

**Al contestar refiérase
al oficio N° 5638**

19 de mayo, 2017
DFOE-PG-0187

Máster
Oscar Alberto León Alonso
Auditor Interno
TRIBUNAL SUPREMO DE ELECCIONES
Correo: oleon@tse.go.cr
auditoria@tse.go.cr

Estimado señor:

Asunto: Emisión de criterio solicitado por el Auditor Interno del Tribunal Supremo de Elecciones, mediante oficio n.º AI-043-2017, sobre la aplicación de mejores prácticas generalmente aceptada en materia de tecnologías de información.

Se refiere esta Área de Fiscalización al oficio n.º AI-043-2017 de fecha 30 de marzo del presente año, mediante el cual se consulta el criterio de la Contraloría General de la República en relación con la aplicación de un marco de trabajo de control interno de las tecnologías de información en las Instituciones Públicas.

I. MOTIVO DE LA GESTIÓN

En el texto de la consulta realizada, se plantean las siguientes interrogantes:

1. ¿Pueden los departamentos y direcciones de tecnologías de información de las instituciones públicas, utilizar marcos de trabajo complementarios (Mejores Prácticas Generalmente Aceptadas) a las Normas técnicas para la gestión y el control de las tecnologías de información, tales como: ISO 27005, COBIT, ISO 22301, PMBOK, ISO 38500, ITIL, DMBOK, NIST, entre otros?

2. Independientemente de que los departamentos y direcciones de tecnologías de información de las referidas instituciones, decidan utilizar o no Mejores Prácticas Generalmente Aceptadas, como parte del apoyo en su marco de gestión y control de las tecnologías de información, ¿pueden las Auditorías Internas de las instituciones públicas emplear esas Mejores Prácticas Generalmente Aceptadas, como apoyo en las evaluaciones, así como en los criterios y recomendaciones que vierta mediante los diferentes servicios que brinda?

Sobre este particular, en la consulta se adiciona una referencia a los marcos de trabajo como COBIT 5 de Information Systems Audit and Control Association (ISACA) e International Standard ISO/IEC 38500 Corporate Governance of Information Technology, relacionándolo con la definición de "mejores prácticas", establecida en el glosario de las Normas Generales de Auditoría para el Sector Público, y disposición 403 del Capítulo IV de la misma. Considerando dicha Auditoría, que los departamentos y direcciones de tecnologías de información de las instituciones públicas, sí pueden utilizar esas Mejores Prácticas Generalmente Aceptadas, como marco de trabajo complementario a las normas técnicas para la gestión y el control de las tecnologías de información, por coadyuvar en la protección y conservación del patrimonio público, fortaleciendo el sistema de control interno y contribuyendo al logro de los objetivos institucionales, y también de apoyo tanto en la toma de decisiones como en las revisiones realizadas y criterios vertidos en los diferentes servicios que brinda.

II. CONSIDERACIONES PRELIMINARES

En primer término, se señala que el ejercicio de la potestad consultiva de la Contraloría General se encuentra regulada en el artículo 29 de la Ley Orgánica (Ley n.º 7428 del 4 de setiembre de 1994) y el Reglamento sobre la recepción y atención de consultas dirigidas a la Contraloría General de la República (Resolución n.º R-DC-197-2011), publicado en el Diario Oficial La Gaceta n.º 244 del 20 de diciembre de 2011.

Según lo dispuesto en la normativa citada, el Órgano Contralor emite criterios vinculantes en el ámbito de su competencia cuando se cumplen los siguientes requisitos:

- a) Cuando la temática tenga relación con los componentes de la Hacienda Pública y en general con el ordenamiento de control y fiscalización superior de la Hacienda Pública.
- b) Cuando la consulta la hayan planteado los sujetos pasivos de fiscalización de la Contraloría General, según definición presente en el artículo 4 de la Ley n.º 7428. Deben entenderse incluidos el auditor y subauditor interno de las instituciones públicas.

Aunado a lo anterior, cabe señalar que el inciso 2 del artículo 8 del Reglamento de referencia, establece como uno de los requisitos de obligatorio cumplimiento para la presentación de las consultas dirigidas al Órgano Contralor, lo siguiente:

Artículo 8º—Requisitos para la presentación de las consultas. Las consultas que ingresen para su atención conforme al artículo 29 de la Ley No. 7428, deberán cumplir los siguientes requisitos:

(...)

2. Plantearse en términos generales, sin que se someta al órgano consultivo a la resolución de circunstancias concretas propias del ámbito de decisión del sujeto consultante, o que atañen a la situación jurídica del gestionante.

(...).

De lo cual se desprende la obligación de plantearse las consultas en términos generales, sin que se someta al Órgano Consultivo a la resolución de circunstancias concretas propias del ámbito de decisión del sujeto consultante, o que atañen a la situación jurídica del gestionante.

Dicho proceder, obedece a la finalidad propia del proceso consultivo, que no pretende sustituir a la Administración en la toma de decisiones respecto de las competencias que le han sido asignadas en el ordenamiento jurídico, a la vez que se trata de evitar el riesgo que genera la emisión de un criterio vinculante sobre la base de supuestos fácticos y jurídicos que no se conocen a plenitud, y por ende, puede generar un pronunciamiento errado en sus conclusiones. De manera que se reitera el carácter general de las observaciones y el análisis que aquí se plantea sobre los temas en consulta.

Por ello, la potestad consultiva no debe verse como un medio por el cual la Contraloría General sustituye a las Administraciones Públicas en el manejo de situaciones particulares en el plano meramente administrativo, la resolución de los conflictos internos que se puedan generar entre las diferentes instancias en el seno de la administración consultante, o la validación o confirmación de conductas previamente adoptadas por la Administración activa.

En ese tanto, lo anterior no impide emitir un criterio vinculante respecto a consultas relacionadas con el ámbito competencial del Órgano Contralor, máxime cuando se trata de temas o materias abordados previamente en el ejercicio de su potestad consultiva, bajo el entendido que se trata de consideraciones y observaciones que se esbozan desde una perspectiva general, y no de una situación específica e individualizada; para que sea utilizado en el análisis sobre la legalidad de las conductas administrativas que serán adoptadas por el sujeto competente, a quien corresponde finalmente tomar las decisiones que considere más ajustadas a derecho

III. CRITERIO JURÍDICO DE LA CONTRALORÍA GENERAL

Expuestas las consideraciones anteriores se procede a rendir criterio sobre el tema consultado, siendo necesario en primera instancia, señalar que el punto 1 del artículo 16 de la Ley General de la Administración Pública, Ley n.º 6227, establece como principio general, que todo acto administrativo debe dictarse con cabal cumplimiento de los mandatos legales, en apego a las reglas unívocas de la ciencia y de la tecnología, así como a principios elementales de justicia, lógica o conveniencia; conceptos que se resumen en la razonabilidad y proporcionalidad de la norma como parámetro.

Dicho de otra manera, no existen potestades ni actos administrativos plenamente discrecionales, sino que sólo hay ciertos elementos discrecionales de la potestad administrativa que operan en observancia a las conductas y mecanismos dispuestos en el ordenamiento, y que el mismo Legislador expresamente los dispuso como elementos de legalidad.

Como segundo orden en atención a la consulta, es de interés resaltar los componentes orgánicos que participan en el control interno, como lo son la Administración activa y la Auditoría Interna, correspondiéndole al primero no sólo implantar los sistemas de control, sino que es el órgano de control¹.

Asimismo, resulta pertinente indicar que el artículo 21 de la Ley General de Control Interno, Ley n.º 8292, establece un concepto funcional de la Auditoría Interna, entendido de la siguiente manera:

La auditoría interna es la actividad independiente, objetiva y asesora, que proporciona seguridad al ente u órgano, puesto que se crea para validar y mejorar sus operaciones. Contribuye a que se alcancen los objetivos institucionales, mediante la práctica de un enfoque sistémico y profesional para evaluar y mejorar la efectividad de la administración del riesgo, del control y de los procesos de dirección en las entidades y los órganos sujetos a esta Ley. Dentro de una organización, la auditoría interna proporciona a la ciudadanía una garantía razonable de que la actuación del jerarca y la del resto, de la administración se ejecuta conforme al marco legal y técnico y a las prácticas sanas.²

En suma a dicho numeral, en el Glosario de las Normas Generales de Auditoría para el Sector Público (en adelante NGASP), resolución n.º R-DC-64-2014 emitida por el Despacho Contralor, retoma y define la actividad de Auditoría Interna en el mismo sentido.

De lo cual cabe subrayar la particular importancia que lo apuntado tiene en la especie, habida cuenta que la Auditoría Interna representa una actividad independiente, objetiva y asesora, dirigida a proporcionar seguridad en la gestión de la organización para que sea realizada una gestión adecuada, coadyuvando a alcanzar los objetivos y metas institucionales, y apoyo en la toma de decisiones; pero a su vez, a proporcionar a la ciudadanía una seguridad razonable en que la actuación del Jerarca y demás titulares de la Administración, se ejecuta conforme al marco legal y técnico vigente, así como garante de las sanas prácticas, entendida ésta última como las prácticas administrativas de reconocida aceptación general y que devienen en un beneficio real para el ente u órgano, en virtud de que fortalecen el sistema de control interno.

En ese tanto, actúa como una instancia de control preventivo, de asesoría y de acompañamiento a la Administración, en la consecución de los objetivos del sistema de control interno a nivel organizacional. Operando como una actividad concebida para dar valor agregado y optimizar las funciones y operaciones de una organización, por medio de un enfoque sistémico y técnico que permita valorar y tomar acciones correctivas oportunas, que conlleve la eficacia de los procesos de valoración de los riesgos de los servicios que presta dicha institución, así como su adecuado control y dirección, al evaluar la efectividad de la administración en el manejo de los temas esenciales en control, gestión del riesgo y gobernabilidad.

¹ Norma 1.4, Normas de Control Interno para el Sector Público.

² En el tanto, los conceptos de seguridad y garantía que se utilizan en el artículo de cita, deben entenderse en términos razonables y no absolutos, debido a las limitaciones inherentes a todos los sistemas de control interno y a las técnicas y procedimientos de auditoría.

Por ello, la Auditoría Interna en la consecución de sus objetivos, debe integrarse haciendo pleno uso de los diferentes instrumentos y herramientas de gestión, comprendiendo los sistemas de control interno de la Administración Pública, así como impulsando el perfeccionamiento y protección de dicho control.

A todo lo indicado ha de agregarse un tercer aspecto relevante de señalar, en el sentido que las tecnologías de información son un instrumento esencial en la prestación de los servicios públicos sujeto a constantes avances tecnológicos, pero siempre en función de los requerimientos y funcionalidades que se pretenda cumplir, y los recursos públicos que se apreste a invertir.

Es así que, los sistemas de información han sido establecidos como uno de los componentes funcionales del sistema de control interno, siendo marco básico lo dispuesto en el artículo 16 de la Ley n.º 8292, como componente funcional.

Aunado a lo indicado, las Normas de Control Interno para el Sector Público (en adelante NCISP), resolución n.º R-CO-9-2009 del Despacho Contralor, desarrolla en el Capítulo V el tema de: "Normas sobre Sistemas de Información", con el propósito de promover un mejoramiento del proceso de auditoría y asegurar la calidad de sus productos, estableciéndose estándares mínimos para que el proceso se ejecute de manera uniforme, competente, íntegra, objetiva e independiente. Indicándose además en el Glosario como definición para los gestores, lo que debe entenderse por "mejores prácticas" del siguiente modo: "*Prácticas administrativas de reconocida aceptación general y que devienen en un beneficio real para el ente u órgano, en virtud de que fortalecen el sistema de control interno, favorecen que la Administración realice una gestión adecuada y por lo tanto, contribuyen en el logro de los objetivos institucionales y apoyan la toma de decisiones.*"

Asimismo, están las Normas Técnicas para la gestión y el control de las Tecnologías de Información (en adelante NTGCTI), resolución del Despacho Contralor n.º R-CO-26-2007, también de acatamiento obligatorio para el propio Órgano Contralor como para las instituciones y órganos sujetos a su fiscalización; prevaleciendo sobre cualquier disposición en contrario que emita la Administración y su inobservancia generará las responsabilidades que correspondan, de conformidad con el marco jurídico que resulte aplicable.

De esta forma, las NTGCTI se constituyen en los criterios básicos de control que deben ser observados en la gestión institucional de las tecnologías, con el propósito de coadyuvar en la gestión como instrumento en la prestación de los servicios públicos; de frente a un adecuado uso de los recursos invertidos en ellas y a facilitar su control y fiscalización. Al respecto, se puede observar el oficio emitido por esta Área de Fiscalización de Servicios Públicos Generales, oficio n.º 4807 (DFOE-PG-0187) de fecha 6 de abril de 2015, en el que además se resaltó la importancia en que estas Normas deben ser valoradas integralmente, de manera que se pueda eliminar cualquier equívoco que surja de la apreciación individual de su articulado, y contradiga su razón de ser.

Resta mencionar que, las tecnologías de información deben gestionarse dentro de un marco de control que procure el logro de los objetivos que se pretende con ellas, y estar debidamente alineados con la estrategia de la organización, garantizando niveles óptimos de funcionalidad y seguridad, de manera que se ajusten a las necesidades actualizadas y planeamientos estratégicos definidos institucionalmente, preservando la confiabilidad, integridad, confidencialidad, disponibilidad y privacidad de la información institucional, así como el buen uso de los recursos invertidos en ellas y, facilitar su control y fiscalización.

De ahí que el jerarca y los titulares subordinados como responsables de esa gestión, deben establecer, mantener, evaluar y perfeccionar ese marco de control de conformidad con la Ley General de Control Interno, las NCISP, las NTGCTI, así como la Función de Tecnologías de Información³, cumpliendo dicho marco de control y facilitando la labor estratégica del jerarca.

Esto significa que el jerarca es el responsable del sistema de control interno institucional, mientras que los titulares subordinados lo son respecto a la unidad, dependencia o proceso a su cargo, presentándose la misma correspondencia en relación con el control y gestión de tecnologías de información (ver en este sentido el oficio n.º 3640 (FOE-ST-0068) del 25 de abril de 2008, emitido por la Secretaría Técnica de la División de Fiscalización Operativa y Evaluativa, del Órgano Contralor).

Este proceder se funda, en que las NTGCTI regulan disposiciones en términos generales, para que posteriormente los responsables en cada administración determinen lo correspondiente según la realidad de sus instituciones.

En ese tanto, la toma de actuaciones debe ser en garantía del cumplimiento, suficiencia y validez del sistema de control interno, que lo fortalezca, y contribuyendo en el logro de los objetivos institucionales y apoyo en la toma de decisiones; con apego al ordenamiento jurídico.

Decisión que debe realizarse bajo un análisis puntual de cada caso en concreto, en el sentido que la Administración deben utilizar las sanas prácticas generalmente aceptadas, definiendo cuáles serán los marcos específicos que se van a utilizar y cómo (según además las competencias y atribuciones propias de la organización, de conformidad con el artículo 10 de la Ley 8292), por el conocimiento a plenitud de los supuestos fácticos y jurídicos que se posee, garantizando la existencia del sistema de control interno y contribuyendo con el logro de sus resultados como prioridad.

Asimismo, corresponde a la Auditoría Interna dentro de la conceptualización de su rol en los diferentes servicios públicos, apoyar en la ejecución de los servicios públicos que brinda, bajo las circunstancias del caso específico que sea de conocimiento, contribuyendo al cumplimiento por parte de la Administración en la rendición de cuentas a la ciudadanía, acorde con el marco legal y técnico, así como a las sanas prácticas.

³ Entendido como la unidad organizacional o conjunto de componentes organizacionales, responsable de los principales procesos relacionados con la gestión de las tecnologías de información en apoyo a la gestión de la organización. Glosario que acompaña las NTGCTI.

IV. CONCLUSIONES

1. La Administración Pública debe adoptar conductas válidas, afectadas a las reglas unívocas de la ciencia y de la técnica, y a los principios elementales de justicia, lógica o conveniencia, con cabal cumplimiento del marco legal y técnico, y uso las buenas prácticas generalmente aceptadas, definiendo sobre éstas últimas con cuáles marcos específicos y cómo serán utilizadas, siendo quien cuenta con el conocimiento a plenitud de los supuestos fácticos y jurídicos.
2. La Auditoría Interna es una instancia de control preventivo, de asesoría y de acompañamiento a la administración en la consecución de los objetivos del sistema de control interno a nivel organizacional, ejercido de manera independiente y objetivo, uniforme, competente, íntegro, con un enfoque sistemático y disciplinario. Siendo la llamada a proporcionar una garantía razonable a la ciudadanía, de que la actuación del Jerarca y demás titulares de la Administración fue ejecutada con apego a sanas prácticas -identificando cuáles son los marcos de buenas prácticas que se utilizarán como criterios- y al marco jurídico y técnico aplicable.
3. La Ley General de Control Interno, las Normas de Control Interno para el Sector Público, así como las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, establecen criterios básicos de control que deben observarse en la gestión de los sistemas de información, teniendo por propósito coadyuvar en la gestión, como instrumento en la prestación de los servicios públicos.

Finalmente, se recuerda la importancia de registrarse y utilizar el Sistema de la Potestad Consultiva, de manera que podamos brindarle un servicio más oportuno y eficiente en la atención de su gestión. El mismo lo encuentra en nuestro sitio web www.cgr.go.cr.

Atentamente,

Lic. José Luis Alvarado Vargas
GERENTE DE ÁREA



Licda. Hilda Natalia Rojas Zamora
FISCALIZADORA

/ghj
Ci: Área Secretaría Técnica DFOE CGR
Archivo
G: 2017001558-1
Exp: CGR-CO-2017002693
NI: 8337 (2017)