Nuevos o Reorganizados

Cambios importantes y rápidos en el sistema de información pueden variar el riesgo relativo del control interno.

3.2.3 Nuevas Tecnologías

El incorporar nuevas tecnologías dentro del proceso productivo o sistemas de información, puede cambiar el riesgo asociado con el control interno.

3.3 Determinación de áreas Críticas

La determinación de las áreas críticas se llevó a cabo en la evaluación, identificación y análisis de los riesgos y los objetivos Institucionales y la injerencia de los tres elementos (Nuevo Personal, los Sistemas de Información

Nuevos o Reorganizados y las Nuevas Tecnologías) concentrados en cada actividad de seguridad que fue evaluada.

3.4 Evaluación del Control Interno

El alcance y amplitud de las pruebas de auditoria dependen de la confiabilidad que el auditor deposite en el ambiente de control, el objetivo de una auditoría no es evaluar la eficiencia del sistema de control interno; esa evaluación es parte de la auditoría. Por esta razón, el auditor no da garantía sobre la adecuación del control interno, sino se limita a expresar una opinión sobre la razonabilidad de éstos en su informe, la visión del control interno aplicado en esta área se obtuvo de la aplicación del cuestionario de Control interno, cuya muestra se puede observar en el anexo Nº 1.

3.5 Elaboración del Programa de Auditoría

Un programa de Auditoría contiene procedimientos compilados en un documento organizado que permite la aplicación eficiente y eficaz de las diferentes etapas de ésta, y cuyos procedimientos establecen la aplicación de las diferentes pruebas que se deben realizar para el análisis de las unidades, áreas o procesos en estudio, un ejemplo de este programa se puede apreciar en el anexo Nº 3.

Generalmente incluyen distintas fases que componen toda la elaboración del trabajo; las fases separan el programa en estratos que permiten trabajar con orden en los procedimientos. Un ejemplo de las fases de una auditoría podría ser: fase de obtención de información, de planeación, de ejecución y de información.

En el programa de auditoría se incluyen las pruebas sustantivas y analíticas que se explican a continuación:

3.5.1 Pruebas sustantivas

Las pruebas sustantivas contienen el análisis de los saldos de las cuentas y operaciones, así como también comparaciones, revisiones analíticas y declaraciones por escrito de la gerencia o de abogados con lo que se adquiere mayor seguridad en la exactitud de la información consecuentemente reduce el alcance de las pruebas sustantivas en la realización de la auditoría.

La naturaleza, oportunidad y amplitud de las pruebas sustantivas que se apliquen, han de ir acordes con los objetivos específicos de la auditoría.

3.5.2 Pruebas de cumplimiento

El propósito de las pruebas de cumplimiento es proporcionar una seguridad razonable de que los procedimientos de Control son aplicados de la forma que fueron descritos. Las pruebas de cumplimiento se relacionan primeramente con las preguntas:

- ¿Están siendo ejecutados los procedimientos necesarios?
- ¿Como están siendo ejecutados?
- ¿Por quién están siendo ejecutados?”

3.6 Preparación de la Auditoría

3.6.1 Elaboración de los papeles de trabajos

El auditor utiliza hojas y papeles de trabajo, en ellas resume sus observaciones y revisiones al ejecutar la auditoría, en esas hojas o papeles de trabajo, ya sean físicas o electrónicas, deja evidencia de las evaluaciones que se abarcan en el estudio.

El auditor analiza si los procedimientos son adecuados y las hojas de control constituyen una herramienta en la que se puede resumir y clasificar fácilmente la información recopilada para propiciar su evaluación.

3.7 Aplicación de las pruebas de Auditoría

Es un proceso utilizado para medir efectivamente la capacidad de un instrumento; es decir, lo que se quiere de él, dada su importancia al momento de juzgar sus resultados.

Una mejor ilustración sobre este aspecto lo brinda F. Jaime Arellano, cuando dice que la validez de contenido es: "El grado en que un instrumento logra medir lo que queremos medir con él, es decir, hasta qué punto mide efectivamente lo que nos proponemos que mida".[11]

---

[11] Arellano F. Jaime. Elementos de Investigación: La investigación a través del Informe. Costa Rica, EUNED, 1990, p. 123

Los datos recopilados durante una investigación son considerados válidos por el investigador cuando le proporcionan la información suficiente para formarse un criterio.

En este orden de ideas, Thomas C. Kinnear y James R. Taylor concluyen: "La validez del contenido comprende un juicio subjetivo elaborado por un experto en relación con lo apropiado de la medición".[12]

Con la aplicación de instrumentos válidos, se obtiene información oportuna y adecuado, necesaria para le desarrollo de una investigación y formulación de criterios que permiten llegar a una conclusión.

3.8 Recolección de Hallazgos (Oportunidades de Mejora)

Cuando, al analizar un proceso utilizando las técnicas y procedimientos de auditoría se encuentran aspectos relevantes que atentaban contra la seguridad de las tecnologías de información de la Organización, se anotan en las cédulas y papeles de trabajo como prueba sustantiva, necesarias para justificar que la auditoría fue practicada tal y como fue planeada.

3.9 Preparación de informes

Una vez recopilada la información, utilizando las técnicas y procedimientos dedicados para cada una de las etapas de la auditoría, se procede a evaluar los resultados con el fin de emitir un juicio profesional acerca de las situaciones evaluadas y así redactar un informe para dar a conocer a la administración las debilidades, las Oportunidades de Mejora (hallazgos) y las Recomendaciones pertinentes para su puesta en práctica.

[12] Kinnear Thomas C., Taylor James R. Metodología de la Investigación. 1996, p. 220

CAPÍTULO 4

Capítulo IV: *Resultados de la Evaluación.*

4.1 Presentación de Hallazgos (Oportunidades de Mejora):

Los Hallazgos u Oportunidades de Mejora detectados en el trabajo de la auditoría se presentan, a continuación, en un formato de tabla, en el que se enumeran en forma secuencial. Se les da un "Título" que ilustre en forma sencilla de qué se trata para facilidad del lector, también tiene un apartado de "Condición", en el qué se explica el hallazgo, un "Criterio" en el que se hace alusión a las mejores prácticas o a una norma establecida, se da una posible "Causa" de la condición y un "Efecto" que bien puede ser una posibilidad o un resultado del hallazgo. Se observa una "Conclusión" de la situación y finalmente una "Recomendación" para mejorar en ese aspecto detectado.

A continuación las Oportunidades de Mejora de este trabajo:

OPORTUNIDAD DE MEJORA
No. 1

TITULO: Ausencia del Comité Gerencial Informático

CONDICIÓN: El Comité Gerencial de Informática constituye la instancia técnica entre el máximo jerarca y la Unidad de Informática, brinda una asesoría al primero en lo relativo a la administración de los sistemas de información y de los recursos humanos, materiales y financieros que se destinen para su

desarrollo. En sana teoría, en el AyA existe un Comité Gerencial de Informática en la estructura del Instituto, todo de acuerdo y en cumplimiento de lo dictaminado por la Contraloría General de la República, y de las mejores prácticas el que se encuentra ubicado estratégicamente debajo de la Gerencia Administrativa, sin embargo, no se obtuvo evidencia de minutas de las reuniones de este Comité.

CRITERIO: Este Comité ha sido implantado por la Contraloría General de la República en el Manual Sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computadorizados (SIC) Norma 302.09.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de información M-XX-2007-CO-DFOE sobre el Comité Gerencial de TI menciona: " La toma de decisiones sobre asuntos estratégicos de TI debe apoyarse en la asesoría de una representación organizacional constituida en un Comité Gerencial de TI.

CAUSA: En la Institución existe un comité conformado por la Gerencia y los distintos Directores en ejercicio, en principio este Comité se encargaría de las funciones del Comité Gerencial Informatico pero desde la perspectiva técnica de los sistemas de información no ha dado los mejores resultados, dejando de lado esta importante labor.

EFECTO: El Comité se debería mantener de forma permanente y reunirse periodicamente o cuando una situación particular lo require, con ello canalizar las tareas, funciones y proyectos a desarrollar en el área de TI, de tal forma que las mismas se adecuen en beneficio de toda la empresa y no

solamente en un área o departamento específico, por lo que al no existir el comité se presentan desde desatenciones hasta duplicaciones en esos procesos con el costo económico que ello implica.

CONCLUSIÓN: Con base en nuestra revisión pudimos comprobar que el Comité Gerencial de Informática, existe solamente a nivel de estructura programática, debido a que éste ha sido desplazado por un Comité Gerencial constituido por los Directores de área cuya función es diferente a lo establecido en la norma SIC 306.09

RECOMENDACIÓN: Instaurar el Comité Gerencial de Informática en las condiciones establecidas por la normativa Contraloría General de la República.

Este Comité debe garantizar la concordancia de la gestión de TI con la estrategia institucional, la representatividad en la toma de decisiones, el establecimiento de prioridades, el equilibrio en la asignación de recursos y una adecuada atención de los requerimientos de todas las unidades organizacionales.

Dicho Comité debe:

a) Ser conformado con una representación suficiente y competente, que considere al jerarca (quien lo preside), los mandos responsables de los principales procesos de la entidad y el responsable de la unidad de TI.
b) Documentar claramente su funcionamiento y los roles de sus integrantes.
c) Atender, analizar y dictaminar asuntos estratégicos relacionados con la función de TI mediante acuerdos favorables o desfavorables.

d) Documentar debidamente lo actuado en sus sesiones.

OPORTUNIDAD DE MEJORA

No. 2

TÌTULO: Inexistencia de un Administrador (Oficial) de la Seguridad Informática

CONDICIÓN: Dentro de la estructura organizacional del departamento de TI no se define al puesto de administrador de la seguridad informática y aunque la función como tal se encuentra asignada “de hecho” a varios funcionarios, también son responsables de otras actividades, lo que limita su disponibilidad para ejecutar actividades más propias de un administrador de la seguridad.

CRITERIO: La organización debe poseer un adecuado proceso de administración de medidas de seguridad.

CAUSA: La Dirección no dispone de recurso humano suficiente como para realizar la segregación de funciones de manera específica; y distribuye actividades afines entre el personal existente. Inadecuada segregación de funciones al asignar roles incompatibles a un mismo funcionario. Esta situación es especialmente riesgosa si no se implementan controles compensatorios, ya que se disminuye considerablemente las posibilidades de errores o actos maliciosos pasen desapercibidos

EFECTO: No se le da el debido control, monitoreo y seguimiento a

eventos que puedan constituir riesgo para los sistemas informáticos institucionales. Carencia de disponibilidad para llevar a cabo proyectos y tareas referentes a la administración de la seguridad, lo que puede disminuir la eficiencia o efectividad con que se ejecuten las mismas. Sobrecarga de tareas al personal de TI, a quienes se les asignan algunas labores correspondientes a seguridad, lo que impide un adecuado desempeño de los funcionarios.

CONCLUSIÓN: El centro de cómputo de la organización no dispone de un puesto de administración de la seguridad; y las funciones son compartidas con otras que le compiten con la disponibilidad de recurso humano y de tiempo.

RECOMENDACIÓN: Efectuar una evaluación de las necesidades reales del recurso humano para el departamento de tecnologías, a efecto de que se tomen las medidas necesarias, para que las funciones de administración de la seguridad puedan ser implementadas en la figura de un responsable, que pueda ejecutar dicha función bajo estándares de seguridad acordes con las mejores prácticas y requerimientos de la entidad. El administrador de seguridad de TI es la figura responsable por la implementación efectiva de la seguridad relacionada con TI sistema y seguridad de datos. Adicionalmente es quien maneja el desarrollo y comunicación de políticas y estándares de seguridad de TI que se encuentren acordes con las mejores prácticas.

Un Oficial o Administrador de la Seguridad tendría las siguientes responsabilidades:

a) La Administración de los riesgos informáticos, prevención, detección, contención y corrección de brechas de seguridad.

b) Conducir compañas de educación al personal para concienciar acerca de la importancia de la seguridad.
c) Definir los requisitos de seguridad en sistemas nuevos y existentes.
d) Planear, desarrollar e implementar las políticas de seguridad en los diferentes sistemas.
e) Asegurar la actualización, monitoreo y cumplimento de las políticas de seguridad de TI.
f) Investigar y documentar la solución de incidentes de seguridad.
g) Asistir a la adquisición de software y hardware de seguridad.
h) Identificar vulnerabilidades y soluciones apropiadas para eliminar y minimizar sus potenciales efectos.
i) Hacer reportes periódicos sobre asuntos de seguridad de información.
j) Investigar violaciones actuales y potenciales en la seguridad de la información, y dar seguimiento a las investigaciones con reportes escritos.
k) Dar entrenamiento al personal con respecto a asuntos de seguridad de información.

OPORTUNIDAD DE MEJORA

No. 3

TITULO: Debilitamiento del control de Acceso al Centro de Cómputo (Eliminación del Equipo Biométrico).

CONDICIÓN: De la revisión sobre el control de acceso físico al cuarto de servidores, permitió comprobar la eliminación del dispositivo Biométrico, que se tenía como control de acceso, ya que este dispositivo se encontraba mal configurado y no cumplía con la función original de controlar el acceso a

personal no autorizado al área de servidores. Ahora utilizan las mismas tarjetas de proximidad que emplean como control de acceso a las Instalaciones de la dirección Informática.

CRITERIO: En el Marco Referencial COBIT (Objetivos de Control para las Tecnologías de Información) se establece que deben instalarse controles físicos y ambientales adecuados que sean revisados regularmente para garantizar su adecuado funcionamiento.(DS12).

CAUSA: Inexistencia de personal técnico especializado que lo reconfigure; debido a que cuando el mecanismo fue adquirido no se recibió la capacitación adecuada, aunado al hecho de que el proveedor que suministró el producto ya no se encuentra activo en el mercado.

EFECTO: Incremento del riesgo de un probable daño a los recursos de TI, que podrían constituir pérdida o deterioro de aplicaciones, de tecnologías, de las instalaciones, o de datos que podrían afectar la continuidad del negocio, además se produjo un debilitamiento de la estructura de acceso al centro de cómputo.

CONCLUSIÓN: La decisión de eliminar este dispositivo a pesar de la solución de utilizar los perfiles de las tarjetas de proximidad, incrementó el riesgo de acceso de funcionarios no autorizados al centro de cómputo. El ingreso de personas y funcionarios no autorizados incrementa el riesgo de que se causen daños a los recursos de TI, que podrían constituir pérdida o deterioro de aplicaciones, de tecnologías, de las instalaciones y /o datos y lo que podría afectar la continuidad del negocio.

RECOMENDACIÓN: Se recomienda como prioridad, al utilizar las mismas tarjetas de proximidad a la dirección, como un mecanismo provisional de control de acceso físico al área de servidores, el revisar, los permisos de acceso de todos los funcionarios de la dirección, puesto que, aunque todos deben tener la posibilidad de ingresar a la dirección, no todos deben tener el acceso al centro de computo.

Reintegrar el dispositivo biométrico a la mayor brevedad posible, mediante el análisis documentado sobre la viabilidad de reconfigurar el dispositivo biométrico, ya sea enviándolo a un lugar especializado, solicitando la asistencia de un técnico especializado, o bien capacitando algún funcionario ya sea en el país o en el exterior, y procurar o eligiendo así la mejor relación costo/beneficio.

OPORTUNIDAD DE MEJORA
No. 4

TÌTULO: Resultado de la poca Cultura de Seguridad Informática: Inadecuado uso de las Claves de Acceso

CONDICIÓN: De la administración del acceso a los recursos que busca salvaguardar la información contra uso no autorizado, divulgación, o revelación, modificación, daño o pérdida, se verificó la existencia de un manual de procedimientos sobre el manejo de claves (acceso lógico). Se evidenció la práctica y existencia de perfiles de usuarios definidos dependiendo el rol de cada funcionario. Se verificó que los códigos de usuario son asignados por un administrador, y que las claves deben ser de al menos 6 dígitos. Sin embargo, se determinó que existen problemas de cultura en el manejo de claves, ya que

algunos usuarios, después de haber accesado su equipo lo dejan solo, incluso que se comparten las claves. Otro aspecto por considerar es que el manual de procedimientos no toma en cuenta acciones que deben seguirse en caso de personal que está en vacaciones, suspendido, pensionado o fuera de labores de manera temporal o permanente. Tampoco existen limitaciones de acceso por horarios de trabajo. De las pruebas de verificación de vencimiento de claves se encontraron seis funcionarios con el check de no vencimiento.

CRITERIO: El acceso lógico y el uso de los recursos de TI deberá restringirse a través de la implementación de mecanismos adecuados de identificación, autenticación y autorización relacionando los usuarios y los recursos con las reglas de acceso.

CAUSA: Falta de cultura informática en gran parte de la población laboral del Instituto y la falta de concientización.

EFECTO: El acceso a los recursos informáticos mediante el uso de una clave es una acción que ofrece seguridad a la Institución y al usuario, ya que ambos se aseguran la posibilidad de utilizar las bondades que los sistemas le otorgan con seguridad. El mal manejo de claves de acceso, puede ocasionar cuantiosas perdidas al Instituto (en cuentas por cobrar a clientes con ajustes no procedentes, o con accesos a sitios no permitidos), estas situaciones se presentan acarreándole serios problemas al usuario propietario de la clave (cobros de sumas de dinero, suspenciones laborales y hasta despidos).

CONCLUSIÓN: Si bien es cierto que este control de acceso esta instaurado en el Instituto y cumple su objetivo de ayudar a la administración de los usuarios de los sistemas, no existe una buena cultura sobre la

confidencialidad y uso de las claves de acceso por parte de algunos funcionarios, también se determinó que a pesar de que el acceso lógico debe estar activo permanentemente y configurado por horarios de trabajo esto último no se cumple.

RECOMENDACIÓN: Establecer un programa de educación continua de la seguridad y la salvaguarda de la información dirigido a los usuarios finales.

Por otro lado, se debe implantar un procedimiento de desactivación de claves de acceso para personal en vacaciones, suspendido, pensionado o fuera de labores de manera temporal o permanente.

Sería recomendable analizar la posibilidad de incorporar a las configuraciones de accesos los horarios de trabajo, máxime que, según los últimos proyectos de atención al clientes, algunos funcionarios trabajaran en horarios no convencionales (sábados y domingos y hasta altas horas de la noche).

OPORTUNIDAD DE MEJORA
No. 5

TÍTULO: Sobre la Segregación de Niveles de Acceso

CONDICIÓN: Se verificó la existencia de Manuales de Puestos de los funcionarios de TI en donde se especifican los roles y responsabilidades, sin embargo, no se pudo comprobar la existencia de un procedimiento de revisión periódica de perfil.

CRITERIO: Los niveles de acceso deben reflejar los roles y responsabilidades acordados entre el usuario final, desarrollo de sistemas,

administración de red y del personal de operaciones del sistema, considerando los aspectos de segregación de cuentas, supervisión y control, Controlar y asegurar que los perfiles de usuario se han asignado de acuerdo con las políticas del Manual de Puestos y resguardo de la seguridad de TI estipulada en el Reglamento informático.

CAUSA: Procedimentar y establecer perfiles que reflejen los roles y responsabilidades acordados entre el usuario final, desarrollo de sistemas, administración de red y del personal de operaciones del sistema, considerando los aspectos de segregación de cuentas, supervisión y control, demandaría la utilización de un grupo de recursos humanos grande, o por un periodo relativamente extenso, situación que no permite terminar con esta labor.

EFECTO: Se deja sin lograr la propuesta de protección total al no complementar debidamente este control con el de las claves de acceso.

CONCLUSIÓN: El nivel de segregación es un complemento a las claves de acceso que resguardan aun más la seguridad en la red.
Este mecanismo necesita fortalecerse con revisiones periódicas de los perfiles de usuarios que garanticen su actualización de acuerdo con el movimiento interno del usuario.

RECOMENDACIÓN: Se debe implantar un manual de procedimientos relacionado con los aspectos de seguridad lógica que contemple tanto

características técnicas como guías para los usuarios. Es necesario diseñar un programa de revisión de perfiles de usuario de acuerdo con los roles y las responsabilidades, con el fin de garantizar que los accesos se encuentren actualizados.

OPORTUNIDAD DE MEJORA
No. 6

TÍTULO: Confusión entre los Planes de Continuidad de TI y el Plan de Contingencias de TI con los Planes Institucionales (Falta de coordinación y enlace con otras unidades del Instituto para la Continuidad del Negocio).

CONDICIÓN: Cuando se comprobó la existencia de un plan de contingencias de TI debidamente aprobado se determinó que el mismo incluye aspectos propios de un Plan de Continuidad, con lo cual se evidencia que no se hace una adecuada diferenciación entre ellos, además este plan no contempla otros aspectos fundamentales de Continuidad del Negocio en concordancia y coordinación con otras unidades del Instituto. Además, muchos aspectos solo se enfocan en procedimientos y respaldos de la información.

CRITERIO: Las mejores prácticas señalan que la Administración debe: Asegurar que los servicios de TI estén disponibles cuando se requieran, y procurar el impacto mínimo ante un evento que implique riesgo a la continuidad del negocio. Por otro lado en el Manual de Normas Técnicas para la Gestión y el Control de TI de la Contraloría General de la República en su apartado 5.7 se advierte:"...Aseguramiento de la continuidad de los servicios: Los procesos de la organización deberán mantener una continuidad razonable y su interrupción no deberá afectar significativamente a sus usuarios. Por ello,

se deberán definir, documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la valoración de riesgos y la clasificación de la criticidad de sus recursos de TI..."

CAUSA: Es normal que se dé este tipo de confusión entre los Planes de Continuidad y el de Contingencias, y como uno (el de Continuidad) contiene al otro es normal que se dé este tipo de confusión, ya que se dan diferentes puntos de vista y por lo tanto se pueden obtener diversas opiniones. El hecho de no existir un Comité Gerencial Informático, aunado a la inexistencia del Oficial o Administrador de la Seguridad son aspectos que facilitan situaciones de este tipo.

EFECTO: El efecto podría ser únicamente la molestia de no tener sistemas por unos minutos, hasta la pérdida de grandes sumas de dinero por no tener sistemas de información para darle continuidad al negocio, para hablar de colones habría que darle un valor a los datos Institucionales.

CONCLUSIÓN: Luego de analizar los Planes de Continuidad y el de Contingencias del Instituto se puede asegurar que los mismos cumplen con su objetivo en TI, aunque se notan en los documentos una confusión entre los contenidos que debe cubrir un Plan de Continuidad y un Plan de Contingencias, asimismo, con independencia del plan del que se hable no tiene coordinación con otras unidades del Instituto

RECOMENDACIÓN: La Administración debería proceder a separar claramente las medidas de los planes de contingencia y de continuidad de la organización. Analizar ambos planes tomando en cuenta entre otros aspectos

importantes, el personal clave para situaciones de este tipo, los respaldos, suministros requeridos y organización, y asignación de responsabilidades, clasificación de riesgo de los sistemas computacionales, período de recuperación crítica, las aplicaciones que deben recuperarse en un período crítico, las interrelaciones entre los usuarios y el procesamiento de datos, prioridades de procesamiento, redes de telecomunicación, seguros, alternativas de recuperación, hardware alternativo, custodia fuera del sitio, respaldo de seguridad de los medios y de la documentación, procedimientos periódicos de respaldo, frecuencia de rotación, las pruebas del plan y análisis de resultados, todo para garantizar que las actividades fundamentales de la organización sigan operando eficientemente luego de que sucediese una amenaza fuerte de desastre.

4.2 Elaboración de Informe Final de Auditoría

Luego de finalizada toda la etapa de ejecución de la auditoría se procede a elaborar el Informe Final de Auditoría, que incluye todos los aspectos de mejora detectados, para presentarlos ante la administración y que ésta tenga otra visión de su trabajo, el fin es que proceda a mejorar en cada uno de ellos en un determinado y razonable periodo. La Administración podrá determinar, si el informe no indica, la priorización de las mejoras, determinando cuáles aspectos son los más críticos para la Institución. La idea es que tomen las medidas del caso y se proponga un plan de acción inmediato. Una muestra con parte del Informe de este trabajo se muestra en el anexo Nº 9.

4.3 Conferencia Final o Discusión del Informe.

Como práctica generalizada de la Auditoría Interna del Instituto Costarricense de Acueductos y Alcantarillados, (AYA), se dará la Conferencia Final, en la que participaran los miembros del equipo de auditoría que realiza una evaluación con los representantes del proceso o de la Unidad Auditada. En esta conferencia se da lectura a los Hallazgos u Oportunidades de Mejora, los que se comentan y aclaran. Normalmente en esta entrevista, se logran salvar aspectos importantes, principalmente de redacción, que de otra forma pueden provocar roces entre el auditor y el auditado, con lo que se logra un mejor provecho del trabajo realizado.

Cada uno de los aspectos sujetos de mejora es valorado por las partes para determinar su pertinencia y aceptación, determinar cuál será el plan de acción futuro y cuáles hallazgos la Administración rechaza, por lo cual tiene otra oportunidad más para su descargo. Esta actividad es muy enriquecedora para las partes Auditadas y el grupo de Auditores.

En esta ocasión, como normalmente sucede, después de la Conferencia Final se llegó a una aceptación de los aspectos de mejora presentados, se consideran pertinentes y evidentemente, serán tomados en consideración inmediata para la optimización de las labores de TI y el logro de los objetivos del Instituto.

4.4 Presentación de Informe Final de Auditoría.

El informe final de auditoría, será presentado al Auditor Interno del AyA, el cual será analizado y transformado al formato en que la Auditoría Interna

suele remitir los Informes de acuerdo con las exigencias de la Contraloría General de la República. El mismo se remitirá y expondrá a la Junta Directiva.

4.5 Seguimiento del Informe Final de Auditoría

Se espera que el seguimiento de los puntos señalados en el Informe y propiamente de las recomendaciones aportadas, se realice al cabo de seis meses cumplidos luego de entregado el Informe Final de Auditoría.

CAPÍTULO 5

Capítulo V: *Conclusiones y Recomendaciones Generales*

5.1 Conclusiones Generales

Luego de realizada la auditoría sobre la seguridad de las Tecnologías de Información del Instituto Costarricense de Acueductos y Alcantarillados, se desprenden las siguientes conclusiones:

a) En el Instituto existe un ambiente físico y lógico seguro y controlado, con medidas de protección fundamentadas en las políticas vigentes y en el análisis de riesgos, lo cual satisface enormemente.

b) La Administración de la Dirección de Tecnologías de Información del Instituto Costarricense de Acueductos y Alcantarillados sí formula y mantiene una serie de políticas y lineamientos de seguridad razonable, las actividades del TI cuentan con políticas procedimientos formales

aprobadas por la Administración, que soportan tanto las labores diarias como periódicas, indican los responsables y recursos de TI necesarios.

c) La Dirección de TI tiene en consideración y practica una serie de actividades de mantenimiento de la seguridad, esas actividades son pertinentes y acordes a buenas prácticas, pero carece de un Oficial Administrador de la Seguridad que sea responsable y líder en este contexto.

d) Que existe un sistema de administración de incidencias bastante aceptable.

e) Que el Instituto Costarricense de Acueductos y Alcantarillados cuenta con un Plan de Contingencias, y con planes para la reducción de riesgos y consecuencias de incidentes de TI, pero que debe ser mejorado a la mayor brevedad posible.

f) Gran parte de la población laboral del Instituto carece de concientización y conocimientos de los aspectos de Seguridad de las Tecnologías de información, aspecto de alta criticidad que debe ser atendido en el menor tiempo posible.

5.2 Recomendaciones Generales

Con base en las conclusiones antes mencionadas, se recomienda:

Considerar la viabilidad de implementación de las recomendaciones para cada uno de los aspectos de mejora mencionados en el Capítulo 4, y en el Informe de Auditoría suministrado a la empresa, con el fin de mejorar las actividades de Seguridad de las Tecnologías de Información del AyA. Esas recomendaciones se pueden generalizar de la siguiente forma:

A la Administración Superior del Instituto:

a) Seguir por esa línea de evaluación de riesgos y fortalecimiento del ambiente y la estructura de seguridad controlada y fundamentada.

b) Crear la figura del Oficial o Administrador de la Seguridad del Instituto que se responsabilice y lidere este aspecto tan importante del quehacer Institucional

c) Corregir y mejorar los aspectos señalados en relación con la confusión y el alcance de los Planes de Contingencias y de Continuidad del Negocio, ya que los que se tienen son aceptables para la Dirección de TI dejando por fuera la coordinación que debe existir con otras Direcciones y Departamentos del Instituto.

d) Establecer un Comité de Informática, o Comisión que vele por el seguimiento de las recomendaciones de auditoría, y que se encargue de coordinar o mediar en la alineación de los objetivos de TI con los objetivos de negocio

A la Administración de la Dirección de Tecnologías de Información:

e) Fortalecer la formulación, las actividades y el mantenimiento de políticas y lineamientos de seguridad, y con la práctica de obtener siempre la aprobación de la Administración de acuerdo con buenas prácticas empleadas hasta la fecha.

f) Mantener y mejorar el sistema de administración de incidencias.

g) Proponer y ejecutar un plan de divulgación sobre el manejo y responsabilidad de la población laboral del Instituto respecto a los aspectos de Seguridad de las Tecnologías de Información, con la creación de un programa de concientización de la importancia de las actividades, recursos y controles sobre las Tecnologías de Información, que se implante como parte de lo filosofía de la Administración, y que venga a ayudar a que todos los colaboradores y usuarios finales sean un factor primordial para que el Departamento de TI opere de la mejor manera posible y contribuya al logro de los objetivos del negocio.

Bibliografía

Libros de texto:

1. Chinchilla, Carlos (2002) Delitos Informáticos. Costa Rica: Editorial Investigaciones Jurídicas.
2. Colmer, Arthur (1998) Principios Básicos de Auditoría. (9º ed.) Editorial CECSA.
3. Cook, J.W. (1992) Auditoría. (3º ed.) México: Editorial Mc Graw Hill.
4. Dávalos, Arcentales (1992) Auditoría. (3º ed.) México: Editorial Mc Graw Hill.
5. Defliese y otros (1983) Auditoría de Mongomory. (2º ed.) México: Editorial LIMUSA.
6. Delgado Xiomara (1993) Auditoría en informática. Costa Rica: Editorial EUNED.

7. Derrien, Yann (1993) Técnicas de la Auditoría Informática. México: Editorial Alfa Omega..
8. Echenique Jorge (2001) Auditoría en Informática. (2º ed.) México: Editorial Mc Graw Hill.
9. Fire, Leonard. (1998) Seguridad en Centros de Cómputos (Políticas y procedimientos). (2º ed.) España: Editorial Trillas.
10. Instituto Mexicano de Contadores Públicos (1995) Declaraciones sobre Normas de Auditoría. México
11. J., Fitzgerald (1992) Controles Internos para Sistemas de Computación. México: Editorial LIMUSA.
12. J.M., Lamére (1987) La Seguridad Informática. España: Editorial Ediciones Arcadia S.A.
13. Muñoz Carlos (2002) Auditoría en Sistemas Computacionales. México Editorial Pearzon Educación.
14. Romeo Carlos (1987) Poder Informático y Seguridad Jurídica. Madrid, España: Editorial FUNDESCO.
15. Siryan, Karanjit y Haren, Chris (2000) Firewalls y la Seguridad en Internet. (2º ed.) Editorial Prentice Hall Hispanoamericana.
16. Thomas, A.J., y Douglas I.J. (1988) Auditoría Informática. (2º ed.) España: Editorial Paraninfo.

Trabajos de Graduación:

1. Guzmán Aguilar, Óscar G y otro (1999) Auditoría Financiera a la Cooperativa de Empleados del Instituto Costarricense de Acueductos y Alcantarillados COOPEAYA, R.L.

Normas Internacionales:

1. Norma BS 7799 : 2002.
2. Norma COBIT Release 3.1 del 2004.
3. Norma COBIT Release 4.0 del 2006.
4. Normas de COSO.
5. Norma de la Internacional Electrotechnical Commission (IEC).
6. Norma ISO 17799 :2000 Information Technology. Code of Practice for Information Management.

Leyes:

1. Constitución Política de Costa Rica del siete de noviembre de mil novecientos cuarenta y nueve y sus reformas.
2. Ley Nº 8292 "General de Control Interno" del treinta y uno de julio del dos mil dos Interno.
3. Ley N° 7600 "Igualdad de Oportunidades para las Personas con Discapacidad" del dieciocho de abril de mil novecientos noventa y seis.
4. Ley Nº 2726 "Ley Constitutiva del Instituto Costarricense de Acueductos y Alcantarillados" del catorce de abril de mil novecientos sesenta y uno y sus reformas.
5. Ley Nº 8220 "De la Protección del ciudadano del exceso de requisitos y Trámites Administrativos" del cuatro de marzo del dos mil dos.
6. Ley Nº 8422 "Contra la Corrupción y el Enriquecimiento Ilícito en la función pública".

7. Ley No. 7494 “de Contratación Administrativa” del dos de mayo de mil novecientos noventa y cinco y sus reformas.
8. Ley No. 8131 “Ley de la Administración Financiera de la República y Presupuestos Públicos” del dieciocho de setiembre del dos mil uno.
9. Ley de Certificados, Firmas Digitales y Documentos Electrónicos, expediente 14276.

Reglamentos:

1. Reglamento Autónomo de Servicio del Instituto Costarricense de Acueductos y Alcantarillados. Publicado en La Gaceta N° 162 del jueves 19 de agosto del 2004.
2. Reglamento para la Adquisición y Administración de los Recursos Informáticos del Instituto Costarricense de Acueductos y Alcantarillados, del veinte de agosto del dos mil tres.

Manuales:

1. Manual sobre normas técnicas de control interno relativas a los sistemas de información computadorizados, emitido por la Contraloría General de la República y que actualmente se encuentra en una etapa de actualización.
2. Manual Institucional de Políticas de Seguridad en Tecnologías de Información, emitido por la Contraloría General de la República, Versión 1, del 18 Noviembre 2003.

3. Plan Estratégico en Tecnologías de Información para el periodo 2005-2014. Abril del 2006 Dirección de Tecnologías de Información del AyA.

Revistas:

1. Actualidad Económica, Nº 344 volumen XIX-2006 noviembre del 2006. Artículos varios.
2. Mundo Informativo, Nº 347. p.p. 32 a 34 y 36 a 39.
3. The Information Systems Control Journal. Revista Bimestral de la ISACA (Information System Audit and Control Association).

Artículos:

1. Security Provisioning: Managing Access in Extended Enterprises by Yuri Pikover and Jeff Drake: Evaluation and Implementation Check Lists.
2. El Recurso de Habeas Data en la Protección del Derecho a la Intimidad de Alejandra Castro B. Artículo suministrado en el curso de Derecho Informático impartido por la Dr. Alejandra Castro Bonilla.
3. Las Diez Vulnerabilidades de Seguridad más Críticas en Aplicaciones Web. Actualizado al 27 de enero del 2004. Artículo suministrado en el curso de Auditoría de la Seguridad, por el profesor MBA. MAG. Ricardo Madrigal L., Lic.
4. Las Vulnerabilidades de la OWASP. Artículo suministrado en el curso de Auditoría de la Seguridad, por el profesor MBA. MAG. Ricardo Madrigal L., Lic.

5. Previniendo el Spyware Malévolo de la Empresa. Por el Dr. Mattthew Willamson, de Seguridad Sana. Artículo suministrado en el curso de Auditoría de la Seguridad, por el profesor MBA. MAG. Ricardo Madrigal L., Lic.

Entrevistas:

1. Funcionarios del Instituto Costarricense de Acueductos y Alcantarillados (AyA) de:
    - La Dirección de Tecnologías de Información.
    - La Dirección de Apoyo Logístico.
2. Empleados de las Empresas Contratas por el AyA para la seguridad.
3. Empleados de las Empresas Contratas por el AyA para otros servicios de Outsourcing de TI.

Sitios de Internet:

1. www.activelex.com
2. www.aya.go.cr
3. www.isaca.org
4. www.iso.com
5. www.monografìas.com
6. www.theiia.com
7. www.theiia.org/itaudit