Control Interno

curso virtual
Contraloría General de la República

SISTEMA DE INFORMACIÓN

Componente 4

SISTEMA DE INFORMACIÓN

- Contenido -

Concepto

Los sistemas de información son el tercer componente del sistema de control interno (SCI), y comprenden los sistemas de información y comunicación existentes en la institución, los cuales deben permitir la generación, la captura, el procesamiento y la transmisión de información relevante sobre las actividades institucionales y los eventos internos y externos que puedan afectar su desempeño positiva o negativamente.

Según el informe COSO, una organización debe identificar, capturar y comunicar la información financiera y no financiera pertinente para la entidad, que le permita a las personas desarrollar sus responsabilidades. Al respecto, los sistemas de información producen informes que contienen información sobre las operaciones, las finanzas y asuntos de cumplimiento, que faculta el desempeño y control de la entidad. Tales sistemas de información consideran datos internos y externos, que pueden afectar el proceso de toma de decisiones y la comunicación para sujetos interesados.

La comunicación efectiva fluye a lo largo de toda la entidad. El personal debe recibir el mensaje de la administración superior sobre tomar con seriedad los deberes y responsabilidad sobre el control interno.

El personal debe conocer y entender su papel en el sistema de control interno y las relaciones de trabajo en la organización, así como contar con mecanismos de comunicación para compartir asuntos importantes hacia niveles superiores de toma de decisiones, y con entes externos, tales como los ciudadanos, los proveedores, entes reguladores, entre otros.

La información: conceptos fundamentales

Todos los niveles institucionales requieren información que les permita alcanzar sus objetivos. La información puede ser:

○ **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

La información se origina en fuentes internas y externas, tanto de naturaleza financiera como no financiera. En general, debe ser relevante para apoyar los tipos de objetivos institucionales: estratégico, táctico y operativo.

Los sistemas de información identifican, capturan, procesan y comunican información. Los sistemas de información generalmente tienen contexto de procesos internos. Sin embargo, el término tiene alcance externo también, al considerar eventos, actividades y condiciones que pueden afectar a la institución, tales como datos sobre el comportamiento financiero nacional, índices económicos, solicitudes de los ciudadanos, y asuntos regulatorios y legales.

Los sistemas de información operan tanto de forma rutinaria, como para obtener datos específicos que son relevantes para los procesos institucionales. Las actividades regulares proporcionan datos sobre las operaciones, y algunos sistemas permiten obtener datos no estructurados, mediante encuestas, comunicaciones con los usuarios y navegación en Internet. Los sistemas coadyuvan a identificar riesgos y oportunidades.

Se puede clasificar los sistemas de información en:

- Formales
- Informales

La información requiere mantener uniformidad y congruencia con las necesidades operativas de las instituciones, requerimientos incrementales de los ciudadanos, cambios e innovación. Los sistemas de información deben cambiar según resulte necesario para apoyar los objetivos institucionales. Es importante diferenciar los datos que sirven como indicadores y aquellos que son fundamentalmente de tipo contable. Ambos tipos de datos son valiosos, y cuando se utilizan conjuntamente, permiten la gestión preactiva de la información, bajo las condiciones de comunicación oportuna, por los medios convenientes, útiles y controlados por la entidad.

Los sistemas de información aportan para la estrategia. Generalmente, los sistemas de información son parte integral de las operaciones, capturan la información para apoyar la toma de decisiones y para control. También, los sistemas de información también pueden apoyar los asuntos estratégicos, tal como en su contribución con la alineación con los objetivos institucionales. El uso de estos recursos puede facilitar la realización de ventajas competitivas y mejores servicios de nuestras instituciones.

Los sistemas de información se integran con las operaciones institucionales. La mejor muestra es la forma en que los sistemas contables han evolucionado hacia sistemas integrados organizacionalmente. Estos sistemas integrados ayudan a controlar los procesos institucionales, registran transacciones en línea, actualizan los datos financieros y presupuestarios según desarrollan aplicaciones operativas, incluyendo múltiples tipos de transacciones en modelos complejos, que propician la eficiencia de las operaciones.

A pesar de las innovaciones en las tecnologías y sistemas de información, un sistema es mejor y aporta control solamente por ser más nuevo. Los sistemas de información antiguos han sido probados y han funcionado, y por tanto, son valiosos. En este contexto, los sistemas evolucionan según las necesidades de los usuarios y derivan en ambientes donde coexisten nuevos y viejos sistemas.

En relación con lo anterior, las adquisiciones son asunto relevante para la estrategia institucional, y la escogencia de tecnología puede ser un asunto que afecte el cumplimiento de objetivos. Algunos factores que influyen en la selección e implantación de tecnologías son:

- Objetivos organizacionales
- Necesidades de la organización y del usuario
- Disponibilidad del mercado
- Efecto de los nuevos sistemas en el control.

La calidad de la información afecta la habilidad de la administración para tomar decisiones. Al respecto, los productos de los sistemas de información deben suministrar datos para controlar efectivamente las operaciones. La calidad de la información debería garantizar:

- Contenido apropiado
- Oportunidad
- Vigencia
- Exactitud, confiable
- Accesible.

Estos factores deben considerarse en el diseño del sistema de información, para que facilite la toma de decisiones. La información correcta y oportuna, en manos adecuadas es fundamental para el control. Aún más, los sistemas de información deben ser controlados, lo cual está relacionado con la calidad de la información, sujeto a su vez con el componente del sistema de control interno denominado "actividades de control".

La comunicación: conceptos fundamentales

La comunicación es inherente a los sistemas de información. Más allá de los asuntos tecnológicos, la comunicación debe aportar para conocer las expectativas, las responsabilidades individuales y grupales, entre otros asuntos.

Comunicación interna:

El personal debe contar con un claro mensaje de la administración superior sobre la importancia de tomar seriamente sus responsabilidades sobre el control interno. Tanto la claridad como la efectividad del mensaje son importantes.

Al respecto, las tareas y funciones deben ser claramente definidas. Cada funcionario debe entender los asuntos más importantes del sistema de control interno, cómo opera y su responsabilidad en éste. Sin este entendimiento, habrá problemas y será difícil lograr acciones correctivas.

Al desempeñar las tareas, el personal debe ser capaz de identificar los incidentes y sus causas. De esta forma, las debilidades potenciales del sistema pueden ser identificadas y tomar acciones para solucionarlas y prevenir su recurrencia.

El personal también debe cómo se relacionan sus tareas con las de otros. Este conocimiento es necesario para identificar situaciones disfuncionales, sus causas y acciones correctivas. Por ejemplo, manipular los datos financieros puede convertirse en un fraude; un funcionario presionado podría alterar este tipo de información con el fin de alcanzar metas financieras, lo cual sería incongruente con el mensaje de ética institucional.

El personal debe ser capaz de comunicar a sus coordinadores sobre asuntos importantes. Para tal fin, debe existir canales bidireccionales de comunicación. Los coordinadores deben ser capaces de recibir este tipo de información y actuar de conformidad. Debe haber líneas de comunicación formal e informal. Debe existir mecanismos para el personal comunique, sin temor a represalias, sobre la existencia de situaciones sospechosas de violación al código de conducta institucional, o a las prácticas y procesos institucionales.

Las comunicaciones entre la administración y el grupo de gobierno corporativo (i.e. Junta Directiva), es un requerimiento para el sistema de control interno. La administración debe mantener al grupo de gobierno corporativo debidamente actualizado sobre el desempeño, riesgos, proyectos importantes, entre otros asuntos. Mientras mejor sea la comunicación con el cuerpo de gobierno corporativo, más efectivo será el cumplimiento de responsabilidades. Por otro lado, el cuerpo de gobierno corporativo debe indicar a la administración sus necesidades de información, suministrar dirección sobre el tema y realimentación.

Comunicación externa:

Los usuarios de los servicios institucionales requieren canales abiertos de comunicación, que habiliten oportunidades para mejorar las operaciones. Las comunicaciones de partes externas facilitan información sobre el funcionamiento del control interno. Algunos ejemplos son: quejas, denuncias, y sugerencias.

Los informes de entes de regulación pueden resultar en importantes fuentes para identificar debilidades de control y de operación. Por ejemplo, las quejas deben ser atendidas por personal diferente al que hizo la transacción original, para tomar acciones correctivas.

La comunicación para los sujetos interesados debe suministrar información relevante para sus necesidades, de forma que puedan entender las circunstancias y riesgos de las operaciones. Tales comunicaciones deben ser legales, oportunas, significativas y pertinentes.

Los medios de comunicación puede ser:

- Manuales
- Correo electrónico
- Páginas web
- Boletines
- Vídeo
- Intranet
- Correspondencia
- El ejemplo de la administración, entre otros.

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

Los sistemas de información en entidades relativamente pequeñas son menos formales, pero su función es importante. La tecnología de información apoya las operaciones, sin perjuicio del tamaño de la entidad, y los sistemas de información también realizan funciones similares que en entidades más complejas. El tema divergente es si la administración es capaz de considerar información externa para tomar decisiones.

La comunicación entre funcionarios y la administración es, generalmente, más sencilla de lograr en entidades relativamente pequeñas, por la menor cantidad de niveles de mando y de coordinación. Las reuniones informales y formales son más participativas, en general. El contacto día a día es un factor determinante junto con la política de puertas abiertas. El ejemplo de la administración es crítico en entidades de este tipo.

Evaluación

Un evaluador que examine el sistema de información y comunicación considerará:

Información

- Obtención de información externa e interna, y la forma en que la administración genera informes sobre el desempeño relacionado con los objetivos
- Suministro de información, suficiente y oportuna, para los sujetos interesados, de forma que puedan cumplir sus responsabilidades
- Desarrollo de sistemas con alienación estratégica
- Compromiso de la administración con el suministro de recursos para desarrollar sus sistemas de información

Comunicación

- Efectividad en la comunicación de responsabilidades sobre el control y las tareas de los funcionarios
- Establecimiento de canales de comunicación para reportar irregularidades
- Receptividad de la administración para recibir sugerencias sobre productividad, calidad y mejora
- Suficiencia y calidad de la información a través de la entidad, así como la totalidad y oportunidad
- Apertura y efectividad de los canales externos de comunicación
- Forma en que las partes externas han sido informadas sobre la ética institucional
- Oportunidad y debido seguimiento de la administración sobre comunicaciones recibidas de partes y sujetos interesados.

Contexto legal

El **artículo 16** de la Ley General de Control Interno (**LGCI**), número 8292, señala el requerimiento de contar con sistemas de información, que permitan a la administración activa su **gestión documental institucional**, mediante el control, almacenamiento y recuperación de la información organizacional, para prevenir desvíos de los objetivos institucionales. Menciona también la importancia de que la gestión documental esté ligada con la **gestión de la información**, considerando bases de datos y aplicaciones de TI. Además, menciona, en cuanto a la **información y comunicación**, los **deberes** del jerarca y los titulares subordinados.

En el contexto de este artículo 16, destacan los siguientes asuntos:

a. En la mayoría de los casos, un sistema de información estará apoyado en tecnologías de información. No obstante, es posible que alguna entidad utilice sistemas de información en etapas semiautomáticas o manuales, como mecanismos incipientes de procesamiento de información. Ante tales situaciones, es importante considerar que la LGCI requiere una gestión documental institucional activa y debidamente administrada. Por otro lado, las instituciones con desarrollo informático deberán considerar lo indicado por las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información.[1]	b. Según el planteamiento de la LGCI, una gestión documental institucional debe considerar actividades que faciliten el control, el almacenamiento y las capacidades para recuperar la información para apoyar las actividades y objetivos de la entidad.
c. La gestión documental debe responder a un principio de alineamiento estratégico que facilite la gestión de la información	d. Los jerarcas y titulares subordinados son responsables de que el sistema de información y comunicación institucional

[1] 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.

institucional. Al respecto, se debe considerar dos componentes tecnológicos: - las bases de datos, como instrumentos fundamentales para la gestión de datos organizacionales - las aplicaciones informáticas, necesarias para capturar, procesar y emitir información.	funcione correctamente. Al respecto, toda entidad pública debe contar con procesos que garanticen la identificación y registro de información con estas características: - **Confiable**: la información debe ser confiable, libre de errores, defectos, omisiones y modificaciones no autorizadas, y emitida por la instancia competente. Además, debe contar con fuentes de referencia fiables. - **Oportuna**: las actividades para recopilar, procesar y generar información deben darse a tiempo, conforme a los fines institucionales. Además, la información debe estar disponible en tiempo, a propósito y cuando convenga para la toma de decisiones institucional. - **Útil:** la información debe tener características que la hagan útil para diversos usuarios, aportando pertinencia, relevancia, suficiencia y requerimientos de presentación. Su contenido debe ser importante y proporcionar significado y provecho al usuario. Los datos en contexto deben tener un propósito y ser concernientes al tema de que traten.
e. La comunicación debe tener calidad. Al respecto, el jerarca y los titulares subordinados deben establecer procesos efectivos y con perspectiva de mejoramiento continuo, para que la comunicación institucional involucre las instancias pertinentes oportunamente, según los requerimientos y necesidades de los usuarios. Algunos criterios particulares de las Normas de Control Interno son: ○ **Canales y medios de comunicación**: la institución debe contar con canales y medios de comunicación para trasladar la información de forma transparente, ágil, segura, correcta y oportuna, hacia los interesados dentro y fuera de la institución. ○ **Destinatarios**: la información se comunica a las instancias competentes internas y externas, para aportar funcionalmente para los objetivos institucionales. ○ **Oportunidad**: la información debe comunicarse a los destinatarios con la debida prontitud que le facilite el cumplimiento de sus responsabilidades.	f. La utilidad de la información está directamente relacionada con su oportunidad. Los responsables de los procesos institucionales requieren que la información esté convenientemente disponible para facilitar la toma de decisiones y el cumplimiento de las tareas y responsabilidades.

○ **Seguridad**: la información debe contar con controles que aseguren su calidad y su traslado en condiciones adecuadas de protección, según su grado de sensibilidad y confidencialidad. También, debe estar disponible y ser accedida por los usuarios en la oportunidad y con la prontitud que requieran.	
Otro elemento de responsabilidad para el jerarca y los titulares subordinados consiste en garantizar la alineación de los sistemas de información con los objetivos institucionales, la cual es una de las premisas más críticas al considerar la inversión en recursos de TI. Debido a la importancia relativa de las iniciativas de TI, toda institución debe contar con mecanismos de gestión estratégica que faciliten armonizar las inversiones tecnológicas con las necesidades y el cumplimiento de objetivos institucionales.	g. Además, la implantación jurídica y técnica sobre el funcionamiento del archivo institucional es un punto clave en materia de responsabilidades.[2]

PREGUNTAS DE REPASO

¿Cuál es el principal propósito de los sistemas de información, según la LGCI?

¿Quiénes son responsables del buen funcionamiento del sistemas de información?

¿Cuáles son las principales características de la información?

¿En qué consiste el concepto de alineación estratégica de los sistemas de información?

[2] Complementariamente, refiérase a la LEY DEL SISTEMA NACIONAL DE ARCHIVOS, Ley No. 7202 de 24 de octubre de 1990

El sistema de información y comunicación y su importancia institucional

Atendiendo la normativa técnica vigente en Costa Rica para las instituciones del sector público, pueden identificarse varios temas importantes sobre el sistema de información institucional.

Seguidamente presentamos un breve comentario sobre cada acápite.

a) Calidad de la información

La calidad de la información es una variable que afecta directamente la eficiencia, eficacia y economía del impacto de la toma de decisiones institucional. Al respecto, contar con información relevante, procesada efectivamente y en mejora continua, mediante procesos de identificación, captura, proceso (transformación) y comunicación con oportunidad y por medio de los canales correctos, facilitará la toma de decisiones y una efectiva gestión del riesgo institucional. La información debe responder a las necesidades de los usuarios, ser útil y relevante. Además, en virtud del marco de responsabilidad indicado en la LGCI, la administración debe enfatizar la responsabilidad del personal frente sobre el sistema de información de la institución, en cuanto a su papel y contribución personal y de equipo.

b) Estrategia y el sistema de información

El sistema de información debe responder integradamente dentro del marco de control interno institucional. Al respecto, es importante que exista mecanismos que habiliten la participación proactiva de planificación estratégica y las tecnologías de información y comunicación organizacionales de tal forma que se logre alinear e integrar los esfuerzos, optimizar el desempeño de las inversiones en TI y alcanzar las prioridades de largo plazo y operacionales de la institución.

c) Perspectiva de las comunicaciones

En materia de sistema de información, la comunicación interna (i.e. entre unidades o procesos institucionales) y externa (i.e. proveedores, ciudadanos, entes reguladores) debe garantizar, tanto al personal como a la organización, los recursos para realizar una gestión efectiva. Debe existir un sentido de conciencia y entendimiento de los objetivos institucionales y el aporte del sistema de información para su logro. Además, el sistema de información y de comunicación habilita las capacidades para gestionar el riesgo institucional. recursos humanos, el ambiente de control comprende tanto la competencia del personal como las políticas y prácticas de recursos humanos. La tecnología puede resultar en un medio óptimo para potenciar las comunicaciones organizacionales.

d) Herramientas tecnológicas

Las tecnologías de información no son un fin en sí mismas; al contrario, son un medio para optimizar la inversión y potenciar el desempeño institucional. Por tanto, antes de recurrir a la inserción de activos tecnológicos, la entidad debe realizar estudios que sustenten la magnitud y orientación de las inversiones. Además, la inserción de TI debe obedecer a la necesidad de apoyar los procesos institucionales y evitar ser simplemente una respuesta al cambiante entorno informático. Las TI institucionales deben responder a las necesidades estratégicas, en primera instancia, para poder soportar las operaciones regulares de nuestras instituciones.

PREGUNTAS DE REPASO

¿Cuáles son variables que afectan la importancia relativa del sistema de información?

¿Por qué es importante la calidad en el sistema de información?

Marco regulatorio

La *Ley General de Control Interno* (LGCI) y las *Normas de control interno para el sector público* (NCI) contienen las regulaciones fundamentales para el tema de "sistema de información" en cuanto a control interno para el sector público costarricense.

La LGCI incluye en el artículo 16 las referencias sobre el concepto de sistemas de información, incluyendo su propósito, contexto, y los deberes del jerarca y los titulares subordinados con respecto a este componente.

El artículo 16 de la Ley General de Control Interno (LGCI) señala que:

> ***Artículo 16.—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".

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.

Por su parte, las NCI contienen diez normas y siete subnormas sobre el particular, de conformidad con la siguiente estructura:

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

El detalle de estas normas y subnormas se incluye en el anexo de este documento.

Con el fin de de coadyuvar con el marco regulatorio y procurar una mejor aplicación del componente de sistemas de información en el Sector Público, la Contraloría General de la República promulgó las "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.

Estas normas desarrollan las prácticas líderes y criterios de control que deben ser observados como parte de la gestión institucional de las TI. El jerarca y los titulares subordinados, como responsables de esa gestión, deben

establecer, mantener, evaluar y perfeccionar el marco de control de TI de conformidad con lo establecido en la Ley General de Control Interno Nro. 8292. Asimismo, la Función de TI debe contribuir con ello cumpliendo con dicho marco de control y facilitando la labor estratégica del jerarca.

Estas normas de gestión y control de TI son de acatamiento obligatorio para la Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización, y su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable.

PREGUNTAS DE REPASO

Mencione los dos principales deberes del jerarca y los titulares subordinados, respecto del sistema de información.

¿La observancia de las NCI relativas al sistema de información garantiza el cumplimiento de las obligaciones en materia de control interno?

Responsabilidades

El tema de las responsabilidades por el sistema de información en una entidad pública implica que cada participante tenga una responsabilidad distintiva:

La administración activa debe establecer los elementos del sistema de información y promover su fortalecimiento en procura de una base sólida para la operación del sistema como un todo. El jerarca debe convertirse en el líder de este proceso y apoyarse en los titulares subordinados para motivar la planificación, diseño, construcción, operación y mejora continua del sistema de información, de tal forma que se habilite como una herramienta de gestión eficaz. Al respecto, la unidad a cargo de las tecnologías y sistemas de información debe cumplir con su responsabilidad de apoyo estratégico y operativo, así como lo indicado en las **Normas Técnicas para la Gestión y el Control de las Tecnologías de Información.**

Debido a la función asesora y de advertencia de la auditoría interna y las competencias requeridas del auditor interno, éste puede constituirse en un actor proactivo, dinámico y funcional para apoyar los esfuerzos de la administración en

consolidar un sistema de información robusto, eficiente, económico y eficaz. Su aporte puede estar sustentado en la realización de estudios de auditorías y el suministro de asesorías y advertencias sobre el sistema de información institucional. Es importante considerar aquí el límite de actuación del auditor interno, pues su contribución debe evitar incurrir en coadministración, o bien, o otras actividades que pudieran crear limitaciones o compromisos en su independencia y objetividad.

Cada funcionario de la institución, en su condición de servidor público, tiene la responsabilidad de observar regulaciones emitidas por el jerarca para fortalecer el sistema de información, y a contribuir en el mantenimiento de sus elementos, según corresponda.

El cumplimiento de las responsabilidades en materia de sistemas de información requiere que las instituciones consideren otro conjunto normativo emitido por la Contraloría General de la República. Además, es conveniente referirse a prácticas líderes al nivel internacional, con el fin de mantener el nivel de competencia adecuado para el nivel de madurez de su gestión de control interno y sistemas de información.

En materia vinculante, nos referimos a las Normas técnicas para la gestión y el control de las tecnologías de información, incluidas en el documento 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. Este grupo normativo es la práctica líder para el sector público costarricense.

Existe en el mercado de mejores práctica una variedad de modelos que pueden ser fuente de referencias valiosa para habilitar gestión y control en materia de sistemas de información. Conviene a cada institución analizar cuál de esos modelos puede ser una fuente complementaria.

PREGUNTAS DE REPASO

¿Cuál es la responsabilidad del jerarca y los titulares subordinados con respecto al sistema de información?

¿Qué papel corresponde a la auditoría interna en relación con el sistema de información?

¿Cuál es la utilidad de modelos de mejores prácticas en materia de tecnologías y sistemas de información?

Normas relacionadas con las tecnologías de información

Las tecnologías de información (TI) constituyen uno de los principales instrumentos que apoyan la gestión de las organizaciones mediante:

- el manejo de grandes volúmenes de datos necesarios para la toma de decisiones
- y la implementación de soluciones para la prestación de servicios ágiles y de gran alcance.

Su uso ha implicado, al menos, tres situaciones relevantes:

1. la dedicación de porciones importantes del presupuesto de las organizaciones, con el costo de oportunidad que ello conlleva, principalmente en organizaciones con recursos limitados y actividades sustantivas esenciales para la sociedad
2. un marco jurídico cambiante tendente a buscar su paralelismo con las nuevas relaciones que se dan a raíz del uso de esas TI
3. y una presión importante de proveedores y consumidores por la implementación de más y mejores servicios apoyados en estas tecnologías.

Dado el impacto de dichas situaciones, las TI deben gestionarse dentro de un marco de control que procure el logro de los objetivos que se pretende con ellas y que dichos objetivos estén debidamente alineados con la estrategia de la organización.

Con el propósito de coadyuvar con ese marco de control y procurar una mejor gestión de dichas tecnologías por parte de las organizaciones, esta Contraloría General sustituye el "Manual sobre normas técnicas de control interno relativas a los sistemas de información automatizados", mediante la promulgación de las presentes "Normas técnicas para la gestión y el control de las tecnologías de información", que se constituyen en una normativa más ajustada a la realidad y necesidad de nuestro ámbito tecnológico actual.

En razón de que dicha normativa establece criterios de control que deben ser observados como parte de la gestión institucional de las TI, el jerarca y los titulares subordinados, como responsables de esa gestión, deben establecer, mantener, evaluar y perfeccionar ese marco de control de conformidad con lo establecido en la Ley General de Control Interno Nro. 8292. Asimismo, la Función de TI debe contribuir con ello cumpliendo con dicho marco de control y facilitando la labor estratégica del jerarca.

Esta normativa es de acatamiento obligatorio para la Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización, y su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable.

En materia de sistemas de información en instituciones de menor tamaño, las NCI señalan:

> *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.*

PREGUNTAS DE REPASO

¿Para qué sirven las "Normas técnicas para la gestión y el control de las tecnologías de información"?

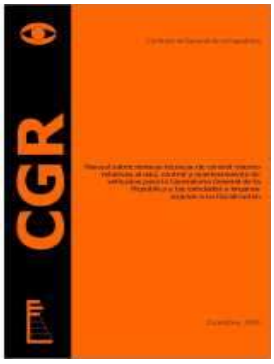
¿Cuáles son tres situaciones relevantes que afectan el uso de las TI en el Sector Público?

¿Qué significa que las normas son "vinculantes"?

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

La estructura definitiva de la normativa se divide en 5 capítulos, de lo cual es importante destacar que el primero contiene un 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.

En términos generales, el capítulo I (**Normas de aplicación general**) señala lo siguiente:

- **Marco estratégico**: 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 los servicios y productos, y establecer lo necesario para lograr esos atributos de manera eficiente.
- **Gestión de Riesgos:** Todo logro está afecto a riesgos, por lo cual 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.

Algunos factores críticos para garantizar un nivel razonable de seguridad son:

- documentar e implantar una política de seguridad de la información, así como los procedimientos respectivos
- asignar recursos para gestionar los niveles de seguridad requeridos por la entidad
- Desarrollar medidas de gestión para temas tales como:

La implementación de un marco de seguridad de la información	La organización debe implementar un marco de seguridad de la información, para lo cual debe: a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la

	identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal. b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización. c. Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.
El compromiso del personal con la seguridad de la información	El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI. Para ello, el jerarca, debe: a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI. b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades. c. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos.
La seguridad física y ambiental	La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos. Como parte de esa protección debe considerar: a. Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas. b. La ubicación física segura de los recursos de TI. c. El ingreso y salida de equipos de la organización. d. El debido control de los servicios de mantenimiento. e. Los controles para el desecho y reutilización de recursos de TI. f. La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas. g. El acceso de terceros. h. Los riesgos asociados con el ambiente.

La seguridad en las operaciones y comunicaciones	La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información. Para ello debe: a. Implementar los mecanismos de control que permitan asegurar la *no negación*, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información. b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios. c. Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus.
El control de acceso	La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe: a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación. b. Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad. c. Definir la propiedad, custodia y responsabilidad sobre los recursos de TI. d. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI. e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de *necesidad de saber* o *menor privilegio*. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones. f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares. i. Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios. j. Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.

	k. Manejar de manera restringida y controlada la información sobre la seguridad de las TI.
La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica	La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información. Para ello debe: a. Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura. b. Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura. c. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción. d. Controlar el acceso a los programas fuente y a los datos de prueba.
La continuidad de los servicios de TI	La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.
Fuente: Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE)	

Además, la entidad debe desarrollar medidas de seguridad relativas a:

- El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.
- El manejo de la documentación.
- La terminación normal de contratos, su rescisión o resolución.
- La salud y seguridad del personal.

La gestión de la seguridad de la información implica que las medidas de protección mantengan una proporción razonable entre el costo de diseñarlas, desarrollarlas, operarlas y darles mantenimiento, y sus riesgos asociados.

- **Gestión de Proyectos:** La gestión de las TI 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 estar basados en propuestas como la del PMI, que resultan muy convenientes.

- **Decisiones sobre asuntos estratégicos de TI:** La toma de decisiones estratégicas en TI y la constitución de los "comités de informática" se han convertido más en un problema que en el beneficio que se quiere lograr. Las decisiones deben sustentarse en 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 sí 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 consensuadas.

    - **Cumplimiento de obligaciones relacionadas con la gestión de TI:** Esto es ***legalidad*****.** El **cumplimiento de las obligaciones** implica conocer todo el marco jurídico que le afecta a la gestión de TI y procurar su debido cumplimiento.

Por su parte, el Capítulo II (**Planificación y organización**), considera los siguientes asuntos:

- **Planificación de las tecnologías de información:** 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.
- **Modelo de arquitectura de información:** Debe considerarse el modelo de arquitectura de información como la esquematización del conocimiento completo de los sistemas

institucionales y del flujo de la información de la entidad por dichos sistemas.

- **Infraestructura tecnológica:** 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.
- **Independencia y recurso humano de la Función de TI:** Para que sea posible la gestión de TI es necesario contar con un equipo de trabajo motivado y con las competencias necesarias, y que goce de la independencia orgánica necesaria para lograr un apoyo uniforme y equilibrado en toda la organización.
- **Administración de recursos financieros:** 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.

El capítulo III (**Implementación de tecnologías de información**) abarca lo siguiente:

- **Consideraciones generales de la implementación de TI:** 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.
- **Implementación de software e infraestructura tecnológica:** 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, y se evalúa su desempeño posteriormente.

- **Contratación de terceros para la implementación y mantenimiento de software e infraestructura:** 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.

El Capítulo IV (**Prestación de servicios y mantenimiento**) manifiesta:

- **Definición y administración de acuerdos de servicio:** 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.
- **Administración y operación de la plataforma tecnológica:** 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.
- **Administración de los datos:** 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.

- **Atención de requerimientos de los usuarios de TI:** Los usuarios de TI demandarán una serie de atenciones que deben ser tramitadas en forma ágil para evitar demoras en la gestión de esos actividades.
- **Manejo de incidentes:** 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.
- **Administración de servicios prestados por terceros:** 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.

Finalmente, el capítulo V (**Seguimiento**) establece las pautas para realimentar el proceso de gestión y control de TI, a saber:

- **Seguimiento de los procesos de TI:** 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.
- **Seguimiento y evaluación del control interno en TI:** Es responsabilidad del jerarca establecer y mantener el sistema de control interno relacionado con la gestión de las tecnologías de información.
- **Participación de la Auditoría Interna:** La Auditoría Interna debe coadyuvar a que el control interno en TI brinde una garantía razonable del cumplimiento de los objetivos de la entidad.

Implementación de las normas

Las instituciones deben atender los requerimientos de implantación de este marco normativo, según los siguientes lineamientos:

"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".

Vigencia de las normas: a partir del 31 de julio del 2007.

Al respecto, 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. Hay que recordar que las entidades cuentan con dos años para poner en práctica lo dispuesto en las normas. También, contar con

apoyo interinstitucional para facilitar este proceso es un factor de éxito, 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.

PREGUNTAS DE REPASO

¿Cuál es el capítulo más importante de las Normas sobre TI?

¿Cuál es el motivo por el cual todas las normas se derivan del marco de normas de aplicación general?

¿Por qué hay un capítulo dedicado exclusivamente a la seguridad de la información?

¿Cuál es la importancia de contar con un grupo de normas dedicadas al seguimiento y vigilancia del control interno y procesos de TI?

Describa el papel de la auditoría interna en el seguimiento de TI.

¿Cuándo deberían estar listos los procesos de implantación de las Normas N-2-2007-CO-DFOE?

¿Cuál es el estado actual en su institución?

Anexo

Regulaciones sobre sistemas de información incluidas en el capítulo V de las "Normas de control interno para el sector público" [3]

5.1 Sistemas de información

El jerarca y los titulares subordinados, según sus competencias, deben disponer los elementos y condiciones necesarias para que de manera organizada, uniforme, consistente y oportuna se ejecuten las actividades de obtener, procesar, generar y comunicar, en forma eficaz, eficiente y económica, y con apego al bloque de legalidad, la información de la gestión institucional y otra de interés para la consecución de los objetivos institucionales. El conjunto de esos elementos y condiciones con las características y fines indicados, se denomina sistema de información, los cuales pueden instaurarse en forma manual, automatizada, o ambas.

5.2 Flexibilidad de los sistemas de información

Los sistemas de información deben ser lo suficientemente flexibles, de modo que sean susceptibles de modificaciones que permitan dar respuesta oportuna a necesidades cambiantes de la institución.

5.3 Armonización de los sistemas de información con los objetivos

La organización y el funcionamiento de los sistemas de información deben estar integrados a nivel organizacional y ser coherentes con los objetivos institucionales y, en consecuencia, con los objetivos del SCI. La adecuación de tales sistemas a los objetivos institucionales involucra, entre otros, su desarrollo de conformidad con el plan estratégico institucional, y con el marco estratégico de las tecnologías de información, cuando se haga uso de

[3] Este Capítulo de las Normas de control Interno para el Sector Público incorpora lo establecido en el artículo 16 de la LGCI.

estas para su funcionamiento.

5.4 Gestión documental

El jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información propicien una debida gestión documental institucional, mediante la que se ejerza control, se almacene y se recupere la información en la organización, de manera oportuna y eficiente, y de conformidad con las necesidades institucionales.

5.5 Archivo institucional

El jerarca y los titulares subordinados, según sus competencias, deben implantar, comunicar, vigilar la aplicación y perfeccionar políticas y procedimientos de archivo apropiados para la preservación de los documentos e información que la institución deba conservar en virtud de su utilidad o por requerimiento técnico o jurídico. En todo caso, deben aplicarse las regulaciones de acatamiento obligatorio atinentes al Sistema Nacional de Archivos.

Lo anterior incluye lo relativo a las políticas y procedimientos para la creación, organización, utilización, disponibilidad, acceso, confidencialidad, autenticidad, migración, respaldo periódico y conservación de los documentos en soporte electrónico, así como otras condiciones pertinentes.

5.6 Calidad de la información

El jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información contemplen los procesos requeridos para recopilar, procesar y generar información que responda a las necesidades de los distintos usuarios. Dichos procesos deben estar basados en un enfoque de efectividad y de mejoramiento continuo.

Los atributos fundamentales de la calidad de la información están referidos a la confiabilidad, oportunidad y utilidad.

5.6.1 Confiabilidad

La información debe poseer las cualidades necesarias que la acrediten como confiable, de modo que se encuentre libre de errores, defectos, omisiones y modificaciones no autorizadas, y sea emitida por la instancia competente.

5.6.2 Oportunidad

Las actividades de recopilar, procesar y generar información, deben realizarse y darse en tiempo a propósito y en el momento adecuado, de acuerdo con los fines institucionales.

5.6.3 Utilidad

La información debe poseer características que la hagan útil para los distintos usuarios, en términos de pertinencia, relevancia, suficiencia y presentación adecuada, de conformidad con las necesidades específicas de cada destinatario.

5.7 Calidad de la comunicación

El jerarca y los titulares subordinados, según sus competencias, deben establecer los procesos necesarios para asegurar razonablemente que la comunicación de la información se da a las instancias pertinentes y en el tiempo propicio, de acuerdo con las necesidades de los usuarios, según los asuntos que se encuentran y son necesarios en su esfera de acción. Dichos procesos deben estar basados en un enfoque de efectividad y mejoramiento continuo.

5.7.1 Canales y medios de comunicación

Deben establecerse y funcionar adecuados canales y medios de comunicación, que permitan trasladar la información de manera transparente, ágil, segura, correcta y oportuna, a los destinatarios idóneos dentro y fuera de la institución.

5.7.2 Destinatarios

La información debe comunicarse a las instancias competentes, dentro y fuera de la institución, para actuar con base en ella en el logro de los objetivos institucionales.

5.7.3 Oportunidad

La información debe comunicarse al destinatario con la prontitud adecuada y en el momento en que se requiere, para el cumplimiento de sus responsabilidades.

5.7.4 Seguridad

Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran.

5.8 Control de sistemas de información

El jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter.

5.9 Tecnologías de información

El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance. Para ello deben observar la normativa relacionada con las tecnologías de información, emitida por la CGR.[4] En todo caso, deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información.

[4] Refiérase al Anexo #2, punto 4 del las Normas de control Interno para el Sector Público.

5.10 Sistemas de información en 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.

Créditos

Segunda Edición © 2011

Lección 3 – Tema 5: Sistema de Información

Componente 4

Curso Virtual "Control Interno"

En la elaboración de este objeto de aprendizaje participaron los siguientes funcionarios de la Contraloría General de la República:

José Roberto Alpízar Fallas,
Grace Madrigal Castro,
Jorge Suárez Esquivel

Expertos de contenidos

División de Fiscalización Operativa y Evaluativa