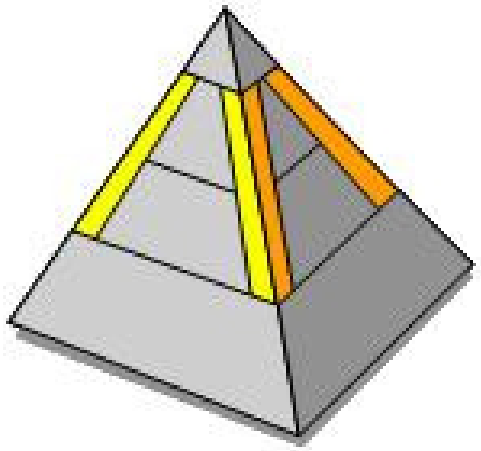
Contraloría General de la República
Costa Rica

Curso Modular sobre CONTROL INTERNO



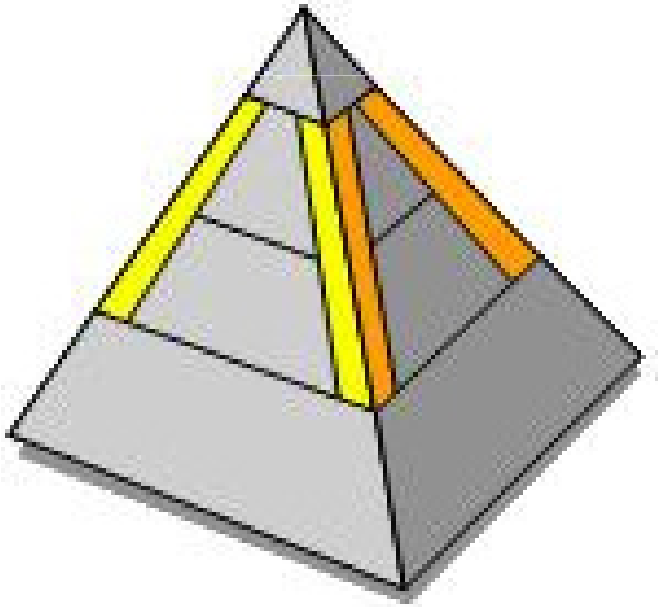
Componente 4:
Sistemas de información

Componente 4: Sistemas de información

1. **Concepto**
2. **El sistema de información y comunicación: su importancia institucional**
3. **Marco regulatorio**
4. **Responsabilidades**
5. **Normas relacionadas con los sistemas de información**

Componente 4: Sistemas de información

1 Concepto



Modelo Coso

Procesos para determinar si los controles internos están adecuadamente diseñados, ejecutados y son efectivos (Disclosure Committee y Auditoría Interna)

Procesos que aseguren que la información relevante es identificada y comunicada en forma y tiempo (formación, políticas y procedimientos, circulares internas, etc.)

Procedimientos de control para asegurar la eficaz consecución de los objetivos anteriormente indicados (segregación de funciones, conciliaciones, controles informáticos, etc.)

Proceso de gestión de riesgos (identificación, medición, seguimiento y control)

Directrices generales de control interno existentes en la Entidad (Códigos de Ética, Políticas y procedimientos, cultura corporativa de control interno, etc.)

Información y comunicación

- Tercer componente del SCI
- En relación con la información ***relevante y comunicada***, relacionada con actividades y eventos ***internos*** y ***externos***, deben:
  - **Generar**
  - **Capturar**
  - **Procesar**
  - **Transmitir**

Información

Tipo de información

- Financiera
- No financiera
  - Operaciones
  - Cumplimiento
  - Desempeño
  - Control

La información afecta el proceso de toma de decisiones y tiene sujetos interesados.

La información *fluye*….

- Importancia de tomar conciencia sobre deberes y responsabilidades sobre el control interno
- Papel de los funcionarios dentro del SCI y sus relaciones organizacionales
- Mecanismos de comunicación:
  - Hacia arriba
  - Hacia afuera

¿Qué es la información?

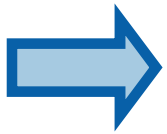
○**De operaciones**	○Gestión del desempeño ○Manejo de inventarios ○Asignación de recursos ○Cumplimiento de planes
○**Financiera**	○Estados financieros ○Rentabilidad ○Presupuesto ○Tendencias financieras ○Estadísticas
○**De rendición de cuentas y general**	○Estados financieros ○Ejecución presupuestaria ○Informes de cumplimiento

- **Estratégicos**
- **Tácticos**
- **Operativos**

Sistemas de información y el SCI:

- El SCI en las organizaciones contemporáneas está basado en **TI/SI**
- El contexto principal es el **INTERNO**
- El alcance **EXTERNO** es vital para la estrategia institucional

¿Por qué existen los sistemas de información?



- Información rutinaria
- Datos específicos
- Apoyo de las operaciones
- Datos no estructurados
- Enlace con los sujetos interesados
- Gestión de riesgos

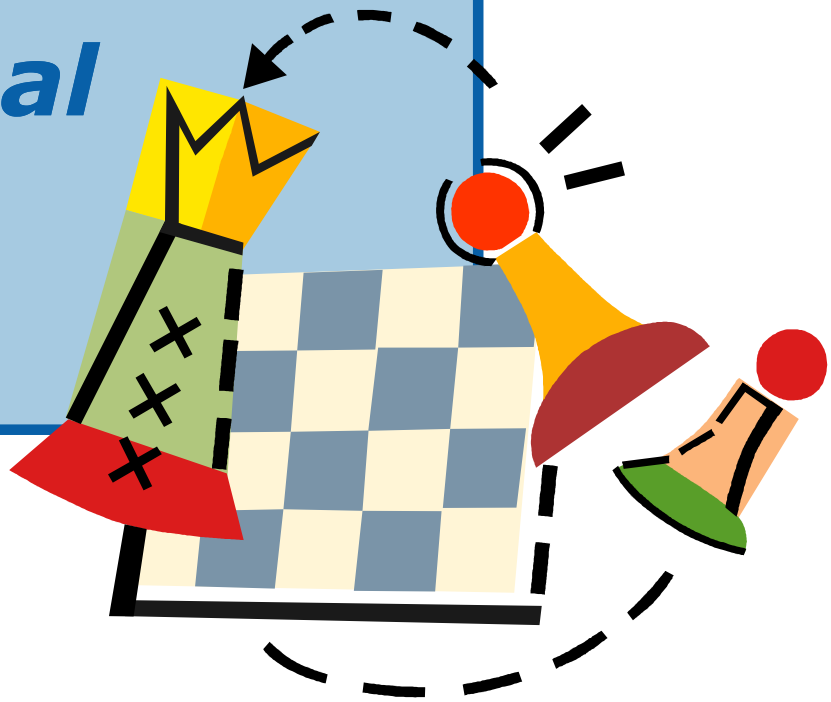
Los sistemas de información son:

- **Formales**
- **Informales**

- Cambiantes
- Ajustables
- Basados en las necesidades de los interesados
- Incrementales
- Indicadores
- Registros históricos
- Instrumentos de comunicación

La función básica de los SI es:

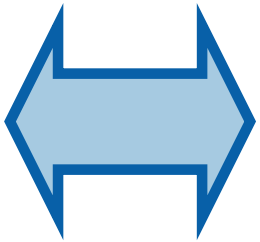
Aportar para la estrategia organizacional



Otra función no menos importante es:

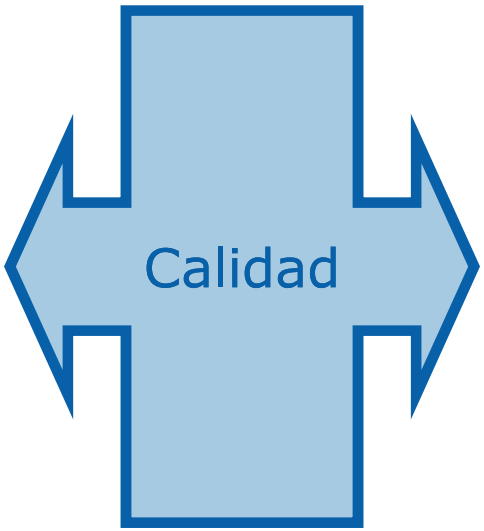
Integrar las operaciones organizacionales

El paradigma de los sistemas "nuevos...

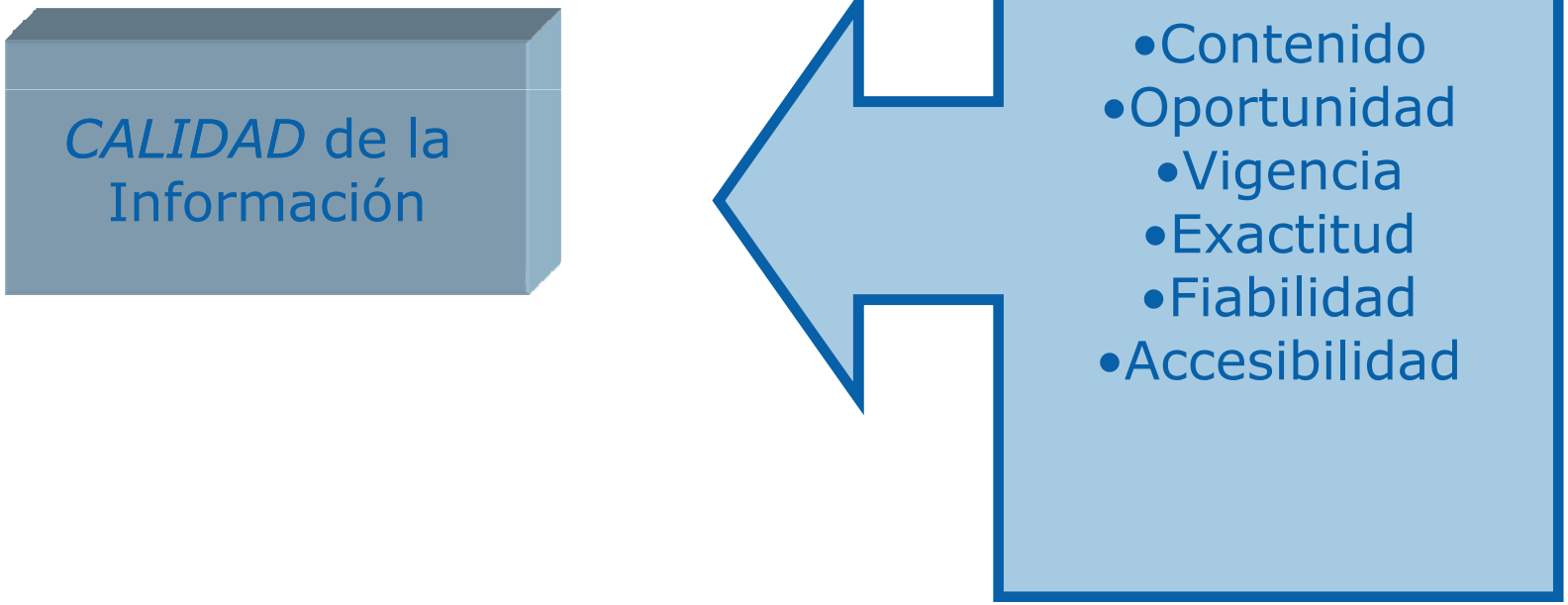


- Objetivos
- Necesidades
- Disponibilidad
- Efectos en el control

Información



Toma de decisiones


CALIDAD de la Información
•Contenido
•Oportunidad
•Vigencia
•Exactitud
•Fiabilidad
•Accesibilidad

Comunicación

La comunicación es inherente a los sistemas de información

La comunicación interna

- Mensaje claro e efectivo sobre las responsabilidades en el SCI
- Tareas y funciones definidas
- Entendimiento sobre los procesos y funcionamiento del SCI

Desempeño y tareas

- El personal debe ser capaz de:
  - identificar los incidentes y sus causas
  - Tomar acciones para solucionarlas y prevenirlas
  - Conocer sus tareas, las de otros y sus relaciones
  - Comunicar a sus coordinadores asuntos importantes
    - Bidireccionalidad
    - Canales
    - Líneas formales e informales

Administración y gobierno corporativo

- Comunicación como requerimiento del SCI
- Comunicación ***hacia*** el GC sobre:
  - Desempeño
  - Riesgos
  - Proyectos
  - Regulación
  - Rendición de cuentas
- Comunicación ***desde*** el GC sobre:
  - Necesidades de información
  - Directrices
  - Realimentación

La comunicación externa

- Canales abiertos para los usuarios
- Habilitar oportunidades de mejora
- Información sobre el SCI

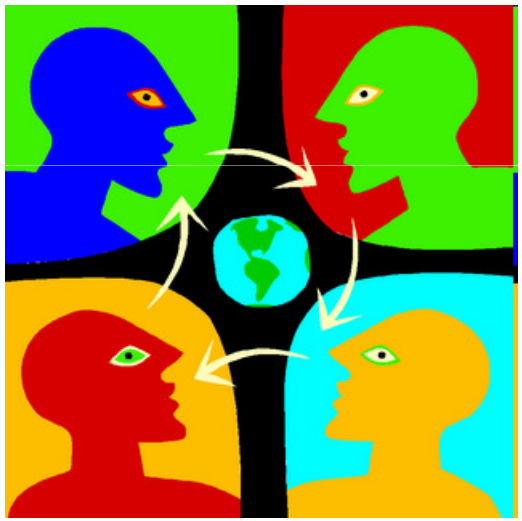
Comunicación externa y entes reguladores

- Fuentes para identificar debilidades en:
  - el SCI
  - las operaciones.

Comunicación para sujetos interesados

- Información relevante
- Según sus necesidades
- Para entender las circunstancias y riesgos operativos
- Legales
- Oportunas
- Significativas
- Pertinentes

Medios de comunicación



- Manuales
- Correo electrónico
- Páginas web
- Boletines
- Vídeo
- Intranet
- Correspondencia
- Ejemplo

Resumen de las variables del componente de información y comunicación		
Información	**Sistemas estratégicos e integrados**	**Comunicación**
○Interna ○Externa ○Manual ○Computadorizada ○Formal ○Informal	○Estratégica ○Operacional ○Pasada y presente ○Nivel de detalle ○Periodicidad ○Calidad	○Interna ○Externa ○Nivel en la entidad ○Expectativas y responsabilidades ○Formatos ○Medios de transmisión

Sistemas de información y comunicación en entidades pequeñas

- SCI menos formal
- TI/SI menos compleja
- Los SI apoyan las operaciones
- Poca capacidad para considerar información externa
- La comunicación es más sencilla
- Reuniones y contacto día a día
- El ejemplo de la administración es fundamental

Evaluación

- Información
  - Fuentes externas e internas
  - Informes sobre desempeño
  - Suministro, suficiencia y oportunidad
  - Destinatarios
  - Alineación estratégica
  - Compromiso de la administración para desarrollar su SI

- Comunicación
  - Efectividad para comunicar las responsabilidades sobre el SCI
  - Canales de comunicación para reportar irregularidades
  - Receptividad para sugerencias
    - Productividad
    - Calidad
    - Mejora
  - Suficiencia y calidad
  - Apertura de los canales externos
  - Divulgación sobre la ética institucional
  - Atención de sujetos interesados

Contexto legal

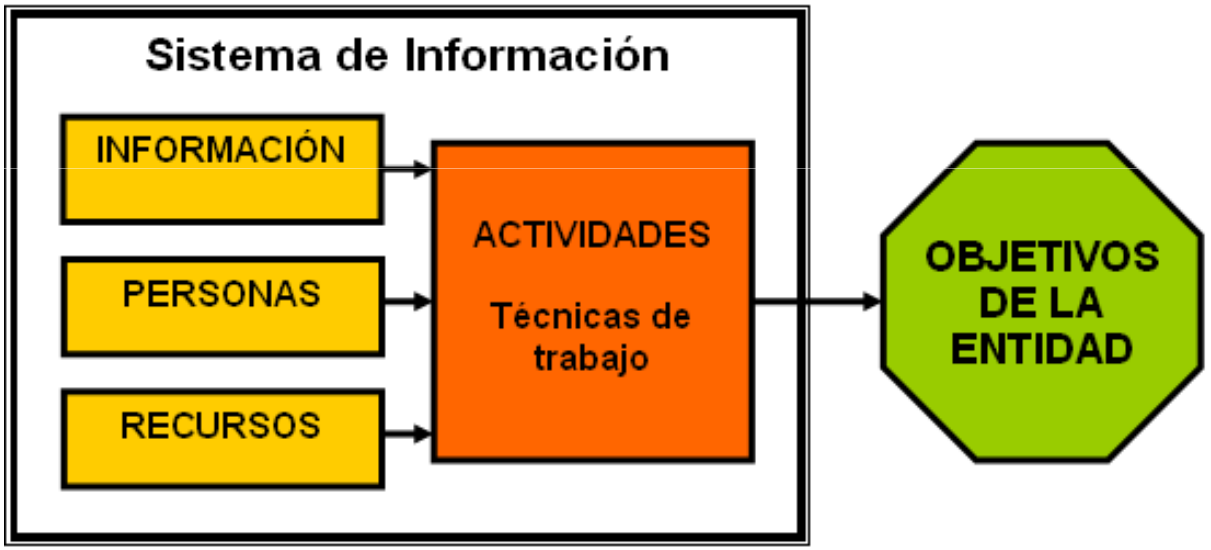
- Artículo 16 de la LGCI #8292
  - Contar con SI
  - Gestión documental
  - Gestión de la información
  - Información y comunicación
  - Deberes

Contexto del artículo 16

Sistemas manuales y sistemas automatizados –Apoyo para los objetivos –NTI	Calidad –Canales y medios de comunicación –Destinatarios –Oportunidad –Seguridad
Alienación institucional y gestión documental –Bases de datos –Aplicaciones informáticas	Utilidad y oportunidad
Jerarca y titulares subordinados como responsables –Confiable –Oportuna –útil	Alineación e inversiones Legalidad

Componente 4: Sistemas de información

2 El sistema de información y comunicación: su importancia institucional


Sistema de Información
INFORMACIÓN
PERSONAS
RECURSOS
ACTIVIDADES
Técnicas de trabajo
OBJETIVOS DE LA ENTIDAD

Calidad de la información

Estrategia y el sistema de información

Perspectiva de la comunicación

Herramientas tecnológicas

Calidad de la información

- Afecta la toma de decisiones
- Proceso
- Responde a las necesidades de los usuarios
- Papel del colaborador

Estrategia y el sistema de información

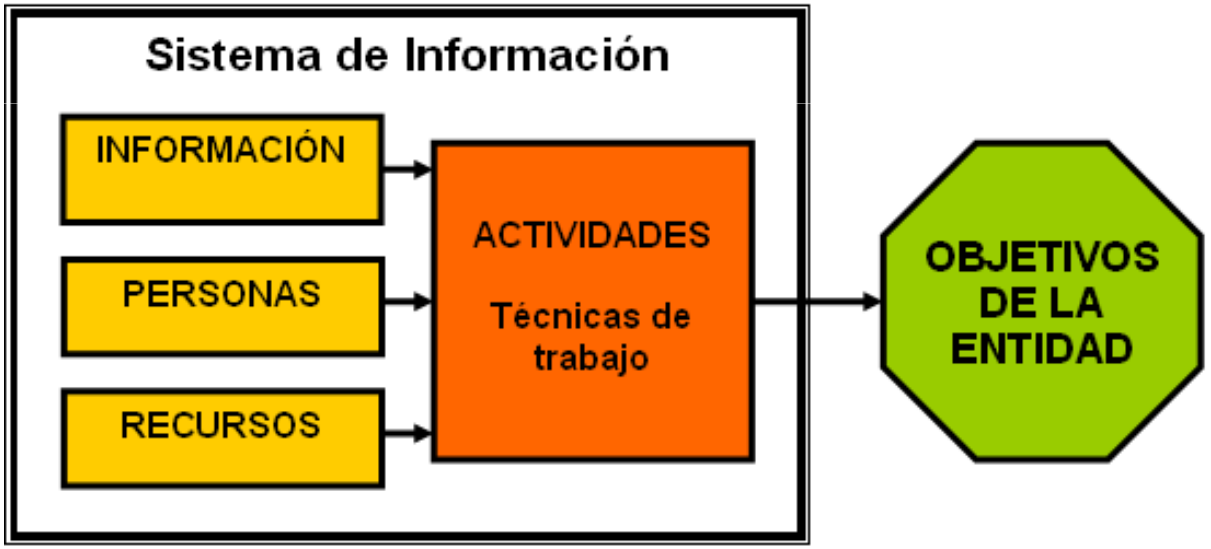
- Integrado al SCI
- Participación y planificación
- Alinear esfuerzos e inversiones
- Alcanzar prioridades

- Interna
- Externa
- Gestión efectiva
- Entendimiento sobre el SCI y objetivos
- Gestionar el riesgo
- TI como medio de comunicación

Perspectiva de la comunicación

- Medio y no fin
- Optimizar inversión y potenciar desempeño
- Estudiar la magnitud de la inversión
- ***Necesidad de…***
- Responder a la estrategia y luego a las operaciones

Herramientas tecnológicas


Sistema de Información
INFORMACIÓN
PERSONAS
RECURSOS
ACTIVIDADES
Técnicas de trabajo
OBJETIVOS DE LA ENTIDAD

Componente 4: Sistemas de información

3 Marco regulatorio

LGCI

- Artículo 16

Regulaciones sobre el componente de sistemas de información en las "Normas de control interno para el sector público"

5.1 Sistemas de información
5.2 Flexibilidad de los sistemas de información
5.3 Armonización de los sistemas de información con los objetivos
5.4 Gestión documental
5.5 Archivo institucional
5.6 Calidad de la información
- 5.6.1 Confiabilidad
- 5.6.2 Oportunidad
- 5.6.3 Utilidad

5.7 Calidad de la comunicación
- 5.7.1 Canales y medios de comunicación
- 5.7.2 Destinatarios
- 5.7.3 Oportunidad
- 5.7.4 Seguridad

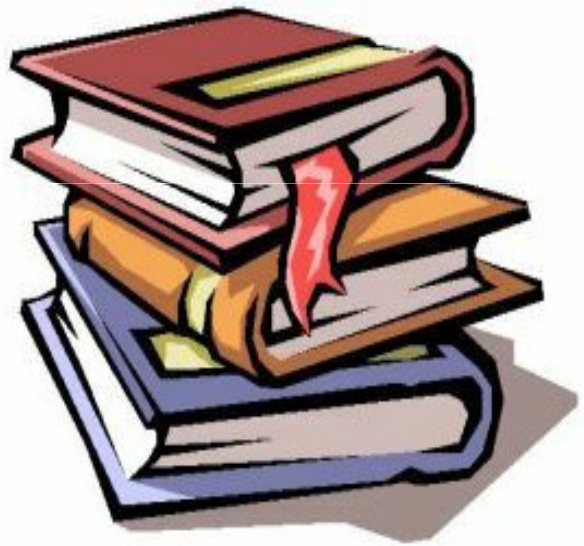
5.8 Control de sistemas de información
5.9 Tecnologías de información
5.10 Sistemas de información en instituciones de menor tamaño

Normas específicas para TI

"Normas técnicas para la gestión y el control de las tecnologías de información", N-2-2007-C0-DFOE, aprobadas mediante la resolución del Despacho de la Contralora General de la República, Número R-CO-26-2007 del 7 de junio del 2007, y publicadas en La Gaceta número 119 del 21 de junio del 2007.

Características de las NTI

- Prácticas líderes
- Criterios de control
- Criterios de gestión
- Para administrar el SCI
- Acatamiento obligatorio
- Su inobservancia genera responsabilidades



Componente 4: Sistemas de información

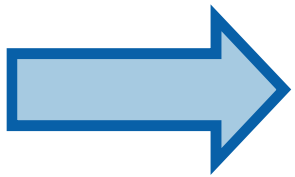
4 Responsabilidades

Responsabilidad sobre información y comunicación

- Administración activa
  - Establecerlo
  - Promover su fortalecimiento
  - ***Integralmente***
  - ***Jerarca como líder***
- Crear una herramienta de gestión eficaz
- Cumplimiento de las NTI en toda la organización

Responsabilidad de la auditoría interna

- Asesorar
- Advertir



- SI:
  - Robusto
  - Eficiente
  - Económico
  - eficaz

Reponsabilidades y normas:

- Normas de control interno
- NTI

Referencias a mejores prácticas

- Para promover la mejora continua del SCI
- Referencia a otros modelos de CI y gestión y control de TI
- Cada entidad analiza su necesidad
- No debe oponerse a lo emitido por la CGR

Componente 4: Sistemas de información

5 Normas relacionadas con los sistemas de información

Antecedentes

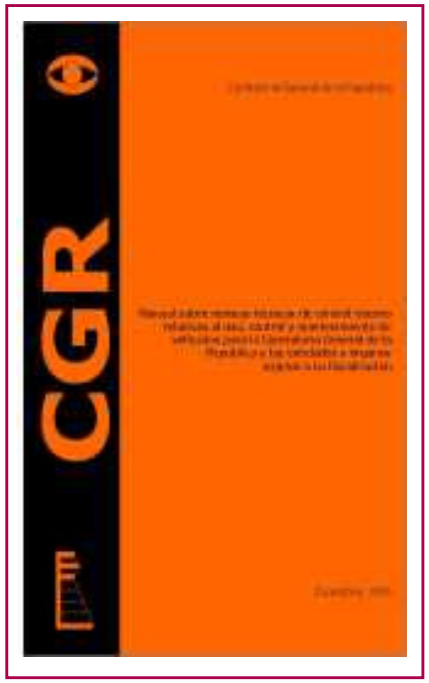
1 Origen y Situación Actual

2 Estrategias DFOE

3 **Normativa**

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

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



Capitulo I : Normas de Aplicación General

Capítulo II: Planificación y Organización

Capítulo III: Implementación y Mantenimiento de las Tecnologías de Información

Capitulo IV : Prestación de Servicios

Capitulo V : Seguimiento

Situaciones relevantes

- Presupuesto e inversión
- Marco jurídico
- Presión por requerimientos

Aclaración importante: instituciones de menor tamaño

El jerarca y los titulares subordinados de las instituciones de menor tamaño, según sus competencias, deben establecer los procedimientos manuales, automatizados o ambos, necesarios para obtener, procesar, controlar, almacenar y comunicar la información sobre la gestión institucional y otra relevante para la consecución de los objetivos institucionales. Dicha información debe ser de fácil acceso y estar disponible en un archivo institucional que, de manera ordenada y conforme a las regulaciones que en esa materia establece el Sistema Nacional de Archivos, pueda ser consultado por usuarios internos o por parte de instancias externas.

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

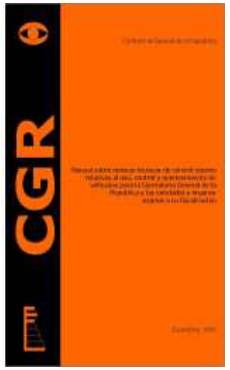
Capítulo IV Prestación de servicios y mantenimiento

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.



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

Del capítulo I en términos generales:

- Marco estratégico: que procura que el jerarca logre traducir sus expectativas en materia de TI en actividades cotidianas. Para ello requiere tener claro cuáles son sus expectativas y luego un buen mecanismo para lograr trasmitirlas al personal y lograr que éste se comprometa con ellas.
- La calidad consiste satisfacer los requerimientos de los usuarios o clientes; por lo que es necesario conocer bien quién o quiénes son nuestros clientes, cuáles son sus requerimientos, fijar esos requerimientos como atributos de nuestros servicios y productos y establecer lo necesario para lograr esos atributos de manera eficiente.
- Todo logro está afecto a riesgos, entonces, hay que lograr identificar los riesgos de todo lo relacionado con la gestión de TI (por ejemplo: del éxito de un proyecto de desarrollo de un sistema o del funcionamiento del sistema mismo), valorarlos (probabilidad e impacto) y definir las medidas para mitigarlos, transferirlos y aceptarlos.

Gestión de la seguridad de la información:

Las entidades públicas deben garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información. Deben entonces habilitar los mecanismos para protegerla contra uso, divulgación o modificación no autorizados, daños y pérdidas, entre otros factores disfuncionales.

Gestión de la seguridad de la información

- La implementación de un marco de seguridad de la información
- El compromiso del personal con la seguridad de la información
- La seguridad física y ambiental
- La seguridad de las operaciones y comunicaciones
- El control de acceso
- La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica
- La continuidad de los servicios de TI

Capítulo I Normas de aplicación general

1.5 Gestión de proyectos

1.6 Decisiones sobre asuntos estratégicos de TI

1.7 Cumplimiento de obligaciones relacionadas con la gestión de TI

- La gestión de las TI, como se ilustró en el diagrama, implica la ejecución de actividades continuas y la realización de proyectos.
- Para tratar de garantizar el éxito de los proyectos, la Administración debe ser cuidadosa en su ejecución. De ahí la necesidad de que defina marcos de gestión de proyectos, los cuales pueden basarse en propuestas como la del PMI, que resultan muy convenientes.
- La toma de decisiones estratégicas en TI y la constitución de los Comités de Informática se ha convertido más en un problema que en el beneficio que se quiere lograr. Las decisiones cuenten con el apoyo de una representación razonable de la organización, con el propósito de basarlas en una visión integral y debidamente priorizada. Sin embargo, ha sucedido que la constitución de dichos comités más se ha convertido en un fin en si mismo y en un obstáculo en algunos procesos. De ahí que la CGR ha decido cambiar el enfoque de esta norma para que más que un "órgano colegiado" la gestión se base en decisiones debidamente concensuadas.
- El cumplimiento de las obligaciones implica conocer todo el marco jurídico que le afecta a la gestión de TI y procurar su cumplimiento.

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

- La planificación constituye la base de la gestión de las TI. De ahí que es imprescindible la definición de un buen plan debidamente alineado con la estrategia institucional (no siempre disponible) mediante la cual se establezcan los objetivos estratégicos y se considere el escenario objetivo y las actividades para lograrlo a partir del análisis del escenario actual.

- Debe considerarse el modelo de arquitectura de información es la esquematización del conocimiento completo de los sistemas institucionales y del flujo de la información de la entidad por dichos sistemas. Por su parte, el modelo de infraestructura tecnológica que es el conjunto del hardware e instalaciones en la cual operan los sistemas y fluye la información.

- Para que sea posible la gestión es necesario contar con un equipo de trabajo motivado y con las competencias necesarias, Asimismo, que goce de la independencia orgánica necesaria para lograr un apoyo uniforme y equilibrado en toda la organización.

- Si bien todas las organizaciones cuentan con una administración presupuestaria, es conveniente que como parte de la gestión de las TI se tenga un control sobre los recursos financieros invertidos, principalmente en cuanto al análisis y seguimiento de los costos asociados con los procesos. No se vale aducir que se desconoce las implicaciones financieras de las decisiones de TI por tratarse de una materia del resorte de otras unidades.

Capítulo III Implementación de tecnologías de información

- Partiendo de un plan de trabajo, se debe atender los requerimientos de información vía actividades de ejecución continua o bien, mediante la implementación de nuevas soluciones.
- Dicha implementación puede implicar software, hardware o instalaciones, o bien, una mezcla.
- Cuando se lleva a cabo este tipo de proyectos resulta necesario un marco metodológico que guíe su ejecución para garantizar que se conoce bien los requerimientos, que se diseña adecuadamente las soluciones, que se desarrolla y pone en operación mediante ambientes seguros y controlados, Se evalúa su desempeño posteriormente.
- Lo anterior tiene gran relevancia cuando se trata de la contratación de terceros, a quienes se les encarga dicha implementación, en cuyo caso, la contraparte técnica establecida por la organización juega un papel preponderante.

Capítulo IV Prestación de servicios y mantenimiento

- Los acuerdos de servicio constituyen un instrumento que permite tener claridad de los resultados que la administración espera de la gestión de TI y de la capacidad de esta última para lograrlos. Ese equilibrio es conveniente que esté documentado pues puede utilizarse como mecanismo de medición del desempeño.
- La administración de la plataforma debe procurar su desempeño adecuado y ajustado en el tiempo a los requerimientos de la organización. Debe evitarse su obsolescencia prematura y la interrupción de su operación por períodos que representen riesgo a la organización o inconvenientes significativos a sus usuarios.
- La calidad de la información está en la calidad de sus datos, de ahí la importancia de los controles de aplicación (entrada, proceso, salida, y pistas de auditoría) así como lo relativo al almacenamiento, transmisión y desecho de los datos. Debe considerarse su disposición -desecho controlado- y que cumplan con criterios de calidad como los ya mencionados.

- En su mayoría, los usuarios de las TI demandarán una serie de atenciones que deben ser tramitadas en forma ágil para evitar demoras en la gestión de esos actividades.

- Todo incidente debe ser debidamente resuelto de manera segura y controlada, documentado y analizado o estudiado para implementar las acciones necesarias para minimizar su recurrencia.

- El *outsourcing* implica que la Administración tome las previsiones necesarias a fin de garantizar la obtención correcta de los servicios prestados por terceros así como que ellos garanticen los términos de calidad, riesgos y seguridad preestablecidos por la organización.

Capítulo V Seguimiento

- La entidad debe contar con un marco de referencia y un proceso de seguimiento para vigilar la gestión de TI. Las responsabilidades del personal deben estar claramente definidas, por ejemplo, mediante la aplicación de un cuadro de mando integral para TI.
- Es responsabilidad del jerarca establecer y mantener el sistema de control interno relacionado con la gestión de las tecnologías de información.
- La Auditoría Interna debe coadyuvar a que el control interno en TI brinde una garantía razonable del cumplimiento de los objetivos de la entidad.

Como parte de todo proceso se da el seguimiento, el cual pretende identificar e implementar oportunamente las mejoras necesarias.

Parte de ese seguimiento se ve en las acciones de la Auditoría Interna y en los procesos de evaluación del control interno.

Deberá la Administración, entonces, implementar lo necesario para dar un adecuado seguimiento a la gestión de las TI y continuar con el ciclo de gestión hacia una nueva planificación que considere lo aprendido e incorpore las mejoras identificadas.

Mediante la vía de resolución, la CGR da vida a la normativa en comentario y respecto del logro de su debido cumplimiento establece una serie de lineamientos que deben ser analizados cuidadosamente.

> Artículo 1—Aprobar el documento denominado “Normas técnicas para la gestión y el control de las tecnologías de información”, normativa que establece los criterios básicos de control que deben observarse en la gestión de esas tecnologías y que tiene como propósito coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios públicos, representando inversiones importantes en el presupuesto del Estado.

- Artículo 2 – Promulgar las “Normas técnicas para la gestión y el control de las tecnologías de información”, Nro. N-2-2007-CO-DFOE.

- Artículo 3 – Acatamiento obligatorio y su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable.

- Artículo 6 – Informar que la Administración contará con dos años a partir de su entrada en vigencia para cumplir con lo regulado en esta normativa, 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.

Hacer un cronograma completo, siguiendo una la metodología de administración de proyectos, sería un bien comienzo, de manera constituya un instrumento para dar seguimiento a la ejecución del plan y al debido cumplimiento de la normativa.

Recordar que es conveniente lograr un apoyo interinstitucional para facilitar este proceso, sobre todo considerando que hay entidades que ya tienen camino andado y que pueden ilustrar o guiar a otras que no tienen igual desarrollo en la materia.

Artículo 7 – Comunicar que la referida normativa entrará a regir a partir del 31 de julio del 2007.

Y las administraciones tendrán dos años para poner en práctica lo dispuesto por las normas.

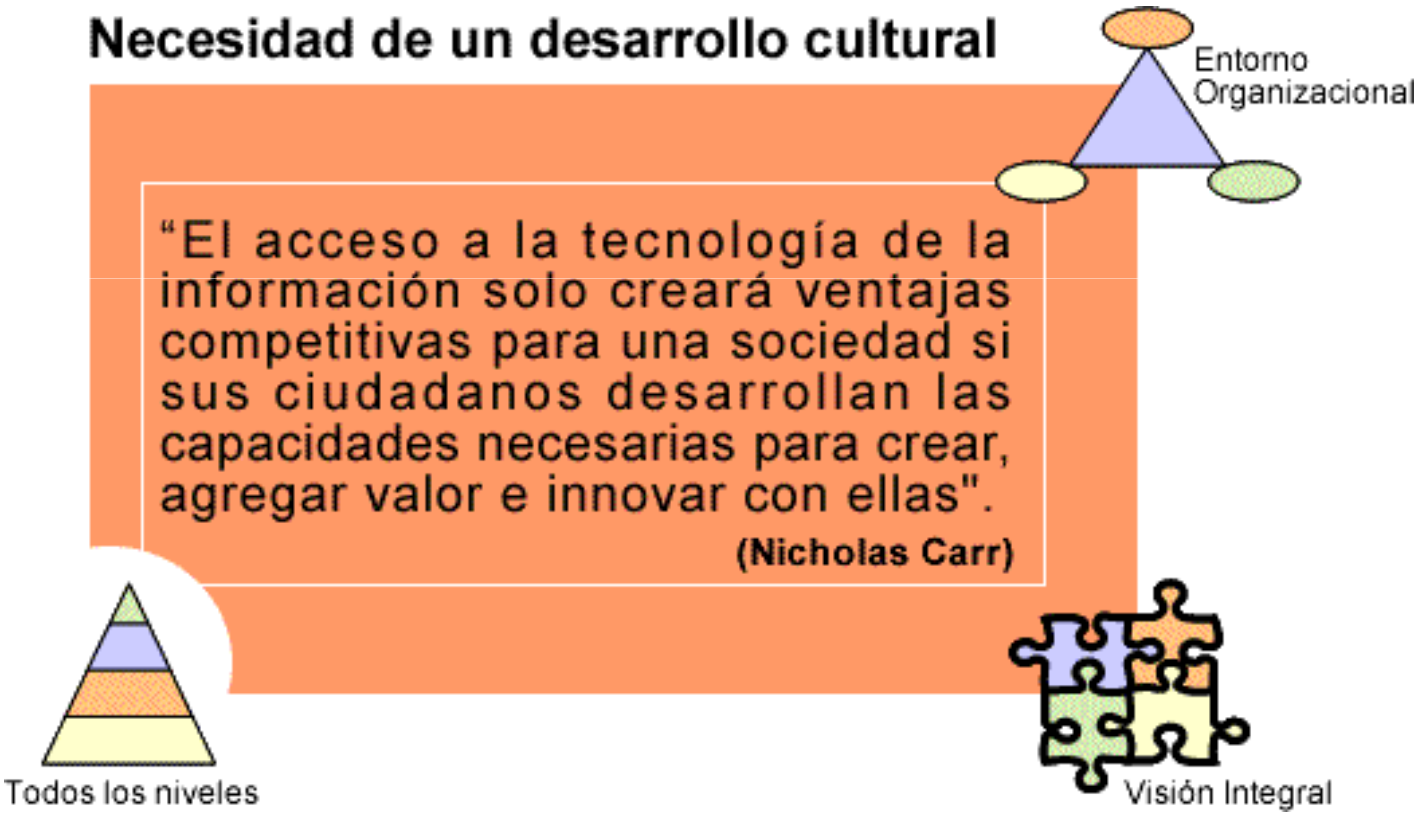
Posteriormente, la CGR fiscalizará su cumplimiento.

1 **Origen y Situación Actual**

2 **Estrategias DFOE**

3 **Normativa**

Competencias e Instrumentos



¡Muchas gracias!