Antecedentes

1. Origen y Situación Actual
2. **Estrategias DFOE**
3. Normativa

Las estrategias contemplan:

- El establecimiento de un **marco normativo**, de conformidad con las sanas prácticas de aceptación general, que tiendan a garantizar una gestión eficiente y eficaz de los recursos asignados a la gestión de las TI.

- El incremento del **conocimiento** que tienen las unidades administrativas, auditorías internas, jefaturas, altos niveles de mando y las unidades informáticas, relacionadas con la **gestión y control** de las TI.

- Una mejora en la **capacidad de fiscalización** con que cuenta la Contraloría para evaluar periódicamente la gestión de las entidades públicas respecto del uso de recursos destinados a TI y promover un crecimiento sostenido de dicha capacidad.

* Una mayor disposición de **herramientas de trabajo** para lograr un mejoramiento continuo en el cometido de sus funciones y el máximo aprovechamiento de sus recursos.

Dichas estrategias consideran:

- La definición de un marco normativo que sirva de guía hacia una mejor gestión de las TI y a su vez actualizar la normativa existente desde 1995 más ajustada a la realidad tecnológica de nuestras organizaciones.
- Incrementar el conocimiento tanto interno como externo en materia de una adecuada GESTIÓN de las TI.
- Mejorar la capacidad de fiscalización, considerando tanto lo interno como externo. CONTROL
- Desarrollar herramientas y procedimientos para hacer más ágil la fiscalización.

Entonces podemos distinguir básicamente tres grupos, a saber:

1. **Formulación de la normativa**
2. **Desarrollo de competencias**
3. **Identificación de instrumentos**

Antecedentes

1 Origen y Situación Actual

2 Estrategias DFOE

3 Normativa

La mejora que se busca en la gestión de las TI no es un fin único ni un fin en si mismo. Lo que se espera es un resultado de mayor alcance relacionado con la reducción de la brecha tecnológica en nuestra sociedad y el aprovechamiento de esas TI para brindar más y mejores servicios públicos a la ciudadanía.

Asimismo, será necesario un esfuerzo importante para incrementar las competencias que en esta materia requieren las autoridades institucionales responsables de la definición de la orientación tecnológica y de los niveles medios respecto de llevar adelante ese desarrollo en un ámbito seguro y controlado. Es necesario un proceso de desarrollo de capacidad.

Por otra parte, es requerido un esfuerzo importante de las auditorías internas para reforzar sus competencias y realizar las evaluaciones no sólo en forma automatizada sino aprovechando lo procesos automatizados institucionales.

Objetivo se resume así:

Coadyuvar al uso óptimo de los recursos invertidos en TI de acuerdo con una orientación clara que procure el desarrollo nacional y la reducción de la brecha tecnológica, por medio de un marco de control que guíe esa gestión y desarrollando las competencias internas y externas necesarias para promover una fiscalización suficiente y oportuna sobre ese uso.

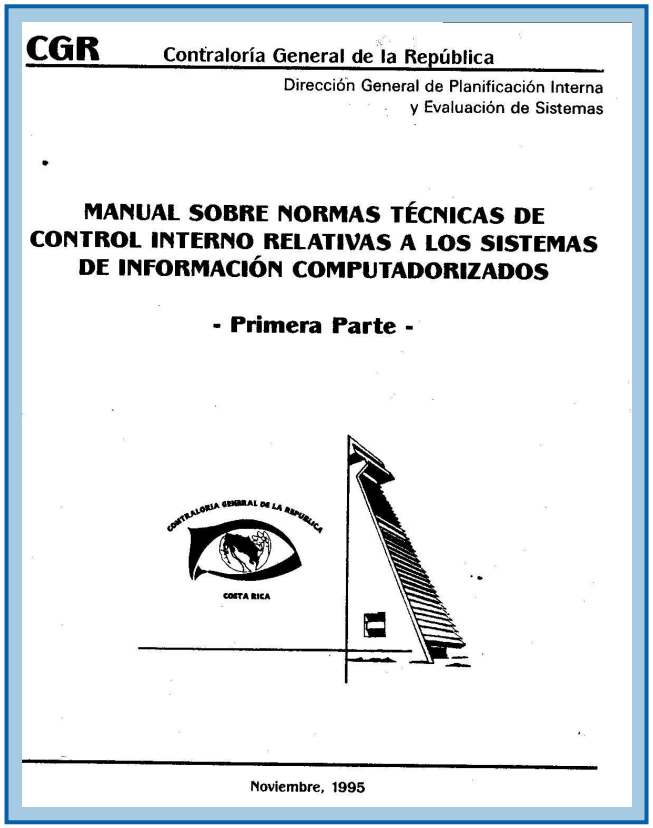
Tal iniciativa de fiscalización de la CGR se ve reforzada, entre otros aspectos por:

- La importancia de las tecnologías de información en los procesos y presupuestos institucionales.
- El surgimiento de nuevos marcos jurídicos asociados con esas mismas tecnologías.
- Las políticas de Estado para promover el desarrollo tecnológico, para reducir la brecha digital e implementar el "Gobierno Digital".

"Normas Técnicas de Control Interno para la gestión de las Tecnologías de Información TI"

El proceso de desarrollo de las normas conllevó tiempo y análisis profundo.

- El proceso en general involucró preparar una propuesta de normativa, para lo cual se siguió el siguiente análisis.
- Partió de las normas publicada en el año 1995 y analizó sus antecedentes para determinar su aplicación en esta nueva propuesta; previa determinación de lo que aplicaba y lo que ya no estaba vigente.


CGR Contraloría General de la República

Dirección General de Planificación Interna y Evaluación de Sistemas

MANUAL SOBRE NORMAS TÉCNICAS DE CONTROL INTERNO RELATIVAS A LOS SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS

- Primera Parte -

CONTRALORIA GENERAL DE LA REPUBLICA
COSTA RICA

Noviembre, 1995

El origen de dicha normativa (1995) se dio en un contexto donde los avances tecnológicos y la inversión en proyectos de TI alcanzaban niveles importantes. A su vez, el manejo de importantes volúmenes de datos implicaban la necesidad de que los ambientes fueran seguros y controlados, se procurara niveles razonables en cuanto a la calidad de la información y se hiciera un uso eficiente y eficaz de los recursos.

Sin embargo, ese contexto fue cambiando rápidamente pues hubo nuevos e importantes avances, se dio una explotación de los servicios en internet y con ello tomó fuerza la implementación de nuevos servicios como el comercio electrónico y el intercambio de datos, y la implementación de aplicaciones específicas pero de gran alcance como los promovidos por el Banco Central y el Ministerio de Hacienda.

Paralelamente surgió nuevas normativas relacionadas con las TI en procura de establecer controles o mecanismos para el establecimiento de responsabilidades respecto del uso de esas TI.

Respecto del marco jurídico se tiene, por ejemplo, normas específicas tales como las establecidas en:

- La Ley de Control Interno
- La Ley de Administración Financiera (Art. 111)
- La Ley General de Aduanas
- Las reformas al Código Penal
- Del Código Tributario
- La Ley de Certificados, Firma Digital y Documentos Electrónicos.
- Ley de Derechos de Autor y otras leyes que tratan asuntos relacionados con prácticas tales como la piratería.

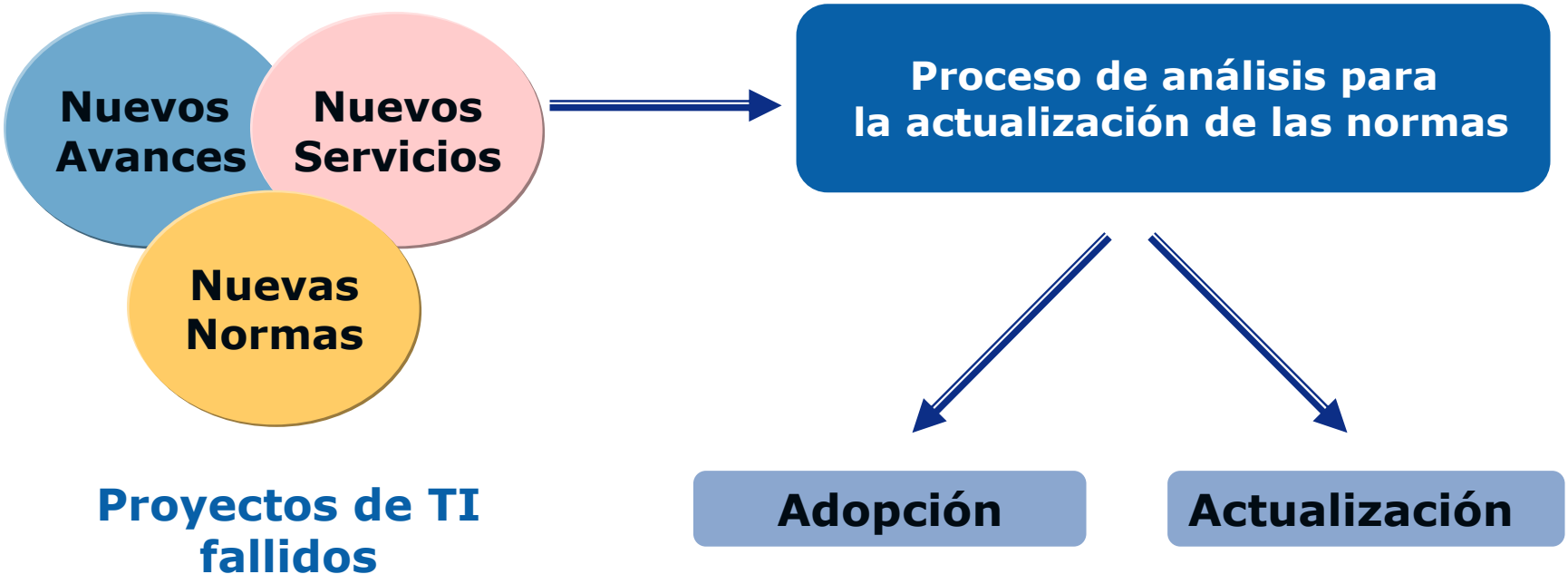
Cambios de los últimos años...

- Nuevos avances
- Crecimiento de Internet
- Internet Avanzado
- Nuevos Servicios
- Comercio Electróni.
- EDI TEF
- Min. Hacienda
- Nuevas Normas
- L.G.A.
- L.A.F.
- Código Penal
- Ley Firma Digiral
- L.C.I.
- NIA's

Esos asuntos, unidos a múltiples proyectos informáticos que han presentado dificultades en su desarrollo, dan una clara señal de la necesidad de llevar a cabo acciones tendentes a resolver tal situación y lograr mejoras significativas en la gestión de TI.

Una de tales acciones es la actualización de las normas sobre TI. Ante esta situación la DFOE analizó dos posibilidades:

1. Adoptar un modelo existente por las eventuales ventajas que ello podría tener.
2. Actualizar la normativa de 1995.


Nuevos Avances
Nuevos Servicios
Nuevas Normas
Proyectos de TI fallidos
Proceso de análisis para la actualización de las normas
Adopción
Actualización

Para analizar la primera opción de adoptar un modelo se identificaron una serie de modelos los cuales fueron evaluados comparativamente considerando una serie de variables.

Adopción → **Modelos**

VARIABLES

- Costo
- Estándar
- Tipo de instrumento
- Idioma
- Aplicación en el sector público o en el privado
- Consultores nacionales
- Curva de inducción
- Software disponible
- Utilizado en otras ISA's

Los modelos más relevantes y más ajustados, según el criterio del equipo de trabajo son los detallados abajo. Fueron comparados considerando las variables anteriores para tener un mejor criterio a la hora de definir cuál podría constituirse en una guía a ser adoptada por la CGR como estándar de gestión y control.

Capability Maturity Model (SEI-CMM)	Software Engineering Institute, Carnegie-Mellon University
Malcolm Baldridge Quiality Award Business Criteria	National Institute for Standards and Technology
ISO 9001	INTECO
"World Class IT" y similar	KPMG
Control Objectives For Information And Related Technology (COBIT)	Information Systems Audit and Control Association (ISACA)
Federal Information System Controls Audit Manual	General Accounting Office (GAO)
Systems Auditability And Control (SAC Report)	Institute of Internal Auditors EEUU
Modelo de Auditoría y Control de ACAI	Asociación Costarricense de Auditores en Informática (ACAI)
Audit Guides, Auditing EDP (4 Módulos)	Office of the Auditor General OAG - CANADA
Auditing of Information Management and Technology	Office of the Auditor General OAG - CANADA
BS-7799, Habilitado en el formulario NAO 905 (V.10)	British Standard Institution National Audit Office (NAO)
Information Technology Investment Management (ITIM)	General Accounting Office (GAO)
IT Security Baseline Controls	INTOSAI
Information System Security Review Methodology	INTOSAI
Normas Internacionales de Auditoría	IFAC
CICA Computer Control Guidelines	CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS
Computerized Information Systems Audit Manual (CIS)	The Information Systems Control Foundation --hoy: ISACA--
ITIl It Management Practices Information Techonolgy Infraestructure Library	Central Computer and Telecommunications Agency (CCTA)

De los modelos analizados, por sus condiciones o características, el COBIT resultó ser la opción que mejor se adaptaba a las necesidades. Como parte de su análisis se realizó una consulta a múltiples entidades (consulta del 2001) para que se manifestaran respecto de la factibilidad técnica y jurídica de su adopción.

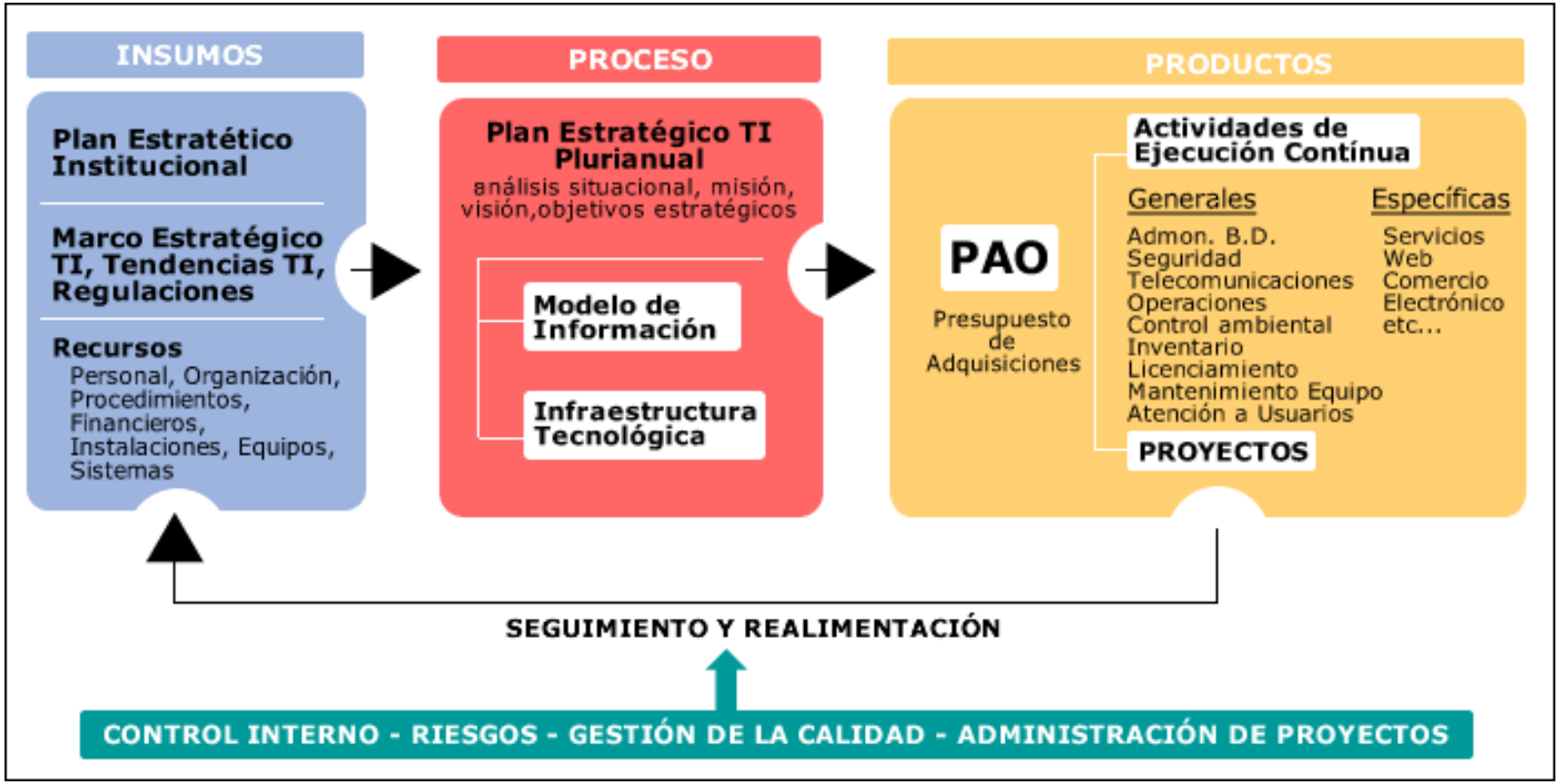
Al respecto de obtuvo respuestas muy variadas, las cuales, junto con un mayor análisis posterior derivó en la conclusión de que no era factible su adopción, principalmente por varias razones:

- No todas las entidades estaban debidamente preparadas o en capacidad de cumplir con la mayor parte del modelo, lo cual implicaba que la CGR permitiera cumplimientos parciales y con ello debilitar la normativa como tal.
- El modelo exigía, en su versión 2 de entonces, la certificación de algunos procesos, actividades o productos de la gestión de TI. Situación que encarecía su cumplimiento sin que se visualizara un valor agregado importante. Además, que el mercado no ofrecía una cantidad razonable de proveedores certificadores.
- No estaba en idioma español oficializado por la ISACA.

En virtud de lo comentado se desestimó la posibilidad de adoptar un modelo y se inició la tarea de emitir nuevas normas actualizadas.

Pero ese ejercicio implicaba tener claro lo que se debe normar - en este caso la gestión de las TI- y por ende sus componentes, el funcionamiento de dichos componentes y la interrelación de las TI con otras unidades de la organización.

El trabajo derivó el siguiente esquema descriptivo.


INSUMOS
PROCESO
PRODUCTOS
Plan Estratético Institucional
Marco Estratégico TI, Tendencias TI, Regulaciones
Recursos
Personal, Organización, Procedimientos, Financieros, Instalaciones, Equipos, Sistemas
Plan Estratégico TI Plurianual
análisis situacional, misión, visión,objetivos estratégicos
Modelo de Información
Infraestructura Tecnológica
PAO
Presupuesto de Adquisiciones
Actividades de Ejecución Contínua
Generales
Admon. B.D.
Seguridad
Telecomunicaciones
Operaciones
Control ambiental
Inventario
Licenciamiento
Mantenimiento Equipo
Atención a Usuarios
Específicas
Servicios Web
Comercio Electrónico
etc...
PROYECTOS
SEGUIMIENTO Y REALIMENTACIÓN
CONTROL INTERNO - RIESGOS - GESTIÓN DE LA CALIDAD - ADMINISTRACIÓN DE PROYECTOS

3 Normativa

El esquema anterior fue utilizado como base para la definición de las normas finalmente propuestas.

Algo muy importante de mencionar es que no se incluye el "Ambiente", pues las normas no incluyen consideraciones sobre ecología, desarrollo sostenible o medio ambiente, debido a limitaciones infraestructurales imperantes en el Sector Público a la fecha del análisis y actualmente no existen los mecanismos necesarios para garantizar su cumplimiento.

En su lugar, las normas consideran un acápite que pretende que todas las decisiones relacionadas principalmente con la adquisición de infraestructura (hardware e instalaciones) tomen en cuenta el impacto en el medio ambiente. Lo anterior pues hay una percepción del problema respecto del desecho de hardware principalmente.

Aún así se incluye ese tema en estos comentarios para hacer énfasis en que las administraciones tomen conciencia de este problema y le busquen soluciones.

Después de un esfuerzo amplio de análisis y estudio, utilizando como base algunos de los modelos analizados, principalmente COBIT reforzado con otros modelos o estándares específicos (CMM, BS- 7799 e ISO17799 en seguridad, AS-NZ 4360y NIST en riesgos, ISO en calidad, PMBoK en proyectos, etc.) se planteó una propuesta de normas inicial que fue sometida a un proceso riguroso de validación.

COBIT®
GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY

El primer planteamiento de las "Normas Técnicas de Control Interno para la gestión de las Tecnologías de Información TI" tenía esta estructura de contenidos:

Capítulo I : Normas de Aplicación General

Capítulo II: Planificación y Organización

Capítulo III: Implementación y Mantenimiento de las Tecnologías de Información

Capítulo IV: Prestación de Servicios

Capítulo V: Seguridad

Capítulo VI: Seguimiento

Dicha validación tuvo dos partes: **Interna y Externa**

1 INTERNA

Una validación interna que estuvo constituida por un proceso de capacitación con la ejecución de proyectos piloto de fiscalización utilizando la normativa propuesta lo cual permitió obtener una serie de resultados para mejora de la gestión de TI.

Al mismo tiempo permitió evaluar preliminarmente la factibilidad de cumplimiento de las normas, de lo cual derivamos que eran viables aunque si requieren de importantes esfuerzos, pero esto último depende más del nivel de automatización de la entidad y del desarrollo cultural tecnológico que también tenga.

La CGR promovió un proceso de capacitación con proyectos piloto:

- Tribunal Supremo de Elecciones
- Ministerio de Hacienda
- Instituto Mixto de Ayuda Social IMAS
- Municipalidad de San José
- Caja Costarricense del Seguro Social CCSS
- Universidad Estatal a Distancia
- Compañía Nacional de Fuerza y Luz

2 EXTERNA

La validación externa implicó la remisión de la propuesta a personas tanto del ámbito público como privado relacionados con la gestión de las TI.

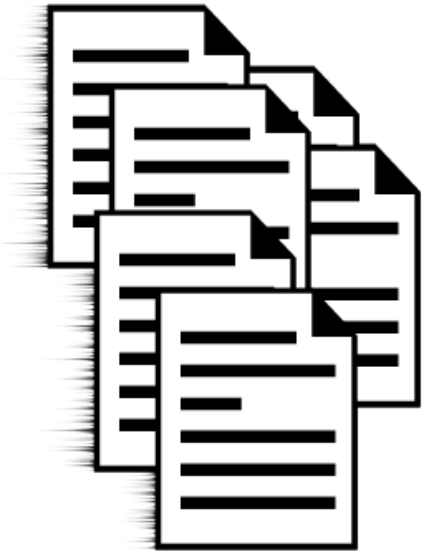
Se incluyó a funcionarios tanto del área de tecnologías como de auditoría interna, así como a consultores en la materia y gente de despachos de auditoría.

Como resultado se obtuvo un conjunto nutrido de sugerencias y observaciones las cuales fueron analizadas una a una para derivar en una propuesta ajustada.

La validación externa implicó la remisión de la propuesta a personas tanto del ámbito público como privado relacionados con la gestión de las TI.

Se incluyó a funcionarios tanto del área de tecnologías como de auditoría interna, así como a consultores en la materia y gente de despachos de auditoría.

Como resultado se obtuvo un conjunto nutrido de sugerencias y observaciones las cuales fueron analizadas una a una para derivar en una propuesta ajustada.



Consulta interna y externa

CGR	ACAI
Banco Nacional	CAMTIC
BPDC	CCPCR
CCSS	CENFOTEC
Hacienda	Consultores independientes
ICE	CPIC
INS	Grupo Gestor Cumbres
MICIT	KPMG
SUGEF	NewTech
SUGEVAL	TI-AUDISEG

Se revisó alrededor de 300 observaciones de 15 respuestas recibidas:

Plazo limitado de recepción de observaciones

Agregados útiles únicamente

Mejoras a la redacción para mayor claridad

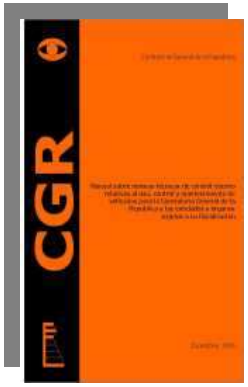
Muy pocas sugerencias de fondo

La propuesta validada fue nuevamente discutida a lo interno de la DFOE y como producto se obtuvo un documento más generalizado y resumido, con la pretensión de que resulte más claro o de más fácil comprensión para quienes no tienen amplio conocimiento o especialidad en la materia. Asimismo se procuró su ajuste o concordancia con el marco jurídico que le aplica.

El resultado es el documento de reciente publicación.

La estructura definitiva de la normativa se divide en 5 capítulos, de lo cual es importante destacar que el primero contiene una conjunto de normas que inciden y deben ser observadas en la aplicación de las demás normas.

Las normas contenidas en los capítulos 2 al 5 están vinculadas al proceso general de gestión de las TI.



Capítulo I Normas de aplicación general

Capítulo II Planificación y organización

Capítulo III Implementación de tecnologías de información

Capítulo IV Prestación de servicios y mantenimiento

Capítulo V Seguimiento

Esta estructura obedece a la intención de que se pretende que los aspectos del capítulo I sean considerados en casi todas las actividades del proceso de gestión de las TI. Por ejemplo: en el desarrollo de sistemas debería ser considerado:

- Lo establecido en el marco estratégico como factor orientador.
- Los criterios de calidad, riesgos y seguridad, tanto para el nuevo sistema como para la ejecución del proyecto.
- La administración de proyectos propiamente.
- La participación de una representación suficiente en las decisiones estratégicas asociadas al proyecto.

Continúa en Parte 3 ->

Contraloría General de la República

GCTI GCTI GCTI GCTI GCTI GCTI GCTI

Gestión y Control de Tecnologías de Información

GCTI

Programa Modular de Capacitación Virtual

Primera Edición © 2008

Este evento de capacitación fue desarrollado y producido por
La Contraloría General de la República de Costa Rica,
con base en el documento **N-2-2007-CO-DFOE:**
Normas Técnicas para la Gestión y Control de las Tecnologías de Información

Participaron funcionarios de:
Unidad del Centro de Capacitación (DEI)
Area de Secretaría Técnica (DFOE)

La producción de este curso estuvo a cargo de:
José Roberto Alpízar,
Coordinador Técnico del Proyecto
Xiomara Cisnado Torres,
Especialista en Diseño e Implementación de Proyectos e-Learning
Gino Ramírez Solís,
Alex Monge Lemaitre,
Guillermo Oviedo Blanco,
y Rocío Alfaro Vargas.
Expertos de Contenido

Contraloría General de
la República (CGR)
Costa Rica