Contraloría General de la República

Guía IV
Información y Comunicación

Pauta n.° IV-001
Diagnóstico del componente información y comunicación

CONTENIDO

SIGLAS Y ACRÓNIMOS

CA	Controles de aplicación
CG	Controles generales
CGR	Contraloría General de la República
COBIT	Objetivos de control para tecnología de información
DDN	Dirección de Desarrollo Normativo
INTOSAI	Organización Internacional de Instituciones Superiores de Auditoría Gubernamental
ISACA	Asociación de Auditoría y Control de Sistemas de la Información (del inglés Information Systems Audit and Control Association)
ITGI	Instituto para el Gobierno de Tecnología
IyC	Información y comunicación
MAE	Máxima autoridad ejecutiva
MH	Ministerio de Hacienda
NOBACI	Normas básicas de control interno
SCI	Sistema de control interno
SIGEF	Sistema Integrado de Información Financiera
TI	Tecnología de información

INFORMACIÓN Y COMUNICACIÓN

I. INTRODUCCIÓN

1.1 De conformidad con lo previsto en el artículo 7 de la Ley 10-07 sobre *Atribuciones y deberes institucionales*, las entidades y organismos bajo el ámbito de esta ley, así como los servidores públicos en todos los niveles, tienen entre otras las siguientes atribuciones y deberes para asegurar la efectividad del control interno institucional:

a. Establecer y mantener el control interno en los términos previstos en la ley.

b. Elaborar, en el marco de la ley y de la normativa básica de control interno que emita la Contraloría General de la República (CGR), las normas secundarias, sistemas y procedimientos para el establecimiento, operación y mantenimiento de su propio proceso de control interno, de acuerdo con la naturaleza de sus operaciones y objetivos.

1.2 La CGR está interesada en apoyar a las instituciones públicas en el proceso de ajuste de sus SCI (sistema de control interno) a lo previsto en el marco legal de control interno. En cumplimiento de sus atribuciones establecidas en los artículos 5 de la Ley 10-07 y 13 de su reglamento, Decreto n° 491-07, con el objeto de apoyar los diagnósticos de necesidades y las soluciones de ajuste, la CGR emite la presente guía especializada sobre la NOBACI IV - «***Información***[1] ***y comunicación***[2]***»,*** mencionado en el artículo 24 de la citada ley.

1.3 Las guías no obligan a las instituciones públicas. Su objetivo es orientarlas para que el proceso de ajuste sea efectivo, de conformidad con lo requerido en la Ley 10–07 y su reglamento. Cada entidad tiene sus particularidades y la forma cómo logre establecer los elementos de la **IyC** tiene íntima relación con estas.

[1] Información debe entenderse como el conjunto de datos organizados (procesados), para cumplir determinados objetivos. Ejemplo, servir de apoyo a otros procesos, reportar un resultado, solicitar determinadas acciones, etc. La información está relacionada con la forma de organizar los datos que se quiere comunicar.

[2] La comunicación debe entenderse como la acción de trasmitir información, de tal forma que contribuya a lograr los objetivos. La comunicación representa el intercambio de información. Está relacionada con la forma en que se trasmite el mensaje a un posible o posibles interesados en la información.

1.4 Este documento se ocupa de desarrollar aspectos considerados básicos sobre cada uno de los elementos que contribuyen a la **información y la comunicación,** enumerados en el artículo 47 numeral 4, del reglamento de la Ley 10–07. En los casos en que se considere necesario por la complejidad o novedad de algún elemento, la guía se acompaña de pautas que en forma focalizada también contribuyen a una mejor interpretación e implantación del elemento que se detalla.

II. MARCO LEGAL DE LA INFORMACIÓN Y LA COMUNICACIÓN

2.1 Las NOBACI (Normas básicas de control interno) fueron actualizadas mediante la Resolución 001/11. Dichas normas, en el artículo 24 de la Ley 10-07 y en el 47 de su reglamento se denominaban «componentes

2.2 La NOBACI IV - «**información y comunicación»** requiere que:

> La información deberá ser preparada y comunicada a la máxima autoridad, a los empleados y a terceros, cuando corresponda, de tal forma que les apoye en el cumplimiento de sus responsabilidades y contribuya a la rendición transparente de cuentas.

Los principales elementos que se consideran en esta norma son:

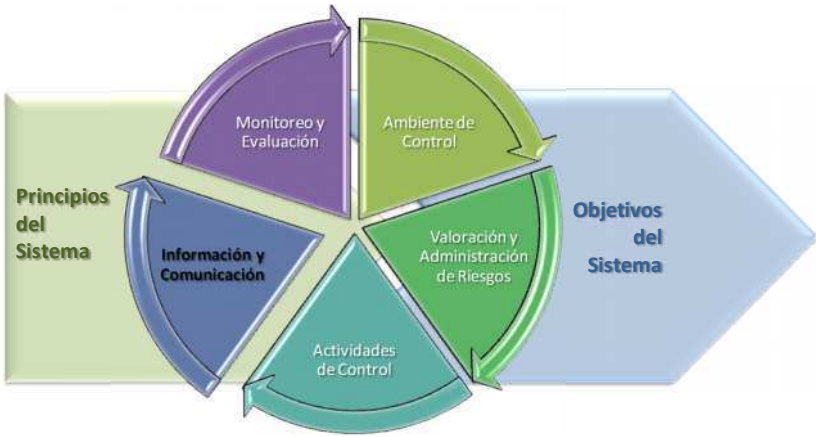
a. Calidad y suficiencia de la información;
b. Sistema integrado de información (financiera y de gestión);
c. Controles de acceso, aplicación y otros de los sistemas integrados;
d. Canales de comunicación interna y externa;
e. *Archivo institucional».*

2.3 De acuerdo con esta definición, es necesario que cada entidad efectúe una cuidadosa revisión para establecer cuál es el estado de los elementos enumerados. A tales efectos la CGR emitió la *Guía para el diagnóstico del SCI*, la cual permite valorar el grado de desarrollo y las necesidades de ajuste de cada NOBACI. En la Pauta IV-001, se incluye la matriz para diagnosticar el estado de la NOBACI IV - «información y comunicación**»**. El resultado del diagnóstico integral de las NOBACI mediante la guía mencionada, permitirá

preparar un plan de acción que debidamente concertado con la MAE (máxima autoridad ejecutiva) de cada entidad, apoyará el cumplimiento de lo previsto en el marco legal vigente para el control interno y, por consiguiente, mejorará la calidad y seguridad de la gestión.

2.4 Al definir las políticas, procedimientos, técnicas y herramientas más apropiadas para la gestión de esta norma, deben considerarse las necesidades específicas de cada entidad en términos de volumen, complejidad y seguridad. Por ello, las consideraciones de control que se presentan en esta guía son puntos de aplicación general y no resultan absolutos.

GRÁFICO N° 1
MODELO DEL SISTEMA DE CONTROL INTERNO



2.5 En el gráfico n° 1 se muestra el modelo del SCI basado en las cinco normas. Se debe entender como un sistema que opera en un engranaje según el cual los principios son el combustible impulsor. Cada norma va activando la otra. La **IyC** son las políticas y procedimientos que contribuyen a revelar los hechos que tienen lugar en una entidad, a trasmitir los datos necesarios para que fluyan las operaciones, y a comunicar los resultados intermedios y finales. La información y la comunicación tienen lugar a través de la organización, a todos los niveles y en todas las funciones. Trascienden la organización cuando dan a conocer a otras instituciones del gobierno y a terceros interesados, el quehacer de una entidad y, por supuesto, en qué estado se encuentran y cómo han sido manejados los recursos de los que esta es responsable. Igualmente, la información y la forma en que esta se comunica son activadores de decisiones que benefician o afectan las entidades.

2.6 La transparencia es el principal requisito para que esta norma cumpla sus objetivos. Sin una información y comunicación apropiadas, no se puede avanzar en las operaciones ni rendir cuenta sobre la entidad. Igualmente, debilidades en la seguridad de la información exponen a graves riesgos de pérdidas reales, imagen y costos elevados de reprocesamiento en caso de daños.

2.7 Para construir la NOBACI IV - «información y comunicación», la Ley 10-07 ha previsto un conjunto de elementos considerados pilares en las mejores prácticas gerenciales de la actualidad. Estos elementos se esquematizan en la tabla n° 1. Básicamente, se representa la NOBACI IV - **IyC** como un sistema con los requerimientos previstos en la ley y su reglamento, seguido de los medios que recomienda la guía para cumplir tales requerimientos y luego, en forma sistémica, se ilustran los resultados o beneficios que se obtienen cuando una entidad desarrolla dichos elementos. Los elementos se explican con mayor detalle en el capítulo III de la guía.

TABLA N° 1
REQUERIMIENTOS, MEDIOS Y RESULTADOS DE INFORMACIÓN Y COMUNICACIÓN

REQUERIMIENTO	MEDIO FACILITADOR	RESULTADO
A. CALIDAD Y SUFICIENCIA DE LA INFORMACIÓN	Para generar información con calidad y suficiencia se debe disponer de políticas, planes de información y comunicación, procedimientos, responsabilidades (gobierno de la información) y medios, preferiblemente basados en tecnología.	▪ Decisiones correctas y oportunas (internas y externas) basadas en la confiabilidad de la información. ▪ Imagen de solidez y transparencia. ▪ Comunicación fluida interna y externamente.
B. SISTEMA INTEGRADO DE INFORMACIÓN (FINANCIERA O DE GESTIÓN)	1. Este elemento es complementario de la calidad y suficiencia. Puede decirse que es uno de los medios más importantes para lograr los objetivos de información y comunicación. 2. Un sistema integrado favorece la confiabilidad cuando centraliza la información en bases de datos, manteniéndola segura y libre de inconsistencias. La integración requiere que cualquier operación que influya o sea influida por otra, cumpla ciertas condiciones para asegurar que, simultáneamente, afecta distintos módulos o componentes integrados sin tener que recurrir a dobles o múltiples procesos, exponiendo a error o inconsistencias.	▪ En general, se emiten informes precisos, actualizados y oportunos. ▪ Cumplimiento de obligaciones legales sobre la rendición de cuentas. ▪ Mayor seguridad de la información. ▪ Facilidad para practicar auditorías, seguimiento o monitoreo de la gestión.

REQUERIMIENTO	MEDIO FACILITADOR	RESULTADO
C. CONTROLES EN LOS SISTEMAS DE INFORMACIÓN BASADOS EN TECNOLOGÍA	1. Este elemento se refiere a las condiciones específicas de la administración de la información, especialmente en ambientes basados en tecnología. 2. De conformidad con este elemento, deben establecerse reglas claras para definir el gobierno de la TI3 (tecnología de información), lo cual incluye la estrategia de inversión en tecnología y los controles que deben diseñarse para gestionar los riesgos cambiantes, tanto en el entorno de la administración de la tecnología como en el funcionamiento propiamente dicho de las aplicaciones. 3. Los medios más frecuentes son: ▪ Plan estratégico de tecnología; ▪ Planes operativos de TI; ▪ Definición de objetivos y mecanismos de control a nivel general; ▪ Definición de objetivos y mecanismos de control a nivel de aplicación.	▪ Confiabilidad y seguridad de la información. ▪ Buen gobierno de la información, fácil asignación de responsabilidad y control posterior. ▪ Agilidad en la respuesta de los sistemas de información.
D. CANALES DE COMUNICACIÓN INTERNA Y EXTERNA	1. La comunicación interna es imprescindible para la comprensión y el seguimiento de las políticas, normas, procedimientos y controles internos incorporados por el personal de una entidad.	▪ Mayor sentido de pertenencia y compromiso del personal. ▪ Mayor calidad de las operaciones; disminuyen las tasas de error.

[3] TI se utiliza en este documento para abreviar el término tecnología de información, pero también para identificar a la unidad organizacional que tiene las funciones de administrar la tecnología de información. En algunos casos se denomina Departamento o Dirección de Sistemas.

REQUERIMIENTO	MEDIO FACILITADOR	RESULTADO
…D. CANALES DE COMUNICACIÓN INTERNA Y EXTERNA	2. La comunicación externa es clave para mantener actualizada la organización sobre lo que ocurre en su entorno y para trasmitir a terceros los mensajes requeridos por sus normas y aquellos facultativos que se consideren necesarios para mantener excelentes relaciones con el entorno. 3. Los medios más idóneos son: ▪ Gobierno de la comunicación; ▪ Planes de comunicación; ▪ Seguimiento a la calidad de la comunicación y mejoramiento continuo.	▪ Informes confiables y oportunos dirigidos a los destinatarios apropiados. ▪ Captación oportuna de la satisfacción de los clientes internos y externos. La entidad consigue saber qué se piensa y espera de ella. ▪ Aumenta la eficiencia operacional y la eficacia del control interno.
E. ARCHIVO INSTITUCIONAL	1. El archivo de una institución constituye su memoria histórica y debe estar regido por las normas que le sean aplicables. Una entidad sin apego a las normas y a las mejores prácticas de conservación se expone a sí misma y a terceros a serios perjuicios. 2. Son medios idóneos para la gestión de archivos como parte del control interno: ▪ La asignación de responsabilidad en la preparación, actualización y conservación del archivo; ▪ Los reglamentos para el acceso, modificación y disposición (eliminación) de la información archivada;	▪ Agilidad en la ubicación de la información. ▪ Seguridad de la información. ▪ Cumplimiento de normas legales sobre custodia y conservación de documentos. ▪

REQUERIMIENTO	MEDIO FACILITADOR	RESULTADO
… E. ARCHIVO INSTITUCIONAL	▪ La planificación y ordenamiento del archivo (copias impresas y medios magnéticos); ▪ Los planes de contingencia (recuperación y continuidad de procesos).	▪ Prevención de litigios o resolución favorable de litigios.

III. DESARROLLO DE LOS ELEMENTOS DE LA INFORMACIÓN Y COMUNICACIÓN

A. CALIDAD Y SUFICIENCIA DE LA INFORMACIÓN

3.1 El objetivo de la guía respecto a este elemento es ofrecer lineamientos que ayuden a las entidades a establecer medios para mejorar la calidad y suficiencia de la información.

3.2 La información tiene calidad cuando se refiere a datos reales (o se aclara que son estimaciones), sustentados y sustentables, libres de errores, irregularidad o inconsistencias y emitidos con la oportunidad debida.

3.3 La información tiene calidad y es suficiente cuando es:

a. Apropiada (está toda la información necesaria, sirve a un propósito relevante);
b. Oportuna (está ahí cuando se la necesita);
c. Actualizada (se tiene lo producido más recientemente);
d. Exacta y significativa (es real y entendible);
e. Objetiva y verificable (no está sesgada, se puede comprobar);
f. Accesible (puede ser obtenida fácilmente por las partes relevantes);
g. Consistente y uniforme (cuando aplique puede ser comparable).

3.4 La información es suficiente cuando los datos y su orden se consideran apropiados para generar un cambio en el conocimiento de quien los recibe y se producen las decisiones esperadas al planificar dicha información.

3.5 Para preservar la calidad y suficiencia de la comunicación, se sugiere tener en consideración una serie de reglas básicas.

REGLA N° 1. LA INFORMACIÓN Y LA COMUNICACIÓN DEBEN SER GOBERNADAS Y PLANIFICADAS

Es denominador común en muchas entidades públicas la proliferación de información y la indisciplina en las comunicaciones. Esto se puede superar si la IyC es planificada y se asigna la responsabilidad de su administración y supervisión.

3.6 Para mantener un nivel de control apropiado, es vital asignar la responsabilidad de asesorar la estrategia y las políticas de información y comunicación a una unidad competente, así como la de diseñar y apoyar su implementación.

3.7 Todo lo que se obtenga con los demás controles podría ser inocuo si no se refleja en la información procesada o entregada dentro y fuera de la organización. Un débil sistema de información o un pobre sistema de comunicación pueden provocar cadenas de error o contingencias. El plan de informes y la estrategia de comunicación son medios imprescindibles para desarrollar esta NOBACI. Es posible que no obstante contarse con unidades de comunicación, organización y métodos o planificación encargadas de aspectos generales de la información y la comunicación, el gobierno se comparta con la unidad responsable de la TI, en los aspectos puntuales y técnicos de seguridad, mantenimiento y desarrollo de herramientas informáticas de apoyo, por lo que debe mantenerse una coordinación activa entre estas áreas.

3.8 Para empezar, en la planeación debe quedar claro que se obtiene y genera información con fines internos y externos. Es decir, datos obtenidos o preparados por una organización para apoyar el flujo de operaciones en los procesos para obtener resultados, y datos que son consolidados u ordenados de una manera tal que sirven de medio para rendir cuenta u obtener alguna reacción de terceras partes.

3.9 De acuerdo con lo anterior, se recomienda que al momento de diseñar, actualizar o ajustar los sistemas de administración y control, con base en las guías de control interno de la CGR y otros parámetros, sin pretender agotar el tema, se preparen matrices como la que se ilustra en la tabla n° 2 para identificar las necesidades de información. Cuando se dispone de una unidad de organización y métodos o equivalente, este es un proceso paralelo al diseño o actualización organizacional.

TABLA N° 2
PLAN DE INFORMACIÓN Y COMUNICACIÓN

INFORMES A EMITIR	CARACTERÍSTICAS DEL INFORME	RESPONSABLE DE PREPARACIÓN	FECHAS (PERIODICIDAD)	DESTINATARIO (A QUIÉN SE COMUNICA)	UTILIZACIÓN	SEGURIDADES Y ARCHIVO
ESTADO DE LA CARTERA	Se genera en el módulo de cartera del sistema de información. Relación de deudores por servicios públicos, clasificados por localidad geográfica, orden alfabético, fecha de vencimiento de la obligación, días vencidos y monto de la obligación	Director de cartera	Cinco días después de cada cierre mensual	Director financiero y MAE	De acuerdo con la escala de atribuciones y con base en el informe, el director financiero toma decisiones o propone medidas de cobranza a la MAE.	Debe emitirse en dos copias, que reposarán en el archivo de la dirección de cartera y de la dirección financiera La seguridad se cataloga como vital.

REGLA N° 2. LA INFORMACIÓN DEBE CLASIFICARSE DE ACUERDO CON SU IMPORTANCIA Y NECESIDAD DE SEGURIDAD

La información, los informes resultantes y los destinatarios tienen implicaciones que deben tomarse en cuenta para la generación, divulgación y conservación de la información. Así podemos tener información vital, confidencial, de circulación cerrada, de circulación pública, operativa, etc.

3.10 En la tabla n° 3 se ilustra la clasificación de la información de acuerdo con sus características.

TABLA N° 3
CARACTERÍSTICAS DE LA INFORMACIÓN Y COMUNICACIÓN

TIPO DE INFORMACIÓN	CLASIFICACIÓN	RAZONES	SEGURIDADES
BASE DE DATOS SOBRE DEUDORES DEL SISTEMA DE IMPUESTOS	Vital	Un daño o pérdida de esta información dejaría sin base el cobro de los impuestos que adeudan los contribuyentes y se desplomarían los ingresos tributarios.	Solo tienen protocolo de acceso y modificación de la base de datos: ▪ La MAE; ▪ El director de cartera de la Dirección de Impuestos; ▪ El director de sistema. Solo podrán tener acceso conjunto dos de las tres personas citadas. Los demás funcionarios solo podrán tener acceso para consultas o modificaciones operativas.
RESULTADOS DE LOS DIAGNÓSTICOS MÉDICOS PRACTICADOS POR EL HOSPITAL	Confidencial	La información sobre los pacientes es protegida por el código médico y las normas vigentes. No debe ser vista por cualquier persona, no se exhibe públicamente. Exponer esta información a partes indebidas puede perjudicar a personas y originar demandas al hospital.	Solo tienen protocolo de acceso a las historias clínicas: ▪ El director del hospital; ▪ El médico; ▪ La enfermera que asiste al médico.
INDICADORES DE GESTIÓN	Privilegiada	La MAE y otras autoridades utilizan datos organizados de manera convencional para interpretar la evolución de la gestión y otros fenómenos que si fueran divulgados a todos los empleados y al público en general, podrían ser interpretados equivocadamente. Es decir, se requiere disponer de más información para formarse un juicio correcto.	Los indicadores son producidos de conformidad con estándares bajo custodia del director de planificación y gestión y solo pueden ser modificados con la autorización formal de la MAE.

TIPO DE INFORMACIÓN	CLASIFICACIÓN	RAZONES	SEGURIDADES
ESTADÍSTICAS PÚBLICAS	De divulgación abierta	Forman parte de informes de rendición de cuentas y deben ser del dominio público, lo que requiere que la formulación y preparación sean hechas cuidadosamente para asegurar la confiabilidad y transparencia.	Debe asignarse la responsabilidad de la formulación, preparación automatizada, revisión de la calidad y autorización previa de la MAE antes de la emisión pública.

3.11 Estas clasificaciones ayudan a decidir qué tipo de controles se deben adoptar para preservar la información y prevenir interpretaciones o decisiones equivocadas con base en dicha información. No debe confundirse la información pública que se suministra de conformidad con las normas vigentes, con la información que se clasifica por su naturaleza, destinatarios, utilización, etc., lo cual se hace para proporcionar seguridad en su manejo, custodia y archivo.

REGLA N° 3. LA INFORMACIÓN DEBE SOMETERSE A VERIFICACIÓN O VALIDACIÓN Y CONTROL DE CALIDAD

En forma separada o como parte de los arreglos que se hagan conforme las dos reglas anteriores, todas las entidades públicas deben advertir a sus empleados de la responsabilidad que asumen por la preparación, cuidado en la utilización y custodia de la información. Por lo general, esto viene en las políticas de ética e integridad (ver Guía I). Adicionalmente, debe asignarse la responsabilidad de verificar la corrección de la información; esto generalmente lo hace el personal que participa en las diferentes partes de un proceso o personas que reciben el encargo puntual de hacerlo, como supervisores.

3.12 En casos específicos de informes de divulgación pública, se extreman los requerimientos de verificación, especialmente dirigidos a prevenir malas interpretaciones por errores o inconsistencias en las cifras que se suministran. Igualmente, en otro tipo de comunicaciones menos cuantitativas, se realizan revisiones a cargo de personas diferentes a quienes elaboran los informes o comunicaciones, para establecer que de conformidad con la cultura corporativa se han seguido pautas de buena redacción, tono, utilización de tiempos verbales, etc., según las necesidades.

B. SISTEMA INTEGRADO DE INFORMACIÓN (FINANCIERA O DE GESTIÓN)

3.13 Un sistema de administración financiera integrado asegura que al momento de solicitarse la ejecución del presupuesto, una base de datos tenga el presupuesto aprobado y, de conformidad con requisitos establecidos, permita el procesamiento de una transacción de compra de bienes y servicios.

3.14 Asimismo, una vez se solicite el pago mediante un módulo o sistema de tesorería conectado al de presupuesto y al de contabilidad, debe autorizarse solo si pasó por fases previas del presupuesto y contabilidad y, a su vez, permitir que se registre apropiadamente tanto la ejecución presupuestal como patrimonial originada en dicho pago. Igualmente, el sistema permite preparar los informes sobre las transacciones realizadas, cerrando el ciclo desde que una operación se origina hasta que se rinde cuenta sobre ella.

3.15 Podría decirse que los sistemas integrados, con excepciones, favorecen la unidad de contenido de toda la información que se procesa en una entidad, de acuerdo con los conceptos afectados.

3.16 Igual pasa con los sistemas de gestión operativa, los cuales son influidos por el tipo de operaciones que se quiere gestionar. Por ejemplo, la emisión de documentos de identidad debe responder a una base de datos debidamente actualizada que solo permite emitir un nuevo documento cuando se verifica en otros módulos la información de respaldo de la solicitud (origen, huellas digitales, antecedentes penales, etc.).

3.17 En la práctica, la República Dominicana dispone del SIGEF (Sistema Integrado de Gestión Financiera), llamado a servir de medio para procesar en forma centralizada las transacciones comunes que se nutren o utilizan el presupuesto del Gobierno Central y los fondos de la Cuenta Única del Tesoro (esta última, a la fecha en proceso de estructuración).

3.18 De acuerdo con lo anterior, excepto para operaciones específicas de cada entidad, puede decirse que en los asuntos de administración financiera ya se dispone del medio apropiado para parte de la información y comunicación.

3.19 Se recomienda establecer si realmente son necesarios módulos separados de administración financiera –que estén utilizando algunas entidades— cuando mediante terminales conectadas en forma remota por el organismo rector, Ministerio de Hacienda (MH), se pueden ahorrar costos de equipos, programas (software) y tiempos de reproceso, si no hay comunicación de tales módulos con el SIGEF.

3.20 Por otra parte, en cuanto los recursos disponibles lo permitan, se recomienda diseñar e implementar sistemas integrados para las operaciones a la medida de cada entidad, los cuales pueden o no conversar con el SIGEF. Por ejemplo, sistemas integrados para el manejo de la gestión hospitalaria y el costo médico pueden no tener manera de interactuar con el SIGEF, pero sí sirven a los hospitales para mejorar la calidad de su control interno.

C. CONTROLES EN LOS SISTEMAS DE INFORMACIÓN BASADOS EN TECNOLOGÍA[4]

3.21 El sistema de control interno impacta en aspectos de TI a tres niveles:

a. Dirección ejecutiva

3.22 Al nivel de dirección ejecutiva se fijan los objetivos de negocio, se establecen políticas y se toman decisiones de cómo aplicar y administrar los recursos para ejecutar la estrategia de la entidad. El enfoque genérico hacia el gobierno y el control es establecido por la MAE y se comunica a toda la organización. El ambiente de control de TI es guiado por este conjunto de objetivos y políticas de alto nivel.

3.23 Estas consideraciones se desarrollan ampliamente en los planes estratégicos de tecnología de información y en los programas operativos anuales específicos del área, los cuales son generalmente apoyados por una unidad organizacional denominada Departamento o Dirección de Sistemas o equivalente.

b. Procesos

3.24 Al nivel de cada proceso (administrativo, financiero u operaciones según el objeto social), se aplican controles para actividades específicas de la entidad. La mayoría de los procesos están automatizados e integrados con los sistemas aplicativos de TI, dando como resultado que muchos de los controles a este nivel estén automatizados. Estos se conocen como CA (controles de aplicación).

[4] Las declaraciones de control que siguen fueron tomadas de COBIT 4.1. Disponible, entre otros sitios web, en http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf

3.25 Sin embargo, algunos controles permanecen como procedimientos manuales, tales como la autorización de transacciones, la separación de funciones y las conciliaciones manuales. Los controles a nivel de procesos son, por lo tanto, una combinación de controles manuales y automatizados. En todo caso, la mayor parte de las actividades de control, sean manuales o automatizadas, nacen de la identificación y valoración de los riesgos.

c. Tecnología de información

3.26 Para soportar los procesos, TI proporciona servicios, por lo general de forma compartida por varios procesos, así como procesos operativos y de desarrollo de TI que se proveen a toda la entidad. Mucha de la infraestructura de TI proporciona un servicio común (es decir, redes, bases de datos, sistemas operativos y almacenamiento).

3.27 Los controles aplicados a todas las actividades de servicio de TI se conocen como CG (controles generales) de TI. La operación formal de estos CG es necesaria para dar confiabilidad a los CA. Por ejemplo, una deficiente administración de cambios podría poner en riesgo (por accidente o de forma deliberada) la confiabilidad de los chequeos automáticos de la integridad de la información.

1. CONTROLES GENERALES

3.28 Los controles generales son aquellos que están inmersos en los procesos y servicios de TI. Algunos ejemplos son:

a. Desarrollo de sistemas;
b. Administración de cambios;
c. Seguridad;
d. Operaciones de cómputo.

3.29 Los CG incluyen generalmente: (a) controles de las operaciones del centro de datos, (b) controles de la adquisición, desarrollo y mantenimiento de las aplicaciones del sistema y, (c) controles de acceso. Esos controles aplican a todos los sistemas, computadoras y ambientes de computación tanto en el centro matriz de procesamiento y administración de servidores como del usuario final.

a. Controles a las operaciones del centro de datos

3.30 Incluyen trabajos de implementación y rutina, funciones del operador, copias de seguridad y procedimientos de recuperación, así como la planificación para casos de contingencias o recuperación por desastres. Estos controles, si se implementan correctamente, ayudan a manejar la capacidad de planeación, asignación y consumo de recursos de la entidad.

b. Controles a la adquisición, desarrollo y mantenimiento de aplicaciones del sistema

3.31 Corresponden a la adquisición, desarrollo y mantenimiento efectivo de las aplicaciones del sistema, el sistema operativo, los sistemas de administración de bases de datos, el programa (software) de seguridad y las utilidades del sistema.

3.32 Estos controles incluyen la estructura para el proceso de ejecución del plan de tecnología, respecto a la compra o desarrollo de aplicaciones. Consideran, por ejemplo, términos de referencia, especificaciones técnicas de necesidades, análisis de propuestas, soporte de las decisiones de adquisición o desarrollo, autorización y aprobación de contratos o diseños, etc. Así mismo, durante la etapa de desarrollo o al recibir los aplicativos, se establecen los requisitos de verificación, pruebas y validaciones y las jerarquías de intervención para aceptar los productos recibidos o desarrollados y la documentación de respaldo como evidencia del debido cuidado ejercido en las verificaciones.

3.33 Para el mantenimiento se establecen como controles los protocolos para mantenimiento preventivo y correctivo de las aplicaciones. Esto implica, en caso de adquisiciones, verificación previa de la inclusión en los contratos de cláusulas que aseguren la continuidad de la operación, sin perjuicio de las intervenciones de mantenimiento o actualización. En caso de aplicativos desarrollados “in house”, los controles incluyen protocolos de revisiones preventivas, como autorizaciones para ajuste y acceso a los archivos, modificaciones al diseño del programa, verificación de cambios, etc. Igualmente, para mantenimientos que requieren inversiones importantes de recursos por adiciones o reemplazos, los controles incluyen acciones similares para los procesos de adquisición.

3.34 La adquisición de aplicaciones, por lo general representa economías en diseño y ejecución, especialmente cuando provienen de proveedores altamente especializados y reconocidos en el mercado. Los controles internos en estos casos, vienen incorporados en el diseño del sistema. Siempre que se adquieran aplicaciones, debe controlarse el riesgo de dependencia del proveedor para mantenimiento del sistema y las limitaciones para expansiones o modificaciones. En todo caso, es parte del control interno de la planificación estratégica de TI, evaluar el beneficio/costo de desarrollar o adquirir aplicativos y dejar documentadas las decisiones que se tomen.

c. Controles de seguridad de acceso

3.35 Los controles de seguridad de acceso son dispositivos que impiden la intromisión no autorizada a los aplicativos, bases de datos y otros recursos de TI que deben estar protegidos. Es importante que estos dispositivos sean diseñados de conformidad con protocolos de seguridad de la TI de tal forma que desde la fuente que se diseñan hasta los usuarios se mantenga independencia e imposibilidad de que unos y otros puedan modificar tales dispositivos. Por lo general, los usuarios, manejan claves autónomas que solo pueden ser modificadas por el administrador, previo el cumplimiento de protocolos de autorización y segregación de funciones definidos formalmente.

3.36 Dentro del protocolo de seguridades deben tenerse en cuenta:

a. Suministrar instrucciones para asegurar que las claves no son fácilmente deducibles y se conservan encriptadas para impedir el acceso de intrusos;

b. Establecer procedimientos de cambio de claves periódicamente, una vez se cumplen ciertas condiciones. Por ejemplo, después de un número determinado de ingresos, o un volumen de documentos procesados o un monto acumulado de valor, según aplique;

c. Establecer cambios cada vez que un empleado rote de puesto, de tal forma que no conserve posibilidad de acceso, cuando ya no está habilitado.

2. CONTROLES DE APLICACIÓN

3.37 Los controles incluidos en las aplicaciones de los procesos se conocen por lo general como controles de aplicación. Algunos ejemplos son:

a. Integridad (completitud);
b. Precisión;
c. Validez;
d. Autorización;
e. Segregación de funciones.

3.38 Los CA han sido creados para proporcionar seguridad de que el procesamiento sea completo y exacto. Debido a que las interfaces de aplicación están a menudo vinculadas con otros sistemas que a su vez necesitan control, debe prestarse atención especial a estos para asegurar que todos los elementos de entrada se recojan correctamente para su procesamiento y todos los elementos de salida se distribuyan apropiadamente.

3.39 COBIT[5] (objetivos de control para tecnología de información) asume que el diseño e implementación de los CA automatizados son responsabilidad de TI, y están cubiertos en el dominio de adquirir e implementar, con base en los requerimientos de los procesos definidos mediante los criterios de información recomendados por COBIT. La responsabilidad operativa de administrar y controlar los CA no es de TI, sino del dueño de cada proceso.

3.40 De acuerdo con lo anterior, la responsabilidad de los CA es una responsabilidad conjunta, fin a fin, entre los procesos y TI (como un asesor en sistemas de información), pero la naturaleza de la responsabilidad cambia de la siguiente manera:

[5] Transcripción de párrafos de COBIT 4 y 5. The Control Objectives for Information and related Technology (COBIT) es un marco de referencia de gobierno de TI y un conjunto de herramientas de soporte, creado por ISACA y el Instituto de Gobierno de Tecnología (ITGI) en 1996 que permite a los gerentes reducir la brecha entre los requerimientos de control, los temas técnicos y los riesgos del negocio. Se considera un referente internacional generalmente aceptado como los lineamientos de mejor práctica para la gestión de TI.

a. La entidad es responsable de:

- Definir apropiadamente los requisitos funcionales y de control;
- Usar adecuadamente los servicios automatizados.

b. TI (aunque sea una dependencia dentro de la entidad) es responsable de:

- Automatizar e implementar los requisitos de las funciones de negocio y de control;
- Establecer los mecanismos para mantener la integridad de los CA.

3.41 A continuación se transcriben los objetivos de CA recomendados por COBIT[6]:

a. Preparación y autorización de información fuente

3.42 Asegurar que los documentos fuente están preparados por personal autorizado y calificado siguiendo los procedimientos establecidos, teniendo en cuenta una adecuada segregación de funciones respecto al origen y aprobación de estos documentos. Los errores y omisiones pueden ser minimizados a través de buenos diseños de formularios de entrada, este mecanismo permite detectar errores e irregularidades para que sean informados y corregidos.

b. Recolección y entrada de información fuente

3.43 Establecer que la entrada de datos se realice en forma oportuna por personal calificado y autorizado. Las correcciones y reenvíos de los datos que fueron erróneamente ingresados se deben realizar sin comprometer los niveles de autorización de las transacciones originales. Cuando se considere apropiado para reconstrucción, se deberán retener los «documentos fuente» originales durante el tiempo necesario.

c. Chequeos de exactitud, integridad y autenticidad

3.44 Asegurar que las transacciones son exactas, completas y válidas. Validar los datos ingresados y editar o devolver para corregir, tan cerca del punto de origen como sea posible.

[6] Las recomendaciones pueden ser consultadas en la página 16 del documento disponible en http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf

d. Integridad y validez del procesamiento

3.45 Mantener la integridad y validación de los datos a través del ciclo de procesamiento. La detección de transacciones erróneas no interrumpe el procesamiento de transacciones validas.

e. Revisión de salidas, reconciliación y manejo de errores

3.46 Establecer procedimientos y responsabilidades asociadas para asegurar que la salida se maneja de una forma autorizada, entregada al destinatario apropiado y protegida durante la transmisión, que se verifica, detecta y corrige la exactitud de la salida, y que se usa la información proporcionada en la salida.

f. Autenticación e Integridad de transacciones

3.47 Antes de pasar datos de la transacción entre aplicaciones internas y funciones de negocio/operativas (dentro o fuera de la entidad), verificar el apropiado direccionamiento, autenticidad del origen e integridad del contenido. Es decir, mantener la autenticidad y la integridad durante la transmisión o el transporte.

3. RELACIONES ENTRE AMBOS CONTROLES

3.48 Los controles generales y de aplicación utilizados para los sistemas computarizados están interrelacionados. Los CG se necesitan para asegurar el funcionamiento de los CA que dependen de los procesos computarizados.

3.49 Si existen controles generales incorrectos, no es posible depender de los controles de aplicación debido a que estos asumen que el sistema funcionará adecuadamente. La relación entre estas dos categorías de control es tal que los controles generales son necesarios para soportar el funcionamiento de los controles de aplicación, y juntos son necesarios para asegurar el procesamiento completo y exacto de la información.

D. CANALES DE COMUNICACIÓN INTERNA Y EXTERNA

1. GOBIERNO DE LA COMUNICACIÓN

3.50 Además de una política clara sobre la comunicación en todos los sentidos, debe disponerse de una unidad organizacional que planifique, propicie y asegure que las políticas, normas y procedimientos son conocidos y entendidos por el personal. La comunicación es tan importante que debe ser monitoreada por una unidad experta para asegurar que se mantengan los estándares de calidad que soportan en parte lo que se denomina «cultura corporativa». La asignación de la responsabilidad de mantener al personal informado, sea mediante circulares, charlas, talleres, etc., es un medio apropiado.

2. PLANES DE COMUNICACIÓN

3.51 Significa disponer de estándares, responsabilidades y métodos para asegurar calidad y para entender la comunicación interior y exterior a la entidad. Los planes se diseñan de conformidad con la importancia y alcance de las comunicaciones.

3.52 Lo que no es posible planificar puede cubrirse con la capacitación periódica del personal, de manera que se asegure que tales comunicaciones suman valor a la cultura corporativa; un ejemplo de esto son las comunicaciones informales.

3.53 Cuando se elabora el plan de informes, como el ilustrado en la tabla n° 2, al menos en los aspectos formales e informales, se tiene la oportunidad de identificar cuatro componentes clave para la comunicación:

a. Quién debe comunicar;
b. A quién se debe comunicar;
c. Cuál es el contenido de la comunicación (estructura del informe);
d. Que debería suceder con la comunicación; es decir, qué se espera que la comunicación genere.

3. SEGUIMIENTO A LA CALIDAD DE LA COMUNICACIÓN Y MEJORAMIENTO CONTINUO[7]

a. Importancia y forma de la comunicación

3.54 La comunicación efectiva debe fluir hacia abajo, a través de y hacia arriba de la organización, tocando todos los componentes y la estructura entera. La comunicación puede ser formal o informal. De la primera generalmente queda evidencia de la segunda, por lo general, solamente se reflejan sus efectos en los cambios producidos por el mensaje.

b. Comunicación al personal sobre el control Interno

3.55 La comunicación es dirigida desde la alta gerencia. La MAE directamente o mediante sus directores comunica las políticas en general, y en particular, las responsabilidades sobre el control interno. Todo el personal debe tener claro que sus funciones y las acciones que le competen tienen relación con las de otros, siendo necesario mantener una focalización en la verificación de la calidad de la información, antes de su comunicación a otros empleados o a terceras partes que la utilizarán.

3.56 Por lo anterior, no solo en relación con el control interno sino con los demás deberes de los empleados, es una buena práctica que periódicamente se obtengan de ellos salvaguardas o constancias sobre el conocimiento y comprensión de las responsabilidades a su cargo.

c. Proceso para la generación de informes

3.57 Se recomienda seguir un proceso estructurado para generar informes internos o externos.

3.58 **Informes internos**. Sea circulares, manuales, instructivos, etc., deben planificarse en tiempo y forma y establecer los mecanismos para asegurar que efectivamente llegan a los destinatarios y se producen los cambios para el mejoramiento continuo; esto implica realimentar tales informes. Las personas deben ser escuchadas para establecer si es necesario hacer ajustes por falta de claridad o deficiencia de los instrumentos comunicados. Pérdidas, ineficacias, ineficiencias y contingencias legales, a menudo son ocasionados por debilidades en las comunicaciones internas. En este aspecto es clave la asignación de responsabilidades y recursos para poder apoyar el gobierno de las comunicaciones.

[7] Los párrafos que aparecen bajo este epígrafe han sido tomados y adaptados de *la Guía para las normas de control Interno del sector público* de INTOSAI.

3.59 **Informes externos**. Deben seguir las más elevadas normas de control de calidad, no solo en la forma, sino en el fondo. Por lo general, este tipo de documentos, además de pasar una revisión de estilo, gramatical, ortográfica, etc., es sometido a una revisión del contenido técnico y se analizan las implicaciones y alcances del mensaje o mensajes trasmitidos. Nada más perjudicial para la imagen de una entidad que cartas o equivalentes escritos en forma difícil de entender y en un lenguaje inapropiado. Asimismo, si no se tiene el debido cuidado con los contenidos se pueden originar problemas con la interpretación y acciones subsecuentes derivadas de tales mensajes.

d. Programas de inducción y actualización

3.60 Apoyan considerablemente la comunicación interna. Deben diseñarse eventos de capacitación, en los cuales las personas puedan visualizar en la práctica los errores frecuentes en los diferentes tipos de comunicación. Es mediante este tipo de eventos y el seguimiento en la práctica que se mejora la calidad de la comunicación.

e. Seguimiento periódico de la calidad

3.61 Es una forma de preservar y prevenir consecuencias indeseadas para los objetivos del SCI. Disponer de mecanismos de verificación de la calidad, centralizar la vocería de la institución y hacer tareas de mejoramiento continuo y talleres de lecciones aprendidas, resultan en un afianzamiento de la imagen de las entidades y favorece la correcta interpretación y ejecución de las decisiones gerenciales.

E. ARCHIVO Y REGISTROS

1. IMPORTANCIA DE MANTENER ARCHIVOS Y REGISTROS APROPIADOS

3.62 Los documentos representativos de transacciones y eventos en los cuales toma parte una entidad deben ser registrados y archivados correcta y oportunamente, de forma que puedan ser ubicados con prontitud. Todo el proceso originado en la ejecución de un evento o transacción debe poder ser controlado desde su registro inicial hasta el archivo de los documentos que lo representan. Es decir, debe ser factible consultar una transacción en cualquier momento del ciclo de operación en la cual tiene influencia. El registro y archivo correcto y oportuno, no solo se refiere a los aspectos de administración financiera, sino que incluye cualquier acto en el cual intervenga la entidad y que de conformidad con las normas vigentes deba ser conservado. (Ver Ley de Libre Acceso a la Información Pública)

3.63 No disponer de registros y archivos apropiados puede ocasionar pérdidas y otros problemas a una entidad. En la ley de comercio y en otras normas, la forma de defenderse o demostrar que se ha recibido un perjuicio empieza por disponer de documentación apropiada. Cuando una de las partes que intervienen en un conflicto de esta naturaleza no tiene los documentos apropiados y no demuestra una contabilización o registro histórico, puede llegar a recibir fallos en su contra. De igual forma, la misma administración y las agencias de control interno y externo pueden experimentar serias dificultades para realizar su trabajo, tomar decisiones o llegar a conclusiones sobre la condición de las operaciones.

2. ACTUALIZACIÓN

3.64 Disponer de registros y archivos apropiados también implica la actualización oportuna de toda la documentación para que siga siendo relevante. La clasificación correcta de las transacciones y hechos es también necesaria para asegurar que la información confiable sea accesible a la gerencia.

3.65 Los sistemas de información basados en tecnología, por si mismos no son suficientes. Se requiere la disponibilidad de funciones y procedimientos para asegurar que la información archivada en la base de datos, de conformidad con reglas de seguridad, pueda ser actualizada cuando corresponda o no pueda ser modificada si así está previsto. La existencia de políticas, responsabilidades y procedimientos relacionados con el manejo de los registros y los documentos que los respaldan es clave para que las entidades dispongan de la información en tiempo y forma acorde con las necesidades.

3.66 La rendición de cuentas mediante estados financieros y otro tipo de informes no será transparente ni oportuna sin el respaldo adecuado de registros y archivos actualizados para su preparación y conservación.

3. GESTIÓN DE ARCHIVOS Y REGISTROS

3.67 En la gestión de archivos y registros se han hecho considerables progresos. Como medios principales se dispone de la tecnología ya que permite conservar importante cantidad de datos en un reducido espacio. Hoy en día, la mayoría de las legislaciones permiten después de unos años (por lo general cinco) hacer copias microfilmadas de los documentos para ahorrar tiempo y espacio. Los registros se conservan en medios electrónicos y si utilizan medidas de protección apropiadas para respaldo y continuidad, en caso de siniestros, seguramente no se tendrán sorpresas desagradables a través del tiempo.

3.68 Como parte del gobierno de la información y la comunicación, deben incluirse la asignación de responsabilidades, atribuciones, funciones y recursos para la preparación, conservación y actualización de registros y archivos. Deben existir un plan y un manual de archivo en copia impresa o electrónica, así como manuales de los sistemas de información que preserven la integridad de los registros. Los riesgos de pérdida o siniestros naturales de la información deben ser previstos y asegurarse que existen planes de contingencia para la recuperación y continuidad del procesamiento.

BIBLIOGRAFÍA

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. *Internal Control-Integrated Framework*, 1994. Disponible en: http://www.snai.edu/cn/service/library/book/0-framework-final.pdf

INTOSAI. *Guía para las normas de control interno del sector público*, 2004. Disponible en: http://intosai.connexcc-hosting.net/blueline/upload/1guicspubsecs.pdf

ISACA. *Normas de Auditoría de SI, S15IT Controls*, 2008. Disponible en: http://www.isaca.org/Knowledge-Center/Standards/Documents/Standards-IT-Spanish-S15.pdf

—*Cobit 4.1*, IT Governance Institute, 2007. Disponible en: http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf

REPÚBLICA DOMINICANA. *Normas básicas de control interno del sector público dominicano*, Resolución CGR n° 001/11, Septiembre 2011

Recursos web

www.coso.org

www.intosai.org

www.isaca.org

www.itgi.org

www.theiia.org