UNIVERSIDAD DE COSTA RICA

SISTEMA DE ESTUDIOS DE POSGRADO

TEMA DE ESTUDIO

DIAGNÓSTICO Y PROPUESTA DE ACTUALIZACIÓN DE LAS NORMAS TÉCNICAS PARA LA GESTIÓN Y EL CONTROL DE LAS TECNOLOGÍAS DE INFORMACIÓN DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA

Trabajo final de investigación aplicada, sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas, para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de la Información.

Licda. Marcela Ramírez Rojas

Ciudad Universitaria Rodrigo Facio, Costa Rica

2013

DEDICATORIA

Le dedico este trabajo a mi esposo, a mis padres y aquellos que me han apoyado en un largo proceso lleno de esfuerzo y dedicación; su motivación constante nunca me permitió apartarme del camino.
A todos gracias porque fueron luz e ilusión, para continuar hasta el final.

AGRADECIMIENTOS

A Dios,
por permitirme llegar hasta este punto y concluir de manera satisfactoria.

A mi esposo José David,
por su gran sacrificio diario durante estos casi tres años;
por todo el amor que me ha dado y por brindarme también su amistad,
por sus madrugadas y sus noches a mi lado durante este proceso.

A mis padres,
por su comprensión y el tiempo que dejaron de percibir,
por haberme inculcado el estudio desde pequeña.

A Fernando,
por ser el mejor amigo que la vida me pudo dar; por su ayuda, su comprensión y su incondicionalidad en todo momento,
durante nuestros estudios, trabajo y vivencias

A todos mis amigos,
en especial a Vivi y Shir por su apoyo incondicional en lo laboral, en lo académico y en mi vida… por sus consejos y su comprensión…

A mis compañeros de la maestría,
en especial a Maga y Jenny, por todas las horas de trabajo que compartimos juntas.

A mis compañeros de trabajo,
en especial a Ronald y Naty, que comparten mi día a día
por todo su apoyo, sus consejos y su compañía.

A mis profesores y lectores,
por todo el tiempo que dedicaron durante el proceso, las enseñanzas, la disponibilidad e interés que mostraron en todo este camino.

Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de la Información.

_____

Doctor Aníbal Barquero Chacón

Director Programa de Posgrado en Administración y Dirección de Empresas

_____

Doctor Sergio Espinoza Guido

Profesor Guía

_____

Máster Gino Ramírez Solís

Lector Académico

_____

Máster Miguel Pérez Montero

Lector empresarial

_____

Licda. Marcela Ramírez Rojas

Sustentante

TABLA DE CONTENIDO

RESUMEN

El objetivo principal de esta práctica profesional consiste, en elaborar un diagnóstico y una propuesta de actualización, de las normas técnicas para la gestión y el control de las tecnologías de información, emitidas por la Contraloría General de la República, mediante la realización de un trabajo investigativo, basado en variadas fuentes que permitan determinar mejoras para la normativa actual, las cuales sirvan de retroalimentación para el órgano contralor, de modo que con base en ellas, sea posible construir una nueva versión de la normativa aplicable al sector público.

Las normas técnicas para la gestión y el control de las tecnologías de información publicadas mediante la resolución N-2-2007-CO-DFOE, han procurado una mejor gestión de las tecnologías por parte de las organizaciones; sin embargo, ante el avance de la tecnología y el surgimiento de nuevas necesidades en este campo, nació el interés de realizar un diagnóstico y una actualización de dicha normativa, a fin de continuar con el proceso de gestión de los marcos de control, necesarios para el país y su gestión tecnológica.

El contenido capitulario consta de cinco capítulos, mediante los cuales se introduce el tema propuesto, seguido de una valoración del estado actual de las normas técnicas, en cuanto a su implementación y fiscalización en el sector público. Posteriormente, se relaciona la norma con otras instancias y marcos de control, como producto de la investigación se realiza una propuesta de actualización de la actual normativa en función de asumir mejores prácticas, para finalizar con un apartado de conclusiones y recomendaciones.

LISTA DE ILUSTRACIONES

LISTA DE ABREVIATURAS

AI	Adquirir e Implementar (COBIT)
BI	Business Intelligence
BYOD	Bring Your Own Device
CGEIT	Certified in the Governance of Enterprise IT
CGR	Contraloría General de la República
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CNCL	Congreso Nacional de Chile
CNTI	Centro Nacional de Tecnologías de Información
COBIT	Control Objectives for Information Systems and Related Technology
CONASSIF	Consejo Nacional de Supervisión del Sistema Financiero
CORFO	Corporación de Fomento de la Producción
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPA	Contador Público Certificado
CRISC	Certified Risk & Information System Control
DFOE	División de Fiscalización Operativa y Evaluativa
DS	Entrega y Soporte (COBIT)
EDGE	Enhanced Data rates for GSM Evolution
FIPS	Federal Information Processing Standards
GPRS	General Packet Radio Service
HSDPA	High-Speed Download Packet Access
IAAS	Infraestructura como un servicio
INN	Instituto Nacional de Normalización
ISACA	Information Systems Audit and Control Association
ISO	Organization for Standardization
ITGI	IT Governance Institute
MBA	Master in Business Administration
MCTI	Ministerio del Poder Popular para Ciencia, Tecnología e Innovación
ME	Monitorear y Evaluar (COBIT)
NIST	National Institute of Standards and Technology
NTGCTI	Normas Técnicas para la Gestión y el Control de las Tecnologías de Información
PaaS	Plataforma como un servicio
PAM	Process Assessment Model
PDA	Portátil tipo Asistente Digital Personal
PDCA	Plan-Do-Check-Act
PEI	Plan Estratégico Institucional
PETI	Plan Estratégico de Tecnologías de Información
PO	Planear y Organizar (COBIT)
RACI	Responsible, Accountable, Consulted, Informed
RFID	Radio Frequency Identification
RU	Reino Unido
SaaS	*Software* como un servicio
SGSI	Sistema de Gestión de Seguridad de la Información
SIP	Sistema Automatizado de Presupuesto
SUDEBAN	Superintendencia de las Instituciones del Sector Bancario
SUGEF	Superintendencia General de Entidades Financieras

TI	Tecnologías de Información
TIC	Tecnologías de Información y Comunicación
UMTS	Universal Mobile Telecommunications System
USB	Portable Universal Serial Bus
UTI	Unidad de Tecnologías de Información
VMM	Monitor de Máquina Virtual
VoIP	Voice over Internet Protocol
VPN	Red Privada Virtual
XML	Extensible Markup Language

1. CAPÍTULO I

1.1. INTRODUCCIÓN

El desarrollo constante y acelerado, de nuevas tecnologías, ha impactado de manera considerable, la forma como las personas se relacionan y hacen negocios en la actualidad; por tanto, el ambiente de trabajo cuenta con recursos de equipo informático y con datos que viajan por canales de comunicación cibernéticos.

En vista de lo anterior, los esfuerzos por la gestión de las tecnologías de la información, de las instituciones gubernamentales, deben orientarse en gran parte a salvaguardar la confidencialidad, disponibilidad e integridad de los activos e información que administran; dichos esfuerzos deben sustentarse en políticas y procedimientos establecidos, formalizados y conocidos por el personal que labora en la institución.

En Costa Rica, las normas técnicas para la gestión y el control de las tecnologías de información publicadas mediante la resolución N-2-2007-CO-DFOE, han procurado una mejor gestión de las tecnologías por parte de las organizaciones; sin embargo, frente al avance de la tecnología y el surgimiento de nuevas necesidades en este campo, nació el interés de realizar un diagnóstico y una actualización de dicha normativa, a fin de continuar con el proceso de gestión de los marcos de control necesarios para el país y su gestión tecnológica.

1.2. OBJETIVO GENERAL

Elaborar un diagnóstico y una propuesta, de actualización de las normas técnicas para la gestión y el control de las tecnologías de información, emitidas por al Contraloría General de la República, fundamentados en la investigación de diversas fuentes que permitan determinar mejoras para la normativa actual, que sirvan de retroalimentación para el órgano contralor, de modo que con base en ellas, sea posible elaborar una nueva versión de la normativa aplicable al sector público.

1.3. OBJETIVOS ESPECÍFICOS

- Listar de manera general, nuevas tendencias en tecnologías de información, como firma digital, computación en la nube, entre otros y determinar si los cambios de esas implican actualizaciones de fondo a las normas establecidas actualmente.
- Indagar sobre la aplicación y cumplimiento de las normas técnicas para la gestión y el control de las Tecnologías de Información, mediante la revisión de los resultados del Macro Proyecto y el diagnóstico que este planteó, en su momento de acuerdo con las normas, así como sobre los informes y disposiciones posteriores a ese estudio, a fin de identificar y analizar lo actuado por la Contraloría General de la República, en su función fiscalizadora, mediante el instrumento normativo.
- Elaborar una propuesta, de acuerdo con los resultados obtenidos del proceso de investigación, a fin de presentarla, junto con el diagnóstico y las respectivas guías de evaluación.

1.4. ALCANCE

El tema de esta investigación se denomina “Diagnóstico y propuesta de actualización de las normas técnicas para la gestión y el control de las tecnologías de información”, emitidas por la Contraloría General de la República. Se desarrolló en el período comprendido entre octubre 2012 y abril 2013, como parte del curso, requisito de graduación, que se designa Práctica Profesional de la Maestría en Auditoría de Tecnologías de Información de la Universidad de Costa Rica y se obtuvo como resultado, un documento que se presentó a los funcionarios competentes de la Contraloría General de la República, para su estudio y valoración.

El alcance de este trabajo toma en cuenta, una revisión de las normas técnicas para la gestión y el control de las tecnologías de información, a la luz del rápido cambio que sufre la tecnología actualmente, y dado el impacto que en los últimos tiempos, esta produce en las operaciones del sector público. Al valorar ese cambio tecnológico, se analizaron nuevas tendencias en el mercado de las tecnologías de información, que podrían significar amenazas al logro de los objetivos.

Para el período 2007-2012, cinco años de vigencia de las normas técnicas, se analizó un diagnóstico emitido por la Contraloría General de la República, que formó parte del Macro Proyecto de Tecnologías de Información, además se revisaron y analizaron los informes publicados por el ente contralor, con el propósito de determinar del uso de las normas técnicas como criterio dentro de esos informes, a fin de establecer si se cumple lo normado, las instituciones de la muestra, las debilidades ya identificadas por el

órgano contralor, el rumbo seguido por la Contraloría General de la República al final del proyecto y el seguimiento dado a la implementación de la normativa.

Cabe mencionar, que la revisión de las normas técnicas para la gestión y el control de las tecnologías de información, no se realizó en función de identificar si están bien construidas, o bien, si con estas se puede lograr cumplir con el objetivo para el que fueron creadas, puesto que el objetivo de este trabajo, se limita a revisar aspectos de desactualización, oportunidades de mejora y aprovechamiento de los recursos existentes en el mercado.

1.5. LIMITACIONES

La creación del diagnóstico y propuesta de actualización de las normas técnicas para la gestión y el control de las tecnologías de información, tuvo como limitaciones: que no se pudiera contactar a algunos de los profesionales escogidos para el proceso de entrevista, en particular por sus agendas de trabajo; las complicaciones de la estudiante para poder planificar reuniones en horas de oficina, debido a sus ocupaciones laborales y la falta de disponibilidad de tiempo para la valorar dicha normativa, en diferentes instituciones del país.

Como parte de esta investigación, se obtuvo conocimiento del diagnóstico efectuado por la Contraloría General de la República, en el período comprendido por el Macro Proyecto de Fiscalización de Tecnologías de Información, durante el cual se efectuaron informes anuales durante el periodo 2008-2010. En este se abarca una serie de resultados sobre los estudios de fiscalización, posterior al proceso de implementación y

cumplimiento de la normativa de TI, los cuales fueron tomados como base, para indicar la situación actual de cumplimiento.

Por lo tanto, se tomaron en consideración esos datos, para generar conocimiento sobre el estado de las instituciones fiscalizadas en ese momento, en cuanto al cumplimiento de las normas técnicas para la gestión y el control de las tecnologías de información. Por otra parte, para complementar el diagnóstico efectuado por el ente contralor, se revisaron los informes correspondientes a los años 2011-2012, y el estado de las disposiciones emitidas, a fin de diagnosticar de esta forma, el estado actual del conocimiento y cumplimiento de la citada normativa en el territorio nacional.

1.6. FINALIDAD

Se analizó el diagnóstico emitido por la Contraloría General de la República y se unió con el de los informes y disposiciones emitidos por ese órgano contralor, a fin de conocer el estado de uso actual de las normas técnicas; se investigaron las tendencias tecnológicas, que distancian a la normativa actual del contexto mundial tecnológico, y que podrían generar brecha, en cuanto a la adecuada gestión de las tecnologías de las instituciones, en pro del logro de sus objetivos de negocio.

Además, se evaluó el resultado del sondeo de opiniones calificadas y se dieron a conocer, de forma general, marcos de control como *COBIT* 4.1 e *ITIL* V3, para plantear una propuesta de actualización de las normas técnicas para la gestión y el control de las tecnologías de información. Con ello se sentaron las bases y supuestos, sobre los cuales construir una nueva versión de la normativa, de cara a cumplir con el objetivo del marco regulador, en cuanto a procurar una mejor gestión de las tecnologías, por parte de las

organizaciones auditadas por la Contraloría General de la República, en función del logro de los objetivos institucionales de cada ente fiscalizado.

1.7. INTERESES PROFESIONALES

Se brindó colaboración a la Contraloría General de la República y su gestión de fiscalización de las instituciones del sector público, al plantearle las oportunidades de mejora en la gestión de la normativa de regulación de las tecnologías de información vigente, mediante la aplicación del criterio de los expertos y el conocimiento obtenido en la Maestría de Auditoría de Tecnologías de Información.

Asimismo, como parte del resultado obtenido del análisis, se concluye que la Contraloría General de la República debe enfocar sus esfuerzos en la revisión, cumplimiento y entendimiento del marco de control que se aplique a las instituciones y evitar el desgaste en la emisión de normas y detalles de procesos, que ya están contemplados en los marcos de control de aceptación mundial, lo cual haría el proceso de fiscalización de tecnologías más eficaz y eficiente, aprovechando los recursos de control, evaluación e implementación que ya se aplican en el mercado.

1.8. APORTE DE LA INVESTIGACIÓN

Investigación, diagnóstico y análisis de la información obtenida, establecimiento de las brechas actuales en las tecnologías de posible aplicación de las instituciones aplicadas, en función del cambiante mundo tecnológico y su fiscalización por parte de las normas técnicas para la gestión y el control de las tecnologías de información, a fin de cumplir

su objetivo de mejorar la gestión de las tecnologías por parte de las organizaciones, en pro del logro de los objetivos de cada ente fiscalizado.

A su vez, el estudio realizado y los resultados obtenidos, le permitirán a la Contraloría General de la República, enfocar de mejor manera los estudios de fiscalización efectuados, sobre la gestión de las tecnologías de información en el sector público, aunados a orientar los esfuerzos de la institución, en cuanto a lograr la mejora continua de las instituciones en relación con el tema.

1.9. METODOLOGÍA DE LA INVESTIGACIÓN

La presente investigación se enmarcó en un modelo de enfoque dominante, tratándose de una investigación cualitativa, alineada a las investigación de las tecnologías de información y los cambios que estas podrían plantear al esquema de la normativa vigente, enriqueciendo diferentes aspectos con un sondeo de opiniones calificadas, que fueron obtenidas mediante entrevista sobre el uso de las normas y su actual construcción (ver anexo Nº1). Además, se agregó un componente cuantitativo, al cotejar los resultados del diagnóstico efectuado por la Contraloría General de la República junto con la valoración de los informes del período 2011-2012 y el estado de sus disposiciones, donde se midió el nivel de cumplimiento de esa normativa.

1.10. CONTENIDO CAPITULARIO

A continuación se estableció el esquema original, con el cual se planteó ejecutar la investigación y desarrollo, para elaborar la propuesta de actualización de las normas técnicas para la gestión y el control de las tecnologías de información:

Capítulo I: Anteproyecto	• Introducción • Objetivo General • Objetivos Específicos • Alcance • Limitaciones • Finalidad • Intereses Profesionales	• Aporte de la Investigación • Contenido Capitulario • Metodología de la Investigación • Referencias • Cronograma de Actividades • Anexos
Capítulo II: Situación Actual	• Investigación General de las Tendencias del Mercado Tecnológico que Puedan Afectar la Normativa • Diagnóstico de las Normas Técnicas Actuales (Macro Proyecto) o Revisión de los Informes de Contraloría General de la República del 2011-2012 o Revisión y Diagnóstico de las Disposiciones Emitidas	
Capítulo III: Relación de la Norma con Otras Instancias de Control	• ¿Qué se Hace en Otros Países? o Normativa Bancaria en Venezuela o Normativa Gubernamental en Chile • Relación *COBIT* 4.1 • Sondeo de Opiniones Calificadas	
Capítulo IV: Propuesta De Actualización	• Análisis de los Resultados • Estructura de la Propuesta • Propuesta a CGR de Realizar una Guía de Revisión Estructurada	
Capítulo V: Conclusiones y Recomendaciones	• Conclusiones • Recomendaciones • Anexos	

2. CAPÍTULO II

2.1. SITUACIÓN ACTUAL

La Contraloría General de la República fue establecida por la Constitución Política como una institución auxiliar de la Asamblea Legislativa, con absoluta independencia en la vigilancia y control de la hacienda pública.

Según ha sido definida, la Contraloría General de la República establece y regula el cumplimiento de la normativa que rige a las instituciones públicas, en atención a lo establecido por la Ley Orgánica de la Contraloría General de la República, donde se le designa como Órgano Rector del Ordenamiento de Control y Fiscalización Superiores de la Hacienda Pública y se le confiere la facultad de emitir disposiciones, normas, políticas y directrices, que coadyuven a garantizar la legalidad y la eficiencia, tanto de los controles internos, como del manejo de los fondos públicos de los entes, sobre los cuales tiene jurisdicción.

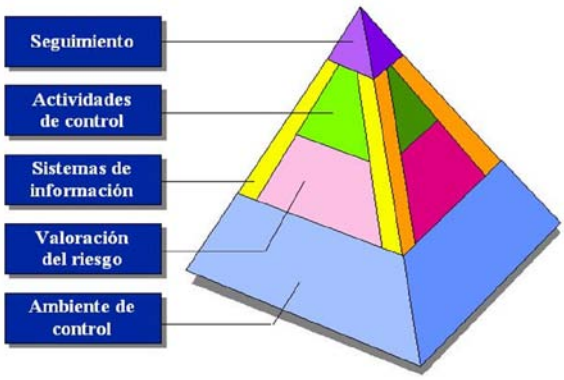
En concordancia con lo anterior, la Ley General de Control Interno refuerza las facultades de la Contraloría General para emitir la normativa técnica necesaria para el funcionamiento efectivo del sistema de control interno de los entes y órganos sujetos a esa ley.

De esta forma, surge el interés del órgano contralor, respecto a regular el manejo de las tecnologías, tomando en cuenta los cinco componentes del control interno, entre ellos el de sistemas de información y su tendente automatización, así como y sus relaciones con los otros cuatro:

- Ambiente de control.
- Valoración del riesgo.
- Actividades de control.
- Sistemas de información.
- Seguimiento del sistema de control interno.

Estos componentes del sistema de control interno, han sido expresados gráficamente, por medio de la siguiente pirámide:

Ilustración 1: Componentes del Sistema de Control Interno



Fuente: Curso Modular sobre Control Interno CGR.

El esquema piramidal del modelo de control interno de la Contraloría General de la República, toma como punto de partida y fundamento sólido el ambiente de control, donde se suman otros aspectos que de acuerdo con su interés, van formando la pirámide de control, siguiendo con valoración del riesgo, sistemas de información, actividades de control y finalmente, en un punto más pequeño, el seguimiento, que se ubica de último, pues debe dar sustento a todos sus antecesores.

Por lo tanto, en el año 1996, se publica el "Manual sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computadorizados", tal y como se indica en el artículo tercero de la ley al respecto:

> Facultad de promulgar normativa técnica sobre control interno. La Contraloría General de la República dictará la normativa técnica de control interno, necesaria para el funcionamiento efectivo del sistema de control interno de los entes y de los órganos sujetos a esta Ley. Dicha normativa será de acatamiento obligatorio y su incumplimiento será causal de responsabilidad administrativa. (CGR, 1996)

Como parte del seguimiento a las normativas que emite la CGR, se observó que las tecnologías de información están en constante movimiento y son cada vez más, un instrumento esencial en la gestión de los servicios institucionales, aunado al rubro presupuestario de las diferentes entidades, el cual ha ido aumentado con los años (ver Tabla 1: Montos Ejecutados por el Sector Público en el Período 2006-2012), con el detalle de los montos ejecutados para TI en el sector público, en comparación con lo ejecutado de forma general por estas instituciones:

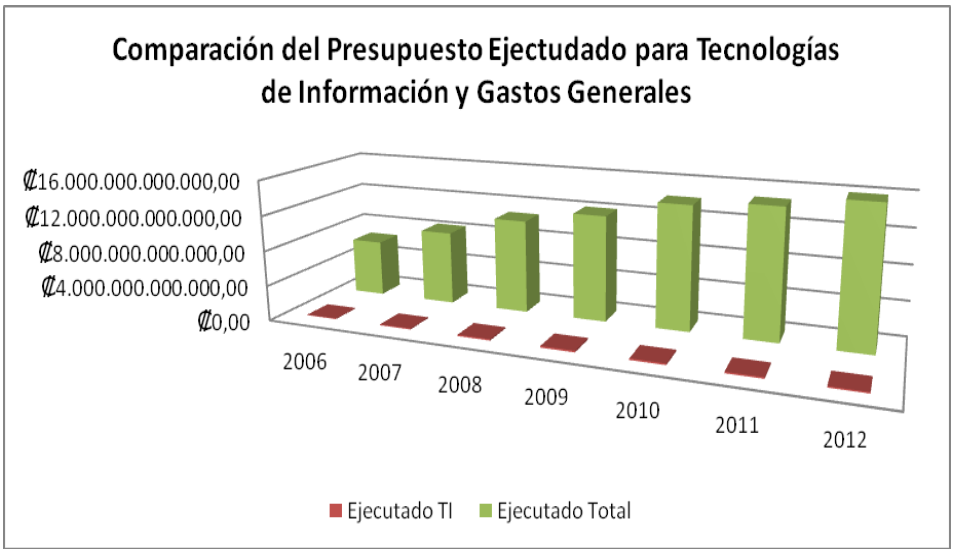
Tabla 1: Montos Ejecutados por el Sector Público en el Período 2006-2012

Año	Ejecutado TI	Ejecutado Total	Porcentaje
2006	₡66 519 231 380,26	₡6 480 728 943 553,81	1,03%
2007	₡11 295 471 991,16	₡8 464 043 154 202,38	1,31%
2008	₡150 491 121 866,31	₡10 711 628 841 719,30	1,40%
2009	₡176 638 493 676,39	₡12 110 313 032 852,10	1,46%
2010	₡173 351 377 467,31	₡14 105 215 990 789,40	1,23%
2011	₡159 326 357 290,45	₡14 705 285 615 512,10	1,08%
2012	₡143 919 619 910,43	₡15 886 436 323 469,00	0,91%

Fuente: Elaboración propia con base en el Reporte del Sistema Automatizado SIP.

Tal como se puede inferir de la tabla anterior, los montos ejecutados por las instituciones, en función de las tecnologías de información, no llegan ni al 2% del presupuesto ejecutado. En la Ilustración 2 Comparación de los Montos Ejecutados por el Sector Público en el Período 2006-2012.

Ilustración 2 Comparación de los Montos Ejecutados por el Sector Público en el Período 2006-2012



Fuente: Elaboración propia con base en el Reporte del Sistema Automatizado SIP

Como se puede observar, llama la atención que a pesar de darse en aumento porcentual en el período 2006-2011, para el 2012 desciende a menos del 1%.

Lo anterior, se suma al hecho de que como parte del establecimiento y seguimiento del control interno, se encuentra el componente denominado sistemas de información, el cual establece que se permita a la administración activa tener una gestión documental institucional, entendiendo esta como el conjunto de actividades realizadas con el fin de controlar, almacenar y, posteriormente recuperar de modo adecuado, la información producida o recibida en la organización, en el desarrollo de sus actividades, con el fin de prevenir cualquier desvío en los objetivos trazados, el cual se cita a continuación:

Sistemas de información. Deberá contarse con sistemas de información que permitan a la administración activa tener una gestión documental institucional, entendiendo esta como el conjunto de actividades realizadas con el fin de controlar, almacenar y, posteriormente, recuperar de modo adecuado la información producida o recibida en la organización, en el desarrollo de sus actividades, con el fin de prevenir cualquier desvío en los objetivos trazados. Dicha gestión documental deberá estar estrechamente relacionada con la gestión de la información, en la que deberán contemplarse las bases de datos corporativas y las demás aplicaciones informáticas, las cuales se constituyen en importantes fuentes de la información registrada.

En cuanto a la información y comunicación, serán deberes del jerarca y de los titulares subordinados, como responsables del buen funcionamiento del sistema de información, entre otros, los siguientes:

a) Contar con procesos que permitan identificar y registrar información confiable, relevante, pertinente y oportuna; asimismo, que la información sea comunicada a la administración activa que la necesite, en la forma y dentro del plazo requerido para el cumplimiento adecuado de sus responsabilidades, incluidas las de control interno.

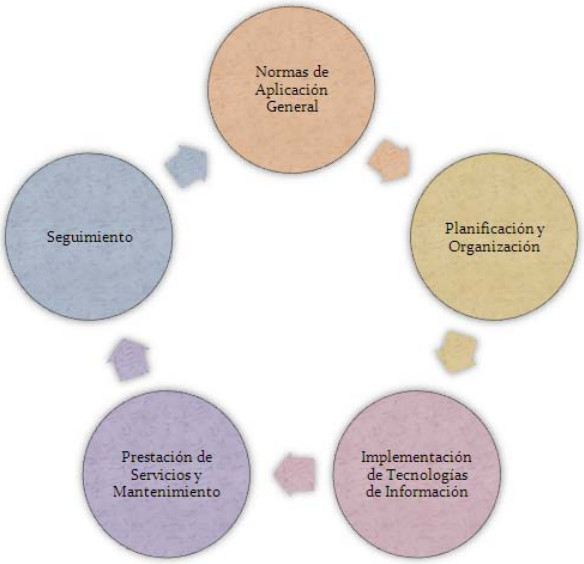
b) Armonizar los sistemas de información con los objetivos institucionales y verificar que sean adecuados para el cuido y manejo eficientes de los recursos públicos.

c) Establecer las políticas, los procedimientos y recursos para disponer de un archivo institucional, de conformidad con lo señalado en el ordenamiento jurídico y técnico. (CGR, Ley General de Control Interno Nº8292, 2002)

Con fundamento en lo anterior, en el año 2007, la Contraloría General de la República consideró pertinente emitir las "Normas técnicas para la gestión y el control de las tecnologías de información" (NTGCTI), para con ello fortalecer la administración de los recursos invertidos en tecnologías de información, estableciendo criterios básicos de control que debían ser observados en la gestión institucional de las tecnologías y que a su vez coadyuvaran en el control y fiscalización que realice el órgano contralor.

Dicho instrumento normativo se basó en cinco áreas generales, definidas como normas de aplicación general, planificación y organización, implementación, prestación de servicios y mantenimiento, finalizando seguimiento, tal y como se observa en la ilustración siguiente:

Ilustración 3: Áreas de NTGCTI



Fuente: Elaboración propia con base en las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información.

La citada normativa, en su artículo tercero establece que: las "Normas técnicas para la gestión y el control de las tecnologías de información, son de acatamiento obligatorio para la Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización, excluyendo a las instituciones de menor tamaño, entendidas como aquellas que dispongan de un total de recursos que ascienda a un monto igual o inferior a seiscientas mil unidades de desarrollo y que cuenten con menos de treinta funcionarios, incluyendo al jerarca, los titulares subordinados, y todo su personal; y que estas normas prevalecerán sobre cualquier disposición en contrario que emita la Administración." (N-2-2007-CO-DFOE, 2007)

Asimismo, que su inobservancia generará las responsabilidades que correspondan, de conformidad con el marco jurídico que resulte aplicable[1].

Por lo tanto, se realiza una clasificación básica sobre el tipo de instituciones, donde las normas técnicas para la gestión y el control de las tecnologías de información serán aplicables y del artículo tercero anterior se deduce, que dichas normas no se aplicarán a las instituciones de menor tamaño, cuyos recursos asciendan a un monto igual o inferior a seiscientas mil unidades de desarrollo y cuenten con menos de treinta funcionarios.

Como parte de la logística para la implementación de las normas técnicas, para la gestión y el control de las tecnologías de información, dentro del cuerpo normativo se establece lo siguiente: "…primeramente la obligatoriedad del instrumento, determinando como plazo dos años a partir de su emisión, además se establecen cuatro pasos iniciales, en función de una ejecución organizada, iniciando por la constitución de un equipo, designación de un responsable de la implementación, realización de un estudio detallado de la normativa donde se identifiquen las aplicables a cada organización, finalizando con el establecimiento de la planificación de la implementación". De tal manera se describe en el artículo sexto:

> Informar que la Administración contará con dos años a partir de su entrada en vigencia para cumplir con lo regulado en esta normativa,

[1] Así modificado según resolución R-CO-9-2009 de las nueve horas del veintiséis de enero del dos mil nueve, mediante la cual se emitieron las "Normas de control interno para el Sector Público", publicada en La Gaceta Nº 26 del 6 de febrero del mismo año.

lapso en el cual, dentro de los primeros seis meses, deberá planificar las actividades necesarias para lograr una implementación efectiva y controlada de lo establecido en dicha normativa, contemplando los siguientes aspectos:

a) La constitución de un equipo de trabajo con representación de las unidades que correspondan.

b) La designación de un responsable del proceso de implementación, quien asumirá la coordinación del equipo de trabajo y deberá contar con la autoridad necesaria, dentro de sus competencias, para ejecutar el referido plan.

c) El estudio detallado de las normas técnicas referidas, con el fin de identificar las que apliquen a la entidad u órgano de conformidad con su realidad tecnológica y con base en ello establecer las prioridades respecto de su implementación.

d) Dicha planificación deberá considerar las actividades por realizar, los plazos establecidos para cada una, los respectivos responsables, los costos estimados, así como cualquier otro requerimiento asociado (tales como infraestructura, personal y recursos técnicos) y quedar debidamente documentada. (N-2-2007-CO-DFOE, 2007)

2.2. DIAGNÓSTICO SOBRE LA IMPLEMENTACIÓN DE LAS NORMAS TÉCNICAS PARA LA GESTIÓN Y EL CONTROL DE LAS TECNOLOGÍAS DE INFORMACIÓN

Con el fin de promover una mejora significativa sobre la inadecuada gestión de las tecnologías de información, que se venía dando por parte de las instituciones públicas, la División de Fiscalización Evaluativa y Operativa de la Contraloría General (DFOE) decidió, en el año 2008, llevar a cabo un macro proyecto de fiscalización en dicha materia.

El estudio se concentró en darle seguimiento a la implementación de las mencionadas normas, conformadas por un conjunto de criterios básicos de control para ser observados de manera obligatoria en la gestión pública de tecnologías de información y que coadyuven en su labor de fiscalización, por parte de la Contraloría General de la República.

Los estudios del macro proyecto estuvieron relacionados con la revisión general de las acciones llevadas a cabo, por un grupo predeterminado de instituciones, donde se quería evaluar:

- La implementación de las normas técnicas.
- El proceso de implementación.
- La suficiencia del plan de implementación.
- La eficacia en cuanto al cumplimiento de la normativa.

En el 2008, la evaluación consistió en determinar si la institución cumplió con las actividades señaladas en el artículo de la cita anterior; además, se evaluó la razonabilidad del referido plan y la suficiencia del cumplimiento de las normas, que según indicó la administración ha implementado. Las instituciones fiscalizadas y los resultados fueron los siguientes:

Tabla 2: Resultados de la Verificación del Artículo 6º de la Resolución N° R-CO-26-2007 y la Razonabilidad de los Planes de Implementación de la Norma N-2-2007-CO-DFOE

	Designación equipo de trabajo	Designación responsable del proyecto	Diagnóstico, identificación de normas, priorización	Elaboración plan implementación
1	Sí	Sí	Insuficiente	Insuficiente
2	Sí	Sí	No	Insuficiente
3	Sí	Sí	No	No tiene
4	Sí	Sí	No	Insuficiente
5	Sí	Sí	No	Insuficiente
6	Designación tardía	Designación tardía	Insuficiente	Insuficiente
7	Sí	Sí	Insuficiente	Insuficiente
8	Sí	Sí	Insuficiente	Insuficiente

Fuente: Informe DFOE-PGAA-I-9-2008 del 11 de diciembre 2008.

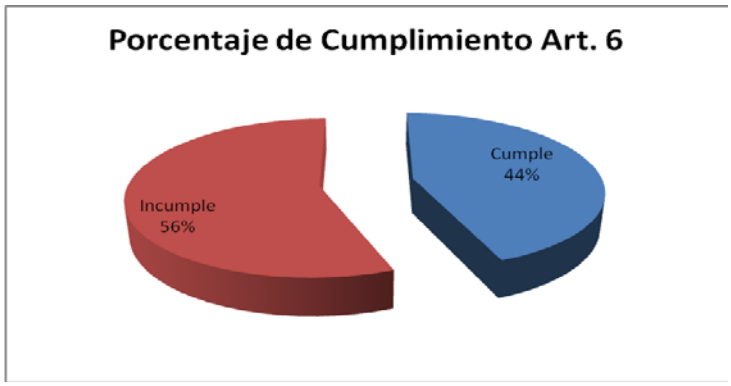
Debido a los resultados anteriores, donde se designaron, tanto el equipo como el responsable del proyecto, pero se observó la insuficiencia de la realización del diagnóstico y del plan de implementación, la Contraloría remite el oficio DFOE-219 (7201) del 18 de julio de 2008, donde se solicita a una muestra de instituciones, confirmar a la Contraloría General si se había cumplido con lo establecido en el artículo sexto. (N-2-2007-CO-DFOE, 2007)

La conformación de la muestra de 58 instituciones fue propuesta por las Áreas de Fiscalización de la DFOE, donde se consideraron variables como:

- El monto del presupuesto anual de la entidad.
- Monto del presupuesto destinado a TI.
- El porcentaje que este representa dentro del presupuesto anual de la entidad.

Los resultados de las respuestas emitidas, por las instituciones consultadas, permitieron contabilizar que el 55,77% (29) de las 58 instituciones consultadas, ha cumplido en su totalidad con lo establecido en el artículo sexto de la citada normativa, mientras el 44,23% (23) de la muestra, aún no cumple de forma completa, lo cual se representa en la siguiente ilustración:

Ilustración 4: Porcentaje de Cumplimiento del Artículo N°6 de la Resolución R-CO-26-2007



Fuente: Elaboración propia con base en el informe DFOE-PGAA-I-9-2008 del 11 de diciembre, 2008.

Los resultados del macro proyecto, para el año 2008, sobre el proceso de implementación, revelaron que el accionar de las instituciones era insuficiente y además, el plazo para que las instituciones cumplieran, con lo regulado en dichas normas, vencía el 31 de julio de 2009; por lo tanto, se decidió que para los años 2009 y 2010, el alcance y enfoque de evaluación del macro proyecto de TI debía cambiarse, de forma tal, que se orientó hacia la realización de estudios de fiscalización sobre:

- La ejecución del plan de implementación de la normativa aprobada por esta Contraloría General.
- La gestión de proyectos.
- La contratación de bienes y servicios relacionados con tecnologías de información.
- La calidad de la información relevante, operada por sistemas de información automatizados y contenida en las bases de datos institucionales.
- La evaluación de la seguridad de la información, que se genera a partir de los sistemas informáticos.

En el 2009, las evaluaciones realizadas durante el año y los resultados de la consulta realizada a 12 instituciones, sobre la implementación de las "Normas técnicas para la gestión y el control de las tecnologías de información", permitieron al órgano contralor determinar, que con excepción del sector bancario, las instituciones no han desarrollado los esfuerzos suficientes para implementar, de forma integral, la citada normativa, aun cuando el plazo establecido a las administraciones, para cumplir con lo regulado, venció el 31 de julio de 2009.

Según la Contraloría General de la República, dicha situación se convirtió en un riesgo para las administraciones, de acuerdo con lo que establece en las conclusiones del informe DFOE-PGAA-I-7-2009 del 27 de enero del 2010, de cita siguiente:

> Esta situación se convierte en un riesgo para las administraciones, por cuanto la gestión de las tecnologías de información podría no estarse dando de una manera controlada, con el agravante de que los recursos

> asignados a las TI no se orienten de una forma planificada, con el fin de garantizar la satisfacción de los usuarios y el logro de los objetivos estratégicos institucionales, así como la seguridad de la información que se genera en las entidades del Estado.

En diciembre del 2010, como parte de los resultados finales del macro-proyecto de tecnologías de información, la DFOE determinó nuevamente como insuficiente la implementación de las NTGCTI, por parte de las entidades fiscalizadas y señaló el crecimiento del riesgo en el uso de recursos públicos asignados a las tecnologías de información, al no orientarlos de manera planificada y organizada hacia el logro de los objetivos estratégicos institucionales y encontrar deficiencias en cuanto a la seguridad y calidad de la información que se genera en la hacienda pública.

Al respecto, se citan algunas de las conclusiones obtenidas, indicadas en los informes de cierre de dicho proyecto:

> En síntesis, producto de este proceso se determinó que las instituciones no han desarrollado los esfuerzos suficientes para implementar las "normas técnicas para la gestión y el control de las tecnologías de información"; justificando tal situación en escasez de personal con el conocimiento suficiente sobre el marco normativo y carencia de tiempo y necesidad de reordenar la prioridad de los proyectos institucionales para la atención de este requerimiento.

Tal situación representa un riesgo, en el tanto no se pueda garantizar que la gestión pública de las tecnologías de información se dé en un ambiente debidamente controlado, que garantice la satisfacción de los requerimientos de los usuarios y el logro de los objetivos estratégicos públicos y la seguridad de la información. (DFOE-PGAA-I-9-2008)

Un agravante de lo anterior, es la ausencia de un ejercicio de rectoría eficaz por parte del Poder Ejecutivo, lo que al mismo tiempo, no ha contribuido como un impulsor del proyecto de gobierno digital que promueve la actual Administración. (DFOE-PGAA-I-9-2008)

Los riesgos asociados con esta problemática podrían acentuarse, si en un entorno que no está debidamente controlado, se pretende desarrollar proyectos que incrementen la cantidad de procesos institucionales soportados en TI y que dan servicio a la ciudadanía. (DFOE-PGAA-I-9-2008)

En relación con la consulta realizada a las auditorías internas sobre su capacidad para realizar estudios enfocados en el tema de las tecnologías de información y comunicación, se determinó que de las 178 auditorías que brindaron la información, el 81% (145 auditorías) carece de una unidad de auditoría de TI que le permita realizar estudios de esa naturaleza, contra un 19% (33 auditorías) que manifestaron sí tener una unidad de ese tipo.

> Ante este panorama es de vital importancia que la Contraloría General de República dentro de la planificación de los estudios de fiscalización posterior oriente recursos a realizar evaluaciones de esa naturaleza, máxime considerando que hoy en día la mayoría de los procesos que realizan las instituciones públicas están soportados en tecnologías de información. (DFOE-PGAA-IF-I-06-2010)

La conclusión del macro proyecto reveló, serias debilidades en el proceso de implementación de las normas técnicas para la gestión y el control de las tecnologías de información, y la conciencia del equipo ejecutor del proyecto de los riesgos que esa situación representaba; no obstante, llama la atención que no se interesó en permitir a este equipo seguir dando seguimiento a tan importante temática.

2.3. REVISIÓN DE LAS DISPOSICIONES Y SU ESTADO DE CUMPLIMIENTO ACTUAL

Como parte del diagnóstico del cumplimiento de las normas técnicas, para la gestión y el control de las tecnologías de información, se determinó relevante realizar una revisión del estado de cumplimiento actual de las disposiciones emitidas por el ente contralor, en los informes que fueron emitidos como parte del macro proyecto de tecnologías de información, anteriormente detallado.

La ejecución del macro proyecto de tecnologías de información, obtuvo como resultado la emisión de 38 informes que abordaron diferentes temas de TI en 32 diferentes instituciones. Tal y como se indicó antes, esos estudios fueron enfocados más que todo

en calidad de la información contenida en las bases de datos y seguridad de la información de esas instituciones.

La composición de los informes emitidos en el período 2008-2010 (ver Tabla 3: Informes Emitidos durante el macro proyecto de Tecnologías de Información) está dada de la siguiente forma: 8 informes para el año 2008, 10 informes para el 2009 y 19 informes en el año 2010, para un total de 38 informes en tres años, mediante los cuales se fiscalizaron 32 instituciones diferentes del sector público, dado que en algunos casos particulares, se emitió más de un informe sobre determinadas instituciones.

Tabla 3: Informes Emitidos durante el macro proyecto de Tecnologías de Información

#	Número de informe	Institución Fiscalizada
1.	DFOE-PGAA-22-2008	Poder Judicial
2.	DFOE-SAF-05-2008	Ministerio de Hacienda
3.	DFOE-SOC-28-2008	Ministerio de Educación Pública
4.	DFOE-SOC-29-2008	Caja Costarricense de Seguro Social
5.	DFOE-SM-4-2008	Municipalidad de San José
6.	DFOE-ED-18-2008	Instituto Costarricense de Acueductos y Alcantarillados
7.	DFOE-ED-21-2008	Empresa de Servicios Públicos de Heredia
8.	DFOE-OP-9-2008	Consejo Técnico de Aviación Civil y la Dirección General de Aviación Civil
9.	DFOE-OP-10-2008	Consejo Técnico de Aviación Civil y la Dirección General de Aviación Civil
#	**Número de informe**	**Institución Fiscalizada**
1.	DFOE-ED-IF-22-2009	Instituto Nacional de Seguros (INS)
2.	DFOE-ED-IF-77-2009	Áreas Administrativo-Financiera y de Costos de RECOPE
3.	DFOE-OP-IF-18-2009	Ministerio de Obras Públicas y Transportes (MOPT)
4.	DFOE-OP-IF-25-2009	Consejo de Seguridad Vial (COSEVI)
5.	DFOE-PGAA-10-2009	Poder Judicial
6.	DFOE-PGAA-IF-14-2009	Registro Nacional
7.	DFOE-SAF-06-2009	Sistema Integrado de Gestión de la Administración Financiera (SIGAF)
8.	DFOE-SM-IF-126-2009	Red de Conectividad Intermunicipal y Sistema Tributario Municipal (SITRIMU)
9.	DFOE-SOC-IF- 30-2009	Caja Costarricense de Seguro Social
10.	DFOE-SOC-IF- 124-2009	PANI
#	**Número de informe**	**Institución Fiscalizada**
1.	DFOE-ED-IF-20-2010	Instituto Costarricense de Electricidad
2.	DFOE-OP-IF-10-2010	Consejo de Seguridad Vial (COSEVI)
3.	DFOE-OP-IF-11-2010	Consejo de Seguridad Vial (COSEVI)

4.	DFOE-OP-IF-16-2010	Consejo de Transporte Público (CTP)
5.	DFOE-OP-IF-17-2010	Consejo de Transporte Público (CTP).
6.	DFOE-OP-IF-19-2010.	Consejo de Seguridad Vial (COSEVI)
7.	DFOE-PGAA-IF-13-2010	Dirección General de Migración y Extranjería
8.	DFOE-PGAA-IF-24-2010	Dirección General de Migración y Extranjería
9.	DFOE-PGAA-IF-29-2010	Ministerio de Ciencia y Tecnología
10.	DFOE-SAF-IF-11-2010	Ministerio de Hacienda
11.	DFOE-SM-IF-21-2010	Municipalidad de Desamparados
12.	DFOE-SM-IF-22-2010	Municipalidad de Talamanca
13.	DFOE-SM-IF-23-2010	Municipalidad de Siquirres
14.	DFOE-SM-IF-24-2010	Municipalidad de Sarapiquí
15.	DFOE-SM-IF-25-2010	Municipalidad de Guácimo
16.	DFOE-SM-IF-26-2010	Municipalidad de Cartago
17.	DFOE-SM-IF-27-2010	Municipalidad de Pococí
18.	DFOE-SOC-IF-69-2010	Ministerio de Educación Pública
19.	DFOE-SOC-IF-77-2010	Ministerio de Educación Pública

Fuente: Elaboración propia con base en los informes del macro proyecto.

Cabe destacar, que durante la vigencia de la normativa, el período definido entre los años 2008-2012, la Contraloría General de la República ha emitido una cantidad de 631 informes de fiscalización, de acuerdo con lo indicado por la DFOE, según la Tabla 4: Informes Emitidos por la Contraloría General de la República durante el 2008-2012:

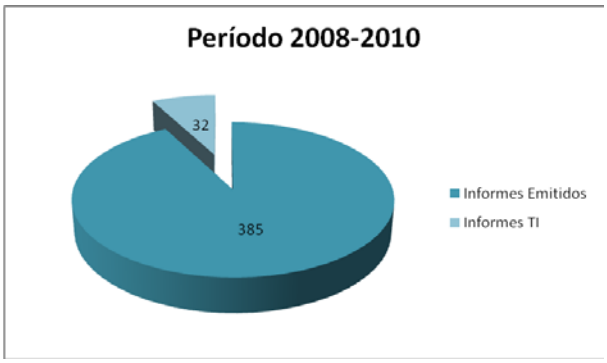
Tabla 4: Informes Emitidos por la Contraloría General de la República durante el 2008-2012

Informes de Fiscalización	
Año	**Cantidad**
2008	129
2009	125
2010	131
2011	121
2012	125
Total	631

Fuente: Equipo de Apoyo Gerencia DFOE efectuado con base en los Planes Operativos Anuales.

De acuerdo con la tabla anterior, para el período 2008-2010, duración del macro proyecto, la Contraloría General de la República emitió en total 385 informes, de los cuales 32 corresponden al tema de TI, el cual representa el 8% del total de estudios efectuados, tal y como se observa en la siguiente ilustración:

Ilustración 5: Informes de TI vs Informes de la Contraloría General de la República



Fuente: Elaboración propia con base en la información remitida por el Equipo de Apoyo Gerencia DFOE.

Como se indicó antes, el macro proyecto tuvo como parte de sus resultados, la generación de 38 informes (32 si se cuentan solo por institución), correspondientes al período 2008-2010. El análisis del cumplimiento de las disposiciones se enfocó en los años 2009 y 2010, debido a que estos corresponden al cambio de enfoque planteado por el generalizado incumplimiento e insuficiencia, en la implementación de las citadas normas técnicas, determinado entre los resultados del informe del año 2008.

De acuerdo con el sistema de información denominado "Seguimiento de Disposiciones", el cual está a cargo del Área de Seguimiento de Disposiciones de la Contraloría General de la República, todas las disposiciones emitidas mediante los informes de fiscalización del 2009 y 2010, se encuentran a marzo del 2013 en el estado denominado "Concluido". Cabe indicar, que algunas de ellas tienen como estado "Dejado sin Efecto", por lo cual, todas las disposiciones ya fueron acatadas por la administración, cuando correspondió.

2.4. REVISIÓN DE LOS INFORMES DE CONTRALORÍA GENERAL DE LA REPÚBLICA DEL 2011-2012

Debido a que el diagnóstico efectuado, por la Contraloría General de la República en el macro proyecto, evaluó a las instituciones durante el período comprendido entre el 2008 y el 2010, se definió como parte de este estudio, la realización de un diagnóstico para los años 2011 y 2012.

Con base en el período indicado, se detalló un listado de los informes emitidos por la Contraloría General de la República, en materia de tecnologías de información. De acuerdo con la revisión del cuerpo del informe, se determinó si estos tomaron en cuenta las normas técnicas para la gestión y el control de las tecnologías de información, al indicar si se hace referencia en ellos a dicha normativa.

La revisión efectuada permitió identificar 17 informes enfocados en el tema de las tecnologías de información. La tabla siguiente detalla el número de informe, nombre del informe, y en la columna denominada “Criterio” se establece un “SÍ”, cuando dentro del informe se utilizó como criterio, alguna de las normas técnicas para la gestión y el control de las tecnologías de información y “NO” en caso contrario.

Tabla 5: Informes Emitidos por la Contraloría General de la República durante el 2011-2012

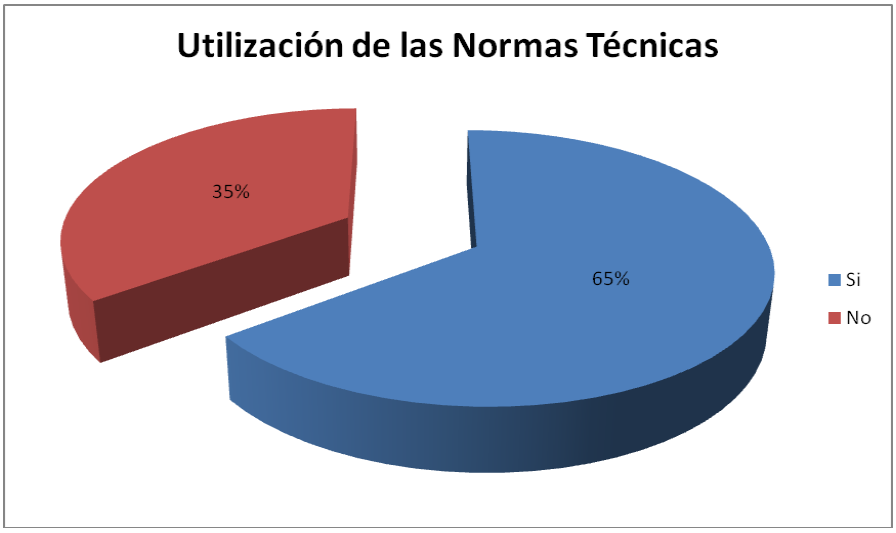
ÁREA	NÚMERO Y TÍTULO DEL INFORME		CRITERIO[2]
AE	1. DFOE-AE-0256-2011	Resultados del estudio efectuado sobre la calidad y seguridad de la información relevante operada por los sistemas de información automatizados y almacenada en las bases de datos del Servicio Nacional de Aguas Subterráneas, Riego y Avenamiento.	Sí
	2. DFOE-AE-IF-09-2012	Sobre la razonabilidad del avance en el suministro de información por parte de la Dirección de Geología y Minas del Ministerio de Ambiente, Energía y Telecomunicaciones para los planes reguladores cantonales.	No Aplica
DL	3. DFOE-DL-IF-13-2012	Debilidades en la calidad de la información relevante contenida en la base de datos para el cobro de los tributos en la Municipalidad de Heredia.	Sí
	4. DFOE-DL-IF-14-2012	Debilidades en la calidad de la información relevante contenida en la base de datos para el cobro de los tributos en la Municipalidad de San Carlos.	Sí
	5. DFOE-DL-IF-15-2012	Informe acerca del sistema contable de la Municipalidad de León Cortés.	No Aplica
	6. DFOE-DL-IF-24-2011	Estado de los sistemas contables en 60 gobiernos locales.	No Aplica
	7. DFOE-DL-IF-35-2011	Sobre las tecnologías de información en el sector municipal	Sí
EC	8. DFOE-EC-0297-2011	Sobre los resultados del estudio efectuado en el Instituto Nacional de Vivienda y Urbanismo (INVU), relacionado con la implementación de las Normas de Gestión y Control de las Tecnologías de Información.	Sí
	9. DFOE-EC-IF-08-2012	Sobre el plan de continuidad de los sistemas de información que soportan las actividades sustantivas del Instituto Nacional de Aprendizaje (INA).	Sí
	10. DFOE-EC-IF-10-2011	Sobre los resultados del estudio efectuado en el INVU relacionado con la gestión de tecnologías de información.	Sí
	11. DFOE-EC-IF-15-2011	Sobre la gestión de las tecnologías de información efectuada en el Banco Hipotecario de la Vivienda.	Sí
IFR	12. DFOE-IFR-0365-2011	Sobre los resultados del estudio relacionado con el cumplimiento por parte del Instituto Costarricense de Electricidad de la normativa sobre tecnologías de información, N° N-2-2007-CO-DFOE.	Sí
	13. DFOE-IFR-IF-5-2012	Sobre las iniciativas que impulsan el desarrollo del gobierno digital y de una sociedad basada en la información y el conocimiento en Costa Rica.	Sí
PG	14. DFOE-PG-IF-05-2011	Sobre la evaluación de los sistemas de información en la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE).	Sí
	15. DFOE-PG-IF-20-2012	Sobre la evaluación de la plataforma de información policial a cargo del Poder Judicial.	No
SOC	16. DFOE-SOC-IF-02-2011	Sobre la utilización del equipo alquilado por el MEP en el desarrollo del proyecto MEP- Digital.	Sí
	17. DFOE-SOC-IF-12-2011	Sobre un sistema de información único de beneficiarios y población objetivo para los programas sociales selectivos.	No

Fuente: Elaboración propia con base en los resultados de la búsqueda efectuada en el sitio Web de la Contraloría General de la República, fecha 08 de abril del 2013.

[2] Utilización de las normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) como criterio.

De la tabla anterior, sobre los informes emitidos por la Contraloría General de la República durante el 2011-2012, se desprende que la utilización de las normas técnicas para la gestión y el control de las tecnologías de información, se está dando en una relación del 65% del total de informes emitidos, sobre el uso de las tecnologías de información en las instituciones fiscalizadas.

Ilustración 6: Informes Emitidos por la Contraloría General de la República durante el 2011-2012



Fuente: Elaboración propia con base en los resultados detallados en
Tabla 5: Informes Emitidos por la Contraloría General de la República durante el 2011-2012

Como se puede observar, las respuestas afirmativas corresponden al 65%. No obstante, los informes emitidos que forman el 35% restante, los cuales no mencionan como criterio la citada norma técnica, corresponden a estudios que tienen relación con las tecnologías de información de forma transversal, o bien, se refieren a estudios de sistemas de información, no automatizados en las instituciones.

2.5. NUEVAS TENDENCIAS EN EL MUNDO DE LAS TECNOLOGÍAS DE INFORMACIÓN

La revisión de las normas técnicas para la gestión y el control de las tecnologías de información y su proceso de implementación y seguimiento, se complementa en función del mejoramiento continuo, que la Contraloría General de la República pretende en su gestión; por tanto, surge la necesidad de determinar, si el esquema normativo actual mantiene su vigencia después de seis años de haber sido emitido, en particular por tratarse de una temática tendente al cambio día con día.

De acuerdo con lo anterior, se realizó una investigación respecto a cuáles son las nuevas tendencias en el mundo informático, a fin de conocerlas brevemente, y con base en ello emitir un criterio, en cuanto a si las citadas normas técnicas permiten su gestión y evaluación.

Entre estas tendencias, se tomaron en cuenta las siguientes, para el análisis e investigación efectuados:

- *BYOD*
- *Big data*
- Computación en la nube
- Virtualización
- Inteligencia de negocios
- Computación móvil
- Firma digital
- Calidad de los datos
- Redes sociales

2.5.1. *BRING YOUR OWN DEVICE (BYOD)* [3]

Es una estrategia alternativa, que permite a los empleados, socios de negocio y otros usuarios, utilizar dispositivos seleccionados y comprados por ellos mismos, para ejecutar aplicaciones y acceso a información dentro de la empresa. Normalmente teléfonos inteligentes, tabletas, en algunos casos computadoras y en otros, se aplican subsidios para la compra de estas.

Esta tendencia se está extendiendo a empresas de todos los tamaños. Los empleados utilizan sus propios dispositivos en el trabajo; sobre todo en Estados Unidos, disponen de un monto cada cierto tiempo, para la compra del equipo que más les guste, con la idea de que quien trabaja a gusto, trabaja mejor.

Al respecto, los administradores de los departamentos de tecnologías de información, no parecen contentos, ya que se complica la función de dar soporte a dispositivos variados sobre los que no tienen control, pero que se conectan a las redes empresariales, suponiendo un riesgo para la seguridad.

Gartner, empresa consultora especializada en Tecnología Informática, encuesta a 938 empresas de todo el mundo con más de 500 empleados, en la cual se demuestra que el *BYOD* es la principal preocupación de los directores de tecnologías de información.

Al respecto, no se cuenta con datos sobre políticas relacionadas. De acuerdo con el porcentaje de respuestas afirmativas respecto al uso de *BYOD*, solo se indica que en “la

[3] http://www.gartner.com/newsroom/id/2136615

mayoría" de las empresas ofrecen soporte para dispositivos personales, los cuales consisten en: el 32% de terminales móviles, el 37% de tabletas y el 44% de dispositivos portátiles.

2.5.2. BIG DATA [4]

Big data es el nombre dado al manejo de grandes y variados volúmenes de información a altas velocidades, conjuntos de datos que demandan conceptos de efectividad y rentabilidad en su manejo, adicionado a la búsqueda de formas innovadoras para mejorar su comprensión, el conocimiento y la toma de decisiones.

El manejo de grandes cantidades de datos, de una manera eficiente, implica una serie de aspectos para propiciar el entorno de su adecuado manejo, como lo son la captura de paquetes de red, sensores, distintos tipos de operaciones, monitoreo de cumplimiento y de inteligencia para detectar amenazas, situación que en la actualidad puede resultar en un hueco de la seguridad informática. A su vez la planificación de las empresas alrededor de este tema debe ser orientada a investigar o analizar el giro de negocio, y las posibilidades y probabilidades de llegar a manejar un tema de *big data*.

2.5.3. COMPUTACIÓN EN LA NUBE

De acuerdo con el *National Institute of Standards and Technology (NIST) y la Cloud Security Alliance*, la computación en la nube se define como un modelo para habilitar un cómodo acceso en red, por demanda a un *pool* compartido de recursos informáticos

[4] http://www.gartner.com/it-glossary/big-data/

configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se puede conformar y proveer rápidamente, con un esfuerzo administrativo mínimo, o una interacción mínima con el proveedor de servicios.

Otra manera de describir los servicios ofrecidos en la nube, es comparándolos con los de una empresa de servicios públicos. Tal como las empresas pagan por la electricidad, el gas y el agua que utilizan, ahora tienen la opción de pagar por los servicios de TI dependiendo del consumo. Esta tendencia se alinea con tres modelos de implementación (ver Tabla 6: Modelos de Servicio de la Computación en la Nube):

Tabla 6: Modelos de Servicio de la Computación en la Nube

Modelo de Servicio	Descripción
Infraestructura como un servicio (*IaaS*)	Capacidad para configurar procesamiento, almacenamiento, redes y otros recursos de computación fundamentales, ofreciendo al cliente la posibilidad de implementar y ejecutar *software* arbitrario, el cual puede incluir sistemas operativos y aplicaciones. *IaaS* coloca estas operaciones de TI en las manos de un tercero.
Plataforma como un servicio (*PaaS*)	Capacidad para implementar en la infraestructura de la nube aplicaciones creadas o adquiridas por el cliente que se hayan creado, utilizando lenguajes y herramientas de programación respaldados por el proveedor.
***Software* como un servicio (*SaaS*)**	Capacidad para utilizar las aplicaciones del proveedor que se ejecutan en la infraestructura de la nube. Se puede acceder a las aplicaciones desde diferentes dispositivos cliente a través de una interfaz de cliente ligero (*thin client*), como un explorador web (por ejemplo, correo electrónico basado en la web).

Fuente: Elaboración propia con base en el artículo.

La computación en la nube produce riesgos asociados, al igual que todas las tendencias en tecnologías. En este caso, no son precisamente nuevos o atinentes sólo a este método; por ende, implica también gestionar el servicio de forma planificada, asegurando así que la información se mantenga tanto disponible como segura; es posible que los gerentes de seguridad de la información, deban ajustar las políticas y los procedimientos de sus empresas, para satisfacer las necesidades del negocio.

Algunos de los riesgos que plantea la computación en la nube, para la empresa, fueron identificados por ISACA (*Information Systems Audit and Control Association*) en su artículo "Computación en la nube: Beneficios de negocio con perspectivas de seguridad, gobierno y aseguramiento" y se enlistan a continuación:

- **Selección del proveedor:** Las empresas deben ser específicas al seleccionar un proveedor. La reputación, los antecedentes y la sostenibilidad son factores que se deben tomar en consideración. La sostenibilidad es particularmente importante para garantizar que los servicios estarán disponibles y los datos se podrán rastrear.

- **Establecimiento de acuerdos de nivel de servicios:** Con frecuencia, el proveedor de la nube asume la responsabilidad de manejar la información, lo cual constituye una parte crítica del negocio. No actuar de conformidad con los niveles de servicio acordados puede perjudicar, no sólo la confidencialidad, sino también la disponibilidad, lo que afecta enormemente las operaciones del negocio.

- **Recuperación de la información:** La naturaleza dinámica podría resultar confusa, en cuanto a dónde reside la información realmente. Cuando se requiere la recuperación de la información, es posible que haya demoras.

- **Protección de la confidencialidad de la información:** El acceso por parte de terceros, a información sensitiva, crea el riesgo de comprometer la confidencialidad de la información. En la computación en la nube, esto pudiera

representar una amenaza significativa a la hora de asegurar la protección de la propiedad intelectual (*IP*) y los secretos comerciales.

- **Disponibilidad de la información:** Las nubes públicas permiten desarrollar sistemas de alta disponibilidad en niveles de servicio que, con frecuencia, son imposibles de crear en redes privadas, a no ser a un costo extremadamente alto. El aspecto negativo de esta disponibilidad es que es posible mezclar los activos de información con los de otros clientes de la nube, incluso de competidores. Cumplir con las regulaciones y leyes de diferentes regiones geográficas puede ser desafiante para las empresas. En estos momentos, es muy limitado el precedente relacionado con la confiabilidad en la nube. Es necesario obtener asesoría legal apropiada para asegurar que el contrato especifique las áreas donde el proveedor de la red es responsable legal y financieramente por las ramificaciones resultantes de problemas potenciales.

- **Continuidad del negocio y recuperación:** Debido a la naturaleza dinámica de la nube, es posible que la información no se localice inmediatamente si ocurriera un desastre. Los planes de continuidad del negocio y de recuperación en caso de desastre deben estar bien documentados y probados. El proveedor de la nube debe entender la función que desempeña en términos de copias de respaldo, respuesta y recuperación en caso de desastre. Los tiempos objetivos de recuperación deben estar especificados en el contrato.

2.5.4. VIRTUALIZACIÓN

ISACA define la virtualización como la representación de algo en forma virtual (en lugar de real). En la tecnología de información empresarial (TI), la virtualización altera la arquitectura técnica, porque permite la ejecución de diferentes recursos en un entorno único (o de varias capas). En general, convierte un elemento de *hardware* en el *host* de muchos otros elementos y en consecuencia, con el tiempo obtiene el potencial para reducir los gastos de capital de la empresa, los costos de administración y otros costos financieros.

Además, establece que este procedimiento conlleva una serie de beneficios asociados a reducción de costos, automatización, flexibilidad, agilidad, equilibrio en las cargas de trabajo, simplificación, sostenibilidad y uso de espacio entre otras. Resumiendo, se pueden mencionar cinco razones para realizarlo:

Ilustración 7: Beneficios de Virtualizar

Figura 1—Cinco razones para virtualizar	
Resultado	**Cómo se logra**
1. Reduce la complejidad de la TI.	Las aplicaciones y sus sistemas operativos se encapsulan en máquinas virtuales que son definidas mediante software, lo cual facilita su disposición y administración.
2. Permite la estandarización.	Dado que las aplicaciones se desacoplan del hardware, el centro de datos puede converger en una serie más limitada de dispositivos de hardware.
3. Aumenta la agilidad.	Las aplicaciones y máquinas virtuales pueden copiarse y trasladarse en tiempo real, y en la nube, en respuesta a las condiciones variables del negocio.
4. Aumenta la rentabilidad.	La máquinas virtuales se pueden trasladar fácilmente para consumir capacidad de reserva dondequiera que exista, por lo que genera más trabajo con menos hardware.
5. Facilita la automatización.	Se puede proveer y orquestar fácilmente la infraestructura virtual mediante procesos ejecutados por software, especialmente cuando se estandariza el hardware subyacente.

Fuente: Virtualización: Beneficios y desafíos, (ISC)² de *ISACA*, 2010.

No obstante, el artículo analizado es claro en indicar los riesgos y problemas de seguridad asociados con la virtualización:

- Ataques a la infraestructura de virtualización.
- Ataques a las características de virtualización.
- Cumplimiento y desafíos en la administración.

De estos riesgos, llaman la atención los tipos de ataques informáticos a la información o a la estructura de las organizaciones, que pongan sus servicios en la nube, entre estos:

- *Hyperjacking* es un método para inyectar un hipervisor fraudulento (también llamado monitor de máquina virtual [VMM]) en una infraestructura legítima (VMM u sistema operativo) con control sobre todas las interacciones entre el sistema atacado y el *hardware*.

- VM *jumping* o *guest-hopping* es una posibilidad más realista y plantea una amenaza grave. Por lo general, este método de ataque explota las vulnerabilidades en los hipervisores, que permiten que *malware* o ataques remotos pongan en peligro las protecciones de separación de las máquinas virtuales y obtengan acceso a otras máquinas virtuales, *hosts* o, incluso, el mismo hipervisor.

2.5.5. INTELIGENCIA DE NEGOCIOS BI[5]

Este término incluye diferentes aspectos entre ellos aplicaciones, infraestructura, herramientas y mejores prácticas que den acceso a la información del negocio, permitiendo su análisis para mejorar y optimizar las decisiones y el desempeño.

[5] http://www.gartner.com/it-glossary/business-intelligence-bi/

Es un método para almacenar y presentar datos claves de la empresa, para que cualquier persona en su empresa pueda hacer preguntas de forma rápida y fácil sobre los datos precisos y oportunos. BI permite al usuario final, utilizar los datos para entender por qué su empresa obtuvo los resultados particulares logrados, a fin de decidir cursos de acción basándose en los datos del pasado, y así pronosticar con precisión los resultados futuros.

Los datos alineados con el BI, se muestran de una manera apropiada para cada tipo de usuario, es decir, los analistas podrán profundizar en datos detallados, los ejecutivos ver resúmenes oportunos y mandos intermedios verán los datos presentados en el nivel de detalle que necesitan, para tomar buenas decisiones de negocios. *Microsoft* identifica una serie de problemáticas asociadas a la implementación de BI en una empresa o institución entre ellas:

- Aumento en el tiempo que tardan las consultas de los sistemas asociados.
- Retrasos en los sistemas.
- Fuente de datos dispares.
- Reportes de datos inconsistentes o inválidos.
- Este tipo de data, no está disponible para todo tipo de usuario.
- Cantidad de datos excesiva.

2.5.6. COMPUTACIÓN MÓVIL (DISPOSITIVOS PORTÁTILES)

Los dispositivos móviles están cambiando el panorama de los negocios. A medida que las empresas optan por las operaciones de negocios globales, estos dispositivos, se han convertido en parte indispensable del negocio. Los dispositivos móviles ofrecen a las empresas la capacidad de mantener a sus empleados conectados en todo momento, lo que ha permitido al público la posibilidad de llevar a cabo negocios en cualquier lugar, ya sea en casa, en la oficina, o viajando entre destinos.

"Los dispositivos móviles" pueden ser muy diferentes, a continuación se mencionan algunos, de manera general:

- Teléfonos móviles con funcionalidad o "*Smartphone*".
- *Laptops* y *Net books.*
- Ordenadores tipo "*TABLET*".
- Portátil tipo Asistente digital personal (*PDA*).
- *Portable Universal Serial Bus (USB)* para el almacenamiento (por ejemplo, "*thumb drives*" y dispositivos *MP3*), además los enfocados en conectividad (tales como *Wi-Fi*, *Bluetooth* y *HSDPA* / *UMTS* / *EDGE* / *GPRS* tarjetas de módem).
- Cámaras digitales.
- Identificación por radiofrecuencia (*RFID*) y *RFID* móvil (*M-RFID*) que utilizan para el almacenamiento de datos, identificación y activo manejo.
- Infrarrojos (*IrDA* habilitados); dispositivos tales como impresoras y tarjetas inteligentes.

Los beneficios asociados a la aplicación de la tendencia sobre el uso de dispositivos portátiles, conlleva una serie de beneficios ya identificados, entre los que destacan los siguientes:

- Aumento de la productividad laboral.
- Mejor servicio al cliente.
- La respuesta a los problemas del cliente o preguntas en cualquier momento.
- La mejora de los tiempos de respuesta para la resolución de problemas.
- El aumento de la eficiencia del proceso de negocio.
- Empleado de seguridad y protección.
- Retención de empleados.

A su vez, el despliegue de dispositivos móviles puede presentar una serie de amenazas para la seguridad global de la empresa. Los dispositivos móviles presentan numerosas vulnerabilidades, ya que son susceptibles a ataques maliciosos, incluyendo amenazas internas y externas.

Irónicamente, muchos de los riesgos asociados surgen como consecuencia de su mayor ventaja: la portabilidad. Dispositivos móviles de datos de transporte a través de redes inalámbricas, que normalmente son menos seguras que las redes cableadas. El dispositivo móvil basa su portabilidad en las redes inalámbricas, las cuales manejan la información en un medio susceptible de intercepción. Adicionalmente, tienen capacidad de almacenamiento y los datos no permiten su cifrado; por lo tanto, la información que transmiten o guardan, puede comprometerse en cuanto a su confidencialidad o propiedad, debido al robo o pérdida del dispositivo.

Además de la pérdida de datos, los dispositivos móviles implican la amenaza de introducir *malware*[6]. Los mismos dispositivos se pueden utilizar como una plataforma para la actividad maliciosa. Los dispositivos y ordenadores portátiles con micrófonos y cámaras son particularmente vulnerables, ya que se puede activar fácilmente el uso de herramientas disponibles para el público, que puede resultar en la propagación de *malware*, pérdida de datos y espionaje. Del mismo modo, Celular IP y Voz sobre- (*VoIP*) también muestran vulnerabilidades que pueden ser explotadas fácilmente, dando lugar a las llamadas interceptadas.

Tabla 7: Vulnerabilidades, Amenazas y Riesgos de la Computación Móvil

Vulnerabilidades	Amenazas	Riesgos
La información viaja a través de las redes inalámbricas que normalmente son menos seguras que las alámbricas.	Extraños maliciosos pueden hacer daño a la empresa.	La interceptación de información puede resultar en una brecha en cuanto a información sensible, reputación, cumplimiento a regulaciones, temas legales.
La movilidad ofrece a los usuarios la oportunidad de abandonar los límites de la empresa y por lo tanto elimina muchos controles de seguridad.	Los dispositivos móviles cruzan las fronteras y la red, los perímetros cargando *malware*, y pueden aportar ese *malware* a la red de la empresa.	Propagación de *malware*, lo que puede resultar en la pérdida de datos, corrupción de datos y la falta de disponibilidad de los datos necesarios
La tecnología *Bluetooth* es conveniente para tener conversaciones a manos libres, sin embargo, comúnmente se deja encendido siendo así fácil de detectar.	Los *hackers* pueden descubrir el dispositivo y ejecutar un ataque.	Corrupción del dispositivo, pérdida de datos, interceptación de llamadas, y la posible exposición de información sensible

[6] Similar a virus, incluyen registradores de teclas y analizadores de sistemas, que recolectan información potencialmente delicada, como números de tarjeta de crédito, detalles bancarios, etcétera, del anfitrión (*host*) y transmite la información al originador cuando se detecta una conexión en línea.

Se almacena información en el dispositivo, que no está cifrada.	En el caso de que un intruso malicioso intercepta los datos en tránsito o se roba un dispositivo, o si el empleado pierde el dispositivo, los datos son legibles y utilizables.	Exposición de datos sensibles, lo que resulta en daño a la empresa, clientes o empleados
La pérdida de datos puede afectar la productividad del empleado.	Los dispositivos móviles, puede perderse o ser robados debido a su portabilidad. Los datos sobre estos dispositivos no son siempre copia de seguridad	Los trabajadores que dependen de dispositivos móviles no pueden trabajar en el caso de los dispositivos descompuestos, perdidos o robados, en especial si los datos no están respaldados.
El dispositivo no tiene requisitos de autenticación.	Cuando el dispositivo se pierde o es robado, extraños a la empresa pueden acceder a este y a todos sus datos.	Exposición de datos, resulta en daño a la empresa y a cuestiones de responsabilidad y cumplimiento de las regulaciones
La empresa no administra el dispositivo.	Si no existe una estrategia para el manejo de dispositivos móviles, los empleados pueden optar por llevar sus propios recursos. Aunque estos dispositivos no pueden conectarse a la red privada virtual (*VPN*), pueden interactuar con el correo electrónico o almacenar documentos confidenciales	Fuga de datos, propagación de *malware*, pérdida de datos, en el caso de pérdida o robo del dispositivo
El dispositivo permite la instalación de aplicaciones que podrían no ser seguras	Las aplicaciones pueden transportar *malware*, que propaga troyanos o virus y también pueden transformar al dispositivo en una puerta de entrada para los extraños maliciosos que pretenden acceder al red de la empresa.	Propagación de *malware*, fuga de datos, intrusión en red de la empresa

Fuente: *Securing Mobile Devices, ISACA* 2010.

2.5.7. FIRMA DIGITAL[7]

En Costa Rica, el sitio "Sistema Nacional de Certificación Digital" define la firma digital como el método que asocia la identidad de una persona o equipo, con un mensaje o documento electrónico, para asegurar la autoría y la integridad de este. La firma digital del documento es el resultado, de aplicar algoritmos matemáticos (denominados función *hash*) a su contenido, a fin de generar su identificación. Para verificar la firma, se requiere validar la vigencia del certificado digital del firmante, el estado de este (pues podría estar revocado) y que el uso pretendido sea el conveniente para la operación que se realiza (firma y no repudio).

Esta misma página indica que para firmar un documento, se requiere de un certificado digital emitido por una autoridad certificadora registrada, el cual debe ser almacenado y custodiado en un dispositivo (*Token* o tarjetas inteligentes -*smart cards*-) que cumpla con el estándar *FIPS* 140 nivel 2. Este dispositivo es muy importante ya que es el responsable de custodiar un secreto único (llave privada), que es utilizado para firmar digitalmente los documentos o archivos.

El dispositivo requiere además los datos de activación, los cuales pueden ser una palabra de paso, una frase clave o información biométrica (huella digital).

[7] http://www.firmadigital.go.cr/

La firma digital cumple una doble autenticación y se basa en el principio de que el usuario se debe autenticar dos veces, primero con algo que sabe (la palabra o frase clave) y posteriormente, con algo que tiene (la llave privada almacenada en el dispositivo criptográfico).

Finalmente, para firmar un documento con relevancia jurídica, se requiere de un servicio de validación en línea que indique la situación del certificado, con el objetivo de no permitir que se tramiten documentos firmados digitalmente, con un certificado revocado o suspendido; asimismo, se debe validar toda la cadena de confianza que respalda a la autoridad certificadora que emitió el certificado.

Las buenas prácticas en materia de firma digital aconsejan:

- Nunca revele el código de activación.
- Utilice contraseñas, para la clave o pin, difíciles de deducir en el código de activación.
- Cambie periódicamente las contraseñas.
- No entregue su dispositivo criptográfico a ningún desconocido.
- Esté atento a la fecha de expiración: el certificado digital emitido por la autoridad certificadora está sujeto a una fecha de vencimiento, por lo cual, se debe cumplir con la precaución de renovarlo antes de esta fecha, para evitar problemas con su uso.
- Reporte problemas o incidentes de seguridad.
- Reporte inmediatamente la pérdida, hurto o robo del dispositivo criptográfico.
- Utilice antivirus actualizado.

2.5.8. CALIDAD DE LOS DATOS

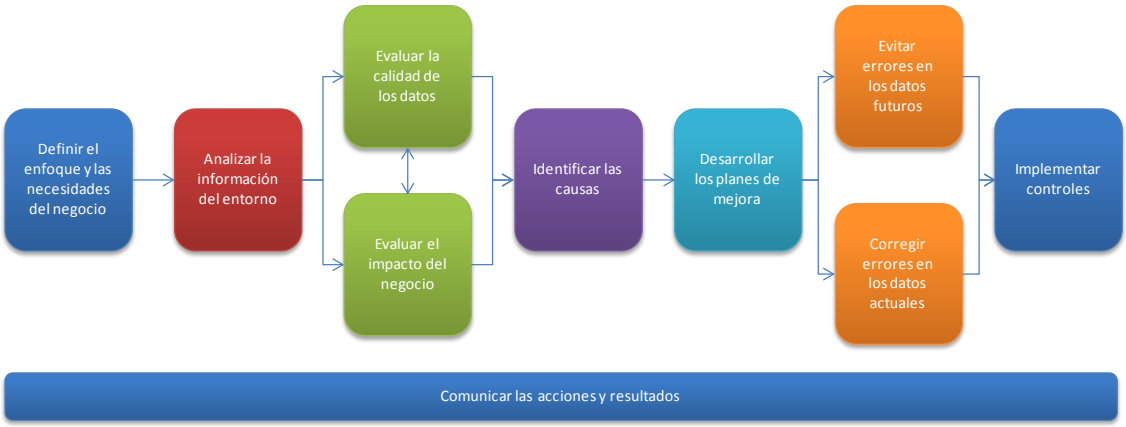
En la actualidad, el manejo de la información marca la tendencia de las organizaciones, y requiere que cada negocio establezca su estrategia al respecto. El gran desafío por el que deben atravesar, consiste en comprender que para integrar los datos provenientes de múltiples fuentes, no se depende únicamente de la tecnología, o de los métodos de calidad, metas altas, o gestión de la información empresarial, sino que el tema gira en torno a la gente; pensar que la adquisición de herramientas o la creación de centros de datos centralizados son los primeros pasos en la gestión de la información, ha venido siendo un error, dado que el primer paso realmente es, comprender la relación que existe entre los individuos y la información.

En ausencia de un modelo de información formal, la tendencia es que los individuos adquieran una extraña propiedad de los datos, el cual a menudo impide que las mejoras se realicen. La calidad de la información contribuye y resulta ventajosa, al ofrecer la información correcta en el momento oportuno, en el lugar correcto, a la gente adecuada, dado que no es posible tomar decisiones de negocio efectivas con datos erróneos, incompletos o engañosos. Se necesita información confiable y actualizada, en pro del logro de los objetivos de negocio.

Es recomendable implementar la calidad de los datos empresariales, estableciendo un proyecto que se enfoque en lograrlo. Al respecto, Danette McGilvray establece una serie de pasos[8] para lograrlo, la cual se describe en la imagen siguiente:

[8] Copyright © 2005–2008 Danette McGilvray, Granite Falls Consulting, Inc.

Ilustración 8: Ciclo para el Mejoramiento de la Calidad de los Datos y la Información Empresarial



Fuente: Elaboración propia con base en la Figura 2.13 del documento denominado "*The Information and Data Quality Improvement Cycle and The Ten Steps process*". Página 64.

Los datos empresariales de pobre calidad, producen un impacto visible en las organizaciones y en su gestión. Al respecto, un estudio del *Knowledge Integrity*[9], Inc., menciona los siguientes:

- Financieros (pérdida del costo de oportunidad, identificación de clientes meta, generar valor al asociar a maestros de clientes, tiempo y costo que implican la limpieza y corrección de datos, mediciones del desempeño de los empleados, imposibilidad de detectar proveedores y realizar análisis de gastos).

[9] Desde 1999, el Knowledge Integrity Inc., ha desarrollado metodologías técnicas y de gestión para instituir la calidad de datos, gestión de datos maestros, normas de datos y los programas de gobierno de datos, dentro de las organizaciones para permitir el análisis, la evaluación y mejora de calidad de los datos de los sistemas transaccionales, inteligencia de negocios, operativos y propósitos de información.

- Confianza (facilidad de uso para el personal, facilitar la interacción con el cliente, incapacidad de proporcionar a los clientes factura unificada, deterioros en la toma de decisiones).
- Productividad (disminución de la capacidad de procesamiento directo a través de los servicios automatizados).
- Riesgo / Cumplimiento (evaluaciones de riesgos incorrectas debido a la imposibilidad de acceder a un historial de información completo, toma de decisiones incorrecta al basarse en información incompleta o inexacta.

2.5.9. REDES SOCIALES

Las recomendaciones de no utilizar los medios de comunicación social en la empresa, conforme ha pasado el tiempo, se han quedado atrás. Actualmente, las empresas saben que el uso de medios sociales ya no es la excepción, sino la regla. Las unidades de negocio, tales como investigación, desarrollo, mercadeo, recursos humanos, ventas y servicio al cliente ven el potencial, del uso de herramientas de medios sociales para estimular la innovación, crear reconocimiento de marca, contratar y retener a los empleados, generar ingresos y mejorar la satisfacción del cliente.

Esta tendencia consiste en la creación y difusión de contenidos a través de redes sociales, por medio de Internet. Las diferencias entre los medios tradicionales y sociales se definen, por el nivel de interacción a disposición del consumidor. El uso de las redes sociales ha creado plataformas de comunicación muy eficaces, donde cualquier usuario, en cualquier parte del mundo, puede libremente crear contenidos y difundir esa información en tiempo real, a una audiencia global.

Los riesgos asociados a esta tendencia se detallan a continuación:

- La introducción de virus y *malware* a la red de la organización.
- La exposición a los clientes y la empresa a través de una presencia corporativa fraudulenta o bajo secuestro.
- Ausencia o poca claridad en la definición de los derechos de contenido de la información publicada en los sitios de medios sociales.
- El cambio a un modelo de negocio digital puede aumentar las expectativas de servicio al cliente; por lo tanto, si el cliente no queda satisfecho, puede dañar la reputación de la empresa, lo cual influirá en la dificultad de mantener esos clientes.
- Una gestión deficiente de las comunicaciones electrónicas puede hacer, que la empresa sea objeto de sanciones debido a las regulaciones.

De acuerdo con lo analizado en esta sección, existen nuevas tendencias en las tecnologías de información que podrían, actualmente o en un futuro cercano, estarse utilizando en el sector público; iniciativas como *BYOD*, en función de utilizar dispositivos propios de los funcionarios en la gestión profesional que realizan en la institución, son técnicas aplicables en la actualidad. A su vez, los altos volúmenes de información, que se manejan en el sector público, son susceptibles de empezar a ser analizados y gestionados desde la visión del *big data*. Por lo tanto, en muchos de esos casos las normas técnicas de la Contraloría General de la República, podrían resultar débiles para la regulación y control en las instituciones fiscalizadas.

3. CAPÍTULO III

3.1. RELACIÓN DE LA NORMA CON OTRAS INSTANCIAS DE CONTROL

Cuando se habla sobre el papel de las tecnologías de información en las empresas e instituciones en la actualidad, se tiende asociar con las actividades cotidianas de la relaciones entre los usuarios y los sistemas, lo que plantea una inadecuada comprensión de la verdadera función de este componente, en la realización y consecución de los objetivos de negocio trazados, y dificulta la justificación de las inversiones en tecnologías de información.

La evolución en este tema sugiere, concentrar los esfuerzos de las organizaciones, en la realización de actividades de planificación, diseño, implementación y concienciación; pero a la vez, la alta gerencia, debe lograr una interpretación positiva del riesgo tecnológico, en función de administrar adecuadamente dicho riesgo y lograr que esta visión agregue valor al negocio.

3.2. ¿QUÉ SE HACE EN PAÍSES COMO CHILE Y VENEZUELA?

De acuerdo con lo anterior, y con el objetivo de proponer mejoras a las normas técnicas para la gestión y el control de las tecnologías de información, se requiere conocer cómo se regula esta actividad en otros países, a fin de conocer el camino que han recorrido, cómo organizan la normativa al respecto y qué se está normando. Cabe destacar, que no se valora en este apartado, el cumplimiento de lo establecido en su normativa actual, dado que ello corresponde a los órganos fiscalizadores de los dos países involucrados.

Los avances sin precedentes del conocimiento tecnológico, en los últimos siglos, continúan incrementándose, con aportes en la mejora de la calidad de vida y profundas implicaciones en las economías mundiales, en las formas de hacer negocios y el modo de ejecutar las tareas diarias de cada profesión.

El reporte anual denominado "*The Global Information Technology Report 2013*", difundido por el Foro Económico Mundial (*The World Economic Forum)*, sugiere que las políticas de algunas economías en desarrollo aún no están logrando traducir las inversiones realizadas en TIC, en beneficios tangibles en términos de competitividad, desarrollo y empleo.

El citado reporte menciona que Chile obtuvo el puesto 34, lo cual lo clasifica como uno de los países latinoamericanos que presenta mejoría en el "*ranking*" cada año. Por su parte, Venezuela, en el puesto 108, contrariamente ha venido decayendo en sus resultados con base en el posicionamiento, establecido por dicho reporte. En relación con Latinoamérica en general el informe establece:

> Aunque varios países de América Latina y el Caribe colocan importantes mejoras o consolidan sus logros en la preparación tecnológica, la región en su conjunto sigue detrás de las mejores prácticas internacionales en el aprovechamiento de los avances de las TIC. (World Economic Forum, 2013)

3.2.1. NORMATIVA BANCARIA EN VENEZUELA

La investigación efectuada, contempló la revisión del sitio web de la Contraloría de la República de Venezuela, con el fin de conocer cómo está constituida y qué relación tiene con la gestión de las tecnologías de información de Venezuela. Al respecto, se detalla la definición de misión y visión institucional, según se publica en su sitio:

> Misión: La Contraloría General de la República es el órgano constitucionalmente autónomo, integrante del Poder Ciudadano y rector del Sistema Nacional de Control Fiscal, al servicio del Estado y del pueblo venezolano para velar por la buena gestión y el correcto uso del patrimonio público. (Venezuela)

> Visión: Ser reconocida como la institución pública de más alto desempeño ético y profesional, que goce de la confianza, credibilidad y apoyo del pueblo venezolano, por la efectividad y transparencia de sus acciones en la salvaguarda del patrimonio público y en el combate a la corrupción. (Venezuela)

La revisión del sitio Web de la Contraloría Venezolana no permitió identificar, si este órgano emite normas enfocadas en el tema de las tecnologías de información. Como parte de las indagaciones, se observó que existe el Centro Nacional de Tecnologías de Información (CNTI), adscrita al Ministerio del Poder Popular para Ciencia, Tecnología e Innovación (MCTI), el cual en su misión y visión establece:

> Misión: El CNTI es una institución adscrita al Ministerio del Poder Popular para Ciencia, Tecnología e Innovación (MCTI) que tiene como razón de ser potenciar los esfuerzos que en materia de informática se desarrollen en el sector gobierno y en las comunidades organizadas, con el fin de contribuir con la eficiencia y efectividad del Estado, así como impulsar el desarrollo y fortalecimiento de la capacidad nacional del sector de las Tecnologías de Información. (CNTI)
>
> Visión: Consolidar un sistema de Tecnologías de Información del Estado, que apoye la gestión de la Administración Pública, a la comunidad organizada y al ciudadano; y haber contribuido a la creación de una fuerte industria nacional de *software*, todo ello en concordancia con los principios de soberanía. (CNTI)

Como parte de las gestiones efectuadas por esta institución, actualmente se está trabajando en el Proyecto de Ley Infogobierno, con el objetivo de establecer los principios, bases y lineamientos que regirán el uso de las tecnologías de información en el poder público.

Siguiendo la investigación, se observa que el Ministerio Popular de Planificación y Finanzas de Venezuela, cuenta con la Superintendencia de las Instituciones del Sector Bancario, definida en su sitio web como:

> La Superintendencia de las Instituciones del Sector Bancario es el ente de regulación del sector bancario bajo la vigilancia y coordinación del

> Órgano Superior del Sistema Financiero Nacional. Es una institución autónoma con personalidad jurídica y patrimonio propio e independiente de los bienes de la República, y se regirá por las disposiciones que establezcan la Ley Orgánica del Sistema Financiero Nacional y la Ley de las Instituciones del Sector Bancario. (SUDEBAN)

El ente de regulación emite la normativa de tecnología de la información, servicios financieros desmaterializados, banca electrónica, virtual y en línea para los entes sometidos al control, regulación y supervisión de la Superintendencia de Bancos y otras instituciones financieras, la cual tiene como objetivo:

> La presente Norma tiene como objetivo establecer los lineamientos básicos que deberán cumplir los sujetos sometidos a la supervisión, control y regulación de la Superintendencia de Bancos y otras instituciones financieras (SUDEBAN) en la implantación y uso de tecnología de la información, así como, en la prestación de servicios financieros desmaterializados, banca en línea, electrónica y virtual. (Marzo, 2007). (SUDEBAN S. W.)

Dicha normativa contempla 11 capítulos, los cuales abordan las diferentes ramas asociadas a las tecnologías de información, y su aplicación en el sector bancario venezolano, entre ellos:

Tabla 8: Capítulos de la Normativa de Tecnología de la Información de SUDEBAN

Capítulos de la Normativa de Tecnología de la Información de SUDEBAN	
Título I: Disposiciones Generales	Título II: Planeación Estratégica y Organización de los Recursos de Información
Título III: Operaciones de los Sistemas de Información	Título IV: Contratación de los Proveedores Externos
Título V: Seguridad de la Información	Título VI: Plan de Contingencia Tecnológica
Título VII: Mantenimiento e Implantación de los Sistemas de Información	Título VIII: Redes
Título IX: Infraestructura de las Telecomunicaciones	Título X: Banca Virtual
Título XI: Disposiciones Finales	

Fuente: Normativa de Tecnología de la Información de SUDEBAN.

La Asamblea Nacional de la República Bolivariana de Venezuela decreta en el 2001 la Ley Especial Contra Los Delitos Informáticos[10], la cual tiene por objeto:

> …la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley. (SUDEBAN)

3.2.2. NORMATIVA GUBERNAMENTAL EN CHILE

La investigación efectuada, contempló la revisión del sitio web de la Contraloría de la República de Chile, con el fin de conocer cómo está constituida y qué relación tiene con

[10] Gaceta Oficial Nº 37.313 del 30 de octubre de 2001

la gestión de las tecnologías de información de Chile. A continuación, se detalla la forma como se define la institución en esta página:

> La Contraloría General de la República (CGR) es un órgano superior de fiscalización de la Administración del Estado, contemplado en la Constitución Política, que goza de autonomía frente al Poder Ejecutivo y demás órganos públicos.
>
> Es esencialmente una entidad de control de legalidad de los actos de la Administración del Estado, que actúa con independencia del Poder Ejecutivo y el Congreso Nacional.
>
> La labor de la Contraloría es eminentemente fiscalizadora; de carácter jurídico, contable y financiero, pues está destinada a cautelar el principio de legalidad, es decir, verificar que los órganos de la Administración del Estado actúen dentro del ámbito de sus atribuciones y con sujeción a los procedimientos que la ley contempla. (CGR)

Además, se cuenta con el Ministerio Secretaría General de la Presidencia de la República de Chile, el cual se define mediante el artículo N° 1 de la Ley 18.993, que indica:

> Artículo N°1.- Créase el Ministerio Secretaría General de la Presidencia de la República que constituirá la Secretaría de Estado encargada de realizar funciones de coordinación y de asesorar directamente al

Presidente de la República, al Ministro del Interior y a cada uno de los Ministros, sin alterar sus atribuciones proveyéndoles, entre otros medios, de las informaciones y análisis político-técnicos necesarios para la adopción de las decisiones que procedan. Artículo N° 2.- Corresponderá especialmente al Ministerio Secretaría General de la Presidencia de la República:

a) Prestar asesoría al Presidente de la República, al Ministro del Interior y a cada uno de los Ministros, en materias políticas, jurídicas y administrativas, como asimismo, asesorar al Presidente de la República y al Ministro del Interior y demás Ministros, cuando así lo requieran, en lo que se refiera a las relaciones del Gobierno con el Congreso Nacional; como también con los Partidos Políticos y otras organizaciones sociales e instituciones de la vida nacional, en coordinación con el Ministerio Secretaría General de Gobierno:

b) Propender al logro de una efectiva coordinación programática general de la gestión de Gobierno;

c) Actuar, "Por orden del Presidente de la República", mancomunadamente con otros Ministerios, y a través de ellos, con los Servicios y Organismos de la Administración del Estado;

d) Efectuar estudios y análisis de corto y de mediano plazo relevantes para las decisiones políticas y someterlos a la consideración del Presidente de la República y del Ministerio del Interior, y

e) Informar al Ministro del Interior respecto de la necesidad de introducir innovaciones a la organización y procedimientos de la Administración del Estado. (MINSEGPRES)

El Ministerio Secretaría General de la Presidencia República de Chile, es quien ha emitido las normas técnicas que se obtuvieron para este estudio, de las cuales se detallan las siguientes:

- Norma número DTO-77, del 23 de diciembre del 2004: "Norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la administración del estado y entre estos y los ciudadanos"
- Norma número DTO-81, del 23 de diciembre del 2004: "Norma técnica para los órganos de la administración del estado sobre interoperabilidad de documentos electrónicos"
- Normativa número DT-83, del 12 de enero del 2005: "Norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos"
- Norma número DTO-93, del 09 de mayo del 2005: "Norma Técnica para la Adopción de Medidas Destinadas a Minimizar los Efectos Perjudiciales de los Mensajes Electrónicos Masivos no Solicitados Recibidos en las Casillas

Electrónicas de los Órganos de la Administración del Estado y de sus Funcionarios"

- Norma número DT-100, del 22 de junio del 2006: "Norma Técnica para el Desarrollo de Sitios Web de los Órganos de la Administración del Estado"

Además, la República de Chile cuenta con el denominado "Reglamento sobre la Inscripción de Esquemas Documentales en el Repositorio del Administrador de Esquemas y Metadatos", emitido por el Ministerio de Economía, Fomento y Reconstrucción, el cual tiene como misión lo indicado de cita literal:

> La Misión del Ministerio de Economía es promover la modernización y competitividad de la estructura productiva del país, la iniciativa privada y la acción eficiente de los mercados, el desarrollo de la innovación y la consolidación de la inserción internacional de la economía del país a fin de lograr un crecimiento sostenido, sustentable y con equidad, mediante la formulación de políticas, programas e instrumentos que faciliten la actividad de las unidades productivas del país y sus organizaciones corporativas y las instituciones relacionadas con el desarrollo productivo y tecnológico del país, tanto públicas y privadas, nacionales y extranjeras. (Chile)

Por otra parte, existe el Congreso Nacional República de Chile, en cuyo sitio web se define de la siguiente forma:

> El Congreso Nacional de Chile fue fundado el 04 de julio de 1811, está compuesto por la Cámara de Diputados, de 120 miembros y por el Senado, integrado por 38 parlamentarios. Se rige por la Constitución Política de 1980 y por la Ley orgánica constitucional Nº 18.918. Sus principales funciones son ejercer la representación de la ciudadanía, concurrir a la formación de leyes junto con el Presidente de la República y fiscalizar los actos del gobierno. (CNCL)

El Congreso Nacional de la República de Chile emitió leyes sobre aspectos de tecnologías de información, tales como:

- Ley número 19223, del 07 de junio de 1993, sobre las "Típicas figuras penales relativas a la informática".
- Ley número 19799, del 12 de abril del 2002, "Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma".

Adicionalmente, el Instituto Nacional de Normalización de la República de Chile es miembro, de la *International Organization for Standardization*, ISO, principal ente normalizador internacional, de la que es fundador a partir de 1947, y que está definido como:

> El Instituto Nacional de Normalización, INN, es una fundación de derecho privado sin fines de lucro, creada por CORFO. Su rol es contribuir al desarrollo productivo del país, fomentando la elaboración y uso de normas chilenas, coordinando la Red Nacional de Metrología y acreditando organismos de evaluación de la conformidad.

> En julio de 1986, el Decreto 533 del Ministerio de Justicia modificó los estatutos, incorporándose entre sus actividades la administración de un Sistema Nacional de Certificación de Conformidad. Ese mismo año, el INN obtuvo la calidad de Instituto de Investigación del Estado. (INN)

Dicho ente establece el denominado "Código de prácticas para la gestión de la seguridad de la información". Esta norma es idéntica a la versión en inglés *ISOIEC* 27002:2005 *Information technology - Security techniques - Code of practice for information security management.*

Para resumir las normativas indicadas anteriormente, se elaboró la siguiente tabla, donde se detalla el nombre de la normativa y una breve descripción de lo que se regula mediante ella:

Tabla 9: Resumen Normativa Técnica de Chile

NOMBRE	DESCRIPCIÓN
a)	Norma número DTO-77, del 23 de diciembre del 2004: "Norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la administración del Estado y entre estos y los ciudadanos"
	• Se debe contar con medidas de seguridad con el fin de evitar interceptación, modificación u otra forma de acceso no permitido • La administración debe declarar los formatos y los medios compatibles con sus sistemas, con el fin de enviar correos electrónicos, autenticarse y acceder al sitio web. Si necesitara utilizar aplicaciones o visores, estos deberán ser de acceso gratuito • Deben quedar constancias de las transmisiones, especificando remitente, destinatario, fecha y hora de estas. Los registros de dichas comunicaciones serán resguardados por la Administración, por un periodo no menor de seis años. Se deberán almacenar los antecedentes. El Registro se cerrará diariamente, sea manual o automatizado, garantizando el no repudio e integridad. El Ministro deberá concurrir, al menos una vez al mes, con firma electrónica al cierre de estos documentos.
b)	Norma número DTO-81, del 23 de diciembre del 2004: "Norma técnica para los órganos de la administración del Estado sobre interoperabilidad de documentos electrónicos"
	• La norma se aplica a los documentos electrónicos administrativos, en su interacción con otras administraciones o sujetos privados. • Podrán ser aplicables las siguientes normas técnicas: ISO/IEC 8825-4 2003, ISO/IEC 10646-1 2000, ISO/IEC DIS 18056, RFC-821:1982, RFC-959:1985, RFC-2068:1997.
c)	Normativa número DT-83, del 12 de enero del 2005: "Norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos

	electrónicos”
	• Se establecen las características obligatorias de seguridad y confidencialidad que deben reunir los documentos electrónicos. Se pretende establecer estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de documentos electrónicos, salvaguardando el uso de los documentos electrónicos.
d)	Norma número DTO-93, del 09 de mayo del 2005: “Norma Técnica para la Adopción de Medidas Destinadas a Minimizar los Efectos Perjudiciales de los Mensajes Electrónicos Masivos no Solicitados Recibidos en las Casillas Electrónicas de los Órganos de la Administración del Estado y de sus Funcionarios”
	• Se busca minimizar la recepción masiva de mensajes no deseados vía correo electrónico, ya que estos pueden ser causa de contraer virus, códigos malignos y demás, que pueden poner en peligro la documentación electrónica
e)	Norma número DT-100, del 22 de junio del 2006: “Norma Técnica para el Desarrollo de Sitios Web de los Órganos de la Administración del Estado”
	• Busca la estandarización, interoperabilidad y protección de datos personales de los sitios web de los órganos de la administración del Estado. • Deben garantizar el acceso y disponibilidad de la información, resguardo de datos personales, e interoperabilidad de los contenidos y funciones de la administración.
f)	Reglamento sobre la Inscripción de Esquemas Documentales en el Repositorio del Administrador de Esquemas y Metadatos
	• Regula el procedimiento de inscripción de esquemas basales (describe datos reutilizables) y documentales por parte de la administración. • Los repositorios deberán permitir acceso por medio del sitio web, contener cierto tipo de información como título, nombre, estado, fecha de publicación, descripción e institución que registra y cumplir con un esquema XML.
g)	Ley número 19223, del 07 de junio de 1993: “Tipifica figuras penales relativas a la informática”, estableciendo como acciones penadas las siguientes:
	• Destrucción o inutilización de un sistema de tratamiento de información, o impedir, modificar u obstaculizar su funcionamiento. • Obtener, conocer, usar, interceptar, interferir o acceder a la información que se encuentra dentro de un sistema de tratamiento de forma indebida. • Alterar, dañar o destruir los datos contenidos en un sistema de información. • Difundir o revelar los datos contenidos en un sistema de información.
h)	Ley número 19799, del 12 de abril del 2002: “Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma”
	• Los actos o contratos firmados electrónicamente tendrán el mismo valor de ley que los de firma física. Excepto aquellos que contengan alguna solemnidad, los que se requieran la concurrencia de otros, así como los relativos a derecho y familia. • Los prestadores de servicios de certificación, son las personas jurídicas, extranjeras o nacionales, públicas o privadas, que otorguen certificados de firma electrónica. Serán responsables por los daños y perjuicios, que en el ejercicio de su actividad se ocasionen.
i)	Código de prácticas para la gestión de la seguridad de la información
	• Busca establecer recomendaciones y principios generales para iniciar, implantar, mantener y mejorar la gestión de seguridad de la información en una organización. • Esta norma es idéntica a la versión en inglés ISOIEC 27002:2005 *Information technology - Security techniques - Code of practice for information security management*; sin embargo, implicó el cambio de algunos significados. • Al ser la información un activo importante del negocio, se requiere una protección adecuada, especialmente en ambientes de negocio interconectados, por lo que se requerirá un conjunto de controles, que incluyen políticas, procesos, procedimientos, estructuras organizativas, funciones de *hardware* y *software*, incluyendo la supervisión, mejoramiento y reemplazo de estos.

Fuente: Normativa atinente a las Tecnologías de Información remitida por el Lic. Jorge Mérida Muñoz funcionario del Gabinete Subcontralor General (24 de octubre, 2012).

Otra forma de contribuir, con el análisis del esquema fiscalizador de Chile, correspondió a la revisión de un informe de auditoría de tecnologías de información, a saber el (CGR, Contraloría General de la República) informe N° 34 del 2010, sobre auditoría de tecnologías de información en la Universidad de los Lagos, cuyo objetivo consistió en revisar y evaluar aspectos que se relacionan con las políticas, normas, prácticas y procedimientos de control, que se vinculan con los sistemas basados en las tecnologías de información y comunicaciones (TIC).

Entre los resultados de dicho informe se detalla que "… se observó que los Sistemas Informáticos no se clasifican para indicar la necesidad, prioridad y grado de protección, incumpliendo el artículo 13 del decreto supremo N°83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba la norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos. Además, no se identifican claramente los bienes asociados a cada sistema de información, tales como bienes de información y de software. Además de los bienes físicos, como lo indica el artículo 37 c) del mencionado Decreto."

Tal y como de denota en la cita anterior, la revisión toma como criterio la tercera norma observada en la Tabla 9: Resumen Normativa Técnica de Chile.

La revisión de la normativa aplicable en países tales como Venezuela y Chile, permitió determinar una serie de aspectos de interés, para la investigación actual, en función de la propuesta de mejoras a las normas técnicas para la gestión y el control de las

tecnologías de información, de la Contraloría General de la República en Costa Rica, entre ellas las siguientes:

- Las tecnologías de información son actualmente un tema de importancia, tanto para las empresas privadas como para las públicas; por lo tanto, los países están realizando variados esfuerzos, a fin de normar su gestión y uso.
- La regulación de las TI, se da en países grandes, de la extensión de Venezuela, y también en países de un tamaño similar a Costa Rica, como es el caso de Chile
- Un elemento llamativo en la revisión efectuada, es la diversidad de normas y organismos que establecen normativa, en cuanto a las tecnologías de información. Al igual que Costa Rica, no existe un esfuerzo común por parte de los gobiernos para regular esta actividad desde una sola vía.

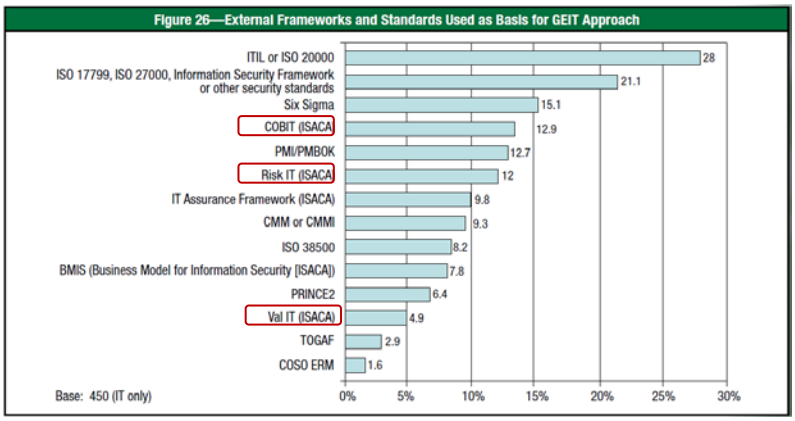
3.3. USO DE MEJORES PRÁCTICAS COMO ELEMENTO DIFERENCIADOR

El uso de los estándares internacionales en la gestión de las tecnologías de información, como elemento diferenciador en las empresas, tanto públicas como privadas, tiende a ir en aumento hoy en día. Esto se debe a que se considera que la aplicación de conceptos asociados a “Mejores Prácticas”, es uno de los instrumentos más efectivos para que las instituciones incrementen las posibilidades de lograr sus objetivos de negocio.

En virtud de lo anterior, surge la necesidad de conocer diferentes estándares internacionales y su aceptación en el mundo, para establecer si constituyen una referencia, para la actualización que plantea el presente estudio, sobre las normas técnicas emitidas por la Contraloría General de la República.

El estudio efectuado por IT *Governance Institute (ITGI)* durante el año 2011, denominado *"Global Status Report on the Governance of IT (CGEIT)* – 2011", el cual busca revelar la contribución que realizan las TI para la consecución del éxito del negocio. Como parte de este estudio, se consulta en 21 países sobre los marcos de control que se utilizan en la gestión de las tecnologías de información, tanto para instituciones del sector público, como del privado. Entre sus resultados obtienen una lista encabezada por *ITIL, Six Sigma, COBIT y PMBOK*, tal como se observa en la ilustración siguiente:

Ilustración 9: Marcos de Control para la Gestión de TI



Fuente: *Global Status Report on the Governance of IT (CGEIT)*—2011.

De esta manera, se inicia un breve recorrido por los marcos de control, que de acuerdo con la ilustración anterior, son de mayor conocimiento en el mundo.

3.3.1. MARCO DE CONTROL *COBIT*® 4.1

COBIT es un marco de referencia y un juego de herramientas de soporte, que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, así como comunicar ese nivel de control a los interesados (*stakeholders*).

COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas y además, constantemente se actualiza y armoniza con otros estándares. Por lo tanto, *COBIT* se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI, que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de *COBIT* y su enfoque de alto nivel orientado al negocio, brindan una visión completa de TI y de las decisiones por tomar acerca de esta. (ITGI, 2007)

Tal y como se desprende de la definición, el *COBIT*, se ha venido asociando a la gestión ordenada de las tecnologías de información, tomando en cuenta en particular, factores como la gobernabilidad de TI y la importancia de que los esquemas gerenciales comprendan la función de la tecnología, en relación con el logro de los objetivos de la institución. De esta forma, los beneficios que han venido asociándose a la implementación de este marco de referencia de gobierno incluyen:

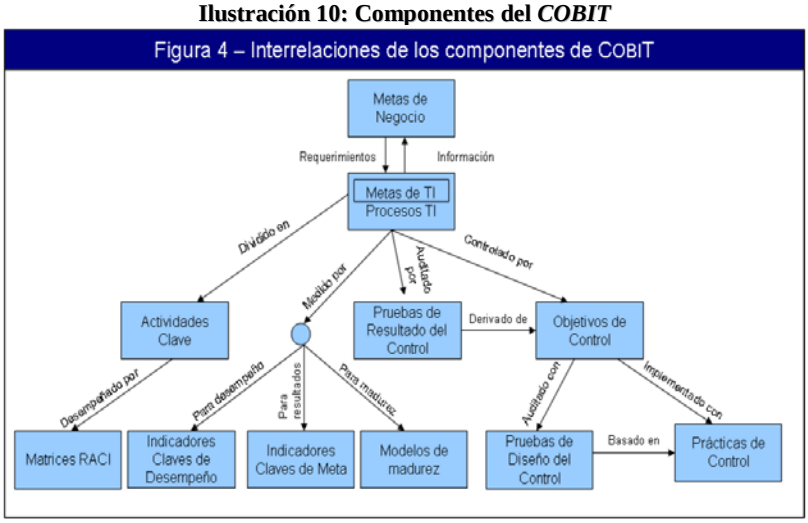
- Mejor alineación, con base en su enfoque de negocios.
- Una visión, entendible para la gerencia, de lo que hace TI.
- Propiedad y responsabilidades claras, con base en su orientación a procesos.
- Aceptación general de terceros y reguladores.
- Entendimiento compartido entre todos los interesados, con base en un lenguaje común.
- Cumplimiento de los requerimientos *COSO* para el ambiente de control de TI.

Es importante observar que el *COBIT*® 4.1, cuenta con una serie de componentes que se interrelacionan entre sí, iniciando con el establecimiento de las metas del negocio, que vienen a establecer los requerimientos necesarios para definir las metas y procesos de TI, de forma que estos brinden información para la toma de decisiones. A su vez, las metas se logran por medio de actividades clave, las cuales son desempeñadas de acuerdo con lo establecido por las matrices *RACI*.

El logro de las metas y procesos de TI, se mide de acuerdo con base en su desempeño, resultados y madurez, respectivamente, al utilizar herramientas como indicadores clave de desempeño, indicadores clave de meta y modelos de madurez.

Además, esos procesos pasan por el de auditoría y control, mediante las pruebas de resultado y objetivos de control, donde se auditan con pruebas de diseño del control y se implementan con las prácticas de este, que también son establecidas por este marco de control. Lo anterior, se expresa gráficamente en el *COBIT*® 4.1, tal y como sigue:

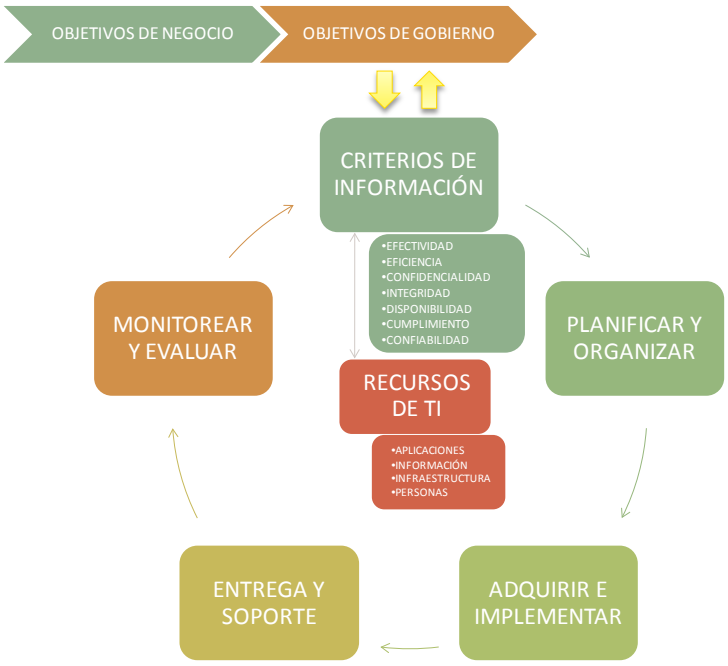
Ilustración 10: Componentes del *COBIT*



Fuente: MARCO DE CONTROL *COBIT*® 4.1

COBIT está orientado a los objetivos y al alcance del gobierno de TI, asegurando que su marco de control sea integral, que esté acorde a los principios de Gobierno Corporativo y por lo tanto, sea aceptable para los consejos directivos, para la dirección ejecutiva e informática, así como para los auditores y reguladores (ITGI, 2007). El siguiente cuadro ofrece un mapa, que muestra cómo los objetivos de control detallados de *COBIT* se relacionan con las cinco áreas de enfoque del gobierno de TI y con las actividades de control de *COSO*.

Ilustración 11: Marco de Trabajo Completo de *COBIT*



Fuente: Elaboración propia con base en *COBIT* 4.1.

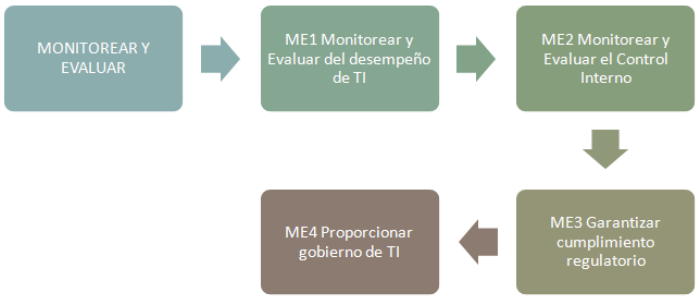
El marco de control *COBIT*® 4.1 define las actividades de TI, en un modelo genérico de procesos organizados, en los dominios que se observaron en la ilustración anterior. De esta forma, cada uno de esos dominios está compuesto por una serie de objetivos de control.

De acuerdo con lo anterior, los objetivos de control de cada dominio se presentan a continuación:

3.3.1.1. MONITOREAR Y EVALUAR

Todos los procesos de TI deben evaluarse, de forma regular en el tiempo, en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. (ITGI, 2007)

Ilustración 12: Objetivos de Control del ME

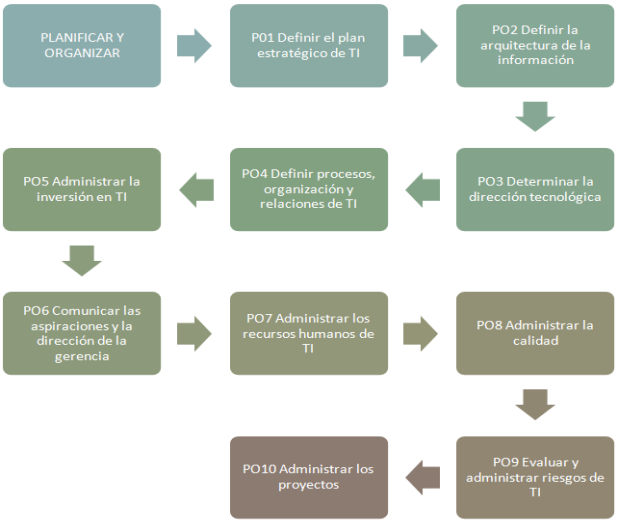


Fuente: Elaboración propia con base en *COBIT*® 4.1.

3.3.1.2. PLANIFICAR Y ORGANIZAR

Cubre las estrategias y las tácticas y tiene que ver con identificar, la forma como TI puede contribuir, de la mejor manera, al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada, desde diferentes perspectivas. Finalmente, se deben implementar, una estructura organizacional y una tecnológica, apropiadas. (ITGI, 2007)

Ilustración 13: Objetivos de Control de PO

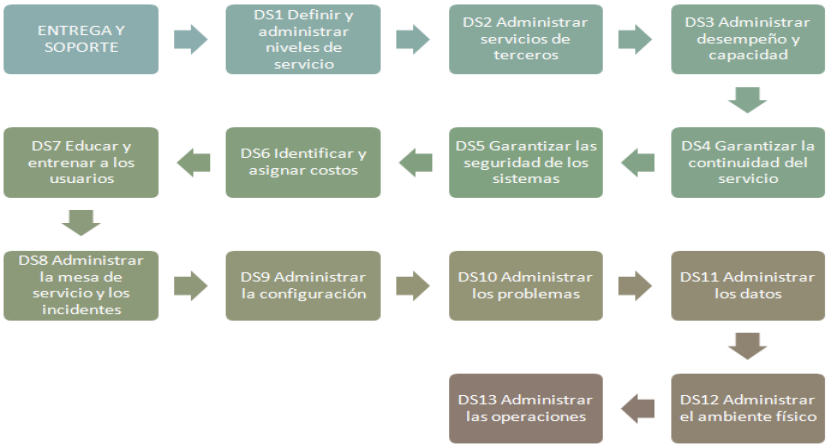


Fuente: Elaboración propia con base en *COBIT*® 4.1.

3.3.1.3. ENTREGA Y SOPORTE

Este dominio cubre la entrega de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, además de la administración de los datos y de las instalaciones operativas. (ITGI, 2007)

Ilustración 14: Objetivos de Control de DS

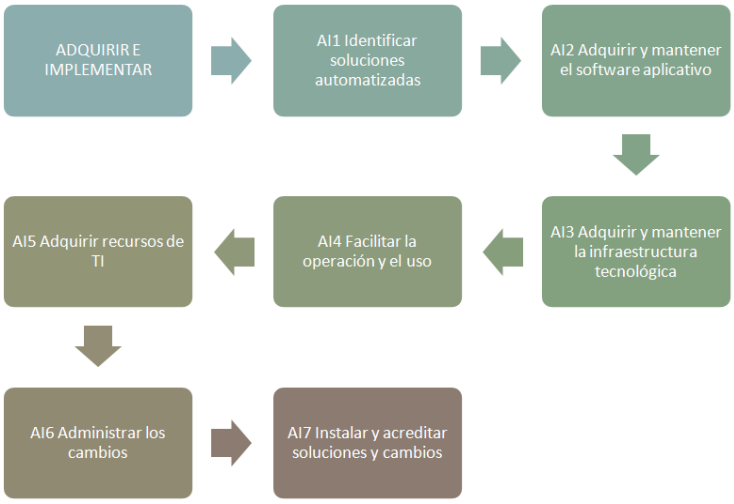


Fuente: Elaboración propia con base en *COBIT*® 4.1.

3.3.1.4. ADQUIRIR E IMPLEMENTAR

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes están cubiertos por este dominio, para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. (ITGI, 2007)

Ilustración 15: Objetivos de Control de AI

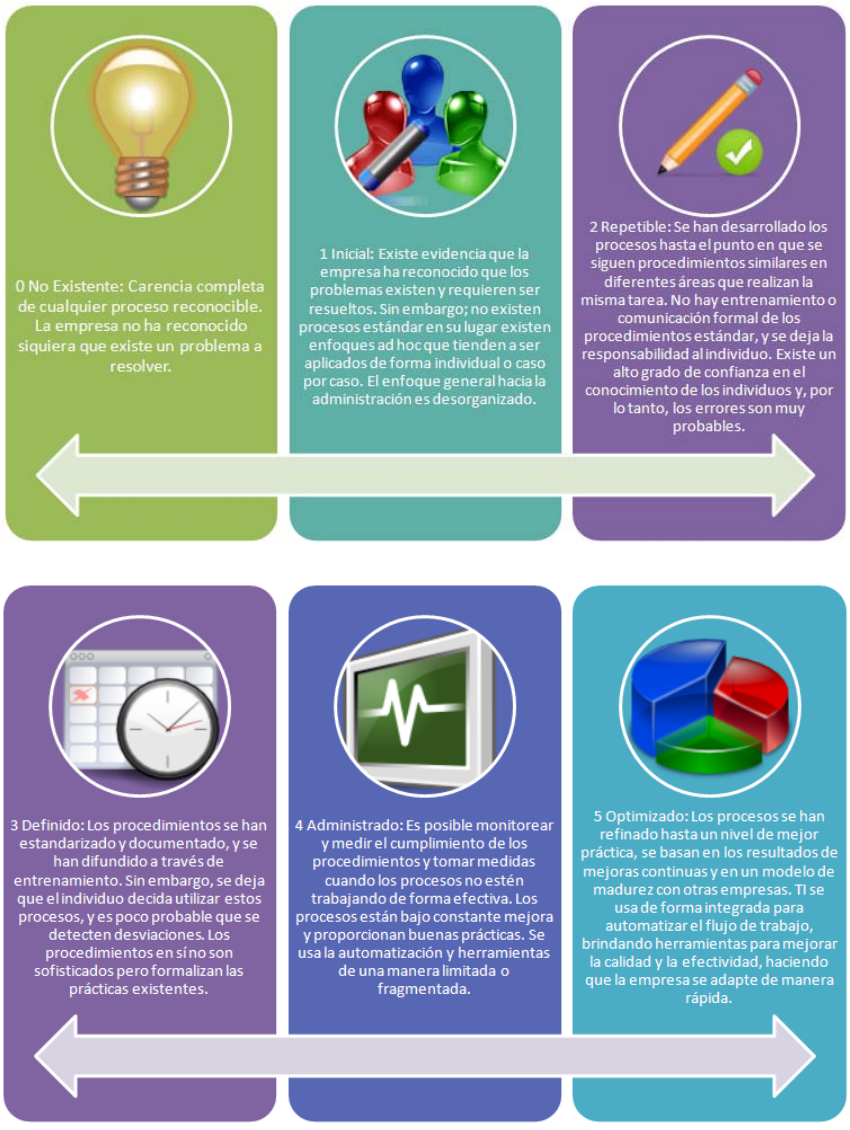


Fuente: Elaboración propia con base en *COBIT*® 4.1.

Otra herramienta, asociada al marco de control *COBIT*® 4.1, es el esquema del modelo de madurez para la administración y el control de los procesos de TI. En este caso, se indica que se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente cero, hasta el de optimizado cinco (ITGI, 2007). Este enfoque se deriva del modelo de madurez que el *Software Engineering Institute* definió, para la madurez de la capacidad del desarrollo de *software.*

El modelo de madurez para la administración y el control de los procesos de TI, cuenta con seis niveles de madurez, en los que se contempla desde la carencia de procesos, hasta el momento en que la organización se encuentra en un proceso de mejora continua. Se detallan a continuación:

Ilustración 16: Modelo Genérico de Madurez



Fuente: Elaboración propia con base en *COBIT*® 4.1.

3.3.2. MARCO DE REFERENCIA *ITIL* V3

ITIL es un marco de referencia de mejores prácticas, para gestionar operaciones y servicios de TI, que fue definido a mediados de los años ochentas, por la Oficina de Comercio del Gobierno del Reino Unido ("*Government of Commerce*"). El objetivo fundamental de *ITIL* es alinear negocio y tecnologías de la información y así permitir a las organizaciones, implementar lo que es relevante para sus negocios.

El esquema de *ITIL* se basa, en la gestión de las tecnologías de información en forma de procesos, con una visión de servicio, el cual está a disposición de los clientes de negocio. De esta forma, su esquema toma en cuenta diferentes pasos, que contribuyen con la consecución de un servicio de calidad, documentado y mejorable.

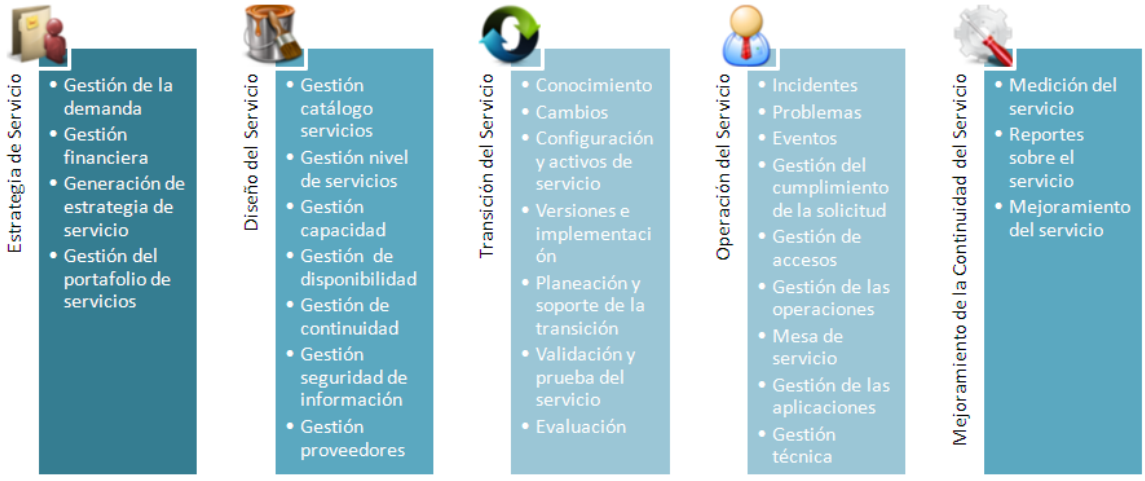
Ilustración 17 Biblioteca de *ITIL* v3

Fuente: Elaboración propia con base en el Manual del Curso: *ITIL* v3 y su apoyo a las normativas de TI de Costa Rica.

En resumen, *ITIL* posee las siguientes características: adopta un enfoque orientado a procesos aplicable, tanto a pequeñas como a grandes organizaciones de TI. Establece la Gestión de Servicios de TI, compuesta por procesos estrechamente relacionados e integrados (ver Ilustración 18: Actividades de la Biblioteca de *ITIL* v3). Para lograr los objetivos clave de la Gestión de Servicios de TI, se debe englobar la perspectiva de las cuatro P (Personas, Procesos, Productos y Proveedores) de forma efectiva, eficiente y rentable. Facilita a las organizaciones de TI asegurar la prestación de servicios innovadores y de calidad, en consonancia con los procesos del negocio. (García, S. 2013)

El objetivo fundamental de *ITIL*: es alinear el negocio y a TI, permitiendo a las organizaciones implementar lo que es relevante para sus negocios, sus objetivos específicos giran en torno a alinear servicios de TI con las necesidades actuales y futuras del negocio y sus clientes, mejorar la calidad de los servicios entregados y reducir los costos a largo plazo en la provisión de servicios. (García, S. 2013)

Ilustración 18: Actividades de la Biblioteca de *ITIL* v3



Fuente: Elaboración propia con base en el Manual del Curso: *ITIL* v3 y su apoyo a las normativas de TI de Costa Rica.

De acuerdo con la ilustración anterior, *ITIL* cuenta con cinco grandes áreas para la gestión de los procesos y servicios, entre ellas estrategia, diseño, transición, operación y mejoramiento de la continuidad del servicio, compuestas por las gestiones mostradas.

3.3.3. ESTÁNDAR *ISO/IEC* 27001

La serie de estándares *ISO/IEC 27001 (ISO 27001)* es un conjunto de buenas prácticas, que proporcionan orientación a las organizaciones, que aplican y mantienen programas de seguridad de la información. *ISO 27001,* originalmente se publicó en el Reino Unido (RU), como el estándar británico 7799 (BS7799) y se convirtió en un estándar muy conocido en la industria. (ISACA, 2011)

El estándar pone especial atención en promover un enfoque del proceso, con el fin de establecer, implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) de la organización.

Desde dicho enfoque, la *ISO (27001, 2005)* fomenta que los usuarios enfaticen en la importancia de:

a) Entender los requerimientos de seguridad de información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
b) Implementar y operar controles para manejar los riesgos de la seguridad de la información.
c) Monitorear y revisar el desempeño y la efectividad del SGSI.

d) Mejoramiento continuo, con base en la medición del objetivo.

El estándar adopta un modelo de proceso identificado por las siglas PDCA (por sus siglas en inglés *Plan-Do-Check-Act)*, el cual se basa en Planear-Hacer-Chequear-Actuar, y es aplicable a todos los procesos del SGSI, tomando como insumo los requerimientos y expectativas de las partes interesadas, ejecutando acciones y procesos, que llegan a resultados sobre seguridad de información, los cuales satisfacen esos requerimientos. La ilustración siguiente, detalla dicho proceso.

Ilustración 19: Modelo PDCA Aplicado a los Procesos SGCI

Fuente: Elaboración propia con base en el Estándar *ISO* 27001.

Entonces, el modelo contempla las partes interesadas que generan los requerimientos y expectativas sobre la seguridad de la información, las cuales son asumidas por el ciclo *Plan-Do-Check-Act*, de forma tal, que los interesados obtengan la seguridad de información ya controlada o manejada.

3.3.4. ACUERDO SUGEF 14-09

La nueva Ley Orgánica del Banco Central de Costa Rica (N° 7558), vigente desde el 27 de noviembre de 1995, declara de interés público la fiscalización de las entidades financieras y crea la Superintendencia General de Entidades Financieras (SUGEF), bajo la misma figura jurídica de la desconcentración máxima, pero esta vez dotada de mayores poderes y mayor autonomía administrativa, mediante la institución de su propio Consejo Directivo.

Su objetivo se definió como velar por la estabilidad, la solidez y el funcionamiento eficiente del sistema financiero nacional, con estricto apego a las disposiciones legales y reglamentarias y de conformidad con las normas, directrices y resoluciones que dicte la propia institución, todo en salvaguarda del interés de la colectividad.

Este reglamento tiene por objeto la definición de los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información (TI). El mismo cuerpo normativo establece los objetivos de la gestión de TI, tal como sigue (SUGEF, 2009):

a) Alineación Estratégica: La TI es congruente con las estrategias y objetivos de la entidad.
b) Administración del Riesgo de TI: Los riesgos relacionados con TI son conocidos y administrados.
c) Entrega de Valor: La TI contribuye con la consecución de los beneficios esperados, eficiencia, productividad y competitividad de la entidad.

d) Gestión de Recursos: La inversión en TI se ajusta a las necesidades de la entidad y es administrada adecuadamente.
e) Medición del Desempeño de TI: El desempeño de TI es medido y sus resultados son utilizados para la toma de decisiones.

El artículo sexto del acuerdo SUGEF 14-09 sobre el marco para la gestión de las tecnologías de información, indica la necesidad que presentan las organizaciones, en cuanto a diseñar, implementar y mantener un marco, para la gestión de la tecnología de información, y su congruencia con el perfil tecnológico de la entidad, la naturaleza y la complejidad de sus operaciones.

Llama la atención, que el mismo artículo establece la obligatoriedad de incluir dentro de ese marco de gestión, al menos los procesos identificados como obligatorios en el anexo primero de ese reglamento, el cual se compone de una categorización de los 34 procesos que integran la versión de *COBIT*® 4.0 y su clasificación.

En función de esa categorización, la SUGEF establece 17 procesos que deberán ser implementados con prioridad, y con base en un nivel de madurez establecido por la misma institución, de acuerdo con la ilustración descrita en el transitorio I:

Ilustración 20: Niveles de Madurez para los Procesos Dispuestos como Obligatorios en el Marco para la Gestión de TI y su Evaluación Externa Independiente, Emitidos por la SUGEF en el Acuerdo 14-09

Procesos COBIT®	Primera Auditoría Externa	Segunda Auditoría Externa	Auditorías subsecuentes
PO9 Evaluar y administrar los riesgos de TI	Nivel madurez mínimo requerido: **tres**	Nivel madurez mínimo requerido: **tres**	Nivel madurez mínimo requerido: **tres**
PO10 Administrar proyectos			
AI6 Administrar cambios			
DS2 Administrar los servicios de terceros			
DS4 Garantizar la continuidad del servicio			
DS5 Garantizar la seguridad de los sistemas			
DS11 Administrar los datos			
ME2 Monitorear y evaluar el control interno			
PO1 Definir un plan estratégico de TI	Nivel madurez mínimo requerido: **dos**	Nivel madurez mínimo requerido: **tres**	Nivel madurez mínimo requerido: **tres**
PO3 Determinar la dirección tecnológica			
PO5 Administrar la inversión en TI			
AI3 Adquirir y mantener infraestructura tecnológica			
AI5 Adquirir recursos de TI			
DS3 Administrar el desempeño y la capacidad			
DS 9 Administrar la configuración			
DS10 Administrar los problemas			
DS12 Administrar el ambiente físico			
Resto de los procesos que integran el marco para la gestión de TI	Nivel madurez mínimo requerido: **uno**	Nivel madurez mínimo requerido: **dos**	Nivel madurez mínimo requerido: **tres**

Fuente: Acuerdo SUGEF 14-09.

De acuerdo con lo supra indicado, los marcos de control de mayor aceptación en el mundo, según el *"Global Status Report on the Governance of IT (CGEIT) – 2011"*, son *ITIL*, *COBIT*® y varios estándares *ISO*; todos ellos enfocados en la mejora de la gestión de las tecnologías de información, utilizados como elemento diferenciador en las empresas agregando valor mediante la aplicación de conceptos de "Mejores Prácticas", en busca de incrementar sus probabilidades de lograr los objetivos de negocio. En Costa Rica, la SUGEF utilizó como marco de control de aplicación obligatoria el citado *COBIT*® y estableció esquemas de madurez necesarios, para la implementación de estas sanas prácticas, en el ambiente de tecnologías de información del sistema bancario nacional.

3.4. SONDEO DE OPINIONES CALIFICADAS

El sondeo de opinión calificada planteado se realizó, con base en el instrumento elaborado en el capítulo I, el cual se compone de ocho preguntas en total, de las cuales tres son dirigidas únicamente a funcionarios de la auditoría interna.

Tabla 10: Preguntas Aplicadas, Período de Aplicación 13 de Febrero al 21 de Marzo, 2013.

Instrumento de consulta aplicado en el Sondeo de Opinión Calificada	
1.	¿Cuáles son las principales dificultades enfrentadas en el proceso de implementación de las normas técnicas para la gestión y el control de las tecnologías de información?
2.	¿Cuál ha sido el rol, liderazgo y compromiso que han asumido los niveles directivos de las organizaciones en cuanto a la implementación de las normas?
3.	¿Cuál es el rol del área de tecnología de información y de las unidades usuarias de las organizaciones en cuanto a la implementación de las normas?
4.	¿Cuáles son las amenazas más relevantes derivadas del incumplimiento de las normas técnicas para la gestión y el control de las tecnologías de información? ¿Cómo espera mitigar esos riesgos?
5.	¿Cuáles son los principales aspectos que considera deben ser ajustados de la citada normativa?
6.	¿Cuáles han sido las experiencias con respecto a la evaluación de las normas técnicas para la gestión y el control de las tecnologías de información?
7.	Enumere los requerimientos o necesidades en las competencias de la auditoría interna para evaluar la citada normativa.
8.	Comente sobre la asesoría recibida por parte de la CGR de acuerdo con la evaluación de las normas técnicas para la gestión y el control de las tecnologías de información.

Fuente: Elaboración propia con la colaboración del Lic. Gino Ramírez Solís, MTI, CISA.

La población que formó parte del sondeo correspondió a 15 personas, cuyos perfiles se encuentran entre auditores internos de tecnologías de información, ingenieros en

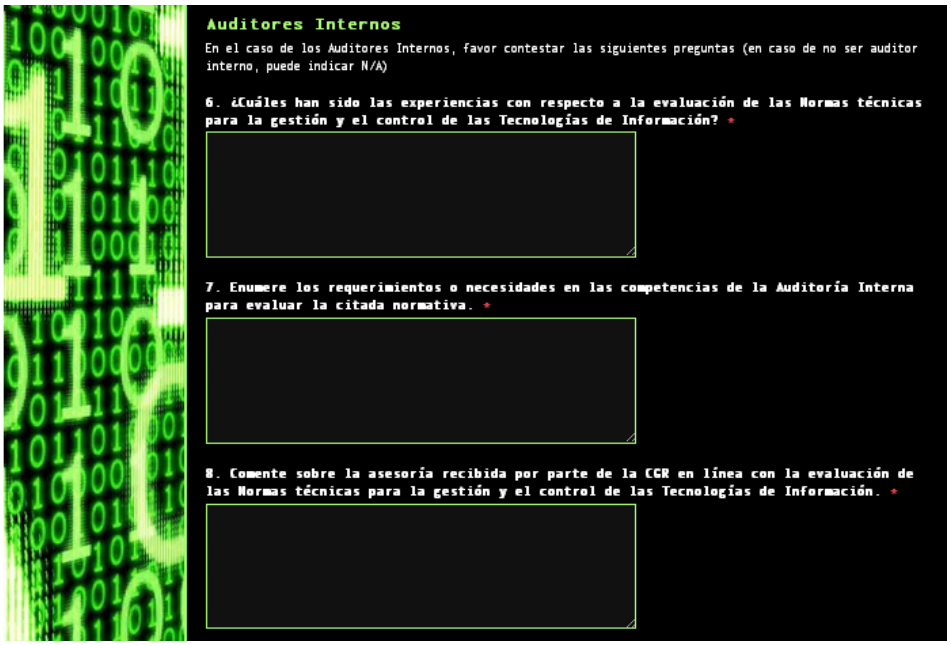
tecnologías de información dedicados a la gestión del riesgo y de la seguridad, auditores de tecnologías de información y funcionarios tanto de la empresa pública como privada.

El instrumento se difundió vía correo electrónico a una cantidad aproximada de 25 personas y consistió en un formulario electrónico (web), compuesto de preguntas abiertas, para mayor expresión de las impresiones del entrevistado.

Ilustración 21: Instrumento de Consulta Aplicado (primera parte)

Fuente: Elaboración propia con la colaboración del Lic. Gino Ramírez Solís, MTI, CISA.

Ilustración 22: Instrumento de Consulta Aplicado (segunda parte)



Fuente: Elaboración propia con la colaboración del Lic. Gino Ramírez Solís, MTI, CISA.

3.4.1. RESULTADOS DEL SONDEO DE OPINIÓN CALIFICADA

Sobre las principales dificultades enfrentadas, en el proceso de implementación de las normas técnicas para la gestión y el control de las tecnologías de información, los entrevistados comentaron aspectos variados, tales como:

a) Contenido escueto, poco detallado, no se establece cómo cumplir.
b) Desequilibrio en el detalle de la normativa, algunas áreas como seguridad de información se detallan a mayor profundidad, que por ejemplo el tema de administración de proyectos o calidad de la información.
c) Ausencia de objetivos.
d) Falta de integrabilidad con otras normas del ente contralor como las de control interno.

e) Ausencia de cultura sobre *COBIT*®, dado que la administración no está obligada a utilizarlo en su gestión de TI.

f) Ausencia de cultura organizacional en TI.

g) Dependencia del punto de vista del auditor.

h) Carencia de herramientas de evaluación.

i) No están adaptadas a estándares internacionales.

j) Debilidades en aspectos de divulgación de la normativa.

k) El perfil de los profesionales en los puestos de TI.

l) Recursos económicos asignados.

m) Diferentes estructuras de las organizaciones auditadas.

n) Distintas interpretaciones del alcance, la amplitud y la profundidad que les dan los funcionarios encargados de implementarlas, difundirlas, evaluarlas y tomar las acciones correctivas.

o) Esquema utilizado por la Contraloría General de la República para crear, implementar, retroalimentar y pedir cuentas sobre las referidas normas.

p) Incumplimiento con el diagnóstico que debían realizar las instituciones, de forma que pudieran priorizar y tomar medidas para la implementación.

En cuanto al rol, liderazgo y compromiso que han asumido los niveles directivos de las organizaciones, el parecer de los entrevistados es muy generalizado, puesto que expresan en su mayor parte, que los altos mandos no han ejercido la autoridad correspondiente, en cuanto a la implementación, siendo ellos, quienes deberían encargarse de extender la normativa y su aplicación a los subordinados. Entre las opiniones emitidas se destacan las siguientes:

a) Aunque no se puede generalizar, tristemente los niveles directivos, solo se preocupan por cumplimiento, no han interiorizado que el cumplimiento de las normas técnicas los ayuda a lograr un gobierno efectivo de su organización y de las tecnologías.

b) De mi experiencia en más de una docena de instituciones a las que aplica, concluyo que en las entrevistas realizadas a esos niveles, el papel que desempeñan es de espectador, totalmente reactivo, sin ejercer liderazgo siquiera para exigir el cumplimiento; por lo tanto, no percibí compromiso.

c) Ha sido muy desinteresado ya que aún identifican TI con un área de gasto y no como un área de servicios y apoyo para el cumplimiento de las metas organizacionales.

d) El Comité de Informática, no ha cumplido con el rol que le asiste reglamentariamente, para liderar los procesos necesarios para la implementación de las normas de TI.

e) El peso mayor en la implementación de estas normas lo ha tenido la Dirección General de Informática, aunque en principio sí se dio la participación de todos los directores y se contó con el apoyo del jerarca superior.

f) De las auditorías efectuadas, he podido observar que el compromiso es mínimo, no he visto un liderazgo importante. El rol asumido prácticamente es de ordenar la implementación, es decir, girar un oficio en donde se pide que se desarrolle el proyecto, pero no hay participación activa. Compromiso, diría que muy leve, no hay preocupación por saber cómo va el proyecto.

En dos casos particulares, los consultados externaron que la implementación ha sido soportada total o parcialmente por los niveles directivos, indicando por ejemplo:

a) Enfocada en mi institución, el tema ha sido ampliamente soportado por una estructura que está apoyada por la administración, dentro de la responsabilidad de cumplimiento.
b) El compromiso ha sido adaptado poco a poco, ya que es un poco difícil inculcar estas normativas cuando las prioridades son otras.

En relación con la pregunta anterior, se requiere contraponer el rol cumplido por los entrevistados, en relación con el área de tecnología de información y de las unidades usuarias de las organizaciones, respecto a la implementación de las normas, aspecto sobre el cual las opiniones no muestran una tendencia específica. Algunos consideran que TI ha tenido que asumir un rol de implementador, a pesar de no estar empoderada para ello. Por otro lado, algunos indican que el rol no ha sido el esperado, que les ha faltado compromiso, participación y liderazgo. En cuanto a las áreas usuarias, la tendencia es que su participación ha sido nula durante el proceso. Algunos ejemplos de lo indicado se citan a continuación:

a) El rol es sustantivo pues son los responsables de implementar, no solo las normas, sino aquellos mecanismos de control que permitan garantizar su correcta ejecución.
b) El área de TI es la encargada de todo el tema de la infraestructura técnica y de usuario, donde regirán y se implementarán las normativas.
c) De cierta manera han tratado de forzar su implementación, pero en definitiva no son ellos los responsables sino el jerarca.
d) En general, es un rol que ha sido delegado fundamentalmente en tecnología de información, obviando otras áreas involucradas, incluyendo los niveles estratégicos, tácticos y otros operacionales.

e) Las áreas usuarias no han jugado ningún rol preponderante en el avance de estas normas, labor que se la han dejado a la Dirección de Informática.
f) El rol es como miembro del comité que implementará las normas TI.
g) En cuanto a las unidades usuarias, yo diría que ha sido casi nulo; en cuanto a las áreas de TI, creo que ha existido preocupación pero no la debida.
h) Son las que han asumido el proyecto, son las que han motivado a desarrollarlo pero no cuentan con el empoderamiento para obligar a cumplir con las diferentes tareas, que requieren otros funcionarios que no son de TI.
i) El rol de estas áreas no ha sido tan protagonista como uno esperaría de un tema como este, ha existido cierta pasividad al respecto.

La existencia de normas y controles, asociados al uso y gestión de las tecnologías de información en las organizaciones, tiene como fin coadyuvar en el logro de los objetivos de estas. Esto conlleva un apego importante al tema de la gestión de los riesgos; por tanto, resulta de interés conocer, cuáles amenazas consideran los entrevistados, que se derivan del incumplimiento de las actuales normas. Entre ellas se mencionaron las siguientes:

a) Pérdida de recursos públicos por la ausencia de un gobierno efectivo de las tecnologías de información.
b) Exposición pública por el aspecto de gestión administrativa de fondos públicos (daño a la imagen pública).
c) Mala gestión y operación de infraestructura.
d) Problemas de seguridad informática.
e) Exposición de información sensible
f) Fraudes, pérdidas monetarias por daños a equipos y aplicaciones.

g) Incompetitividad.

h) Obsolescencia de la infraestructura de TI.

i) Continuidad del negocio, ataques internos y externos intencionados o no.

j) No cumplir los objetivos de la institución.

k) Debilitamiento del control interno

El sondeo de opinión, permitió además, generar una batería de conocimiento, en aspectos como la implementación actual de las normas, las amenazas de su incumplimiento, así como las oportunidades de mejora al indicar, según su experiencia, los principales aspectos, los cuales consideran que deben ser ajustados de la citada normativa. Dichos aspectos serán considerados como parte de los insumos recopilados, para presentar la propuesta de actualización a las referidas normas técnicas.

Entre los principales aportes de los entrevistados, se obtuvieron consideraciones, tales como el guiar a las instituciones al uso y al cumplimiento, no solo de cada norma particular, sino también del objetivo que persiguió la CGR al redactarla, el establecimiento de evaluaciones del proceso de madurez de la organización *Process Assessment Model (PAM),* el uso obligatorio del *COBIT* como referencia para complementar, considerar el uso de herramientas de autoevaluación, indicaciones sobre mejoras en el uso del lenguaje y la redacción actual de la normativa, actualizar la norma en función del avance tecnológico y los riesgos asociados a dicho cambio. A manera de ejemplo, se observan los siguientes comentarios:

a) Debido a que es una normativa de aplicación general, hay algunos aspectos que no se profundizaron adecuadamente. Sin embargo, siempre existe el *COBIT* como referencia.
b) Ser más específicas, indicar como medir el cumplimiento.
c) Debería ser más expresa en los temas principales que involucra la TI y no tan general, esto en las normas que se deben aplicar conforme las particularidades de nuestro país.
d) La normativa no contiene suficientes elementos sobre el plan de continuidad, dependencia tecnológica, entre otros.

Finalmente, se plantearon tres preguntas enfocadas al Auditor Interno, con el fin de obtener un breve conocimiento sobre las experiencias, en el proceso de fiscalización de las normas técnicas, para la gestión y el control de las tecnologías de información, los requerimientos que durante este proceso consideran necesarios para esas evaluaciones y la asesoría que han recibido, por parte de la Contraloría General de la República.

Partiendo de lo anterior, las opiniones en cuanto a las experiencias que han vivido los auditores internos, se enlistan las siguientes:

a) El auditado no tiene claro qué pretende cada norma, lo que aplica es su interpretación personal de lo que se quiso decir; por su parte, el Auditor también llega a validar su cumplimiento con base en su interpretación.
b) Menosprecio por parte del área de TI, por considerarla un trabajo extra, sin analizar el beneficio que representa su aplicación y cumplimiento.

c) No existe un debido perfil de los profesionales en los puestos de TI.
d) Falta de recursos económicos.
e) Falta de cultura informática en las empresas y de compromiso por parte de los usuarios internos.
f) Poco seguimiento por parte de la Contraloría General de la República.
g) No se proporcionó material de apoyo adicional para la implementación, como casos de estudio, o cómo medir el cumplimiento (por ejemplo: nivel de madurez).

Las ideas y reflexiones expresadas por los auditores, en cuanto a sus necesidades para realizar el proceso de fiscalización de la normativa, se centran en temas como capacitación y conocimiento de marcos de control y mejores prácticas, relacionados con la gestión de las tecnologías de información, entre ellos:

a) Amplio conocimiento en estándares internacionales que regulan las tecnologías de información y su control (*COBIT*, *ITIL*, *COSO*, etcétera).
b) Conocimiento de la normativa de control interno, que rige al sector público costarricense.
c) Amplísimo conocimiento técnico de la infraestructura por evaluar.
d) Capacidad de análisis de la suficiencia de controles implementados y su valor supletorio de lo expuesto en las normas, a la luz del fin y no del cumplimiento de esta per se.
e) Certificaciones de nivel mundial en cuanto a mejores prácticas y normas aplicables.
f) Aumento del tiempo dedicado en actualizaciones profesionales y educación profesional.
g) Una guía para la validación de las normas.

h) Contar con mayor recurso profesional en TI, debidamente capacitado en la aplicación de esta normativa.
i) Mayor capacitación y coordinación con CGR, para definir y tener mayor claridad sobre los alcances de evaluación de los distintos rubros de la normativa.

Lo expuesto anteriormente se complementa, con los resultados de la consulta efectuada sobre la asesoría recibida por parte de la Contraloría General de la República, para la evaluación de las normas técnicas para la gestión y el control de las tecnologías de información. La mayoría de las manifestaciones, apuntan a que la asesoría recibida ha sido muy pobre respecto al tema. A continuación, algunas de las participaciones:

a) Es insuficiente, un proceso de inducción al inicio, a un limitado número de representantes por cada institución, no es suficiente.
b) Se ve una problemática asociada a que solo el Auditor General, puede enviar consultas directas al órgano contralor, entrabando una respuesta ágil a los auditores de TI
c) De pésima a nula. La realidad es que muchos auditores de la CGR se han dedicado a dar capacitación al respecto en sus horas no laborales, haciendo de esto un negocio redondo para ellos.
d) Las dos capacitaciones recibidas en CGR, considero que han sido de un muy buen nivel, pero muy dispersas; deberían estar dentro de un programa anual de apoyo de CGR, donde los gastos pueden ser asumidos por las entidades por capacitar.
e) Hasta el momento ha sido nula, no hemos recibido seminarios o foros, donde se haya puesto en conocimiento de nosotros, roles de fiscalización o monitoreo.

f) Recibimos una formación general sobre normas de TI, previa a la emisión de las normas. No se ha solicitado asesoría de la CGR en este tema, tampoco hemos recibido capacitación por parte de la CGR.
g) No puedo dar una opinión certera de esa asesoría porque no la he recibido, a la fecha.

Adicionalmente, el instrumento de consulta se aplicó de forma personal, en caso de que los interesados lo tuvieran a bien, a varios expertos calificados de diferentes áreas como educación, seguridad de la información, auditoría, riesgos y gobernanza de las tecnologías de información.

El resultado de esas entrevistas personalizadas, se resume a continuación:

3.4.2. ENTREVISTA LIC. ÁLVARO JAIKEL

CISA, CISM, CGEIT, CRISC MBA CPA,
Ex presidente del Capítulo ISACA Costa Rica (2007-2010)

En adición a lo expuesto en el formulario que se completó de manera electrónica, es importante complementar el estudio que se está realizando para la propuesta, con aspectos como el propósito para el cual se creó la normativa y la intención con la cual se estaría gestionando una actualización, considerar qué se pretende conseguir con el cambio y si ello ofrecerá los resultados o efectos esperados.

Por otra parte, el entrevistado comenta la necesidad de que la Contraloría General de la República, realice un esfuerzo para adecuar la norma, a los diferentes tipos de institución del universo de fiscalización, tomando en cuenta los cambios tecnológicos de las instituciones, e incluso, la relación con los servicios que dan las instituciones, que se encuentren apoyados por las tecnologías de información.

Entre las ideas expresadas, estableció la importancia de contar con esquemas de madurez de los procesos, o bien una clasificación o estratificación del universo auditado, donde se puedan establecer diferentes objetivos de cumplimiento, en función del logro de los objetivos de cada tipo de organización.

3.4.3. ENTREVISTA LIC. IGNACIO TREJOS ZELAYA

Ingeniero en Computación del Instituto Tecnológico de Costa Rica, Máster en Computación e Ingeniería del software de la Universidad de Oxford y candidato a doctor de la Universidad de Oxford. Ha sido profesor universitario desde 1984 en el Instituto Tecnológico de Costa Rica. Actualmente es profesor y Rector de Cenfotec (un centro educativo especializado en Ingeniería del software y Tecnología de Información) y profesor del Instituto Tecnológico de Costa Rica.

A pesar de no trabajar en el sector público, tuvo un acercamiento con las normas técnicas para la gestión y el control de las tecnologías de información, cuando se emitieron, debido a su gestión educativa y de interés por la gestión de las tecnologías en el país. En ese momento, su observación se concentró en la falta de detalle que presenta la normativa, se tienen áreas muy desarrolladas como la de seguridad informática, la cual está más detallada y muy inspirada en algunos estándares *ISO*, a diferencia de otras que se presentan muy escuetas.

Posteriormente, la SUGEF desarrolla el acuerdo 14-09, muy inspirado en el *COBIT*, aspecto que en ese momento, lo llevó a la comparación de ambos instrumentos, llegando a la conclusión, de que resulta más fácil dar seguimiento y cumplimiento a lo establecido por la SUGEF.

Otro tema ha sido la comunicación del cuerpo normativo, puesto que no va enfocado sólo a los auditores, sino también a las jefaturas de tecnologías de información; por ende, resultaba necesario realizar una capacitación planificada, teniendo presente en ese momento a quiénes se dirigía.

El cumplimiento de las normas se dificulta, dado que las instituciones aún no están preparadas para darles seguimiento, por ejemplo, en cuanto a la administración de los datos, no se tiene claro el tema de fondo. La importancia de este aspecto para la toma de decisiones y el control de la gestión de las tecnologías de información, las dificultades y reprocesos que conlleva que la calidad de los datos sea deficiente, se debe enfocar en temas como el monitoreo y validación de los datos, sin dejar de lado la capacitación que debe recibir, el personal a cargo de estos procesos.

En cuanto a su rol como educador, el acercamiento con las normas existe, dado que en algunos de los cursos que se imparten en la institución donde es rector actualmente, se aborda la relación entre *COBIT*, *ITIL* y las normas técnicas para la gestión y el control de las tecnologías de información, en particular en tercer año de carrera, en cursos enfocados en la seguridad de la información.

3.4.4. ENTREVISTA LIC. CILLIAM CUADRA

Ingeniero en Sistemas, graduado del Instituto Tecnológico de Costa Rica, Maestría en Auditoría de Tecnologías de Información por la Universidad de Costa Rica, Director de Seguridad Informática del Banco Nacional de Costa Rica, definición de políticas, normativas y procedimientos de seguridad de la información basados en conjunto de normas ISO 27000 e ISO 38500

En su caso particular el Lic. Cuadra, labora para el área bancaria, por ende, debe velar por que se cumplan las normas técnicas para la gestión y el control de las tecnologías de información y el Acuerdo 14-09 emitido por SUGEF. En cuanto a las dificultades de la implementación, sus comentarios están en función de que las normas del ente contralor son mucho más abiertas, que las otras regulaciones a las que deben dar cumplimiento, aunado al tema del carecimiento de herramientas de autoevaluación, que le permitan al auditado saber qué es lo que la CGR requiere y satisfaga el cumplimiento deseado, de forma tal, que esa autoevaluación permita medir cómo está la institución, antes de la llegada del auditor.

En cuanto a los roles de los niveles directivos, el banco ha contado con una estructura de soporte, por parte de la administración, la cual cuenta con un área denominada entes reguladores, donde se encargan de atender los requerimientos de los fiscalizadores externos del banco. Además, su Departamento de Seguridad y Cumplimiento cuenta con un vocero, quien realiza las actividades necesarias en relación con el cumplimiento de normativa SUGEF, CGR.

Entre las debilidades que observa del cuerpo normativo, se encuentran, que la norma no refiere su incumplimiento al control interno y no afecta al patrimonio, como en el caso de la SUGEF (1% del patrimonio).

Asimismo, es débil en establecer responsabilidades, al enfocar todo el cumplimiento en el jerarca superior, a pesar de que muchas decisiones están asociadas, más a los mandos medios. Sus riesgos, como entidad bancaria, se centran en la posible exposición pública por incumplimiento o materialización de alguna de las amenazas identificadas.

Como comentario adicional, el Lic. Cuadra sugiere que la Contraloría General de la República estudie el modelo *PAM* (adapte el contenido existente de *COBIT* 4.1 dentro de un modelo de evaluación de procesos que cumple con el estándar *ISO* 15504), para la gestión de la actualización a la normativa, también indicó, la importancia de que el CONASSIF[11] aprobó el adherirse a *COBIT* como mejores prácticas internacionales.

[11] Consejo Nacional de Supervisión del Sistema Financiero

3.4.5. ENTREVISTA LIC. LUIS ROJAS OROZCO CISA

Máster en Administración y Dirección de Empresas de la UCR, CISA y CPA. Ex Subauditor Interno del Banco de Costa Rica Actualmente Gerente de Gestión Riesgo Operacional Corporativo, del Banco de Costa Rica

En principio, la implementación de las normas de ambos entes reguladores, tuvieron su problemática asociada a la falta de involucramiento de las altas direcciones, en la gestión de las tecnologías de información, en el gobierno de TI. Actualmente, no debido a que la estrategia se basó en crear comités estratégicos aprobados, donde participan dos miembros de la directiva, allí se da seguimiento a la implementación de las normas y por ende, la problemática se vio altamente disminuida.

Actualmente, existe congruencia entre los objetivos institucionales y los procesos de tecnologías de información, ese tema se ha venido mejorando mucho, hoy se cuenta con un Plan Estratégico de Tecnologías de Información (PETI) aprobado y que se encuentra alienado con el Plan Estratégico Institucional (PEI); estos puntos fueron superados de previo a las normas técnicas para la gestión y el control de las tecnologías de información, debido a la reglamentación de SUGEF, que obligatoriamente se debe cumplir.

Una vez superados los temas anteriores, el rol de las altas direcciones ha sido de liderazgo, mejorado en función de la creación de los citados comités estratégicos de tecnologías, los cuales, por ejemplo, se encargan de llevar a junta los temas asociados a riesgos, al menos tres veces al año.

En cuanto al rol de tecnologías de información, el Banco considera que ambos son responsables, dado que en nivel del comité estratégico de TI, se encarga de darle control y poder al encargado del proyecto de implementación, el cual actualmente se dividió en equipos, con un objetivo de control del *COBIT* para cada uno, verificando que ello cumpla con la Contraloría General de la República también, y todos esos encargados responden al director del proyecto (subgerente general).

Muchos de esos equipos encargados de objetivos de *COBIT* están compuestos en su totalidad por funcionarios de TI, y otros sí están combinados con personal del giro de negocio; no obstante, el peso más fuerte está en TI.

Si no se cumpliera con el esquema normativo que rige al Banco, se corre el riesgo de sanciones por parte de los entes reguladores, (ambos) terminando en pérdidas económicas y de reputación para el Banco. Actualmente la mitigación se canaliza con un adecuado esquema de gobierno corporativo y de tecnologías de información, dándole seguimiento al referido comité, estableciendo el tema como un proyecto de importancia para el Banco y asignándole un patrocinador.

En cuanto a las mejoras deseables para las normas técnicas para la gestión y el control de las tecnologías de información, el Lic. Rojas comentó, sobre la necesidad de establecer categorías institucionales, que permitan definir un alcance apropiado al giro de negocio de estas y del uso de tecnología, asociado al panorama tecnológico institucional.

También es factible, que la Contraloría General de la República estudie *COBIT* y realice un esfuerzo similar al de la SUGEF. De esta forma, las instituciones pueden incluso certificarse en el cumplimiento de mejores prácticas internacionales, de acuerdo con su capacidad y negocio.

Las opiniones obtenidas mediante el sondeo de opinión calificada, resultan de suma importancia en la generación de la propuesta de actualización de las normas técnicas para la gestión y el control de las tecnologías de información, dado que el conocimiento que los profesionales en estos campos, han ido amalgamando durante la vigencia de las normas, es una ventana que permite dilucidar aspectos de interés en cuanto a formas de implementar, lecciones aprendidas en los proyectos ejecutados, nuevos esquemas, entre otros.

El aprendizaje obtenido junto con los resultados del diagnóstico efectuado, serán analizados en el capítulo IV, con el fin de establecer los lineamientos de la propuesta creada.

4. CAPÍTULO IV

4.1. ANÁLISIS DE RESULTADOS

Las normas técnicas para la gestión y el control de las tecnologías de información, fueron emitidas en el año 2007. Tal y como se ha indicado a lo largo del presente trabajo, la Contraloría General de la República tomó como base para la generación de este instrumento, mejores prácticas y estándares internacionales, tales como *COBIT* 3.0, *ITIL* e *ISO*, entre otros. (N-2-2007-CO-DFOE, 2007)

La presente propuesta ahonda, en los resultados obtenidos durante los cinco años en que este cuerpo normativo ha tenido vigencia, tomando en cuenta aspectos tales como el macro proyecto de tecnologías, los tipos de informes y disposiciones emitidos a las instituciones, el equipo de trabajo, los marcos de control existentes, la normativa internacional, entre otros; de forma tal, que se origina la propuesta en cuestión.

4.1.1. RESULTADOS OBTENIDOS DURANTE EL MACRO PROYECTO DE TECNOLOGÍAS DE INFORMACIÓN

Una vez publicada la normativa, se establece para el año 2008 un macro proyecto de tecnologías de información, donde se buscó verificar el cumplimiento de esas normas y se obtuvo como resultado un alto nivel de incumplimiento en la muestra de instituciones fiscalizadas, siendo el área bancaria, aquella que se encontraba en mejor estado de cumplimiento debido a su obligatoriedad con el marco normativo, emitido por la SUGEF.

El macro proyecto reveló, que en muchos casos existía desconocimiento del cuerpo normativo, por parte de los fiscalizados, aunado a malas interpretaciones de lo que esa norma establecía, o bien, a la forma en que podía darse cumplimiento.

Al final del macro proyecto, los resultados evidenciaron que las auditorías internas de las instituciones tampoco estaban preparadas para comprender la norma y lograr fiscalizar su cumplimiento en las instituciones que auditaban. En particular, la ausencia de profesionales en auditoría informática o la insuficiente cantidad de personal asignado a ese departamento, fundamentaron el resultado.

Debido a los resultados del primer año del macro proyecto, los estudios del período 2009-2010, se enfocaron en temas donde se pudiera demostrar el incumplimiento de la normativa y se evidenciara la necesidad de las instituciones de dar cumplimiento, debido al alejamiento de los objetivos institucionales, que su inobservancia pudiera estar provocando.

De acuerdo con lo anterior, resulta necesario valorar también las diferentes disposiciones que se giraron durante ese macro proyecto, observando su temática y su estado actual de cumplimiento.

4.1.2. SOBRE LAS DISPOSICIONES GIRADAS DURANTE EL MACRO PROYECTO DE TECNOLOGÍAS DE INFORMACIÓN

Algunas de las disposiciones que fueron giradas, en torno a los informes emitidos, mostraron una debilidad en cuanto al objetivo original de los estudios efectuados, por cuanto se dirigieron a la resolución de problemas concernientes a las tecnologías de información, de forma ciertamente específica y en ese momento no se enfocaron en dar seguimiento y conocimiento a la normativa en cuestión, o bien, en establecer los vínculos entre la debilidad observada y el criterio en cuanto a las normas técnicas que podía solventar dicha falencia. Al respecto, se identificaron las siguientes (ver texto resaltado):

Tabla 11: Disposiciones de los Informes Emitidos en el Período 2009-2010

#	Número de informe	Ejemplos de Disposiciones giradas por la Contraloría General de la República a la institución fiscalizada
11.	DFOE-ED-IF-22-2009	En concordancia con lo establecido en el manual de normas para la gestión y control de las tecnologías de información y lo establecido en el plan que desarrolló ese instituto para la implementación de dicha norma, específicamente con respecto a las normas 3.4, inciso f) y 4.6, inciso d), la Junta Directiva deberá garantizar que el Instituto realice una valoración exhaustiva sobre su situación de dependencia respecto a sus proveedores de tecnologías de información y desarrolle una estrategia para minimizar los riesgos que ella le pueda generar.
12.	DFOE-ED-IF-77-2009	Girar las instrucciones necesarias para que en cumplimiento de las normas para la gestión y control de las tecnologías de información emitidas por esta Contraloría General se desarrolle e implemente una metodología para la gestión de proyectos de tecnologías información y, como parte de ello, se exija, cuando sea pertinente, el uso adecuado de herramientas automatizadas que faciliten la gestión de los proyectos y disponer en todo momento de información confiable, exacta, y actualizada de su ejecución, de tal manera que la Administración de RECOPE pueda dar seguimiento y efectuar las modificaciones pertinentes en relación con el avance real del proyecto respecto a lo programado.
13.	DFOE-OP-IF-18-2009	Ordenar de inmediato que el equipo responsable del proceso de implementación de las "Normas para la gestión y el control de las tecnologías de información", elabore el plan de implementación indicado en el artículo 6 de la Resolución N° R-CO-26-2007 emitida por esta Contraloría General. Ordenar a la Dirección de Informática, que como parte de la implementación de las normas incluya como actividades fundamentales la actualización del PETI, de acuerdo con la realidad institucional actual, y debidamente vinculado con el Plan Estratégico Institucional y el Plan Anual Operativo.
14.	DFOE-OP-IF-25-2009	Ordenar que en un plazo máximo de 22 días hábiles, contados a partir del conocimiento del presente informe, se realice una revisión exhaustiva del formato de las tablas que conforman la base de datos del Sistema de Infracciones, que permita solucionar los problemas señalados en esta nota informe, que imposibilitaron realizar las pruebas pertinentes sobre la calidad de la información que contiene el referido sistema.
15.	DFOE-PGAA-10-2009	Dejadas sin efecto
16.	DFOE-PGAA-IF-14-2009	Dictar los acuerdos por medio de los cuales se aprueba y se ordena la puesta en marcha del plan establecido para concluir la elaboración del modelo de arquitectura de información del Registro Nacional. Dictar y divulgar una política orientada a la revisión y actualización periódica del modelo de arquitectura de información institucional que se adopte y de medición del impacto de esas actualizaciones en la infraestructura tecnológica.
17.	DFOE-	Ordenar las acciones pertinentes para que se desarrollen las interfaces de los sistemas de

	SAF-06-2009	información de las entidades usuarias del SIGAF, que se encuentran pendientes de ejecución, y se conecten, en línea, para que opere, eficientemente, y pueda satisfacer los requerimientos de estos. Para tal efecto, deberán coordinarse las acciones del caso, con los jerarcas de las instituciones usuarias del SIGAF, para diseñar, implementar y conectar las interfaces requeridas para la transferencia de información, en ambas direcciones. Por otra parte, ese ministerio deberá determinar la factibilidad de adoptar las soluciones tecnológicas que tiene el s*oftware* SAP (Sistema de aplicación y procesamiento de datos); solución tecnológica en la que está basado el desarrollo del SIGAF, las cuales podrían cubrir los requerimientos y las necesidades tecnológicas actuales del SIGAF.
18.	DFOE-SM-IF-126-2009	Este informe no hace referencia a disposiciones sobre tecnologías de información
19.	DFOE-SOC-IF-30-2009	Girar las instrucciones necesarias a quien corresponda con el propósito de que de inmediato se proceda a realizar una revisión minuciosa de las actividades incluidas en el plan de implementación de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, a fin de obtener una visión clara de las labores por realizar, incorporar en el plan aquellas actividades necesarias para la implementación de las normas y que este no contenga, determinar las acciones correctivas que deben efectuarse en el corto plazo para cumplir dicho plan y, asimismo, establecer la asignación de recursos indispensables para garantizar el logro de los objetivos planteados en ese instrumento de planificación. Además, como parte de dicha labor, deberán revisarse los plazos concedidos para las diferentes tareas, así como las prioridades establecidas para su realización, con la finalidad de, en la medida de lo posible, agilizar los procesos de integración.
20.	DFOE-SOC-IF-124-2009	Ordenar al Presidente Ejecutivo la realización de las acciones necesarias para que el PANI se ajuste a la normativa técnica para la gestión y control de tecnologías de información emitidas mediante la Resolución R-CO-26-2007 del 7 de junio de 2007. El PANI deberá ajustarse a esa normativa a más tardar el 30 de setiembre de 2010, para lo cual se deberá observar el plan de implementación que se desarrolle en cumplimiento de la disposición 4.1. a) de este informe. Durante el proceso de ajuste que se realice, esa Junta Directiva deberá solicitar, a la Presidencia Ejecutiva, informes periódicos (al menos bimensuales) de los avances que se obtengan, con el propósito de que mediante un acuerdo se valide la finalización de ese proceso de ajuste.
#	**Número de informe**	**Ejemplos de disposiciones giradas por la Contraloría General de la República a la institución fiscalizada**
20.	DFOE-ED-IF-20-2010	En relación con el proyecto de modernización del sistema SACE y el desarrollo de @CE+ deberá estructurar y documentar un plan en el que se establezcan las acciones necesarias que garanticen la implementación completa del sistema @CE+, que se garantice la satisfacción de los requerimientos derivados de los procesos de negocio que soporta dicho sistema, así como la estructuración, acorde con un modelo relacional, normalización y depuración de su base de datos. Dicho plan deberá incorporar las actividades relativas al análisis e implementación de mejoras que pudieran identificarse como parte de una revisión de los procesos de negocio soportados por la aplicación, así como del desarrollo mismo de @CE+.
21.	DFOE-OP-IF-10-2010	Ordenar, en un plazo máximo de cinco días hábiles contados a partir de la recepción del presente documento por parte de esa Dirección, al equipo responsable del proceso de implementación de las “Normas para la gestión y el control de las tecnologías de información”, que elabore los ajustes necesarios para que el estudio de las normas cumpla específicamente con los requerimientos establecidos en el inciso c) del artículo 6 de la Resolución N° R-CO-26-2007 emitida por esta Contraloría General.
22.	DFOE-OP-IF-11-2010	Ordenar en un plazo de cinco días hábiles a partir del recibo de este documento, a la Dirección General de Tránsito, la elaboración de un diagnóstico que identifique las limitaciones que presentan los equipos móviles, así como de las necesidades de capacitación, para los oficiales de tránsito que lo requieran en el uso de los citados equipos. Una vez elaborado dicho diagnóstico deberá remitirse a la Junta Directiva del COSEVI para que en coordinación con ese despacho adopten las medidas correctivas procedentes. El diagnóstico deberá estar elaborado a más tardar el 30 de setiembre del 2010 y comunicar a esta Contraloría General en un plazo de cinco días hábiles a partir de esa fecha, sobre la remisión del diagnóstico respectivo al COSEVI.
23.	DFOE-OP-IF-16-2010	Ordenar, en un plazo máximo de cinco días hábiles contados a partir de la recepción del presente documento por parte de esa Dirección, que el equipo responsable del proceso de implementación de las “Normas para la gestión y el control de las tecnologías de información”, elabore los ajustes necesarios para que el estudio de las normas cumpla específicamente con los requerimientos establecidos en el inciso c) del artículo 6 de la Resolución N° R-CO-26-2007 emitida por esta Contraloría General.
24.	DFOE-OP-IF-17-2010	Ordenar al Departamento de Informática que proceda a incorporar como parte de su gestión un plan táctico y un portafolio de proyectos, debidamente vinculados con el PETI, con el propósito de mejorar la gestión de TI en el CTP. El citado plan y el portafolio de proyectos, deberán estar elaborados a más tardar el 30 de marzo de 2011.
25.	DFOE-OP-IF-19-2010	Ordenar en el plazo de los próximos cinco días hábiles, contados a partir del recibo del presente informe, la elaboración de una estrategia para el fortalecimiento del sistema de valoración de riesgo institucional, que incluya las actividades que se llevarán a cabo, así como los plazos y recursos estimados para cumplirlas. El citado plan deberá estar elaborado a más tardar el 30 de marzo de 2011 e informar en esa misma fecha a esta Contraloría General de su

		elaboración, remitiendo la documentación de respaldo correspondiente.
26.	DFOE-PGAA-IF-13-2010	Dictar una directriz para que se proceda a vincular los planes estratégicos institucionales para los años 2010-2014 y de tecnologías de información 2009-2014, a efecto de que estos documentos estén debidamente coordinados y alineados entre sí; con el propósito de que las tecnologías de información logren potenciar la consecución de los objetivos institucionales; asimismo, para que este requisito sea de acatamiento obligatorio por parte de la Administración para futuros documentos.
27.	DFOE-PGAA-IF-24-2010	Elaborar un cronograma mediante el cual se determinen las acciones para concluir la implementación de las normas técnicas para la gestión y el control de tecnologías de información, N° N-2-2007-CO-DFOE, publicadas por este órgano contralor, el referido cronograma deberá contener al menos las acciones por desarrollar, sus responsables y los plazos definidos para su consecución.
28.	DFOE-PGAA-IF-29-2010	Emitir una directriz a la persona designada para coordinar el equipo encargado del proceso de implementación de las normas TI, para que elabore y remita al despacho de la señora Ministra, informes de avance periódicos con los resultados y las recomendaciones de mejora, producto de la ejecución del plan de implementación de las normas, con el propósito de que ese despacho se asegure de que se están obteniendo mejoras significativas en la gestión de las tecnologías de información.
29.	DFOE-SAF-IF-11-2010	Establecer las acciones y plazos específicos que le permitan dar a ese despacho un seguimiento adecuado y oportuno al avance en la aplicación de las normas técnicas para la gestión y el control de las tecnologías de información, durante el período de ejecución de la contratación que ese Ministerio ha efectuado para el modelo de los procesos y el cumplimiento de dicha normativa, con el fin de garantizarse al término del plazo fijado para dicha contratación, el cumplimiento pleno de las normas.
30.	DFOE-SM-IF-21-2010	Diseñar, en el término de seis meses, contados a partir de la recepción del presente informe, con la participación activa del Comité Gerencial de Informática y de las demás unidades administrativas y funcionarios que se consideren pertinentes, un plan de acción que permita solucionar de manera integral, oportuna, efectiva y permanente, las deficiencias expuestas en este informe, relacionadas con la calidad de información del Sistema "Elisiam", en el que se incluyan como mínimo, las actividades específicas por realizar, los recursos necesarios, los funcionarios responsables de su ejecución y seguimiento, así como el plazo máximo para su cumplimiento, el cual no podrá sobrepasar el lapso de 12 meses después de propuesto el plan.
31.	DFOE-SM-IF-22-2010	Diseñar, en el término de seis meses, con la participación activa de las unidades administrativas y funcionarios que se consideren pertinentes, un plan de acción que permita solucionar de manera integral, oportuna, efectiva y permanente, las deficiencias expuestas en este informe, relacionadas con la calidad de información del sistema "SIIM", en el que se incluyan como mínimo, las actividades específicas por realizar, los recursos necesarios, los funcionarios responsables de su ejecución y seguimiento, así como, el plazo máximo para su cumplimiento, el cual no podrá sobrepasar el lapso de 12 meses después de propuesto el plan.
32.	DFOE-SM-IF-23-2010	
33.	DFOE-SM-IF-24-2010	
34.	DFOE-SM-IF-25-2010	
35.	DFOE-SM-IF-26-2010	Diseñar, en el término de seis meses, con la participación activa de las unidades administrativas y funcionarios que se consideren pertinentes, un plan de acción que permita solucionar de manera integral, oportuna, efectiva y permanente, las deficiencias expuestas en este informe, relacionadas con la calidad de información del sistema "RUC", en el que se incluyan como mínimo, las actividades específicas por realizar, los recursos necesarios, los funcionarios responsables de su ejecución y seguimiento, así como el plazo máximo para su cumplimiento, el cual no podrá sobrepasar el lapso de 12 meses después de propuesto el plan.
36.	DFOE-SM-IF-27-2010	Diseñar, en el término de seis meses, con la participación activa de las unidades administrativas y funcionarios que se consideren pertinentes, un plan de acción que permita solucionar de manera integral, oportuna, efectiva y permanente, las deficiencias expuestas en este informe, relacionadas con la calidad de información del sistema "Integra", en el que se incluyan como mínimo, las actividades específicas por realizar, los recursos necesarios, los funcionarios responsables de su ejecución y seguimiento, así como el plazo máximo para su cumplimiento, el cual no podrá sobrepasar el lapso de 12 meses después de propuesto el plan.
37.	DFOE-SOC-IF-69-2010	Girar las instrucciones pertinentes para que se realice un análisis de lo actuado por la Comisión Gerencial de Tecnologías de Información, en relación con la implementación de la normas técnicas para la gestión y control de las tecnologías de información, de modo que se revise si las acciones propuestas por dicha comisión en el "PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES 2008-2009", son suficientes para lograr de manera razonable, los propósitos establecidos en las citadas normas; tomar las medidas correctivas pertinentes y además, se subsanen las omisiones detectadas en relación con las normas que en dicho documento no contaban con acciones para su implementación.
38.	DFOE-SOC-IF-77-2010	Consignar en las actas que documentan las sesiones de ese comité, los acuerdos y decisiones que se toman, de manera que quede explícita la acción que se decidió tomar. Remitir a esta Contraloría General el documento en el que consignen las acciones realizadas para el cumplimiento de esta disposición, a más tardar el 14 de enero de 2011.

Fuente: Elaboración propia con base en el contenido de los informes de fiscalización emitidos por la Contraloría General de la República.

En la Tabla 11, se muestran las disposiciones de los informes emitidos en el período 2009-2010, por ejemplo, realizar una revisión exhaustiva del formato de las tablas que conforman la base de datos del sistema, o bien desarrollar las interfaces de los sistemas de información de las entidades usuarias, aspectos que van orientados a resolver efectos y no se atacan las causas que están generando esas debilidades, las cuales posiblemente se vean asociadas a problemáticas relacionadas con la forma como se vinculan las instituciones con los objetivos del negocio, y el aporte que TI al respecto.

Al finalizar el macro proyecto, la gestión de la Contraloría General de la República para seguir controlando la aplicación de las normas, pasó a ser parte del giro operacional acostumbrado en el ente contralor, es decir, la ejecución de estudios de fiscalización en las instituciones, en este caso con temática de tecnologías, cuyo análisis se aborda a continuación.

4.1.3. SOBRE LOS INFORMES EMITIDOS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA (POSTERIORES AL MACRO PROYECTO DE TI)

Para el periodo comprendido entre los años 2011-2012, la División de Fiscalización Operativa y Evaluativa, emitió 17 informes de auditoría[12], de los cuales solamente cuatro se enfocan en la gestión de las tecnologías de información, o bien, en el seguimiento de la implementación de las normas técnicas para la gestión y el control de las tecnologías de información.

[12] Ver Informes de TI 2009-2012 (DIVISIÓN DE FISCALIZACIÓN OPERATIVA Y EVALUATIVA INFORMES DE FISCALIZACIÓN POSTERIOR EMITIDOS POR INSTITUCIÓN FISCALIZADA EN MATERIA DE TI 2009-2010-2011-2012)

Tabla 12: Informes emitidos en el período comprendido entre los años 2011-2012

INSTITUCIÓN FISCALIZADA	NOMBRE DEL INFORME	NÚMERO
1. MINISTERIO DE SALUD	INFORME ACERCA DEL CUMPLIMIENTO POR PARTE DEL MINISTERIO DE SALUD DE LAS OBLIGACIONES ESTABLECIDAS EN LA LEY PARA LA GESTIÓN INTEGRAL DE RESIDUOS N° 8839 GESTIÓN INTEGRAL DE RESIDUOS N° 8839	DFOE-AE-IF-15-2011
2. MUNICIPALIDADES DEL PAÍS	INFORME SOBRE LAS TECNOLOGÍAS DE INFORMACIÓN EN EL SECTOR MUNICIPAL	DFOE-DL-IF-35-2011
3. SENARA	SOBRE LA CALIDAD Y SEGURIDAD DE LA INFORMACIÓN RELEVANTE OPERADA POR LOS SISTEMAS DE INFORMACIÓN AUTOMATIZADOS Y ALMACENADA EN LAS BASES DE DATOS DEL SERVICIO NACIONAL DE AGUAS SUBTERRÁNEAS, RIEGO Y AVENAMIENTO.	DFOE-AE-IF-09-2011
4. DESAF	SOBRE EL SISTEMA DE INFORMACIÓN ÚNICO DE BENEFICIARIOS Y POBLACIÓN OBJETIVO PARA LOS PROGRAMAS SOCIALES SELECTIVOS.	DFOE-SOC-IF-12
5. COMISIÓN NACIONAL DE PREVENCIÓN DE RIESGOS Y ATENCIÓN DE EMERGENCIAS	SOBRE EL ESTUDIO DE FISCALIZACIÓN SOBRE LA EVALUACIÓN DE LOS SISTEMAS DE INFORMACIÓN EN LA COMISIÓN NACIONAL DE PREVENCIÓN DE RIESGOS Y ATENCIÓN DE EMERGENCIAS	DFOE-PG-IF-05-2011
6. ICE	SOBRE LOS RESULTADOS DEL ESTUDIO RELACIONADO CON EL CUMPLIMIENTO POR PARTE DEL INSTITUTO COSTARRICENSE DE ELECTRICIDAD DE LA NORMATIVA SOBRE TECNOLOGÍAS DE INFORMACIÓN	DFOE-IFR-IF-7-2011
7. INVU	ESTUDIO SOBRE EL CUMPLIENTO DE LA NORMATIVA EN TI EN EL INVU	DFOE-EC-IF-04-2011
8. INVU	SOBRE LOS RESULTADOS DEL ESTUDIO EFECTUADO EN EL INSTITUTO NACIONAL DE VIVIENDA Y URBANISMO RELACIONADO CON LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN.	DFOE-EC-IF-10-2011
9. INVU	SOBRE LOS RESULTADOS DEL ESTUDIO EFECTUADO EN EL INSTITUTO NACIONAL DE VIVIENDA Y URBANISMO RELACIONADO CON LAS CONTRATACIONES PARA EL MANTENIMIENTO Y MODERNIZACIÓN DE SU PLATAFORMA TECNOLÓGICA.	DFOE-EC-IF-12-2011
10. BANHVI	SOBRE LOS RESULTADOS DEL ESTUDIO SOBRE LA GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN EFECTUADO EN EL BANCO HIPOTECARIO DE LA VIVIENDA.	DFOE-EC-IF-15-2011
11. BANCO CENTRAL DE COSTA RICA (BCCR)	SOBRE EL CUMPLIMIENTO DE REQUERIMIENTOS RELACIONADOS CON LA ADQUISICIÓN DE LICENCIAS DE *SOFTWARE* EN EL BANCO CENTRAL DE COSTA RICA (BCCR).	DFOE-EC-IF-15-2012
12. MINAET, SUTEL, MICIT Y SECRETARÍA TÉCNICA DE GOBIERNO DIGITAL	AUDITORÍA OPERATIVA SOBRE LAS INICIATIVAS QUE IMPULSAN EL DESARROLLO DEL GOBIERNO DIGITAL Y DE UNA SOCIEDAD BASADA EN LA INFORMACIÓN Y EL CONOCIMIENTO EN COSTA RICA.	DFOE-IFR-IF-5-2012
13. MUNICIPALIDAD DE HEREDIA	AUDITORÍA DE CARÁCTER ESPECIAL ACERCA DE DEBILIDADES EN LA CALIDAD DE LA INFORMACIÓN CONTENIDA EN LAS BASES DE DATOS DE COBROS DE TRIBUTOS EN LA MUNICIPALIDAD DE HEREDIA.	DFOE-DL-IF-13-2012

14. MUNICIPALIDAD DE SAN CARLOS.	SOBRE DEBILIDADES EN LA CALIDAD DE LA INFORMACIÓN CONTENIDA EN LAS BASES DE DATOS DE COBROS DE TRIBUTOS EN LA MUNICIPALIDAD DE SAN CARLOS.	DFOE-DL-IF-14-2012
15. INSTITUTO NACIONAL DE APRENDIZAJE (INA)	AUDITORÍA DE CARÁCTER ESPECIAL SOBRE EL PLAN DE CONTINUIDAD DE LOS SISTEMAS DE INFORMACIÓN QUE SOPORTAN LAS ACTIVIDADES SUSTANTIVAS DEL INSTITUTO NACIONAL DE APRENDIZAJE.	DFOE-EC-IF-08-2012
16. BANCO POPULAR Y DE DESARROLLO COMUNAL (BPDC)	AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA GESTIÓN DEL PROYECTO *CORE SYSTEM* POR PARTE DEL BANCO POPULAR Y DE DESARROLLO COMUNAL.	DFOE-EC-IF-11-2012
17. DIRECCIÓN GENERAL DE MIGRACIÓN Y EXTRANJERÍA (DGME)	AUDITORÍA DE CARÁCTER ESPECIAL SOBRE EL PROCESO DE ADQUISICIÓN DEL DOCUMENTO DE IDENTIDAD MIGRATORIA PARA EXTRANJEROS (DIMEX)	DFOE-PG-IF-21-2012

Fuente: Elaboración propia con base en reporte emitido por la División de Fiscalización Operativa y Evaluativa.

Como se observa en los 13 informes restantes, la temática de TI se aborda en función de temas específicos como contrataciones, calidad de la información, continuidad de los sistemas, entre otros.

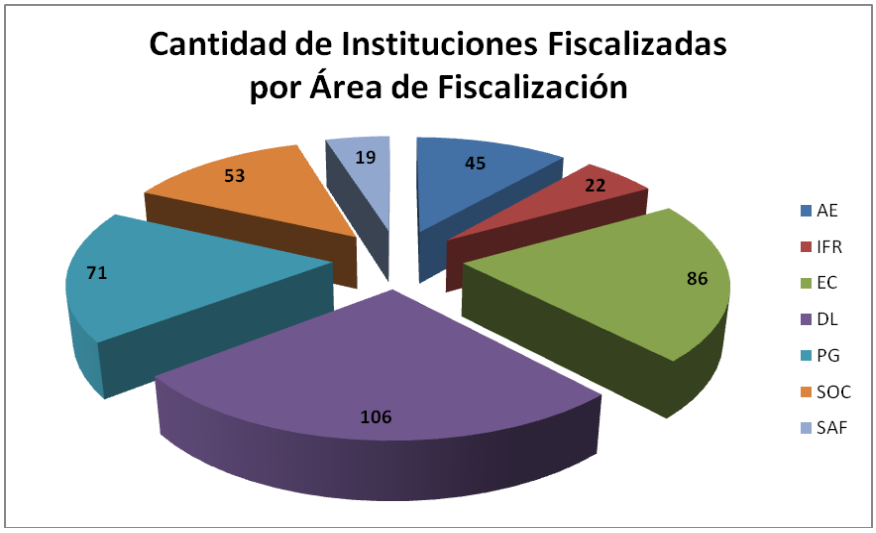
La situación descrita, podría ir en detrimento de la adecuada fiscalización de las normas técnicas en las instituciones, dado que las gestiones de la Contraloría General de la República, se están enfocando en situaciones particulares atinentes a las tecnologías de información, sin ahondar en aspectos de la gestión como tal, de forma que se evidencien aspectos de los fiscalizados, que podrían generar más valor, en cuanto a la gobernabilidad de las tecnologías de información en el sector público y así disponer, en función de generar cambios positivos, en la gestión de las TI.

En virtud de lo anterior, la finalización del macro proyecto y la gestión efectuada sin su guía, parecen indicar que los esfuerzos realizados para la creación de las normas técnicas para la gestión y el control de las tecnologías de información, han perdido el norte en cuanto a la aspiración original, de lograr que las instituciones fiscalizadas

gestionaran de la mejor manera su uso de las tecnologías, en función del aporte que estas puedan brindar, para el logro de los objetivos de negocio.

Aunada a lo anterior, la ausencia de una gestión organizada por parte de la Contraloría General de la República, en torno a la fiscalización de las normas técnicas para la gestión y el control de las tecnologías de información, revela una leve planificación y seguimiento de este tema (posterior al macro proyecto), aspecto que se evidencia en la forma como se está abordando el universo de fiscalización del órgano contralor, el cual actualmente ronda en 402 instituciones[13], asignadas a una de las siete áreas de fiscalización que forman parte de la DFOE, tal y como se observa en la siguiente ilustración:

Ilustración 23: Instituciones fiscalizadas por la DFOE

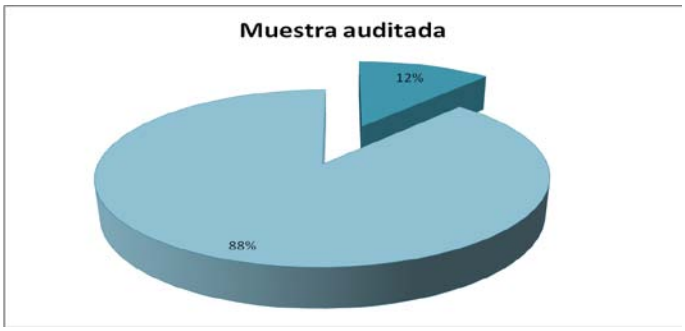


Fuente: Elaboración propia con base en reporte emitido por la División de Fiscalización Operativa y Evaluativa.

[13] Ver DFOE LISTA DE INSTITUCIONES DE FISCALIZACIÓN A Enero 2013

De esas 402 instituciones que conforman el universo auditable de la Contraloría General de la República, se han fiscalizado en el tema de tecnologías de información una cantidad de 47 instituciones diferentes[14] en un período de cinco años, desde la emisión de la normativa, es decir, el 12% de la totalidad, tal y como se representa en la ilustración siguiente:

Ilustración 24: Porcentaje de Instituciones fiscalizadas



Fuente: Elaboración propia con base en los diferentes reportes presentados.

Con base en los resultados de la investigación, sobre los informes emitidos, posteriores al macro proyecto, se observa falta de consistencia en cuanto al seguimiento que se realizó, respecto de la implementación de las normas técnicas por parte de la Contraloría General de la República. Además, la forma de abordar el universo auditable, pareciera no tener un enfoque establecido, basado en gestión de riesgos u otro criterio de interés.

Asimismo, una vez que se verificó lo actuado por la Contraloría General de la República, en materia de informes y disposiciones, resulta de interés analizar los resultados del estudio de tendencias tecnológicas, realizado con el fin de indagar sobre la posible desactualización de la norma actual.

[14] Ver Diferentes instituciones fiscalizadas en el período 2007-2012 en TI

4.1.4. SOBRE LAS NUEVAS TENDENCIAS DE TI Y LA APLICACIÓN DE LA NORMATIVA DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA

Otro aspecto que ha afectado el tema de la fiscalización de las tecnologías en Costa Rica, está asociado a que esta temática es sumamente cambiante, las tecnologías avanzan y se modifican a un ritmo vertiginoso, por lo cual, resulta difícil que el ente contralor le siga el paso, en cuanto a la actualización de la normativa vigente y al personal que tiene destacado para su fiscalización.

Las actuales normas técnicas, para la gestión y el control de las tecnologías de información, han experimentado cierta desactualización en los cinco años de su vigencia, situación que se evidencia con el estudio de nuevas tendencias, realizado en el capítulo anterior, donde se enlistan las novedades en materia de TI, respecto de las cuales la normativa presenta algunas debilidades, en su fiscalización, por ejemplo, aspectos tales como *BYOD*, computación en la nube, virtualización, redes sociales, computación móvil, entre otros.

Lo anterior se evidenció mediante la siguiente tabla, donde se agregaron las tendencias estudiadas en el capítulo II, y se estableció si las normas técnicas para la gestión y el control de las tecnologías de información actuales, permiten realizar una fiscalización de dichos temas.

Tabla 13: Revisión de las Tendencias en TI y si las Normas Técnicas Permiten su Fiscalización

Tendencia	Concepto	Normativa aplicable
BYOD	Estrategia alternativa, que permite a los empleados, socios de negocio y otros usuarios, utilizar dispositivos seleccionados y comprados por ellos mismos, para ejecutar aplicaciones y acceso a información dentro de la empresa.	No

Big data	*Big data* es el nombre dado al manejo de grandes y variados volúmenes de información a altas velocidades, conjuntos de datos que demandan conceptos de efectividad y rentabilidad en su manejo, adicionado a la búsqueda de formas innovadoras para mejorar su comprensión, para mejorar el conocimiento y la toma de decisiones.	No
Computación en la nube	Modelo para habilitar un cómodo acceso en red por demanda a un *pool* compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se puede conformar y proveer rápidamente con un esfuerzo administrativo mínimo o una interacción mínima con el proveedor de servicios.	No
Virtualización	Representación de algo en forma virtual (en lugar de real). En la tecnología de información empresarial (TI), la virtualización altera la arquitectura técnica porque permite la ejecución de diferentes recursos en un entorno único (o de varias capas).	No
Inteligencia de negocios *(Business Intelligence BI)*	Método para almacenar y presentar datos claves de la empresa para que cualquier persona pueda hacer preguntas de forma rápida y fácil sobre los datos precisos y oportunos. *BI* permite al usuario final utilizar los datos para entender por qué su empresa obtuvo los resultados particulares logrados, para decidir cursos de acción basándose en los datos del pasado, y así pronosticar con precisión los resultados futuros.	N/A
Computación móvil	Computación basada en los dispositivos móviles que ofrecen a las empresas la capacidad de mantener a sus empleados conectados en todo momento, lo que ha permitido al público la posibilidad de llevar a cabo negocios en cualquier lugar, ya sea en casa, en la oficina, o viajando entre destinos.	No
Firma digital	Método que asocia la identidad de una persona o equipo, con un mensaje o documento electrónico, para asegurar la autoría y la integridad de este. La firma digital del documento es el resultado de aplicar algoritmos matemáticos, (denominados función *hash*), a su contenido y así generan una firma digital del documento.	Sí
Calidad de los datos	La calidad de la información contribuye y resulta ventajosa al ofrecer la información correcta, en el momento adecuado, en el lugar correcto, a la gente adecuada, dado que no es posible tomar decisiones de negocio efectivas con datos erróneos, incompletos o engañosos. Se necesita información confiable y actualizada en pro del logro de los objetivos de negocio.	Sí
Redes sociales	Consiste en la creación y difusión de contenidos a través de redes sociales, por medio de Internet. Las diferencias entre los medios tradicionales y sociales se definen por el nivel de interacción a disposición del consumidor. El uso de las redes sociales ha creado plataformas de comunicación muy eficaces donde cualquier usuario, en cualquier parte del mundo, puede libremente crear contenidos y difundir esta información en tiempo real a una audiencia global.	No

Fuente: Elaboración propia con base en las tendencias investigadas en el capítulo II.

La revisión de las tendencias en TI permite identificar, que algunas de las nuevas tendencias en el mundo de las tecnologías, no están siendo abordadas o aseguradas por las normas técnicas para la gestión y el control de las tecnologías de información, entre ellas *BYOD*, *Big data* y computación en la nube.

Esta situación es previsible, ya que en el caso de la Contraloría General de la República el giro de negocio va en función de la fiscalización, no directamente en estar a la vanguardia en temas de tecnologías; por lo tanto, su gestión de normativa enfocada en este tema, puede contemplar como debilidad aspectos de conocimiento experto en TI y en su oportunidad de actualización.

Por otra parte, existen en el mercado diferentes marcos de control asociados a la gestión de las tecnologías de información; en la Contraloría General de la República, la tendencia ha sido la utilización de *COBIT*; por lo tanto, su uso se aborda seguidamente.

4.1.5. SOBRE EL USO DE COBIT Y OTRAS MEJORES PRÁCTICAS EN LA CONTRALORÍA GENERAL DE LA REPÚBLICA

Debido a las debilidades observadas en la fiscalización de las tecnologías de información, por causa de la tímida implementación de las normas técnicas, para la gestión y el control de las tecnologías de información, aunada a la falta de detalle que esta norma ha representado, tanto para el auditado como para el auditor, ha resultado una práctica común entre los informes de auditoría, el relacionar los temas abordados con el cuerpo normativo, asociándolos directamente, con las mejores prácticas de nivel internacional, como *COBIT*, por ejemplo:

Informe DFOE-SOC-IF-30-2009: Respecto a los documentos suministrados, ninguno corresponde al Modelo de Arquitectura de Información, que según el *COBIT*, en el apartado "P02", está constituido por el Diccionario Corporativo de Datos, las Reglas de Sintaxis de datos de la organización, Esquema de Clasificación de Datos y Niveles de Seguridad.

Informe DFOE-PGAA-10-2009: Para más abundamiento sobre el particular, en el objetivo PO1 de las mejores prácticas recogidas en el documento denominado *COBIT4*, se establece que "Se requiere una planeación estratégica de TI para administrar y dirigir todos los recursos de TI de acuerdo con la estrategia del negocio y las prioridades.

Informe DFOE-PGAA-IF-13-2010: Sobre el particular, es importante resaltar lo que se señala en el objetivo PO1 de las mejores prácticas recogidas en el documento denominado *COBIT*, en el que se establece, que "Se requiere una planeación estratégica de TI para administrar y dirigir todos los recursos de TI, de acuerdo con la estrategia del negocio y las prioridades.

Informe DFOE-PG-IF-05-2011: Es importante resaltar lo que se señala en el objetivo PO1 de las mejores prácticas recogidas en el documento denominado *COBIT6*, en el que se establece, que "Se requiere una planeación estratégica de TI para administrar y dirigir todos los recursos de TI, de acuerdo con la estrategia del negocio y las prioridades.

Llama la atención, el informe DFOE-SAF-IF-11-2010 sobre el avance en la implementación de las normas de un ministerio, donde se anexa un cuadro denominado *"Consultas para la verificación de aspectos de tecnologías de información según las Normas de Tecnologías de Información emitidas por la Contraloría General y relación con los dominios del Control Objectives for Information and Related Technology (COBIT)"*, en el cual se realiza un mapeo entre las normas técnicas para la gestión y el control de las tecnologías de información y el *COBIT*, agregando una serie de preguntas que permitan al auditor identificar su cumplimiento; por lo tanto, existe la tendencia del uso de *COBIT* en las diferentes líneas de fiscalización de la Contraloría General de la República.

A su vez, para el año 2011, se gestiona en la Contraloría General de la República un proyecto denominado "Desarrollo de herramientas metodológicas para fiscalización de tecnologías de información y seguimiento a las necesidades de las diferentes gerencias de fiscalización y la aplicación de dichas herramientas", cuyo objetivo consistió en *"aportar elementos metodológicos tendientes a reorganizar y fortalecer la fiscalización de tecnologías de información en instituciones del sector público"*.

Como parte de la descripción del modelo para el manejo de información sobre la gestión de TI del sector público, que se presentó con dicho proyecto, se estableció que:

> Por otra parte los "Objetivos de Control para Tecnologías de Información y Tecnologías Relacionadas" (*COBIT* por sus siglas en inglés) aportan una arquitectura completa de procesos para la gestión de

TI, que al mapearse con las normas técnicas (NTGCTI) pemiten identificar los procesos de TI, cuya ejecución impulsa el cumplimiento de las NTGCTI.

Elementos proporcionados por *COBIT* para describir cada proceso se convierten en elementos de referencia para construir índices de cumplimiento de las NTGCTI. Como parte de esos elementos para cada proceso se encuentran descripciones sobre objetivos de control, insumos, productos, matrices *RACI*[15], metas, métricas y modelos de madurez.

En virtud de lo anterior, se observa en la Contraloría General de la República una marcada tendencia en la utilización del *COBIT* y sus diferentes herramientas, para promover mejoras en los estudios de fiscalización, en la interpretación de la normativa actual, e incluso en mapeos generados para facilitar la implementación y seguimiento de las normas técnicas para la gestión y el control de las tecnologías de información.

Además, se indagó sobre la existencia de normativas en función de la gestión de las tecnologías de información, en otros países como Venezuela y Chile.

4.1.6. NORMATIVAS INTERNACIONALES SOBRE TECNOLOGÍAS DE INFORMACIÓN

[15] Matriz RACI: Ilustra quién es responsable, quién debe rendir cuentas, a quién se debe consultar e informar dentro de un marco de trabajo organizacional estándar.

La investigación permitió identificar qué países, como Venezuela y Chile (considerados desarrollados en la temática de tecnologías de información), cuentan con un compendio de normativa atinente a las tecnologías de información. No obstante, el análisis permitió corroborar, que este esfuerzo parte de lo particular hacia lo general, siendo que se atienden por medio de regulaciones específicas, aspectos que han venido generando incidentes como delitos informáticos, para los cuales la falta de un esquema normativo que permita generar sanciones ha sido la motivación, en algunos de esos casos, para la creación o emisión de dichas normativas.

En el caso particular de Chile, el fuerte de la gestión de TI se revisa o aborda desde la perspectiva del control interno como tal, y se han emitido algunos reglamentos específicos para tratar temas como la confidencialidad y seguridad de los datos.

Para Venezuela, existe el CNTI, institución adscrita al Ministerio del Poder Popular para Ciencia, Tecnología e Innovación (MCTI) que permite potenciar los esfuerzos que en materia de informática se desarrollen en el Sector Gobierno y en las Comunidades Organizadas.

Por lo tanto, la Contraloría General de la República es innovadora en su gestión de las tecnologías mediante el instrumento normas técnicas para la gestión y el control de las tecnologías de información, desde el cual se observa la prevención y gestión de los fondos públicos que se asignan al uso de las TI.

4.2. PROPUESTA DE ACTUALIZACIÓN

Las organizaciones, grandes y pequeñas, ven en los controles la oportunidad de asegurarse que se está avanzando satisfactoriamente, hacia las metas y objetivos trazados y con ello verificar que lo que hacen, se realiza de la mejor manera posible.

Las actividades comprenden políticas, procedimientos, mecanismos, prácticas y una serie de medidas que se adoptan para conducir la gestión y asegurar que esta se oriente eficazmente, al logro de los objetivos institucionales.

Las actividades y controles deben establecerse y ejecutarse como parte de las operaciones, en toda la organización, en todos los niveles y en todas las funciones, como medio para asegurar que se apliquen las acciones necesarias para manejar y minimizar los riesgos y realizar una gestión eficiente y eficaz.

Los controles no aportan una certeza absoluta a la institución respecto del logro de los objetivos, sino sólo una seguridad razonable en tal sentido. Esto obedece a que, dada la necesidad de priorizar las asignaciones de recursos, los controles no pueden cubrir todos los riesgos que la institución enfrenta, sino sólo aquellos que se consideren relevantes, y además, que pueden estar expuestas a desacato, error o colusión.

Las organizaciones actuales se desempeñan en un contexto caracterizado por el cambio constante, y en consecuencia, por retos siempre nuevos.

El advenimiento de la tecnología a los ambientes organizacionales, condujo a tomar en cuenta, como parte de toda esa gestión de controles en pro del logro de los objetivos, lo atinente a la aplicación de las tecnologías de información en los procesos operativos, estratégicos y demás, propios de las labores de cada institución.

De acuerdo con lo indagado, las normas técnicas para la gestión y el control de las tecnologías de información, han experimentado dificultades en cuanto a su establecimiento, implementación y cumplimiento en el sector público nacional y en los cinco años de estar en vigencia, no se ha logrado un entendimiento de la norma como tal, ni se ha interiorizado su importancia para obtener una seguridad razonable en cuanto a lograr los objetivos trazados.

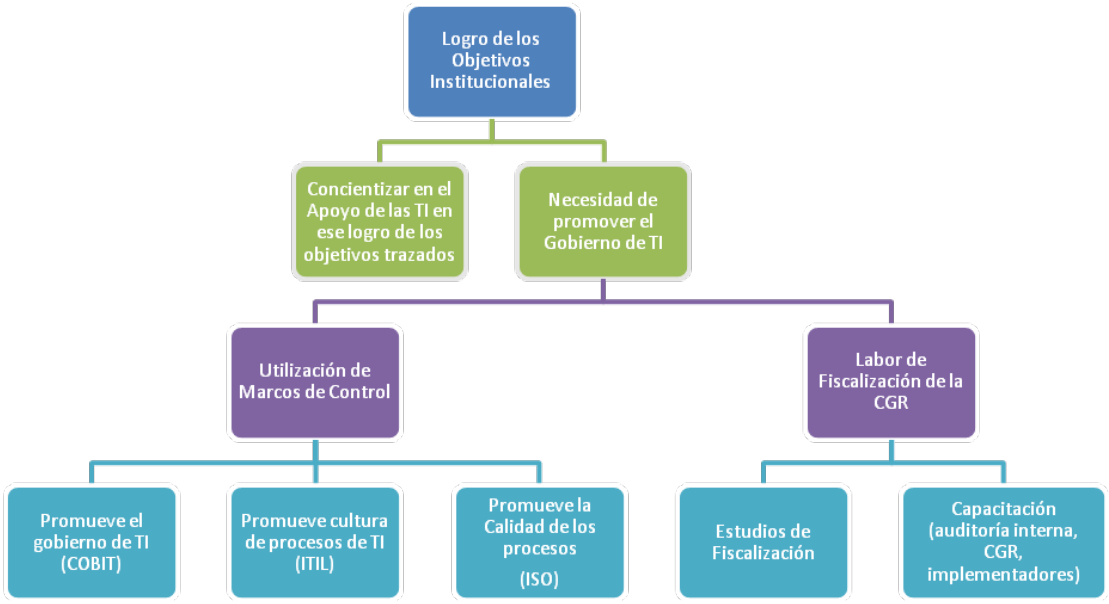
Lo expuesto anteriormente, así como los resultados que se han venido documentando a lo largo del presente trabajo, son la motivación para promover una nueva forma de abordar las tecnologías de información y su fiscalización, en la Contraloría General de la República, partiendo de un enfoque basado en el aprovechamiento de los recursos que ya existen en el mercado, y que con los años han desarrollado un nivel de experiencia reconocido en el mundo.

Las normas técnicas vigentes, a pesar de no detallarlo como parte de su contenido, buscaron coadyuvar en el logro de los objetivos institucionales, en todo el espectro fiscalizable del sector público. No obstante, según se ha estudiado en este documento, existen otros organismos que se han dedicado a establecer cómo TI puede apoyar dicho logro, definiendo marcos de control de aceptación internacional, que incluso han sido

asumidos por entidades como la SUGEF, promoviendo su implementación y cumplimiento en el sector bancario .

De acuerdo con lo anterior, la propuesta de actualización de la forma como se fiscalizan las tecnologías de información en la CGR, se detallan en la siguiente ilustración, la cual resume los componentes de mayor importancia, por ser considerados en la gestión que debe realizar el órgano contralor.

Ilustración 25: Principales Componentes de la Propuesta de Actualización de las Normas Técnicas para la GT Gestión y el Control de las Tecnologías de Información



Fuente: Elaboración propia con base en el estudio y análisis efectuado.

Tal como se indica, la propuesta de actualización de las normas técnicas para la gestión y el control de las tecnologías de información, está en función de cooperar con la gestión de las instituciones, en cuanto al aprovechamiento de las tecnologías en la consecución de los objetivos organizacionales.

En función de lo anterior, compete a la CGR enfocar su esfuerzo en dos aspectos de suma importancia, concienciar respecto a la aplicación de las tecnologías de información en los procesos operativos, estratégicos de las instituciones, siendo este un proceso que conlleva un esfuerzo de capacitación, tanto en el ámbito interno, como en el externo, de la Contraloría.

Ese proceso de concienciación necesita, ser liderado por un equipo de funcionarios que se especialice y dedique completamente a gestionar la implementación de la propuesta, a generar los productos necesarios para la implementación en las instituciones, dándole seguimiento por un tiempo prudencial (al menos cinco años o bien hasta cumplir con un esquema de madurez establecido) al proceso que se lleve a cabo. Lo anterior se concluye, de acuerdo con lo que se observó como resultado del macro proyecto de TI, efectuado por la CGR en el período 2008-2010, donde fue posible apreciar claramente, el efecto negativo de que este equipo no estuviera directamente concentrado en dicho proceso, aunado a que la duración de este no fue suficiente.

El equipo mencionado anteriormente debe considerar, como parte de los procesos de una nueva fiscalización de TI, promover el interés, conocimiento, implementación y seguimiento del establecimiento de gobierno de TI interna y externamente de la CGR.
Para lograrlo, la propuesta se enfoca en la utilización de aquellos estándares que han sido emitidos por organismos altamente calificados, en la difícil y cambiante temática de TI, los cuales tienen dicho tema como giro de negocio perenne, y se encuentran a la vanguardia de las nuevas tendencias del mercado tecnológico, así como en la protección de los activos, ante los riesgos que las estas conllevan.

De acuerdo con el párrafo anterior, se propone que la Contraloría General de la República valore ampliamente los marcos de control ya existentes, seleccione uno y gestione su obligatoriedad en el sector público. Al respecto, esta propuesta manifiesta que la mejor elección sería la utilización de los Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas (*COBIT*, por sus siglas en inglés); debido a que dicho recurso está orientado a los objetivos y al alcance del gobierno de TI, asegurando que su marco de control sea integral, que se alinee con los principios de gobierno corporativo y, por lo tanto, que sea aceptable para los consejos directivos, para la dirección ejecutiva e informática, los auditores y los reguladores.

Si bien existen otros marcos de control o estándares, de suma validez y calidad, por ejemplo *ITIL* y algunos *ISO*, estos podrían ser utilizados directamente por las instituciones fiscalizadas, como parte del cómo hacer sus procesos y llegar al cumplimiento; no obstante, en esos casos, cada organismo puede adoptar el marco deseado y la Contraloría General de la República puede realizar su fiscalización, sobre lo establecido por la institución.

En el caso particular de la gestión de TI, el órgano contralor puede establecer la obligatoriedad del marco de control *COBIT*, dentro de un programa de trabajo ordenado, determinado a lograr una implementación conjunta de las instituciones, estableciendo tal y como lo hizo SUGEF, la implementación de los 34 objetivos de control, de forma escalonada en variables de tiempo y tipo de institución.

Por ende, se propone que la CGR realice una clasificación apropiada de las instituciones que forman parte de su espectro de fiscalización, para lo cual debería contemplar al

menos aspectos tales como: tamaño de la institución, presupuesto general, el presupuesto asignado a las tecnologías de información, recurso humano especializado en TI, riesgo del giro de negocio de la institución.

Con base en esa clasificación, la CGR puede establecer cuáles son los objetivos de control que deben ser primeramente atendidos por las instituciones. En esta propuesta, se considera que la mejor opción sería iniciar con los objetivos de control, que permitan implementar el gobierno de TI dentro de cada institución, que consiste en el liderazgo, los procesos y las estructuras, capaces de asegurar que las tecnologías de la organización apoyan los objetivos y estrategias de la empresa.

El gobierno de TI efectivo, representa un proceso (no un fin), el cual se enfoca en un valor sustentable y confiabilidad a través del negocio. La implementación de un adecuado gobierno de TI, se debe dar considerando diferentes condiciones y circunstancias, determinadas por numerosos factores, tanto del ambiente interno como externo de la organización, tales como: (Sáenz, 2012)

- Ética y cultura de la comunidad y la organización.
- Legislación, regulaciones y políticas internas y externas.
- Prácticas de la industria.
- Misión, visión, metas y valores de la organización.
- Modelos organizacionales de roles y responsabilidades.
- Políticas y prácticas sobre gobernabilidad establecidas en la organización.
- Planes de negocio y expectativas estratégicas.
- Nivel de madurez del modelo de operación de la organización.

- Cultura y estilo de administración de la organización.
- Madurez de la organización.

Como parte de ese proceso escalonado, necesario para que la implementación del marco de control se realice, enfocada en logros a corto plazo y la priorización de las mejoras más beneficiosas y más fáciles de implementar, esta propuesta plantea la pertinencia de adoptar los modelos de madurez que ofrece *COBIT*, asociándolos a la clasificación que se haya realizado de las instituciones y a la selección de los objetivos de control establecidos, de mayor prioridad.

Por ejemplo, la SUGEF estableció en el transitorio I, que para efectos de la aplicación de lo dispuesto en los artículos 6, 11 y 12 de ese reglamento, se establece la siguiente gradualidad en los niveles de madurez, para los procesos dispuestos como obligatorios en el marco para la gestión de TI y su evaluación externa independiente: (SUGEF, 2013)

Ilustración 26: Gradualidad en los Niveles de Madurez para los Procesos Dispuestos como Obligatorios

Procesos COBIT®	Primera Auditoría Externa	Segunda Auditoría Externa	Auditorías subsecuentes
PO9 Evaluar y administrar los riesgos de TI PO10 Administrar proyectos AI6 Administrar cambios DS2 Administrar los servicios de terceros DS4 Garantizar la continuidad del servicio DS5 Garantizar la seguridad de los sistemas DS11 Administrar los datos ME2 Monitorear y evaluar el control interno	Nivel madurez mínimo requerido: **tres**	Nivel madurez mínimo requerido: **tres**	Nivel madurez mínimo requerido: **tres**
PO1 Definir un plan estratégico de TI PO3 Determinar la dirección tecnológica PO5 Administrar la inversión en TI AI3 Adquirir y mantener infraestructura tecnológica AI5 Adquirir recursos de TI DS3 Administrar el desempeño y la capacidad DS 9 Administrar la configuración DS10 Administrar los problemas DS12 Administrar el ambiente físico	Nivel madurez mínimo requerido: **dos**	Nivel madurez mínimo requerido: **tres**	Nivel madurez mínimo requerido: **tres**
Resto de los procesos que integran el marco para la gestión de TI	Nivel madurez mínimo requerido: **uno**	Nivel madurez mínimo requerido: **dos**	Nivel madurez mínimo requerido: **tres**

Fuente: ACUERDO SUGEF 14-09 REGLAMENTO SOBRE LA GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

En el caso de la Contraloría General de la República, se propone que se realice un esfuerzo similar, adoptando ciertas diferencias, al relacionarlo con la clasificación de las instituciones que se realice previamente, dado que el ámbito de fiscalización de la Contraloría difiere del que compete a la SUGEF, donde el acuerdo fue difundido para el 100% de su población por igual.

Entre las fortalezas que se pueden observar en la propuesta de adoptar un marco de control como *COBIT*, y su obligatoriedad para el sector público general, cabe mencionar:

- Utilización de Modelos de Madurez

El modelo de madurez, para la administración y el control de los procesos de TI, se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta el de optimizado (5). Este enfoque se deriva del modelo de madurez que el *Software Engineering Institute* definió para la madurez de la capacidad del desarrollo de *software*. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión, que no es justificable, debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es avaluar el nivel de adherencia a los objetivos de control. (ITGI, 2007)

Ilustración 27: Modelos de Madurez de COBIT

Figura 12 – Representación Gráfica de los Modelos de Madurez

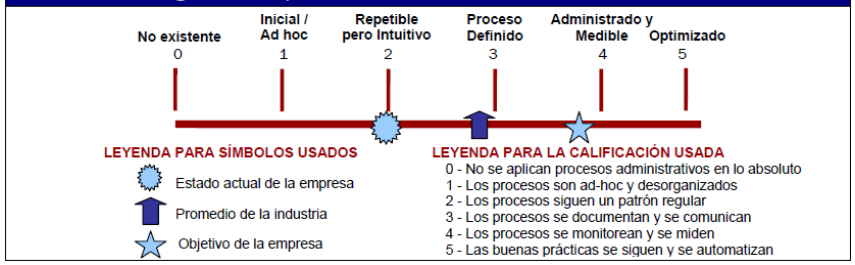


Figura 13 – Modelo Genérico de Madurez

0 No Existente- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

1 Inicial- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4 Administrado- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado- Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Fuente: MARCO DE CONTROL *COBIT*® 4.1.

La ventaja de un modelo de madurez es, que para la dirección, resulta relativamente fácil ubicarse a sí misma en la escala y evaluar qué se debe hacer, si se requiere desarrollar una mejora. La escala incluye al 0, ya que es muy posible que no existan procesos en lo absoluto. La escala del 0-5 se basa en un grado de madurez simple que muestra cómo un proceso evoluciona desde una capacidad no existente, hasta una capacidad optimizada. (ITGI, 2007)

La posibilidad de implementar *COBIT* en el sector público se propone, enmarcada en la utilización de las herramientas que dicho marco de control contempla, tales como lo mencionado antes sobre modelos de madurez, que permita evaluar la organización, conforme al proceso como tal, así como al sistema escalonado de implementación que se establezca en el órgano contralor.

- Matrices *RACI*, Metas y Métricas de Medición

Ilustra quién es responsable, quién debe rendir cuentas y a quién se debe consultar e informar dentro de un marco de trabajo organizacional estándar. (ITGI, 2007)

Estas matrices son de mucha utilidad para conocer quién es responsable de realizar cada proceso, o bien conocer hasta dónde llegan las competencias de un funcionario específico en determinada actividad.

A su vez, en cada proceso se documenta una serie de metas que se establecen en nivel de TI, y que se pueden implementar con el establecimiento de procesos y actividades, que el mismo *COBIT* detalla, agregando la posibilidad de realizar mediciones que permitan conocer los resultados del avance del proceso, y con base en dichos resultados, dirigir nuevamente las mejoras de las metas y procesos.

- Capacitación

El modelo de control *COBIT*, está respaldado por *ISACA*, organización que cuenta con más de 86 000 miembros en más de 160 países. *ISACA*® (www.isaca.org) es un líder mundialmente reconocido, proveedor de conocimiento, certificaciones, comunidad, apoyo y educación en seguridad y aseguramiento de sistemas de información, gobierno empresarial de TI y riesgos y cumplimiento relacionados con la TI. (ISACA)

ISACA desarrolla y actualiza continuamente los marcos referenciales *COBIT*®, *Val IT*™ *y Risk IT*, los cuales ayudan a los profesionales de TI y líderes empresariales, a

complementar sus responsabilidades en el gobierno de TI y a entregar valor a sus negocios.

- Herramientas de Implementación.

COBIT es el marco de trabajo de control interno, generalmente aceptado para TI, el cual cuenta con una serie de herramientas que facilitan su entendimiento e implementación, entre las que menciona:

- El resumen informativo al consejo sobre el gobierno de TI, 2ª Edición: Diseñado para ayudar a los ejecutivos a entender por qué el gobierno de TI es importante, cuáles son sus intereses y cuáles son sus responsabilidades para administrarlo.
- Directrices gerenciales / Modelos de madurez: Ayudan a asignar responsabilidades, medir el desempeño, llevar a cabo *benchmarks* y manejar brechas en la capacidad.
- Marco de Referencia: Explica cómo *COBIT* organiza los objetivos de gobierno y las mejores prácticas de TI, con base en dominios y procesos de TI, y los alinea a los requerimientos del negocio.
- Objetivos de control: Brindan objetivos a la dirección basados en las mejores prácticas genéricas para todos los procesos de TI.
- Guía de Implementación de Gobierno de TI: Usando *COBIT y Val TI 2*ª Edición. Proporciona un mapa de ruta para implementar gobierno TI 7.

Por otra parte, *ISACA* organiza conferencias internacionales, publica el *ISACA*® *Journal*, y desarrolla estándares internacionales de auditoría y control de sistemas de información, que ayudan a sus miembros a garantizar confianza y el valor de los sistemas de informacion.

Por ejemplo, “esta organización pone a disposición diferentes programas de auditoría, que se constituyen en valiosas herramientas, ya que proporcionan una plantilla para ayudar a los auditores de todo el mundo a completar procesos específicos de seguridad", dijo Norm Kelson, CISA, CGEIT, CPA, autor líder de los programas. “Estos programas han sido desarrolladas por un equipo de profesionales experimentados en seguridad de todo el mundo. De tal manera, representan la más reciente experiencia global, y son objeto de análisis de sus compañeros. Además, los materiales pueden descargarse en un documento de *Word* y se pueden personalizar fácilmente para adaptarse a un entorno operativo específico”. (ISACA)

El marco general de los estándares de aseguramiento y auditoría de TI de *ISACA*, presenta múltiples niveles, como se explica a continuación: (ISACA C. , 2011)

- Los estándares definen requerimientos obligatorios para el aseguramiento y la auditoría de TI y para los informes.

- Las directrices proporcionan asesoría para aplicar los estándares de aseguramiento y auditoría de TI. EI auditor de SI debe tomarlas en cuenta, para determinar cómo implementar los estándares anteriormente citados, usar su

juicio profesional al aplicarlas y estar preparado para justificar cualquier diferencia.

- Los procedimientos ofrecen ejemplos de los procesos que podría seguir un auditor de SI en una asignación de auditoría. Los documentos de procedimientos brindan información, sobre la manera de cumplir con los estándares cuando se está realizando un trabajo de auditoría de SI, pero no establecen requerimientos.

- Mapeos con otros Estándares

Aunado a lo anterior, cabe afirmar que *COBIT* es una herramienta de amplia trayectoria en el ambiente de la gestión de TI, aspecto que agrega valor a su utilización, debido a que ha sido utilizado y probado por diferentes instituciones, para distintos giros de negocio. Además, debido a su aceptación en el mercado internacional y a los resultados que genera, existen en el mercado diferentes mapeos o asociaciones a otros estándares como *ITIL* e *ISO*, que permiten ajustar la utilización de estándares y prácticas a los requerimientos individuales de cada organización.

COBIT puede ser utilizado en los más altos niveles de gobierno de TI, proporcionando un marco de referencia global de control basado en el modelo de procesos de TI que el *ITGI* pretende se pueda adaptar a cada empresa. También hay una necesidad de procesos detallados y estandarizados para profesionales. Prácticas específicas y estándares como *ITIL* e *ISO/IEC 27002*, cubren áreas específicas y pueden ser mapeadas al marco de referencia *COBIT*, proporcionando así una jerarquía de materiales de orientación. (ITGI, 2008)

La estructura detrás de *COBIT* ofrece una serie de oportunidades, las cuales son de mención importante en esta propuesta, para obtener el mayor beneficio conocido del marco de control propuesto a la Contraloría General de la República. Entre ellas, los procesos de acreditación en el uso e implementación de *COBIT*, y las posibilidades de generar herramientas de autoevaluación enfocadas en el mismo marco, o bien utilizar algunos de los modelos de autoevaluación existentes.

- Certificación o Acreditación

Existe un examen de acreditación denominado "*COBIT Foundation*", el cual se aplica a los profesionales de TI en todos los sectores y todas las empresas, al aprobar este examen, el candidato garantiza que entiende los principios, elementos y aplicaciones recomendadas de *COBIT*. Además, existe el examen denominado Aplicación de la Gobernanza en TI utilizando *COBIT*, el cual aplica para los profesionales de TI en todos los sectores y todas las empresas y se obtiene el reconocimiento de que el candidato entiende los elementos básicos de la aplicación del marco *COBIT* para apoyar a la empresa de gobierno de TI.

La propuesta de optar por *COBIT* como una arquitectura completa de procesos para la gestión de TI y su fiscalización en el sector público, se vería ampliamente fortalecida por los procesos de acreditación que se vienen realizando con esa herramienta, tanto nacional como internacionalmente, de forma tal que los profesionales que se certifican deben contar con habilidades como:

- Entender cómo la administración de TI afecta a las organizaciones.
- Comprender las condiciones de un marco de control dirigido por las necesidades de un gobierno de TI.
- Establecer los requerimientos para un marco de Gobierno de TI.
- Utilizar *COBIT* con otros estándares y mejores prácticas.
- Aplicar las funciones que *COBIT* provee y los beneficios de su uso.
- Aplicar este marco de referencia en una situación práctica.

Lo anterior da confianza a la Contraloría General de la República en dos aspectos, primeramente que el tema de capacitación de los funcionarios públicos, puede ser abordado por las empresas de mayor renombre en el tema, o bien, la CGR podría contratar esos capacitadores para impartir el conocimiento, con la certeza de obtener cursos de calidad, que no le generen al ente contralor la presión de generar la capacitación desde cero. Por otra parte, el tema de acreditación plantea un grado de seguridad aceptable, sobre los profesionales que certificados en *COBIT*, desarrollen los procesos de implementación en las diferentes instituciones.

- Herramienta de Autoevaluación

En el caso de la Superintendencia General de Entidades Financieras, como parte de su interés en definir los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información (TI), en las instituciones que fiscalizan, establece la Matriz de Calificación de la Gestión de TI, (SUGEF, Guía para completar la Matriz de Calificación) instrumento que establece un conjunto de preguntas de respuesta cerrada, asociado a cada proceso *COBIT*.

En caso de que la Contraloría General de la República, asuma la propuesta de asumir *COBIT*, se propone a su vez, el optar por la creación de alguna herramienta de autoevaluación, que le permita a las instituciones fiscalizadas indagar sobre sus prácticas en control de las TI y obtener un criterio general de la suficiencia de su esquema, según la percepción de los funcionarios a partir de su experiencia laboral cotidiana.

- Plan Piloto

Como parte de la propuesta, se considera pertinente aunado al establecimiento de un equipo de funcionarios especializado que guíe la implementación, considerar la realización de un plan piloto a nivel de la Contraloría General de la República, donde se tomen los objetivos de control que la CGR establezca como prioritarios y sus niveles de madurez correspondientes, y se implementen a cabalidad dentro de la Unidad de Tecnologías de Información (UTI), de forma tal que se valoren las mejores prácticas y su efecto en generación de valor del componente tecnológico en el logro de los objetivos de la misma Contraloría.

¿Existen razones para no adoptar *COBIT* como modelo de gestión de las TI y su fiscalización?

De acuerdo con lo indagado durante el desarrollo de este trabajo, los beneficios resultan visibles, en diferentes términos capacitación, experiencia, organización, mayor cantidad de cerebros trabajando en productos de calidad, cooperación de diferentes países y sus experiencias en diferentes giros de negocio, grado de avance que posee el sector

bancario en su utilización, herramientas de evaluación, control de madurez y auditoría de los procesos, aspectos que la Contraloría General de la República podría valorar en función de actuar con seguridad, y finalmente, dedicar los recursos de que dispone, en la fiscalización como tal de la hacienda pública, asumiendo los estándares y marcos de control de aceptación mundial, altamente probados y utilizados en el globo.

5. CAPÍTULO V

5.1. CONCLUSIONES

De acuerdo con lo estudiado, las tecnologías de la información y las comunicaciones (TIC) tienen el potencial de ayudar a mejorar tanto la eficiencia como la eficacia de los servicios públicos, si se aprovechan correctamente. Son capaces, en efecto, de suministrar una combinación de ventajas en cuanto a eficiencia y eficacia; no obstante, utilizadas incorrectamente, pueden dañar gravemente el buen nombre de los gobiernos y causar costos muy superiores a los previstos.

Las organizaciones exitosas, entienden los riesgos y aprovechan los beneficios de TI, para la consecución de los objetivos; sin embargo, este es un proceso largo en el sector público de Costa Rica, debido posiblemente a un trasfondo cultural e histórico; por ende, surgen de manera general, los esfuerzos por normar y controlar a las instituciones, promoviendo que se aprovechen las TI, de la mejor manera.

El desarrollo del trabajo final de investigación aplicada, permitió llegar al objetivo planteado de elaborar un diagnóstico y una propuesta de actualización de las normas técnicas, para la gestión y el control de las tecnologías de información, emitidas por al Contraloría General de la República.

En el año 2007, la Contraloría General de la República establece las normas técnicas para la gestión y el control de las tecnologías de información, cuya vigencia ha sido de casi seis años.

El diagnóstico efectuado mediante la revisión de los informes y disposiciones, ejecutados por la Contraloría General de la República, en su labor de fiscalización del sector público, reveló que su implementación y cumplimiento ha sido insuficiente, por lo que se planteó a la Contraloría General de la República, realizar un nuevo esfuerzo por variar el cuerpo normativo existente, asumiendo como norma el marco de control *COBIT* 4.1, o bien un extracto de este en función de los 34 objetivos de control con que cuenta, debido a su reconocimiento internacional, ventajas en cuanto a la experiencia en su uso, herramientas asociadas y capacitación. Además, su versión anterior fue parte de los pilares de la normativa actual.

Resulta importante aclarar, que el diagnóstico efectuado sobre los informes y disposiciones emitidos por la Contraloría General de la República, no pretende revelar actuaciones débiles por parte del ente contralor, sino hacer hincapié en la necesidad de planificar, de mejor manera, el tema del control de la gestión de las tecnologías de información, e incentivar el acompañamiento que debe darse a las áreas de fiscalización de la DFOE en este relevante aspecto.

Existen nuevas tendencias en las tecnologías de información, que podrían utilizarse en el sector público, actualmente o en un futuro cercano; por lo tanto, en muchos de esos casos, las normas técnicas de la Contraloría General de la República, podrían resultar débiles para la regulación y control de las instituciones fiscalizadas.

La revisión del tema normativo en países como Chile y Venezuela, evidenció que la regulación de las TI, se da en países grandes como Venezuela, así como de un tamaño similar a Costa Rica. Además, llama la atención la diversidad de normas y organismos

que establecen normativas en cuanto a las tecnologías de información; al igual que Costa Rica, no existe un esfuerzo común por parte de los gobiernos para regular esta actividad desde una sola vía, resaltando que en los países observados, el esquema normativo muestra una tendencia a lo particular, es decir se abordan temas de delito informático, confidencialidad de datos, pero no tanto la gestión de las tecnologías como tal.

Las opiniones obtenidas mediante el sondeo de opinión calificada, resultaron de suma importancia para la propuesta de actualización de las normas técnicas, para la gestión y el control de las tecnologías de información, dado que el conocimiento que los profesionales en estos campos, han ido amalgamando durante la vigencia de las normas, permitió conocer aspectos de interés, en cuanto a formas de implementar, lecciones aprendidas en los proyectos ejecutados, nuevos esquemas, entre otros; además, su visión del provecho del conocimiento que encierra el uso de *COBIT* y su herramientas en las instituciones.

5.2. RECOMENDACIONES

Como parte de la elaboración de este diagnóstico y propuesta de actualización, de las normas técnicas para la gestión y el control de las tecnologías de información, emitidas por al Contraloría General de la República, se plantea una serie de recomendaciones que el ente contralor podría poner en práctica, si acepta la propuesta establecida en el presente documento, a saber:

- Valorar la posibilidad de establecer la actualización de la norma y su implementación, como un proyecto, tomando en cuenta para ello las mejores prácticas en materia de proyectos, que le garanticen el logro del objetivo trazado, es decir, que se cumpla con el alcance definido para dicho proyecto.

- Establecer un grupo determinado de profesionales, que ejecute dicho proyecto de actualización e implementación de las normas o controles, para la gestión de las tecnologías de información en el sector público; dicho equipo debería estar integrado por recursos capacitados en *COBIT* y en gobierno de TI, entre otros.

- Ese equipo deberá valorar los elementos del marco de control, de forma tal que establezcan el esquema de cumplimiento que deberá acatarse, de acuerdo con la clasificación de instituciones, lo cual plantea la propuesta, como parte del trabajo por ejecutar.

- Dicho equipo de trabajo debe proponerse, generar alianzas estratégicas con instituciones como la SUPEN, que ya pasaron por un proceso similar, donde se

compartan conocimientos y lecciones aprendidas, que la Contraloría General de la República pueda aprovechar si pone en práctica la propuesta.

- Finalmente, un gran aporte al trabajo que realice la Contraloría General de la República, sería la ejecución de una investigación sobre casos de éxito en la implementación del *COBIT*, tanto en Costa Rica (caso de *ScotiaBank*), como internacionalmente; donde se observen las acciones realizadas para la implementación, así como los beneficios obtenidos de esta.

6. ANEXOS

6.1. PROPUESTA DE ENCUESTA/ENTREVISTA:

Se incluyen las consultas, la versión web de la Encuesta/Entrevista se encuentra en el sitio: https://docs.google.com/spreadsheet/viewform?fromEmail=true&formkey=dDZRaWhSdmNKWmtjbHM3S3p5R1J6TWc6MQ

1. ¿Cuáles son las principales dificultades enfrentadas en el proceso de implementación de las normas técnicas para la gestión y el control de las tecnologías de información?
2. ¿Cuál ha sido el rol, liderazgo y compromiso que han asumido los niveles directivos de las organizaciones en cuanto a la implementación de las normas?
3. ¿Cuál es el rol del área de tecnología de información y de las unidades usuarias de las organizaciones en cuanto a la implementación de las normas?
4. ¿Cuál es el riesgo más relevante derivado del incumplimiento de las normas técnicas para la gestión y el control de las tecnologías de información? ¿Cómo espera mitigar esos riesgos?
5. ¿Cuáles son los principales aspectos de la citada normativa, los cuales considera que deben ser ajustados?

Auditores Internos:

6. ¿Cuáles han sido las experiencias con respecto a la evaluación de las normas técnicas para la gestión y el control de las tecnologías de información?
7. Enumere los requerimientos o necesidades en las competencias de la auditoría interna para evaluar la citada normativa.

8. Comente sobre la asesoría recibida, por parte de la CGR, respecto a la evaluación de las normas técnicas para la gestión y el control de las tecnologías de información.

Capacitación CGR

9. Refiérase al proceso de planificación y ejecución de la capacitación ofrecida a las auditorías internas, sobre la evaluación de las normas técnicas, para la gestión y el control de las tecnologías de información.

6.2. ESQUEMA DE LA NORMATIVA DE LA CGR

Introducción

Capítulo I Normas de aplicación general

1.1 Marco estratégico de TI
1.2 Gestión de la calidad
1.3 Gestión de riesgos
1.4 Gestión de la seguridad de la información
- 1.4.1 Implementación de un marco de seguridad de la información
- 1.4.2 Compromiso del personal con la seguridad de la información
- 1.4.3 Seguridad física y ambiental
- 1.4.4 Seguridad en las operaciones y comunicaciones
- 1.4.5 Control de acceso
- 1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica
- 1.4.7 Continuidad de los servicios de TI

1.5 Gestión de proyectos
1.6 Decisiones sobre asuntos estratégicos de TI
1.7 Cumplimiento de obligaciones relacionadas con la gestión de TI

Capítulo II Planificación y organización

2.1 Planificación de las tecnologías de información
2.2 Modelo de arquitectura de información
2.3 Infraestructura tecnológica
2.4 Independencia y recurso humano de la Función de TI
2.5 Administración de recursos financieros

Capítulo III Implementación de tecnologías de información

3.1 Consideraciones generales de la implementación de TI
3.2 Implementación de software
3.3 Implementación de infraestructura tecnológica
3.4 Contratación de terceros para la implementación y mantenimiento de software e infraestructura

Capítulo IV Prestación de servicios y mantenimiento

4.1 Definición y administración de acuerdos de servicio
4.2 Administración y operación de la plataforma tecnológica
4.3 Administración de los datos
4.4 Atención de requerimientos de los usuarios de TI
4.5 Manejo de incidentes
4.6 Administración de servicios prestados por terceros

Capítulo V Seguimiento

5.1 Seguimiento de los procesos de TI
5.2 Seguimiento y evaluación del control interno en TI
5.3 Participación de la Auditoría Interna

Fuente: Normas Técnicas para la Gestión y el Control de las Tecnologías de Información

7. BIBLIOGRAFÍA

27001, I. (2005). *Organización Internacional para la Estandarización.* ISO.

CGR. (s.f.). *Contraloría General de la República*. Recuperado el 8 de abril de 2013, de Chile: http://www.contraloria.cl/appinf/basesDocumentales/bifaPortalCGR.nsf/0/50BAD15D8BCD92D98425781100518F4A/$File/INFORME%20FINAL%2034-10%20UNIVERSIDAD%20DE%20LOS%20LAGOS%20AUDITORIA%20DE%20TECNOLOGIAS%20DE%20INFORMACION%20DICEMBRE%202010.pdf?OpenElement

CGR. (2002). *Ley General de Control Interno Nº8292.* Gaceta 169 del 04/09/2002.

CGR. (1996). *Manual sobre Normas Técnicas de Control Interno relativas a los Sistemas de Información Computadorizados.*

Chile, G. d. (s.f.). *Ministerio de Economía, Fomento y Reconstrucción*. Recuperado el 09 de abril de 2013, de http://www.economia.gob.cl/acerca-de/rol-ministerial/

CNCL. (s.f.). *Congreso Nacional*. Recuperado el 01 de Abril de 2013, de Chile: http://www.congreso.cl/

CNTI. (s.f.). *Centro Nacional de Tecnologías de Información*. Recuperado el 10 de abril de 2013, de Venezuela: http://www.cnti.gob.ve/index.php?option=com_content&view=article&id=121&Itemid=55

Forum, W. E. (2013). *The Global Information Technology Report 2013.* http://www3.weforum.org/docs/WEF_GITR_Report_2013.pdf: Beñat Bilbao-Osorio, Soumitra Dutta, and Bruno Lanvin, Editors.

INN. (s.f.). *Instituto de Investigación del Estado*. Recuperado el 03 de Abril de 2013, de Chile: http://www.inn.cl/inn/portada/index.php

ISACA. (s.f.). *ISACA.* Recuperado el 06 de mayo de 2013, de ISACA: http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/COBIT5-ultimas-noticias.aspx

ISACA, C. (2011). *Manual de Preparacion al Examen CISA® 2011.* Estados Unidos de América: ISACA.

ITGI. (2008). *IT Governance Institute* . Recuperado el 23 de enero de 2013, de http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf

ITGI, I. G. (2007). *Objetivos de Control para la Información y la Tecnología.* United States of America: IT Governance Institute.

MINSEGPRES. (s.f.). *Ministerio Secretaría General de la Presidencia*. Recuperado el 29 de marzo de 2013, de Chile: http://transparencia.minsegpres.gob.cl/Index.asp

N-2-2007-CO-DFOE. (2007). *Publicada en La Gaceta N°119 del 21 de junio, 2007.* Costa Rica: La Gaceta.

Sáenz, I. S. (29 de Agosto de 2012). *ASEGURAMIENTO DEL GOBIERNO DE TI.* Recuperado el 8 de mayo de 2013, de ISACA: http://www.isacacr.org/archivos/Aseg_%20Gobierno_TI.pdf

Sandra García, I. E. (18 de marzo de 2013). Curso ITIL v3 y su apoyo a las normativas de TI de Costa Rica.

SUDEBAN. (s.f.). *Ministerio del Poder Popular de Planificación y Finanzas*. Recuperado el 09 de enero de 2013, de Venezuela: http://sudeban.gob.ve/uploads/-B/Xk/-BXkhYa2byi_i86ER0hlxw/Normativa-2011-04-28.pdf

SUDEBAN, S. W. (s.f.). *Ministerio del Poder Popular de Planificación y Finanzas*. Recuperado el 10 de abril de 2013, de Superintendencia de las Instituciones del Sector Bancario: http://sudeban.gob.ve/webgui/inicio/quienes

SUGEF. (2009). *ACUERDO SUGEF 14-09 - Reglamento sobre la gestión de la tecnología de información.* Costa Rica: SUGEF.

SUGEF. (s.f.). *Guía para completar la Matriz de Calificación*. Recuperado el 10 de mayo de 2013, de Versión 1.0: http://www.sugef.fi.cr/servicios/documentos/normativa/reglamento%2014-09/Descarga/FormulariosyGuias/Gu%C3%ADa%20para%20completar%20la%20Matriz%20de%20Calificaci%C3%B3n.pdf

SUGEF. (12 de abril de 2013). *SUPERINTENDENCIA GENERAL DE ENTIDADES FINANCIERAS*. Obtenido de http://www.sugef.fi.cr/pagina.asp?lang=0&pagina=servicios/documentos/infgeneral/antecedentes/antecedentes.html

SUPEN. (17 de 04 de 2013). *Superintendencia de Pensiones*. Obtenido de http://www.supen.fi.cr/Fondos%20de%20pension%20basicos/IVM.html

Venezuela, C. (s.f.). *Contraloría General de la República*. Recuperado el 2010 de abril de 2013, de Venezuela: http://www.cgr.gob.ve/contenido.php?Cod=045

Venezuela, C. (s.f.). *Contraloría General de la República*. Recuperado el 10 de abril de 2013, de Venezuela: http://www.cgr.gob.ve/contenido.php?Cod=045