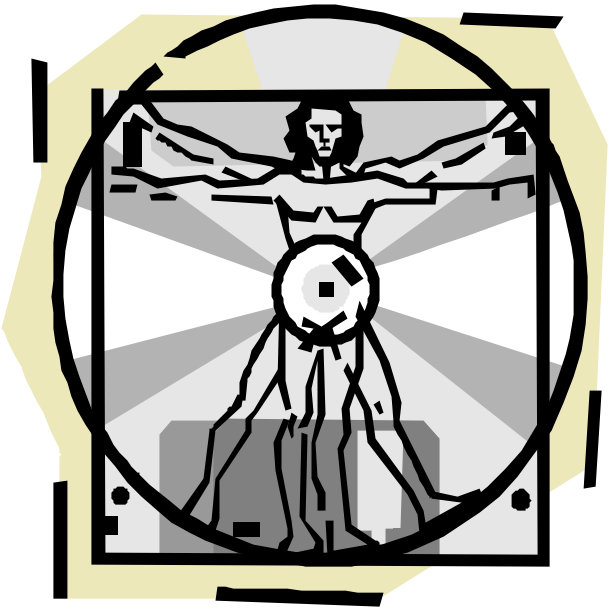
Estándares para la Práctica Profesional de la Auditoría Sistemas de Información



Information Systems Audit and Control Association

Capítulo Buenos Aires

Information Systems Audit and Control Association®

Traducción del texto aprobado en inglés realizada por el
Capítulo Buenos Aires - Argentina

COMITÉ DE TRADUCCIÓN DE NORMAS

-Julio de 2002-

Juan de Dios Bel, CISA,CFE – Coordinador	
IT Assurance & Control S.A.	
Jorge N. Nunes, CISA	Administración Nacional de la Seguridad Social
Fabiana Marges, CISA	PricewaterhouseCoopers, Argentina
Ana C. Russo, CISA	Sindicatura General de la Nación
Marcelo H. González, CISA	Banco Central de la República Argentina
Marina L. Varela, CISA	Sindicatura General de la Nación
Guillermo H. Casal, CISA, CIA	Instituto de Auditores Internos de Argentina

Original publicado por la
Information Systems Audit and Control Association®
Copyright © 1998-2002, Information Systems Audit and Control Association®,
3701 Algonquin Road, Suite 1010 - Rolling Meadows, Illinois 60008, USA
E-mail: research@isaca.org
Web site: www.isaca.org

Se hace reserva de todos los derechos.
Impreso en Argentina
Marzo de 2002

PRONUNCIAMIENTOS Y COMENTARIOS

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA), funciona como autoridad de la profesión de Auditoría de los Sistemas de Información que aborda cuestiones significativas que afectan a los auditores de SI, y es la única organización dedicada exclusivamente al progreso del auditor de SI y a su profesión en todo el mundo. ISACA es el líder mundial en cuestiones educativas y de investigación para los auditores de SI, además de ser el organismo emisor de normas de la profesión. Como entidad líder, ISACA monitorea la legislación, las regulaciones o pronunciamientos de otras organizaciones profesionales de todo el mundo sobre asuntos que directa o indirectamente impactan en la práctica de la auditoría de SI. ISACA se manifiesta ante organismos de contralor e instituciones gubernamentales nacionales e internacionales. Asimismo, desarrolla y publica documentos en los que fija su posición, guías de sugerencias y comentarios sobre legislación y regulaciones, pronunciamientos y cuestiones en curso y/o que puedan surgir, que revistan importancia para la profesión de auditoría de SI.

Al nivel internacional, ISACA es miembro y participa en las Naciones Unidas como Organismo No Gubernamental (ONG), en el International Consortium on Government Financial Management (Consorcio Internacional sobre Administración Financiera Gubernamental), en la International Organization of Supreme Audit Institutions o INTOSAI (Organización Internacional de las Instituciones Supremas de Auditoría) y en la International Federation of Accountants o IFAC (Federación Internacional de Contadores).

Además, ISACA es miembro y/o participa en distintos proyectos en cooperación con el American Institute of Certified Public Accountants – AICPA (Instituto Norteamericano de Contadores Públicos Certificados), con el American National Standards Institute (Instituto de Normas Nacionales Norteamericanas), con la American Accounting Association - AAA (Asociación Norteamericana de Contadores), con la Association of Government Accountants (Asociación de Contadores Gubernamentales), con el Financial Executive Institute (Instituto de Ejecutivos de Finanzas), con el Institute of Management Accountants – IMA (Instituto de Contadores de Gestión), con el National Intergovernmental Auditors Forum (Foro Nacional de Auditores Intergubernamentales), con la National Association of Local Government Auditors (Asociación Nacional de Auditores Gubernamentales Locales) y con el Canadian Institute of Chartered Accountants (Instituto Canadiense de Perito Contadores), entre otros.

También es miembro especializado del COSO - Committee of Sponsoring Organizations de la Treadway Commission, y contribuyó al *Control Interno – Marco Integrado*, que provee una guía amplia sobre el control interno y su estructura.

Tabla de Contenido

Information Systems Audit and Control Association
CAPÍTULO BUENOS AIRES

ESTRUCTURA DE LOS ESTANDARES PARA LA PRÁCTICA PROFESIONAL DE LA AUDITORIA DE SISTEMAS DE INFORMACIÓN

Introducción a las Normas Generales para Auditoría de Sistemas de Información

Los sistemas basados en computadoras son herramientas útiles y omnipresentes que se aplican en la gestión y operación de muchas organizaciones. Tales sistemas pueden efectuar el control sobre muchos activos y operaciones de una organización. El desarrollo y respaldo de estos sistemas puede exigir una porción significativa de todos los recursos de la organización. Cuando se presentan tales condiciones, la misión del auditor puede incluir auditar el desarrollo, implementación, mantenimiento y operación de los sistemas.

El trabajo de los auditores, sean externos o internos, se rigen en general por estándares desarrollados por una cantidad de organizaciones profesionales, cada una de las cuales busca asegurarse de la calidad del trabajo de auditoría que se realiza.

Necesidad de Normas de Auditoría de Sistemas de Información

El carácter especializado de la auditoría de sistemas de información y las habilidades necesarias para llevar a cabo una auditoría de esta índole requieren normas generales específicamente aplicables a la auditoría de sistemas de información. Como consecuencia de ello, uno de los objetivos de ISACA es proponer normas para satisfacer esta necesidad. El desarrollo y la difusión de las Normas de Auditoría de Sistemas de Información constituyen un hito en la contribución profesional de ISACA a la comunidad de auditores.

Definición de la Auditoría de Sistemas de Información

A los efectos de estas normas, la auditoría de sistemas de información se define como cualquier auditoría que cubre la revisión y evaluación de todos los aspectos (o alguna parte) de sistemas de procesamiento automatizado de información, incluyendo los procesos relacionados no automatizados, y las interfaces con ellos.

Los auditores de sistemas de información examinan y evalúan el desarrollo, implementación, mantenimiento y operación de los componentes de sistemas automatizados (o tales sistemas como un todo) y sus interfaces con áreas no automatizadas de las operaciones de la organización. Los objetivos de tales auditorías por lo general son evaluar el grado en que estos sistemas o componentes de los mismos producen información confiable y exacta y determinar si tal información está en conformidad con requerimientos de la gerencia y cualquier disposición normativa aplicable.

Objetivos

Los objetivos de las Normas de Auditoría de Sistemas de Información de ISACA son informar a

- Los auditores de sistemas de información del nivel mínimo de rendimiento aceptable que se requiere para cumplir con las responsabilidades profesionales expuestas en el Código de Ética Profesional para auditores de sistemas de información.

- La gerencia y otras partes interesadas de las expectativas de los profesionales respecto de su propio trabajo.

El objetivo de los Directivas de Auditoría de Sistemas de Información es proporcionar información adicional sobre la manera de cumplir con las Normas de Auditoría de Sistemas de Información.

Alcance y Autoridad de las Normas de Auditoría de Sistemas de Información

La estructura de las Normas de Auditoría de Sistemas de Información emitidas por ISACA establece múltiples niveles de estándares, como se indica a continuación :

Normas: definen los requisitos obligatorios para la auditoría de sistemas de información y la presentación de informes.

Directivas: brindan una orientación para la correcta aplicación de las normas de auditoría de SI. El Auditor de SI debe tenerlos en cuenta al determinar cómo llevar a cabo la implementación de las normas mencionadas, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto de los mismos.

Procedimientos: brindan ejemplos de procedimientos que podría seguir un auditor de sistemas de información en un contrato de auditoría. Los documentos contienen procedimientos que proporcionan información sobre la manera de cumplir con las normas al realizar tareas de auditoría de sistemas de información, pero no establecen requisitos.

El Código de Ética Profesional de ISACA exige que los miembros de la Asociación y los titulares de la designación CISA (Auditor Certificado de Sistemas de Información) cumplan con las Normas de Auditoría de Sistemas de Información adoptadas por ISACA.

El manifiesto incumplimiento de las mismas puede conducir a una investigación de la conducta del miembro de la Asociación o del titular de la designación CISA por parte del Consejo Directivo de ISACA o del comité de ISACA que corresponda, con la eventual ocurrencia de acciones disciplinarias.

Relación entre las Normas de Auditoría de Sistemas de Información y otras Normas de Auditoría

No se pretende que las normas de auditoría de sistemas de información promulgadas por ISACA reemplacen las normas de auditoría o reglamentaciones desarrolladas por otras organizaciones profesionales o entes gubernamentales. En situaciones en las que se perciba un conflicto entre las normas de ISACA y los de otro ente, es responsabilidad del auditor utilizar su juicio profesional, a partir de los hechos específicos de las situación, a fin de resolver la cuestión.

Desarrollo de Normas, Directivas y Procedimientos

El Comité de Normas de ISACA está comprometida con la realización de una extensa consulta que asista en la preparación de Normas, Directivas y Procedimientos de Auditoría de Sistemas de Información. Antes de emitir los documentos, la Comité de Normas emite borradores para discusión de alcance internacional a fin de recibir observaciones por parte del público. Asimismo, el Comité de Normas está interesada en realizar consultas con aquellos que cuenten con un especial interés o experiencia en el tópico que se esté examinando.

El Comité de Normas está implementando un programa de desarrollo y recibiría con agrado sugerencias de miembros de ISACA y titulares de la designación CISA que identifiquen problemas emergentes que requieran la producción de nuevas normas. Cualquier sugerencia debe ser enviada por correo electrónico (*research@isaca.org*) o fax (+1.847.253.1443) a la Oficina Internacional de ISACA, dirigida al Director de Investigaciones, Normas y Relaciones Académicas.

Information Systems Audit and Control Association

CODIGO DE ETICA PROFESIONAL

La Asociación fija el siguiente Código de Ética Profesional para guiar la conducta profesional y personal de los miembros de la Information Systems Audit and Control Association y poseedores del Certificado en Auditoría de Sistemas de Información.

Los Auditores de Sistemas de Información están comprometidos a sostener las siguientes prácticas:

- **Apoyar el establecimiento** y cumplimiento de normas, procedimientos, controles y procesos de auditoría de Sistemas de Información.
- **Cumplir las Normas de Auditoría de Sistemas de Información** adoptados por la Asociación.
- **Actuar en interés** de sus empleadores, accionistas, clientes y del público en general en forma diligente, leal y honesta y no a sabiendas de ser parte de actividades impropias o ilícitas.
- **Mantener la confidencialidad** de la información obtenida en el curso de las actividades asignadas. La información no será utilizada para beneficio propio o divulgada a terceros no legitimados.
- **Cumplir con sus deberes** en forma independiente y objetiva, y evitar toda actividad que comprometa, o parezca comprometer su independencia.
- **Mantener su competencia** en los campos interrelacionados de la auditoría y los sistemas de información por medio de su participación en actividades de desarrollo profesional.
- **Poner sumo cuidado** al obtener y documentar suficiente material provisto por el cliente cuya consistencia servirá para basar sus conclusiones y recomendaciones.
- **Informar a las partes involucradas** acerca de los resultados de las tareas de auditoría llevadas a cabo.
- **Apoyar la educación** de la gerencia, los clientes, sus colegas y al público en general para mejorar la comprensión en materia de auditoría y de sistemas de información.
- **Mantener altos los estándares** de conducta y carácter tanto en las actividades profesionales como en las privadas.

© 1998 Capítulo Buenos Aires de la *Information Systems Audit and Control Association*.
Este documento es una traducción del texto original en inglés del
Code of Ethics establecido por la ***Information Systems Audit & Control Foundation*** ®

Information Systems Audit and Control Association

NORMAS GENERALES DE AUDITORIA DE SISTEMAS DE INFORMACIÓN

Emitidas por el Comité de Normas de la Information Systems Audit and Control Association (ISACA)

010 Mandato de Auditoría

010.010 Responsabilidad, Autoridad y Rendición de Cuentas

La responsabilidad, autoridad y rendición de cuentas de la función de auditoría de sistemas de información deben ser adecuadamente documentadas en un estatuto de auditoría o términos de referencia de contratación.

020 Independencia

020.010 Independencia Profesional

En todos los asuntos relacionados con la auditoría, el auditor de sistemas de información debe ser independiente del auditado en actitud y apariencia.

020.020 Relación dentro de la Organización

La función de auditoría de sistemas de información debe ser lo suficientemente independiente del área auditada como para permitir la realización objetiva de la auditoría.

030 Ética y Normas Profesionales

030.010 Código de Ética Profesional

El auditor de sistemas de información debe observar *el Código de Ética Profesional* de ISACA (Information Systems Audit and Control Association).

030.020 Debido Cuidado Profesional

Se debe proceder con el debido cuidado profesional y deben observarse las normas aplicables de auditoría profesional en todos los aspectos del trabajo del auditor de sistemas de información.

040 Competencia

040.010 Habilidades y Conocimiento

El auditor de sistemas de información debe ser técnicamente competente y contar con las habilidades y el conocimiento necesarios para llevar a cabo sus tareas.

040.020 Capacitación Profesional Permanente

El auditor de sistemas de información debe mantener su competencia técnica por medio de una continua y adecuada capacitación profesional.

050 Planificación

050.010 Planificación de la Auditoría

El auditor de sistemas de información debe planificar las tareas de auditoría de tal manera que se aborden los objetivos pertinentes y se cumpla con las normas aplicables de auditoría profesional.

060 Realización de las Tareas de Auditoría

060.010 Supervisión

El personal de auditoría de sistemas de información debe ser adecuadamente supervisado a fin de garantizar que se alcancen los objetivos de auditoría y se cumpla con las normas aplicables de auditoría profesional.

060.020 Evidencia

En el transcurso de la auditoría, el auditor de sistemas de información debe obtener evidencia suficiente, confiable, pertinente y útil a fin de que se alcancen los objetivos de auditoría con eficacia. Los hallazgos y las conclusiones de la auditoría deben ser sustentados mediante el análisis y la interpretación adecuados de dicha evidencia.

070 Presentación de Informes

070.010 Contenido y Estructura de Informes

El auditor de sistemas de información debe proporcionar a los destinatarios correspondientes un informe – con una estructura apropiada –sobre la realización de las tareas de auditoría. En dicho informe deben constar el campo de aplicación, los objetivos, el período de aplicación y la naturaleza y alcance de las tareas de auditoría realizadas. El informe debe identificar la organización, los destinatarios correspondientes y cualquier restricción a su difusión; asimismo, debe exponer los hallazgos, las conclusiones y recomendaciones y cualquier reserva o restricción que tenga el auditor con respecto a la auditoría.

080 Actividades de Seguimiento

080.010 Seguimiento

El auditor de sistemas de información debe solicitar y evaluar la información apropiada sobre anteriores hallazgos, conclusiones y recomendaciones pertinentes para determinar si se han implementado las medidas adecuadas de manera oportuna.

Fecha de Vigencia

Estas normas rigen para todas las auditorías de sistemas de información a partir del 25 de julio de 1997.

Copyright © 1994 - 2002 by Information Systems Audit & Control Association.

DIRECTIVA DE AUDITORIA DE SI

MANDATO DE AUDITORIA

1. ANTECEDENTES

1.1 Articulación con Normas

1.1.1 La Norma 010.010 (Responsabilidad, Autoridad y Rendición de Cuentas) determina que “La responsabilidad, autoridad y rendición de cuentas de la función de Auditoría de sistemas de información deben ser adecuadamente documentadas en un mandato de auditoría o en los términos de referencia de la misma.”

1.2 Necesidad de un Directiva

1.2.1 El propósito de esta Directiva es asistir al Auditor de SI en la preparación de un mandato de Auditoría que defina la responsabilidad, autoridad y rendición de cuentas de la función de Auditoría de SI. Esta Directiva está destinado principalmente a la función de Auditoría Interna de SI ; sin embargo, pueden considerarse ciertos aspectos para otras circunstancias.

1.2.2 Esta Directiva brinda una orientación para la correcta aplicación de las normas de Auditoría de SI. El Auditor de SI debe tenerlo en cuenta al determinar cómo llevar a cabo la implementación de las normas mencionadas, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto del mismo.

2 MANDATO DE AUDITORÍA

2.1 Mandato

2.1.1 El Auditor de SI debe contar con un claro mandato para el desempeño de su función. Normalmente, este mandato es documentado en un estatuto de Auditoría que debe ser formalmente aprobado. En los casos en que exista un estatuto para la función de Auditoría, éste debe contener el mandato de Auditoría de SI.

2.2 Contenido del Mandato de Auditoría

2.2.1 El mandato de Auditoría debe abordar claramente los aspectos de responsabilidad, autoridad y rendición de cuentas. A continuación se exponen los aspectos a tener en cuenta.

2.2.2 Responsabilidad

- Declaración de Misión
- Propósitos/metas
- Alcance
- Objetivos
- Independencia
- Relación con la Auditoría externa
- Requerimientos del auditado
- Factores críticos del éxito
- Indicadores clave del desempeño
- Otras medidas de desempeño
- Autoridad
- Evaluación de riesgos
- Derecho de acceso a la información, el personal, las instalaciones y los sistemas relacionados con la realización de las auditorías
- Alcance o limitaciones al alcance
- Funciones a auditar
- Expectativas del auditado
- Estructura organizacional, con inclusión de las líneas de comunicación jerárquica con el Directorio y la gerencia senior
- Orden jerárquico del personal de Auditoría de SI

2.2.4 Rendición de cuentas

- Líneas de comunicación jerárquica con la gerencia senior
- Evaluaciones del cumplimiento de las tareas
- Evaluaciones del desempeño del personal
- Desarrollo de carrera/Dotación de personal
- Derechos de los auditados
- Revisiones de calidad independientes
- Evaluación del cumplimiento de las normas
- Benchmarking del desempeño y las funciones
- Evaluación de la ejecución del plan de Auditoría
- Comparación del presupuesto con los costos reales
- Medidas acordadas ; por ej., sanciones ante el incumplimiento de responsabilidades por alguna de las partes

2.3 Comunicación con los Auditados

2.3.1 La comunicación eficaz con los auditados implica

- Describir el servicio, su alcance, su disponibilidad y la oportunidad de su prestación
- Suministrar estimaciones de costos o presupuestos
- Describir los problemas y las posibles soluciones de los mismos
- Suministrar instalaciones adecuadas y prontamente accesibles para la comunicación eficaz
- Determinar la relación entre el servicio ofrecido y las necesidades del auditado

2.3.2 El mandato de Auditoría constituye una sólida base para la comunicación con los auditados y debe incluir referencias a los acuerdos de nivel de servicio con respecto a

- La disponibilidad para el trabajo imprevisto
- La entrega de informes
- Los costos
- La respuesta a las quejas del auditado
- La calidad del servicio
- La revisión del desempeño
- La comunicación con los auditados
- La evaluación de las necesidades
- La auto-evaluación de los riesgos de control
- El acuerdo sobre los términos de referencia para las Auditorías
- El proceso de presentación de informes

- El acuerdo sobre los hallazgos

2.4 Proceso de Garantía de Calidad

2.4.1 El Auditor de SI debe tener en cuenta la tarea de establecer un proceso de garantía de calidad (por ej., entrevistas, mediciones del nivel de satisfacción del cliente, mediciones del cumplimiento de las tareas, etc.) para comprender las necesidades y expectativas de los auditados relacionadas con la función de Auditoría de SI. Estas necesidades deben evaluarse en comparación con el mandato con miras a mejorar el servicio o a modificar la prestación del mismo o el estatuto de Auditoría, según corresponda.

3. TERMINOS DE REFERENCIA

3.1 Propósito

3.1.1 Los términos de referencia de la auditoría se utilizan frecuentemente para misiones específicas o para establecer el alcance y los objetivos de la relación entre la Auditoría Externa de SI y la organización.

3.2 Contenido

3.2.1 Los términos de referencia de la auditoría deben abordar claramente los aspectos de responsabilidad, autoridad y rendición de cuentas. A continuación se exponen los aspectos a tener en cuenta

3.2.2 Responsabilidad

- Alcance
- Objetivos
- Independencia
- Evaluación de riesgos
- Requerimientos específicos del auditado
- Resultados

3.2.3 Autoridad

- Derecho de acceso a la información, el personal, las instalaciones y los sistemas relacionados con la realización de las auditorías
- Alcance o limitaciones del alcance
- Evidencia de la aceptación de los términos de referencia y condiciones del contrato

3.2.4 Rendición de cuentas

- Destinatarios de los informes
- Derechos de los auditados
- Revisiones de calidad
- Fechas de finalización acordadas
- Presupuestos/honorarios acordados, si corresponde

4. FECHA DE VIGENCIA

4.1 Esta Directiva rige para todas las Auditorías de sistemas de información a partir del 1° de Septiembre de 1999.

APÉNDICE – GLOSARIO

Rendición de Cuentas de la Auditoría – medición de rendimiento de la prestación del servicio con inclusión del costo, la oportunidad y la calidad en comparación con los niveles de servicio acordados.

Autoridad de la Auditoría – la declaración de la posición dentro de la organización, con inclusión de las líneas de comunicación jerárquicas y los derechos de acceso.

Mandato de Auditoría **–** un documento que define la responsabilidad, autoridad y rendición de cuentas de la función de auditoría de SI.

Responsabilidad de la Auditoría – las funciones, el alcance y los objetivos documentados en el acuerdo de nivel de servicio entre la gerencia y la Auditoría.

Términos de Referencia – un documento formal que define la responsabilidad, autoridad y rendición de cuentas del Auditor de SI con respecto a una misión específica.

Information Systems Audit and Control Association

DIRECTIVA DE AUDITORIA DE SI

EFECTO DE LA PARTICIPACION EN EL PROCESO DE DESARROLLO, ADQUISICION, IMPLEMENTACION O MANTENIMIENTO EN LA INDEPENDENCIA DEL AUDITOR DE SI

1. ANTECEDENTES

1.1 Articulación con Normas

1.1.1 La Norma 020.010 (Independencia Profesional) determina que “En todos los asuntos relacionados con la auditoría, el Auditor de Sistemas de Información debe ser independiente del auditado en actitud y apariencia.”

1.1.2 La Norma 020.020 (Relación en la Organización) estipula que “La función de Auditoría de Sistemas de Información debe ser lo suficientemente independiente del área auditada como para permitir la realización objetiva de la auditoría.”

1.2 Necesidad de una Directiva

1.2.1 En muchas organizaciones, la Dirección, el personal de SI, los reguladores y las funciones de auditoría interna y externa esperan que los Auditores de SI participen en las iniciativas de desarrollo, adquisición o implementación de tecnología o sistemas de información nuevos o mejorados. La naturaleza de esta participación puede incluir, por ejemplo:

- Asignación o transferencia temporarias de tiempo completo de personal de Auditoría de SI al equipo del proyecto de sistemas
- Evaluación de controles en la etapa de diseño del sistema
- Realización de revisiones previas y posteriores a la implementación, desde una perspectiva de administración de usuarios
- Desempeño en calidad de consultores o revisores independientes con fines específicos

1.2.2 Tales servicios de consultoría de gestión constituyen una parte importante de la contribución del Auditor de SI a la educación y capacitación de otros miembros de la organización. Éstos hacen posible que los Auditores de SI utilicen su competencia y su conocimiento de la organización para brindar una contribución única y valiosa a la eficiencia y eficacia de las inversiones de la organización en nuevos sistemas. También brindan oportunidades para elevar el perfil de la función de Auditoría de SI y permitir al personal de Auditoría de SI capitalizar una experiencia práctica valiosa.

1.2.3 Sin embargo, cuando el Auditor de SI ha participado en el desarrollo, la adquisición, implementación o mantenimiento de un sistema nuevo o mejorado, y una auditoría se lleva a cabo con posterioridad, es probable que los destinatarios consideren que los hallazgos, recomendaciones y conclusiones de esa auditoría no son objetivos. En tales circunstancias, puede interpretarse que tanto la independencia cuanto la objetividad del Auditor de SI se han visto desvirtuadas por la participación mencionada.

1.2.4 El propósito de esta Directiva es proporcionar un marco que permita al Auditor de SI:

- Determinar en qué casos se requiere independencia
- Establecer en qué casos la independencia requerida puede ser, o parecer, desvirtuada
- Considerar posibles enfoques alternativos para el proceso de auditoría en los casos en que la independencia requerida es, o parece, desvirtuada
- Determinar los requisitos de divulgación para tales auditorías

1.2.5 Esta Directiva brinda una orientación para la correcta aplicación de las normas de auditoría de SI. El Auditor de SI debe tenerlo en cuenta al determinar cómo llevar a cabo la implementación de las normas citadas, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto del mismo.

2. MANDATO DE AUDITORÍA

2.1 Principios de la Participación del Auditor de SI

2.1.1 El Auditor de SI debe considerar la posibilidad de establecer conjuntamente con la gerencia los principios que regirán su participación en los proyectos de cambios del sistema. Tales principios deben ser documentados en el Mandato de Auditoría o en los Términos de Referencia. Esto debería tender a evitar la necesidad de elaborar nuevamente los principios para cada proyecto de desarrollo, adquisición, implementación o mantenimiento del sistema.

3. INDEPENDENCIA

3.1 Trabajo Ajeno a la Auditoría para el cual no se Requiere Independencia

3.1.1 La Norma de Auditoría de SI 020.010 requiere que el Auditor de SI sea independiente “en todos los asuntos relacionados con la auditoría”. No se requiere que el Auditor de SI sea, o parezca ser, independiente del equipo del proyecto de desarrollo, adquisición, implementación o mantenimiento del sistema cuando el tipo de trabajo requerido no es de auditoría. Los ejemplos de actividades ajenas a la auditoría cuya realización puede requerirse al Auditor de SI incluyen aquéllas que se llevan a cabo cuando:

- Se busca asesoramiento de Auditoría de SI sobre mejores prácticas
- Se solicita al Auditor de SI una variedad de alternativas de procedimientos aceptables, etc.
- Se solicita al Auditor de SI un Informe de los Requerimientos del Usuario, donde los requerimientos a especificar son aquellos relacionados con. la auditoría

pertinente del sistema (por ej., los requerimientos respecto de un módulo de auditoría incorporado)
- Se busca que el Auditor de SI ayude a definir los requerimientos del usuario final, a redactar la invitación para participar de una licitación, etc.
- Se busca la preferencia del Auditor de SI sobre una variedad de opciones
- El Auditor de SI lleva a cabo tareas operativas para asistir al equipo del proyecto bajo la dirección y control de un miembro del equipo; por ej., durante una asignación o transferencia temporarias de tiempo completo de personal de Auditoría de SI al equipo del proyecto
- El Auditor de SI cumple la función de dirigir el equipo del proyecto, o a algunos integrantes del mismo, por ej., después de haber sido transferido al equipo
- Se solicita al Auditor de SI que asista en el trabajo de programación
- El Auditor de SI participa en el diseño de la metodología integral de administración o desarrollo del proyecto que se aplica en la organización

3.1.2 Aunque no se requiere que el Auditor de SI sea independiente del equipo del proyecto cuando lleva a cabo las tareas citadas anteriormente, la objetividad sigue siendo un requisito profesional. Si se emprenden dichas tareas, el Auditor de SI debe llevarlas a cabo imparcial y objetivamente.

3.1.3 Si se considera que la asistencia solicitada podría disminuir la independencia y posteriormente se le asigna al Auditor de SI la realización de una auditoría de las actividades o productos del proyecto, éste debe advertir al usuario y a la gerencia de SI acerca de este punto. Asimismo, el Auditor de SI debe tener en cuenta, entre otros, los temas expuestos en la sección 3.3, más abajo.

3.2 Situaciones en las que se Requiere Independencia

3.2.1 El Auditor debe ser, y aparentar ser, independiente del equipo de un proyecto de desarrollo, adquisición, implementación o mantenimiento de un sistema y de los gerentes del mismo cuando se audita el desempeño del equipo. Esto puede ocurrir cuando:
- Se solicita específicamente una revisión o auditoría independiente, o se requiere legalmente, como en el caso de una auditoría externa de información financiera que incluya el aspecto de SI de tal auditoría
- El alcance de una revisión o auditoría incluye la revisión de la calidad de las decisiones o medidas que se hayan tomado, de la ejecución de las mismas o de los procesos requeridos para llevarlas a cabo
- Se requiere una opinión sobre la eficacia de la contribución al proyecto por parte de otro Auditor
- Los hallazgos del Auditor contribuirán a la puesta en funcionamiento de algún esquema de premios o castigos que afectará a los miembros del equipo del proyecto
- Se requiere que el Auditor apruebe el sistema en la etapa de aceptación

3.3 Opción de Disminución de la Independencia

3.3.1 En caso de que se le solicite asistir o colaborar con el equipo del proyecto, y no se requiriese la independencia del mismo para llevar a cabo la tarea solicitada (por ej. cuando la naturaleza de la asistencia es tal como se describió en la sección 3.1), el Auditor de SI debe tener en cuenta que si se le asignara posteriormente la realización de una auditoría de los productos o actividades del proyecto el desempeño de la asistencia solicitada podría considerarse como un factor de disminución de su independencia. En los casos en que esto sea previsible, y exista la posibilidad de que este hecho ocasione dificultades en una etapa posterior (por ejemplo si se requiere posteriormente una auditoría independiente y sólo se dispone de un Auditor de SI con las habilidades necesarias para llevar a cabo tanto la auditoría como la asistencia al proyecto), el Auditor de SI debe discutir este punto con los usuarios y la gerencia de SI antes de emprender la tarea de asistencia al proyecto.

3.3.2 Cuando los recursos son limitados, el equilibrio entre la provisión de asistencia al proyecto durante las actividades de desarrollo, adquisición, implementación y mantenimiento y la posterior realización de una auditoría independiente debe ser determinado por los usuarios y la gerencia de SI. Los puntos que más probablemente influirán en esta decisión son, entre otros, los siguientes:
- Recursos alternativos para cada función
- Comprensión por parte de la gerencia del valor relativo agregado por las actividades en conflicto
- Posibilidad de educar a los miembros de los equipos para mejorar el desempeño en proyectos futuros
- Oportunidades de desarrollo de carrera y planificación de sucesión para el Auditor de SI
- Nivel de riesgo asociado con las tareas de asistencia al proyecto. Esto puede resultar más relevante para un prestador externo de servicios de Auditoría de SI, en cuyo caso es probable que afecte también el costo
- Efecto en la visibilidad, el perfil, la imagen, etc., de la función de Auditoría de SI
- Efecto de la decisión en los requerimientos de los reguladores o auditores externos, si hubiere
- Las disposiciones del Mandato de Auditoría de SI o los términos y condiciones de referencia

3.3.3 En caso de que se acepte el trabajo de asistencia al proyecto, en la sección 4.4.1 de este documento se exponen alternativas de posible consideración durante la planificación de auditorías posteriores.

3.4 Ser, y Aparentar Ser, Independiente

3.4.1 Al realizar una auditoría de desarrollo, adquisición, implementación o mantenimiento de aplicaciones, o una auditoría anterior o posterior a la implementación de las mismas, el Auditor de SI debe mantener una actitud y una apariencia apropiadas para el logro de los objetivos de tales misiones.

3.4.2 Normalmente, esto requerirá que el Auditor de SI sea independiente de las siguientes personas:
- El Auditado (con inclusión del responsable del proceso de negocio relacionado con el sistema auditado, junto con su gerencia y personal)
- El equipo o los equipos de proyectos de desarrollo, adquisición, implementación y mantenimiento
- El patrocinador del proyecto

3.4.3 Durante el desarrollo, la adquisición, implementación o mantenimiento de un sistema de aplicación, el equipo del proyecto es responsable de aplicar las políticas y los procesos definidos por la gerencia (formal o informalmente) para estas actividades. Por lo general, estos procesos incluyen tanto el diseño como la implementación de controles del sistema y la administración y el monitoreo diarios del mismo proyecto. El

equipo del proyecto puede o no estar constituido por el mismo grupo de personas de que consta “el auditado”. Si son otras las personas involucradas, los Auditores de SI deben tener en cuenta la conservación de su independencia con respecto a ambos grupos.

3.4.4 El patrocinador del proyecto es responsable de las decisiones de alto nivel, como los cambios en el alcance y/o presupuesto del proyecto, y si se implementan o no. El patrocinador del proyecto puede o no ser el responsable del proceso de negocio o el auditado, o ambos. Cuando participan diferentes personas, los Auditores de SI deben tener en cuenta la conservación de su independencia con respecto a todas ellas.

3.4.5 Si un Auditor de SI que ha participado en un proyecto de desarrollo, adquisición, implementación o mantenimiento de un sistema de aplicación posteriormente (o simultáneamente) lleva a cabo un trabajo de auditoría relacionado con dicho sistema, los factores críticos que determinan si es o no independiente comprenden los siguientes puntos:

- Naturaleza, oportunidad y alcance de la participación de la Auditoría de SI en los procesos pertinentes de toma de decisiones del equipo o del patrocinador del proyecto, o de ambos
- Existencia de algún plan de premios o castigos basado en los resultados y/o la aprobación del proyecto que afecte individualmente al Auditor de SI o a la función de Auditoría de SI de manera general
- Capacidad del Auditor de SI de permanecer imparcial y objetivo mientras dirige la auditoría
- Autonomía del Auditor de SI para determinar el alcance y la conducción de la auditoría
- Buena disposición del Auditor de SI para comunicar puntos débiles o errores

3.4.6 Entre los factores críticos que determinan la apariencia independiente del Auditor de SI se encuentran los siguientes:

- Función desempeñada por el Auditor de SI, con inclusión de la toma de decisiones
- Conducta del Auditor de SI mientras lleva a cabo la auditoría
- Circunstancias que pueden interpretarse como una disminución de la independencia
- Divulgación de los datos mencionados por parte del Auditor de SI

3.5 Características de la Independencia

3.5.1 Al realizar una revisión de desarrollo, adquisición, implementación o mantenimiento de aplicaciones, o una revisión posterior a la implementación de las mismas, el Auditor de SI debe tener la libertad de determinar objetivamente, sin interferencias, los siguientes aspectos del trabajo:

- Alcance y oportunidad de la revisión
- Procedimientos a aplicar
- Personal y contratistas del proyecto/sistema a entrevistar
- Naturaleza, contenido y destinatarios del informe

3.5.2 El acuerdo sobre estos puntos con los usuarios y la gerencia de SI como una parte normal de la planificación de auditoría y el proceso de ejecución no constituye una falta de independencia siempre que el Auditor de SI tenga la libertad de aceptar o rechazar las recomendaciones de cambios realizadas por los mismos.

3.5.3 Asimismo, el Auditor de SI no debe padecer restricciones en lo que se refiere a la comunicación de puntos débiles o a la recomendación de controles y otras mejoras del sistema.

3.5.4 La independencia del Auditor de SI se vería desvirtuada si éste no tuviera la libertad de decidir sobre los elementos del trabajo mencionados, o advirtiera que la comunicación de los mismos estaría limitada por una renuencia a señalar problemas no identificados durante la ejecución del trabajo con el equipo del proyecto.

3.5.5 Las características mencionadas precedentemente se aplican aun en los casos en que la revisión se lleve a cabo en respuesta a una solicitud del patrocinador del proyecto.

4. PLANIFICACIÓN

4.1 Independencia

4.1.1 La independencia de la gerencia de Auditoría de SI y del personal asignado a la revisión debe ser considerada en la etapa de planificación.

4.2 Participaciones Anteriores que No Disminuyen la Independencia

4.2.1 La revisión anterior de un proyecto de desarrollo, adquisición, implementación o mantenimiento de aplicaciones puede no disminuir la capacidad del Auditor de SI para llevar a cabo una evaluación adecuadamente objetiva de la aplicación después de su implementación.

4.2.2 La participación del Auditor de SI, exclusivamente como miembro del personal del equipo del proyecto, en el diseño e implementación de módulos de sistema destinados al uso exclusivo de la función de auditoría (por ej., módulo de auditoría incorporado) no disminuye normalmente su objetividad.

4.2.3 La participación del Auditor de SI como miembro del equipo del proyecto sin responsabilidades operativas o de gestión (por ej., como observador, o como consultor experto, pero no como responsable de tomar decisiones) no disminuye normalmente su objetividad.

4.3 Participaciones Anteriores que Pueden Disminuir la Independencia

4.3.1 La independencia del Auditor de SI puede verse desvirtuada si éste participa, o ha participado, activamente en el desarrollo, la adquisición, implementación y/o mantenimiento del sistema de aplicación. Por ejemplo, si el Auditor de SI es, o ha sido, un miembro del equipo del proyecto con facultad para tomar decisiones (por ejemplo decisiones relativas a controles específicos), normalmente disminuirá su capacidad para llevar a cabo una revisión objetiva del desarrollo, la adquisición, implementación o mantenimiento del sistema de aplicación. Esto también puede disminuir la capacidad del Auditor de SI para llevar a cabo una evaluación objetiva del sistema de aplicación después de su implementación.

4.4 Alternativas en las cuales Disminuye la Independencia

4.4.1 En los casos en que se considere que la independencia del personal y/o la gerencia de Auditoría de SI resulta desvirtuada, el Auditor de SI debe tener en cuenta las siguientes opciones:

- Continuar con el personal y la gerencia de Auditoría de SI asignados, dando a conocer la participación anterior de manera completa y perceptible en el informe, junto con las medidas tomadas para mantener la objetividad
- Asignar otros gerentes y miembros del personal de la función de Auditoría de SI que no hayan participado en el proyecto, dando a conocer de igual manera si una sustitución total no es provechosa o práctica (por ej., si se requiere

que una persona con un gran conocimiento del sistema sea parte del equipo de auditoría con el fin de transmitir conocimientos al resto del equipo de manera eficaz en cuanto al costo)
- Asignar gerentes y personal que no pertenezcan a la función de Auditoría de SI, por ej., solicitar la transferencia de personal de otra función, de otro sector, de una organización externa, etc. Como ya se mencionó, esto puede constituir una sustitución parcial o total, siempre que la sustitución parcial estuviera acompañada de la divulgación apropiada. En estas circunstancias, la responsabilidad por la auditoría recaerá, como siempre, en la gerencia de auditoría
- Asignar un gerente adjunto, de cualquiera de las procedencias mencionadas, para que lleve a cabo una revisión de pares y actúe como árbitro independiente durante la planificación, el trabajo de campo y la preparación y presentación de informes
- Consultar a la persona que solicita la auditoría sobre la opción más conveniente para cumplir con sus requerimientos

5. PRESENTACIÓN DE INFORMES

5.1 Requerimientos de Divulgación

5.1.1 En los casos en que se vea desvirtuada la independencia del personal y/o la gerencia de Auditoría de SI, o el Auditor de SI considere que esto podría interpretarse así, éste debe dar a conocer, en el informe de auditoría, información suficiente sobre la disminución de la independencia con el fin de permitir que los destinatarios del informe comprendan tanto la magnitud de dicha disminución como las medidas tomadas para mitigar sus efectos. La información cuya divulgación debe tener en cuenta el Auditor de SI abarca los siguientes puntos:
- Nombres y antigüedad de los miembros del personal y la gerencia de Auditoría de SI que participan en la revisión
- Naturaleza, oportunidad y alcance de su participación en el proyecto
- Razones de su participación en la auditoría
- Medidas tomadas para garantizar que la objetividad no se haya visto materialmente desvirtuada en el transcurso del trabajo de auditoría y del proceso de presentación de informes

6. FECHA DE VIGENCIA

6.1 Esta Directiva rige para todas las auditorías de sistemas de información a partir del 1° de marzo de 2000.

APÉNDICE – GLOSARIO

Revisión de Adquisición de Aplicaciones – una evaluación de un sistema de aplicación referida a su adquisición o evaluación, la que examina las siguientes cuestiones: que dentro del sistema estén diseñados los controles adecuados; que la aplicación procese información de manera completa, exacta y confiable; que funcione según lo proyectado; que funcione de acuerdo con las disposiciones estatutarias aplicables; que el sistema se adquiera de acuerdo con el proceso de adquisición de sistemas establecido.

Revisión de Desarrollo de Aplicaciones – una evaluación de un sistema de aplicación en desarrollo que examina las siguientes cuestiones: que dentro del sistema estén diseñados los controles adecuados; que la aplicación procese información de manera completa, exacta y confiable; que funcione según lo proyectado; que funcione de acuerdo con las disposiciones estatutarias aplicables; que el sistema se desarrolle de acuerdo con el proceso de ciclo de vida de desarrollo de sistemas establecido.

Revisión de Implementación de Aplicaciones – una evaluación de alguna parte de un proyecto de implementación (por ej., administración del proyecto, planes de prueba, procedimientos de pruebas de aceptación del usuario)

Sistema de Aplicación – un conjunto integrado de programas informáticos diseñados para cumplir una función determinada que comprende actividades específicas de entrada, procesamiento y salida (por ej., contabilidad general, planificación de recursos industriales, administración de recursos humanos).

Revisión de Mantenimiento de Aplicaciones – una evaluación de alguna parte de un proyecto de mantenimiento de un sistema de aplicación (por ej., administración del proyecto, planes de pruebas, procedimientos de pruebas de aceptación del usuario).

Módulo de Auditoría Incorporado – parte integrante de un sistema de aplicación que es diseñada para identificar y comunicar transacciones específicas u otra información en base a criterios determinados previamente. La identificación de ítems a comunicar constituye una parte del procesamiento en tiempo real. La comunicación puede realizarse en línea en tiempo real, o utilizando métodos de almacenamiento y remisión (store and forward). También conocido como Instalación de Prueba Integrada o Módulo de Auditoría Continua.

Independencia – auto-gobierno, ausencia de conflicto de intereses e influencia indebida. El Auditor de SI debe tener libertad para tomar sus propias decisiones, sin ser presionado por la organización auditada y sus integrantes (gerentes y empleadores)

Apariencia Independiente – la impresión exterior de ser autónomo y estar libre de conflictos de intereses e influencia indebida.

Actitud Independiente – punto de vista imparcial que permite al Auditor de SI actuar objetivamente y con equidad.

Objetividad – capacidad de ejercer el buen juicio, expresar opiniones y plantear recomendaciones con imparcialidad.

Patrocinador del Proyecto – la persona responsable de las decisiones de alto nivel, como los cambios en el alcance y/o presupuesto del proyecto, y si proceder o no con la implementación.

Equipo del Proyecto – grupo de personas responsables de un proyecto, cuyos términos de referencia pueden incluir el desarrollo, la adquisición, la implementación o el mantenimiento de un sistema de aplicación. El equipo puede estar integrado por gerentes de línea, personal de línea operativa, contratistas externos y Auditores de SI.

Proceso de Adquisición de Sistemas – los procedimientos establecidos para adquirir software de aplicación, o una mejora, con inclusión de una evaluación de la estabilidad financiera del proveedor, su registro de trayectoria, sus recursos y las referencias aportadas por sus clientes actuales.

Proceso de Ciclo de Vida de Desarrollo de Sistemas – un enfoque utilizado para planificar, diseñar, desarrollar, probar e implementar un sistema de aplicación o una modificación del mismo.

DIRECTIVA DE AUDITORIA DE SI

DEBIDO CUIDADO PROFESIONAL

1. ANTECEDENTES

1.1 Articulación con Normas

1.1.1 La Norma 030.010 (Código de Ética Profesional) establece que "El Auditor de Sistemas de Información debe observar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información".

1.1.2 La Norma 030.020 (Debido Cuidado Profesional) establece que "Se debe proceder con el debido cuidado profesional y deben observarse las normas aplicables de auditoría profesional en todos los aspectos del trabajo del Auditor de Sistemas de información."

1.2 Necesidad de una Directiva

1.2.1 El propósito de esta Directiva es clarificar el término "debido cuidado profesional" según se aplica a la realización de una auditoría de acuerdo con las Normas 030.010 y 030.020 de Auditoría de Sistemas de Información.

1.2.2 Esta Directiva brinda orientación para la aplicación de las normas de auditoría de SI. El Auditor de SI debe tenerlo en cuenta al determinar cómo lograr la implementación de las Normas citadas, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto del mismo.

2. REALIZACIÓN DE LAS TAREAS DE AUDITORÍA

2.1 Debido Cuidado

2.1.1 La norma de "debido cuidado" es el nivel de diligencia con que procedería una persona providente y competente en circunstancias determinadas. El término "debido cuidado profesional" se aplica a un individuo que pretende ejercer una competencia particular como la auditoría de sistemas de información. El debido cuidado profesional requiere que el individuo ejerza dicha competencia en el nivel que comúnmente poseen los profesionales de esa especialidad.

2.1.1 El debido cuidado profesional se aplica al ejercicio del juicio profesional en la realización de las tareas. Este cuidado implica que el profesional debe abordar las cuestiones que requieren juicio profesional con la diligencia apropiada. A pesar del ejercicio del debido cuidado y juicio profesionales es probable que aún se presenten situaciones en que pueda llegarse a conclusiones inexactas a partir de una revisión diligente de los hechos y circunstancias disponibles. Por lo tanto, el eventual descubrimiento posterior de conclusiones erróneas no indica necesariamente un juicio profesional inadecuado o una falta de diligencia por parte del Auditor de SI.

2.1.2 El debido cuidado profesional debe extenderse a todos los aspectos de la auditoría, incluyendo la evaluación del riesgo de auditoría, la formulación de los objetivos, el establecimiento del alcance, la selección de las pruebas y la evaluación de los resultados de las mismas. Al proceder de este modo, el Auditor de SI debe determinar o evaluar :

- El tipo y nivel de los recursos de auditoría requeridos para alcanzar los objetivos de la misma
- La importancia de los riesgos identificados y su efecto potencial en la auditoría
- La evidencia de auditoría recopilada
- La competencia, la integridad y las conclusiones de otros individuos en cuyo trabajo deposita confianza el Auditor de SI

2.1.4 Los destinatarios previstos de los informes de auditoría esperan que el Auditor de SI ejerza el debido cuidado profesional durante todo el desarrollo de la auditoría. El Auditor de SI no debe aceptar una misión a menos que pueda disponer de personal con habilidades, conocimientos y otros recursos adecuados para llevar a cabo las tareas de la manera en que debe realizarlas un profesional.

2.1.5 El Auditor de SI debe llevar a cabo la auditoría con diligencia mientras que cumple con las normas profesionales aplicables. El Auditor de SI debe divulgar cualquier circunstancia de incumplimiento de estas normas profesionales de acuerdo con la comunicación de los resultados de la auditoría.

3. FECHA DE VIGENCIA

3.1 Esta Directiva rige para todas las auditorías de sistemas de información a partir del 1° de Septiembre de 1999.

APÉNDICE – GLOSARIO

Debido Cuidado – La diligencia con que procedería una persona en determinadas circunstancias.

Debido Cuidado Profesional – La diligencia con que procedería, en determinadas circunstancias, una persona que posea una aptitud particular.

Information Systems Audit and Control Association

DIRECTIVA DE AUDITORIA DE SI

CONSIDERACIONES DE AUDITORIA CON RESPECTO A LA OCURRENCIA DE IRREGULARIDADES

1.1 ANTECEDENTES

1.2 Articulación con Normas

1.1.1 La norma 030.020 (Debido Cuidado Profesional) establece que "Se debe proceder con el debido cuidado profesional y deben observarse las normas aplicables de auditoría profesional en todos los aspectos del trabajo del Auditor de Sistemas de Información."

1.1.2 La norma 050.010 (Planificación de la Auditoría) establece que "El Auditor de Sistemas de información debe planificar las tareas de auditoría de sistemas de información de manera que se aborden los objetivos de auditoría y se cumpla con las normas aplicables de auditoría profesional."

1.1.3 La norma 060.020 (Evidencia) establece que "En el transcurso de la auditoría, el Auditor de Sistemas de información debe obtener evidencia suficiente, confiable, pertinente y útil a fin de que se alcancen los objetivos de auditoría con eficacia. Los hallazgos y las conclusiones de la auditoría deben ser sustentados mediante el análisis y la interpretación adecuados de dicha evidencia."

1.1.4 La norma 070.010 (Contenido y Estructura de Informes) establece que "El Auditor de Sistemas de información debe proporcionar a los destinatarios correspondientes un informe – con una estructura apropiada –sobre la realización de las tareas de auditoría. En dicho informe deben constar el campo de aplicación, los objetivos, el período de aplicación y la naturaleza y alcance de las tareas de auditoría realizadas. El informe debe identificar la organización, los destinatarios correspondientes y cualquier restricción a su difusión; asimismo, debe exponer los hallazgos, las conclusiones y recomendaciones y cualquier reserva o restricción que tenga el auditor con respecto a la auditoría."

1.2 Necesidad de una Directiva

1.2.1 Algunos actos irregulares pueden ser considerados como actividades fraudulentas. Esto depende de la definición jurídica de fraude vigente en la jurisdicción que corresponda a la auditoría pertinente. Los actos irregulares comprenden, entre otros, la acción de pasar deliberadamente por alto ciertos controles con el objetivo de encubrir la perpetuación de un fraude, el uso no autorizado de bienes o servicios, etc., e incitar o ayudar a encubrir este tipo de actividades. Los actos irregulares no fraudulentos pueden incluir:

- Violaciones intencionales de la política de gestión establecida
- Violaciones intencionales de los requisitos reglamentarios
- Errores u omisiones deliberados de consignación de información concerniente al área auditada o a la organización en su conjunto
- Negligencia grave
- Actos ilícitos no intencionados

1.2.2 Este Lineamiento brinda una orientación para la correcta aplicación de las normas de auditoría de SI. El Auditor de SI debe tenerlo en cuenta al determinar cómo llevar a cabo la implementación de las normas citadas, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto del mismo.

2 MANDATO DE AUDITORÍA

2.2 Responsabilidades

2.1.1 El Auditor de SI debe tener en cuenta la tarea de definir en el estatuto de auditoría o carta de compromiso las responsabilidades de la gerencia y la función de auditoría con respecto a la prevención, detección y comunicación de actos irregulares, a fin de que sean claramente comprendidos para todas las tareas de auditoría. Cuando estas responsabilidades ya están documentadas en la política de fraude de la organización o documento similar, el estatuto de auditoría debe incluir una declaración a tal efecto.

2.1.2 La gerencia es responsable del diseño, la implementación y el mantenimiento de un sistema de controles internos que incluya la prevención y detección de fraudes.

2.1.3 El Auditor de SI es responsable de evaluar el riesgo de fraude y de diseñar y realizar pruebas adecuadas para la naturaleza de la misión de auditoría; asimismo, es razonable esperar que detecte:

- Actos irregulares que pudieran tener un efecto significativo en el área auditada o en la organización en su conjunto
- Debilidades en los controles internos que pudieran tener como resultado la imposibilidad de impedir o detectar tales actos

2.1.4 Una auditoría no puede garantizar la detección de actos irregulares. Esto puede ocurrir aun cuando la auditoría se planifica y lleva a cabo adecuadamente, por ejemplo, si existe connivencia entre empleados, o entre empleados y personas ajenas a la organización, o participación de la gerencia en los actos irregulares. Asimismo, el Auditor de SI debe tener en cuenta la tarea de documentar este punto en el Estatuto de Auditoría o carta de compromiso.

3 COMPETENCIA

3.2 Conocimiento en materia de fraude

3.1.1 El Auditor de SI debe ser lo suficientemente experto en materia de fraude como para poder identificar factores de riesgo que podrían contribuir a la ocurrencia de actos irregulares.

Information Systems Audit and Control Association

DIRECTIVA DE AUDITORIA DE SI

CONSIDERACIONES DE AUDITORIA CON RESPECTO A LA OCURRENCIA DE IRREGULARIDADES

4. PLANIFICACIÓN

4.1 Evaluación de Riesgos

4.1.1 El Auditor de SI debe evaluar el riesgo de ocurrencia de actos irregulares asociado al área auditada. Al preparar esta evaluación, el Auditor de SI debe tener en cuenta, entre otros, los siguientes factores:

- Características organizacionales, por ej., ética corporativa, estructura organizacional, adecuación de las estructuras de supervisión, compensación y gratificación, nivel de exigencia en el cumplimiento de las metas corporativas
- Antecedentes de la organización
- Cambios recientes en materia de gestión, operaciones o sistemas información
- El tipo de bienes producidos, o servicios ofrecidos, y la probabilidad específica de que sean afectados por la ocurrencia de actos irregulares
- Solidez de los controles pertinentes
- Requisitos reglamentarios o legales aplicables
- Historial de hallazgos de auditorías anteriores
- La industria y el ambiente competitivo en el que opera la organización
- Hallazgos de revisiones que se llevaron a cabo fuera del alcance de la auditoría como, por ejemplo, hallazgos de consultores, equipos de garantía de calidad o investigaciones de gestión específicas
- Hallazgos que han surgido en el transcurso normal de las actividades
- Sofisticación y complejidad técnicas del sistema o los sistemas de información que dan soporte al área auditada
- Existencia de sistemas de aplicaciones desarrollados/mantenidos internamente, en comparación con software comercial, para sistemas de negocio críticos

4.1.2 Al planificar las tareas de auditoría adecuadas para la naturaleza de la misión, el Auditor de SI debe utilizar los resultados de la evaluación de riesgos a fin de determinar la naturaleza, oportunidad y alcance de las pruebas requeridas para obtener evidencia de auditoría suficiente con el objeto de garantizar razonablemente que:

- Se identificarán los actos irregulares que pudieran tener un efecto significativo en el área auditada, o en la organización en su conjunto
- Se identificarán los puntos débiles del control que no pudieran prevenir o detectar la ocurrencia de actos irregulares significativos

5. REALIZACIÓN DE LAS TAREAS DE AUDITORÍA

5.1 Efecto de la Detección de Actos Irregulares

5.1.1 Si se detectan actos irregulares, el Auditor de SI deberá evaluar el efecto de estas actividades en los objetivos de auditoría y en la confiabilidad de la evidencia recopilada. Asimismo, el Auditor de SI deberá considerar si continúa o no con la auditoría en los casos en que:

- El efecto de los actos irregulares parece ser tan significativo que no puede obtenerse evidencia de auditoría confiable y suficiente
- La evidencia de auditoría sugiere que la gerencia participó en actos irregulares o que los ha condonado

5.2 Efecto de la Detección de Indicadores de Actos Irregulares

5.2.1 Si la evidencia de auditoría indica la probabilidad de ocurrencia de actos irregulares, el Auditor de SI debe:

- Recomendar a la gerencia que el asunto se investigue en detalle o que se tomen las medidas apropiadas. Si sospechara que la gerencia está involucrada en el acto irregular, el Auditor de SI deberá identificar dentro de la organización a la persona responsable adecuada a quien se deberían comunicar estas conclusiones. Si resultara imposible comunicarlas internamente, el Auditor de SI debería considerar la posibilidad de consultar al comité de auditoría y al departamento de asuntos legales acerca de la conveniencia y los riesgos de comunicar los hallazgos fuera de los límites de la organización
- Ejecutar acciones adecuadas a fin de sustentar los hallazgos, conclusiones y recomendaciones de la auditoría

5.3 Consideraciones Legales

5.3.1 Si la evidencia de auditoría indica que un acto irregular podría implicar una acción ilegal, el Auditor de SI debe recomendar que la gerencia solicite asesoramiento jurídico, o bien considerar la posibilidad de solicitarlo directamente.

6. PRESENTACIÓN DE INFORMES

6.1 Informes Internos

6.1.1 La detección de actos irregulares debe ser comunicada a las personas apropiadas de la organización de manera oportuna. La notificación debe ser dirigida a un nivel gerencial superior a aquél en el cual se sospecha la ocurrencia de los actos irregulares. Asimismo, los actos irregulares deben ser comunicados al directorio, al comité de auditoría, o a un cuerpo equivalente, a reserva de los asuntos manifiestamente insignificantes tanto con respecto a sus repercusiones financieras como a los puntos débiles

Information Systems Audit and Control Association

DIRECTIVA DE AUDITORIA DE SI

CONSIDERACIONES DE AUDITORIA CON RESPECTO A LA OCURRENCIA DE IRREGULARIDADES

del control que se detectan en consecuencia.

6.1.2 La distribución interna de los informes sobre actos irregulares debe ser considerada cuidadosamente. La ocurrencia y el efecto de los actos irregulares constituyen un tema crítico y la comunicación del mismo lleva consigo sus propios riesgos, con inclusión de:

- Un mayor abuso de los puntos débiles del control como resultado de la publicación de información detallada sobre los mismos
- Pérdida de clientes, proveedores e inversores al llevarse a cabo la divulgación (autorizada o no) fuera de la organización
- Pérdida de gerentes y personal clave, con inclusión de aquellas personas que no estuvieron involucradas en el acto irregular, al perderse la confianza en la gestión y en el futuro de la organización

6.1.3 El Auditor de SI debe considerar la posibilidad de comunicar la ocurrencia del acto irregular separadamente en relación con otras conclusiones de la auditoría si esto resulta útil para controlar la distribución del informe.

6.2 Informes Externos

6.2.1 La presentación de informes externos puede ser una obligación legal o reglamentaria. Esta obligación puede ser aplicable a la gerencia de la organización, o a los individuos que participaron en la detección de los actos irregulares, o a ambos.

6.2.2 En los casos en que se requiere la presentación de un informe externo, éste debe ser aprobado por el nivel apropiado de la gerencia de auditoría con anterioridad a su distribución externa; asimismo, debe ser revisado conjuntamente con la gerencia del auditado con antelación, a menos que lo impidan las reglamentaciones aplicables o circunstancias excepcionales de la auditoría. Los siguientes son ejemplos de circunstancias excepcionales que pueden impedir que se alcance el acuerdo de la gerencia del auditado:

- La participación activa de la gerencia del auditado en el acto irregular
- La aquiescencia pasiva de la gerencia del auditado frente al acto irregular

6.2.3 Si la gerencia del auditado no aprueba la distribución externa del informe, y la presentación de informes externos constituye una obligación estatutaria o reglamentaria, el Auditor de SI debe considerar la posibilidad de consultar al comité de auditoría y al departamento de asuntos legales acerca de la conveniencia y los riesgos de comunicar los hallazgos fuera de los límites de la organización.

6.2.4 El Auditor de SI, previa aprobación de la gerencia de auditoría, debe someter el informe a la consideración de los entes reguladores pertinentes de manera oportuna.

6.2.5 En los casos en que el Auditor de SI sepa que la gerencia debe informar de las actividades fraudulentas a una organización externa, éste debe notificar formalmente a la gerencia de su responsabilidad a este respecto.

6.2.6 Si un Auditor de SI que no forma parte del equipo de auditoría externa detectara la ocurrencia de un acto irregular, éste deberá considerar la posibilidad de someter el informe a la consideración de los auditores externos de manera oportuna.

6.3 Limitación del Alcance de Auditoría

6.3.1 En los casos en que se limite el alcance de la auditoría, el Auditor de SI debe incluir una explicación de la naturaleza y el efecto de esta limitación en el informe de auditoría. Una limitación de esta índole puede ocurrir si:

- El Auditor de SI no logra llevar a cabo el trabajo adicional que se considere necesario para alcanzar los objetivos originales de la auditoría y para sustentar las conclusiones de la misma, por ejemplo por falta de evidencia de auditoría confiable, insuficiencia de recursos o limitaciones impuestas por la gerencia a las actividades de auditoría
- La gerencia no lleva a cabo las investigaciones recomendadas por el Auditor de SI

7. FECHA DE VIGENCIA

7.1 Esta Directiva rige para todas las auditorías de sistemas de información a partir del 1° de marzo de 2000.

APÉNDICE – GLOSARIO

Actos Irregulares
Violaciones intencionales de la política de gestión o de los requisitos reglamentarios establecidos, errores u omisiones deliberados de consignación de información concerniente al área auditada o a la organización en su conjunto, negligencia grave o actos ilícitos no intencionados.

Copyright 1998
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows,IL 60008 USA
Telephone: +1.847.253.1545
Fax: +1.847.253.1443
Email: research@isaca.org
Web Site:http://www.isaca.org

DIRECTIVA DE AUDITORIA DE SI

PLANIFICACION DE LA AUDITORIA DE SI

1. ANTECEDENTES

1.1 Articulación con normas

1.1.1 La norma 050.010 (Planificación de Auditoría) estipula que “El auditor de sistemas de información debe planificar las tareas de auditoría de tal manera que se aborden los objetivos y se cumpla con las normas aplicables de auditoría profesional.”

1.2 Necesidad de una Directiva

1.2.1 El propósito de esta Directiva es definir el proceso de planificación según la Norma 050.010 de las Normas de Auditoría de Sistemas de Información e identificar los niveles de planificación y documentación del trabajo a realizar por los auditores de SI una vez aprobados los objetivos.

1.2.2 Esta Directiva expone de qué manera el auditor de SI debe cumplir con la norma citada anteriormente. El cumplimiento de este lineamiento no es obligatorio; no obstante, el auditor de SI debería estar preparado para justificar cualquier desviación respecto del mismo.

2. PLANIFICACIÓN

2.1 Conocimiento de la Organización

2.1.1 Antes de comenzar una auditoría, el trabajo del auditor de SI debe planificarse adecuadamente para cumplir con los objetivos de la misma. Como parte del proceso de planificación, los auditores de SI deben llegar a comprender la organización y sus procesos. Además de brindarle al auditor de SI un conocimiento de las operaciones de la organización y sus requerimientos de SI, esto lo asistirá en la determinación de los niveles de materialidad de los recursos de SI auditados en relación con los objetivos de la organización. Los auditores de SI también deben establecer el alcance de la auditoría y llevar a cabo una evaluación preliminar de control interno de la función auditada.

2.1.2 El grado de conocimiento de la organización y sus procesos requerido por el auditor de SI será determinado por la naturaleza de la organización y el nivel en el cual se lleva a cabo la auditoría. Una organización con operaciones complejas o poco comunes puede requerir que el auditor obtenga un mayor conocimiento de la misma que en el caso de una organización similar sin operaciones especializadas. Normalmente se requerirá un conocimiento más extenso de la organización y sus procesos cuando el objetivo de auditoría involucre una amplia variedad de funciones de sistema de información que cuando los objetivos están referidos a escasas funciones. Por ejemplo, una auditoría con el objetivo de evaluar el control del sistema de haberes de una organización normalmente requiere una comprensión más profunda de la misma que una auditoría con el objetivo de probar los controles de un sistema de biblioteca de programas específicos.

2.1.3 El auditor de SI debe llegar a comprender los distintos tipos de eventos, transacciones y prácticas que pueden tener un efecto significativo en la función auditada. El conocimiento de la organización debe incluir los riesgos de negocio y financieros con los que se enfrenta la misma, así como sus condiciones de mercado. El auditor de SI debe utilizar esta información al identificar problemas potenciales, al establecer el alcance del trabajo, al evaluar la evidencia de auditoría y al considerar las acciones de la gerencia a las que debe estar alerta.

2.2 Materialidad

2.2.1 Durante el proceso de planificación, el auditor de SI normalmente debe establecer niveles de materialidad de tal manera que el trabajo de auditoría sea suficiente para cumplir con los objetivos y utilice los recursos de auditoría con eficiencia. Por ejemplo, en la revisión de un sistema existente el auditor evalúa la materialidad de los diferentes componentes del sistema al planificar el programa de auditoría en lo que se refiere al contrato y las tareas de auditoría a realizar. A medida que aumenta el alcance de la auditoría es probable que se incremente el nivel de materialidad por encima del cual se identificarán todas las excepciones.

2.2.2 Debe realizarse una evaluación de riesgo para garantizar razonablemente que se cubrirán de manera adecuada los ítems materiales en el transcurso de las tareas de auditoría. Esta evaluación debe identificar las áreas con un riesgo relativamente alto de existencia de problemas materiales.

2.3 Programa de Auditoría

2.3.1 El programa preliminar para un contrato de auditoría debería ser establecido por los auditores de SI antes del comienzo de las tareas. Este programa de auditoría debe ser documentado de tal forma que permita al auditor de SI registrar la ejecución de las distintas partes de la auditoría e identificar el trabajo que queda por hacer. A medida que progresa el trabajo, el auditor de SI debe evaluar la adecuación del programa de auditoría en base a la información reunida en el transcurso de la misma y a la indicación de las áreas que podrían requerir un examen prolongado.

2.3.2 Además del listado de las tareas a realizar, el auditor puede preparar una lista de los recursos necesarios para concluir el trabajo, un cronograma de tareas y un presupuesto.

2.3.3 En el transcurso de las tareas el auditor de SI debe considerar la posibilidad de modificar el programa de auditoría en base a su evaluación de la adecuación del programa y sus hallazgos preliminares.

2.4 Evaluación de Control Interno

2.4.1 La mayor parte de los contratos de auditoría debe incluir una evaluación de control interno en forma directa como parte de los objetivos de la auditoría o como base para la confianza en la información reunida como parte de la misma. Cuando el objetivo es la

evaluación de los controles internos, el auditor de SI debe distinguir entre distintos tipos de contratos. Cuando el objetivo es evaluar la eficacia de los controles durante un período determinado el auditor incluirá procedimientos adecuados para cumplir con los objetivos de auditoría. Estos procedimientos pueden incluir pruebas de cumplimiento de los controles. Cuando el objetivo es identificar procedimientos de control en un momento dado, el plan puede ser menos extensivo.

2.4.2 Cuando se evalúa el control interno con el propósito de tener confianza en los procedimientos de control como respaldo a la información que se reúne como parte de la auditoría, el auditor de SI debería realizar una evaluación preliminar de control y desarrollar el plan de auditoría en base a la misma. Durante una auditoría, el auditor considerará la conveniencia de esta evaluación al determinar hasta qué punto se puede confiar en los controles durante las pruebas. Por ejemplo, al utilizar programas computarizados para probar archivos de datos el auditor de SI puede evaluar el control de las bibliotecas que contienen programas que se utilizan con fines de auditoría para determinar hasta qué punto los programas están protegidos contra modificaciones no autorizadas.

3. DOCUMENTACIÓN DEL PLAN

3.1 Documentos de trabajo de auditoría

3.1.1 El plan del auditor de SI debe ser documentado en documentos de trabajo de auditoría de tal manera que el auditor pueda determinar si se han llevado a cabo las etapas del plan.

3.1.2 El plan del auditor de SI puede ser documentado en papel o en alguna otra forma adecuada y recuperable.

4. FECHA DE VIGENCIA

4.1 Esta Directiva rige para todas las auditorías de sistemas de información a partir del 1° de junio de 1998.

APÉNDICE – GLOSARIO

Programa de Auditoría **–** Serie de etapas para alcanzar un objetivo de auditoría.

Control Interno – "Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que se alcanzarán los objetivos de negocio y se evitarán o detectarán y corregirán los eventos no deseados." (Fuente : Marco COBIT).

Materialidad – Una expresión de la trascendencia o importancia relativa de un asunto determinado en el contexto de la organización en su totalidad.

Copyright 1998
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows,IL 60008 USA
Web Site:http://www.isaca.org

Information Systems Audit and Control Association

DIRECTIVA DE AUDITORIA DE SI

CONCEPTOS DE MATERIALIDAD PARA LA AUDITORIA DE SISTEMAS DE INFORMACION

1. ANTECEDENTES

1.1 Articulación con Normas

1.1.1 La Norma 050.010 (Planificación de la Auditoría) establece que "El auditor de sistemas de información debe planificar las tareas de auditoría de tal manera que se aborden los objetivos pertinentes y se cumpla con las normas aplicables de auditoría profesional."

1.2 Necesidad de una Directiva

1.2.1 La Directiva sobre Planificación de la Auditoría de SI establece que "Durante el proceso de planificación, el auditor de SI normalmente debe establecer niveles de materialidad de tal manera que el trabajo de auditoría sea suficiente para cumplir con los objetivos de auditoría y utilice los recursos de auditoría con eficiencia." (Apartado 2.2.1)

1.2.2 Los auditores financieros normalmente miden la materialidad en términos monetarios, dado que lo que auditan también se mide e informa en estos términos. Los auditores de SI pueden auditar ítems no financieros, por ej., controles de acceso físico, controles de acceso lógico, controles de cambios a programas y sistemas para administración de personal, control industrial (o de fabricación), diseño, control de calidad, generación de contraseñas, producción de tarjetas de crédito y asistencia médica. Los auditores de SI pueden por tanto necesitar orientación sobre la manera en que debe evaluarse la materialidad en función de la planificación eficaz de sus auditorías, la concentración de su esfuerzo en las áreas de alto riesgo y la evaluación de la gravedad de los errores o puntos débiles encontrados.

1.2.3 Esta Directiva expone la manera en que el Auditor de SI debe cumplir con la norma 050.010 al evaluar materialidad para una auditoría de SI. El cumplimiento de este lineamiento no es obligatorio; no obstante, el auditor debería estar preparado para justificar cualquier desviación respecto del mismo.

2. PLANIFICACIÓN

2.1 Evaluación de la Materialidad

2.1.1 La evaluación de la materialidad constituye una cuestión de juicio profesional e implica considerar el efecto que pueden tener en toda la organización los errores, omisiones, actos irregulares y acciones ilegales que pueden surgir como consecuencia de los puntos débiles de control en el área auditada.

2.1.2 Al evaluar materialidad el auditor de SI debe tener en cuenta :

- El nivel global (acumulado) de error aceptable para la gerencia y el auditor de SI
- La posibilidad de que el efecto acumulativo de los pequeños errores o puntos débiles se torne significativo.

2.1.3 Al planificar un trabajo de auditoría suficiente como para alcanzar los objetivos pertinentes, el auditor de SI debe determinar, basándose en la materialidad, los controles a examinar. Con respecto a un objetivo de control específico, un control material se define como el control o grupo de controles sin los cuales los procedimientos de control no podrán garantizar razonablemente que se alcanzarán los objetivos.

2.1.4 Cuando el objetivo de auditoría de SI se relaciona con los sistemas u operaciones que procesan transacciones financieras, debe tenerse en cuenta el valor de los bienes controlados por el/los sistema/s o el valor de las transacciones procesadas por día/semana/mes/año al evaluar materialidad.

2.1.5 Cuando no se procesan transacciones financieras, deben tenerse en cuenta los siguientes ejemplos de medidas al evaluar materialidad

- Nivel crítico de los procesos de negocio a los que da soporte el sistema u operación
- Costo del sistema u operación (hardware, software, personal, servicios de terceros, gastos generales o una combinación de estos ítems)
- Costo potencial de los errores (probablemente en términos de ventas perdidas, reclamos con garantía, costos de desarrollo irrecuperables, costo de publicidad requerido para avisos o notificaciones, costos de rectificación, costos de sanidad y seguridad, costos de producción innecesariamente elevados, grandes pérdidas, etc.)
- Total de accesos/transacciones/solicitudes (de información) procesados por período
- Naturaleza, oportunidad y alcance de los informes preparados y los archivos mantenidos
- Naturaleza y cantidad de artículos que se comercian (o en stock) [por ej., cuando los movimientos de stock se registran sin valores)
- Requisitos del acuerdo de nivel de servicio y costo de las sanciones potenciales
- Sanciones por incumplimiento de los requisitos legales y contractuales
- Sanciones por incumplimiento de los requisitos de seguridad y salud pública

3. PRESENTACIÓN DE INFORMES

3.1 Identificación de Problemas a Comunicar

3.1.1 Al determinar los hallazgos, conclusiones y recomendaciones a

comunicar, el auditor de SI debe tener en cuenta tanto la materialidad de los errores encontrados como la materialidad potencial de los errores que podrían surgir como resultado de los puntos débiles de control.

3.1.2 Cuando la auditoría es utilizada por la gerencia para obtener una declaración de garantía con respecto a los controles de SI, un juicio aprobatorio sobre la adecuación de los controles debería referirse a que los controles implementados están de acuerdo con las prácticas de control generalmente aceptadas para alcanzar los objetivos de control, sin ninguna debilidad de control material.

3.1.3 Una debilidad de control debe considerarse material, y por lo tanto comunicable, si la falta del mismo tiene como resultado la imposibilidad de garantizar razonablemente que se alcanzará el objetivo de control. Si en el transcurso de las tareas de auditoría se identifican debilidades de control materiales, el auditor de SI debería emitir un juicio con reservas o adverso sobre el objetivo de auditoría.

3.1.4 Teniendo en cuenta los objetivos de la auditoría, el auditor de SI debería comunicar a la gerencia las debilidades que no son materiales, especialmente cuando los costos para reforzar los controles son bajos.

4. FECHA DE VIGENCIA

4.1 Esta Directiva rige para todas las auditorías de sistemas de información a partir del 1° de septiembre de 1999.

APÉNDICE – GLOSARIO

Materialidad **–** una expresión de la significación o importancia relativa de un asunto determinado en el contexto de la organización en su totalidad.

Information Systems Audit and Control Association

LINEAMIENTO DE AUDITORIA DE SI

TERCERIZACION DE ACTIVIDADES DE SI

1. ANTECEDENTES

1.1 Articulación con Normas

1.1.1 La Norma 010.010 (Responsabilidad, Autoridad y Rendición de Cuentas) establece que “La responsabilidad, autoridad y rendición de cuentas de la función de auditoría de sistemas de información deben ser adecuadamente documentadas en un mandato de auditoría o en los términos de referencia de la misma.”

1.1.2 La Norma 050.010 (Planificación de la Auditoría) establece que “El Auditor de Sistemas de información debe planificar las tareas de auditoría de tal manera que se aborden los objetivos pertinentes y se cumpla con las normas aplicables de auditoría profesional.”

1.1.3 La Norma 060.020 (Evidencia) establece que “En el transcurso de la auditoría, el Auditor de Sistemas de información debe obtener evidencia suficiente, confiable, pertinente y útil a fin de que se alcancen los objetivos de auditoría con eficacia. Los hallazgos y las conclusiones de la auditoría deben ser sustentados mediante el análisis y la interpretación adecuados de dicha evidencia.”

1.2 Necesidad de un Lineamiento

1.2.1 Una organización (el usuario del servicio) puede delegar parcial o totalmente algunas o todas sus actividades de SI a un prestador externo de tales servicios (el prestador del servicio). Las actividades de SI que pueden tercerizarse comprenden funciones de SI como operaciones de centros de datos, seguridad y desarrollo y mantenimiento de sistemas de aplicación.

1.2.2 La responsabilidad de verificar el cumplimiento de los contratos, acuerdos y reglamentaciones queda a cargo del usuario del servicio.

1.2.3 Frecuentemente, los derechos de auditoría y la responsabilidad de auditar el cumplimiento no están bien clarificados. El propósito de este lineamiento es exponer el modo en que el Auditor de SI debe cumplir con las Normas 010.010, 050.010 y 060.020 en esta situación.

1.2.4 Este Lineamiento brinda una orientación para la correcta aplicación de las normas de auditoría de SI. El Auditor de SI debe tenerlo en cuenta al determinar cómo llevar a cabo la implementación de las normas mencionadas, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto del mismo.

2. MANDATO DE AUDITORÍA

2.1 Responsabilidad, Autoridad y Rendición de Cuentas

2.1.1 Cuando algún aspecto de la función de SI se terceriza en un prestador de servicios, éste debe incluirse en el alcance del mandato de auditoría.

2.1.2 En el mandato de auditoría debe constar claramente el derecho del Auditor de SI a

- Revisar el acuerdo entre el usuario y el prestador del servicio (antes o después de su puesta en vigencia)
- Llevar a cabo las tareas de auditoría que se consideren necesarias con relación a la función tercerizada
- Comunicar los hallazgos, las conclusiones y las recomendaciones a la gerencia del usuario del servicio

3. PLANIFICACIÓN

3.1 Indagación de Información

3.1.1 El Auditor de SI debe comprender la naturaleza, oportunidad y alcance de los servicios tercerizados.

3.1.2 El Auditor de SI debe establecer qué controles implementó el usuario del servicio para abordar el requerimiento de negocio “de garantizar que las funciones y responsabilidades de terceros estén claramente definidas, se cumplan y continúen satisfaciendo los requerimientos pertinentes” (Objetivo de Control de Alto Nivel de CobiT DS2).

3.1.3 Deben identificarse y evaluarse los riesgos relacionados con los servicios tercerizados.

3.1.4 El Auditor de SI debe evaluar hasta qué punto los controles del usuario del servicio garantizan razonablemente que se alcanzarán los objetivos de negocio y que se evitarán o detectarán y corregirán los eventos no deseados.

3.1.5 El Auditor de SI debe determinar hasta qué punto el acuerdo de tercerización contempla la realización de auditorías del prestador del servicio, y considerar si esta disposición es adecuada. Esto comprende la evaluación de la confianza potencial en cualquiera de las tareas de auditoría de SI que lleven a cabo los auditores internos del prestador del servicio o un tercero independiente contratado por el prestador.

3.2 Planificación

3.2.1 El Auditor de SI debe tener en cuenta la posibilidad de obtener adecuado asesoramiento jurídico de profesionales expertos.

3.2.2 El Auditor de SI debe evaluar los informes de auditoría que se hayan preparado anteriormente para el prestador del servicio y planificar las tareas de auditoría de sistemas de información a fin de abordar los objetivos de auditoría relacionados con el ambiente del prestador del servicio,

teniendo en cuenta la información obtenida durante la planificación.

3.2.3 Los objetivos de auditoría deben ser acordados con la gerencia del usuario del servicio antes de ser comunicados al prestador. Los cambios solicitados por el prestador deben ser acordados con la gerencia del usuario.

3.2.4 El Auditor de SI debe planificar las tareas de auditoría de sistemas de información a fin de cumplir con las normas aplicables de auditoría profesional, como si la auditoría se llevara a cabo en el ambiente del usuario del servicio.

4. REALIZACIÓN DE LAS TAREAS DE AUDITORÍA

4.1 Requisito de Evidencia de Auditoría

4.1.1 La auditoría debe llevarse a cabo como si el servicio fuera provisto en el ambiente de SI del usuario del servicio.

4.2 El Acuerdo con el Prestador del Servicio

4.2.1 El Auditor de SI debe verificar si

- Existe un acuerdo formal entre el prestador y el usuario del servicio
- El acuerdo de tercerización incluye una cláusula que establece claramente que el prestador del servicio está obligado a satisfacer todos los requisitos legales que se aplican a sus actividades y a cumplir con las leyes y normas relativas a las funciones que debe desempeñar en nombre del usuario del servicio.
- El acuerdo de tercerización estipula que las actividades realizadas por el prestador del servicio están sujetas a controles y auditorías como si fueran realizadas por el usuario del servicio.
- Los derechos de acceso de la auditoría están contemplados en el acuerdo con el prestador del servicio.
- Se implementan los Acuerdos de Nivel de Servicio (ANS) y se aplican procedimientos de monitoreo del desempeño**.**
- Se cumplen las políticas de seguridad del usuario del servicio.
- Los acuerdos de seguros de fidelidad del prestador del servicio son adecuados.
- Las políticas y los procedimientos del personal del prestador del servicio son adecuados.

4.3 Gestión de Servicios Tercerizados

4.3.1 El Auditor de SI debe verificar si

- Se controlan adecuadamente los procesos de Negocio que producen la información que se utiliza para monitorear el cumplimiento de los ANS
- De no haberse cumplido los ANS, el usuario del servicio ha buscado una solución y se ha considerado la posibilidad de tomar medidas correctivas para alcanzar el nivel de servicio acordado
- El usuario del servicio tiene la capacidad y la competencia para realizar el seguimiento y la revisión de los servicios prestados

4.4 Limitaciones al Alcance

4.4.1 En los casos en que el prestador del servicio no se muestra dispuesto a cooperar con el Auditor de SI, éste debe comunicar el problema a la gerencia del usuario del servicio.

5. PRESENTACIÓN DE INFORMES

5.1 Emisión y Aceptación del Informe

Al finalizar las tareas de auditoría, el Auditor de SI debe proporcionar un informe – con una estructura apropiada – a los usuarios previstos del servicio.

5.1.1 El Auditor de SI debe considerar la posibilidad de discutir el informe con el prestador del servicio antes de su emisión ; no obstante, el Auditor de SI no debería ser responsable de entregar el informe definitivo al prestador del servicio. Si éste ha de recibir una copia, la misma debería ser remitida por la gerencia del usuario del servicio.

5.1.2 El informe debe especificar cualquier restricción a la distribución que desee imponer el Auditor de SI o la gerencia del usuario del servicio. Por ejemplo, no se debe permitir que el prestador del servicio distribuya copias del informe entre otros usuarios de su servicio sin obtener permiso de la organización del Auditor de SI y, cuando corresponda, del usuario. Asimismo, el Auditor de SI debe considerar la inclusión de un apartado que excluya responsabilidad hacia terceros.

5.2 Limitaciones al Alcance

5.2.1 El informe de auditoría debe identificar claramente una limitación al alcance cuando se nieguen los derechos de acceso de la auditoría y debe explicar el efecto de esta limitación con respecto a la misma.

6. ACTIVIDADES DE SEGUIMIENTO

6.1 Efecto de Auditorías Anteriores

6.1.1 Como en el caso de las auditorías realizadas en el ambiente del usuario del servicio, el Auditor de SI debe solicitar información adecuada, tanto al usuario como al prestador del servicio, sobre hallazgos, conclusiones y recomendaciones pertinentes de auditorías anteriores. El Auditor de SI debe determinar si el prestador del servicio implementó medidas correctivas adecuadas en forma oportuna.

7. FECHA DE VIGENCIA

7.1 Este Lineamiento rige para todas las auditorías de sistemas de información a partir del 1° de Septiembre de 1999.

APÉNDICE – GLOSARIO

Tercerización – un acuerdo formal con un tercero para desempeñar una función de SI de una organización.

Acuerdo de Nivel de Servicio (ANS) – definición de medidas de rendimiento mínimo por las cuales, o por encima de las cuales, el servicio prestado se considera aceptable.

Prestador del Servicio – la organización que presta el servicio tercerizado.

Usuario del Servicio – la organización que utiliza el servicio tercerizado.

LINEAMIENTO DE AUDITORIA DE SI

REQUISITO DE EVIDENCIA DE AUDITORIA

1. ANTECEDENTES

1.1 Articulación con Normas

1.1.1 La Norma 060.020 (Evidencia) establece que “En el transcurso de la auditoría, el auditor de sistemas de información debe obtener evidencia suficiente, confiable, pertinente y útil a fin de que se alcancen los objetivos de auditoría con eficacia. Los hallazgos y las conclusiones de la auditoría deben ser sustentados mediante el análisis y la interpretación adecuados de dicha evidencia.”

1.2 Necesidad de un Lineamiento

1.2.1 El propósito de este Lineamiento es definir la palabra “evidencia” según se la utiliza en la Norma 060.020 de Auditoría de Sistemas de Información y abordar la suficiencia y el tipo de evidencia utilizada al auditar sistemas de información.

1.2.2 Este Lineamiento brinda orientación para la aplicación de las normas de auditoría de SI. El Auditor de SI debe tenerlo en cuenta al determinar cómo lograr la implementación de la Norma citada, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto del mismo.

2. PLANIFICACIÓN

2.1 Tipos de Evidencia de Auditoría

2.1.1 Al planificar las tareas de auditoría de SI, el Auditor de SI debe tener en cuenta el tipo de evidencia de auditoría a recopilar, su uso para alcanzar los objetivos de la misma y sus diferentes niveles de confiabilidad. Entre los factores a tener en cuenta se encuentran la independencia y las limitaciones de quien suministra dicha evidencia. Por ejemplo, la evidencia de auditoría corroborativa que aporta una persona independiente por lo general es más confiable que la evidencia presentada por la organización auditada. La evidencia física de auditoría generalmente es más confiable que las declaraciones de un individuo.

2.1.2 Los diferentes tipos de evidencia de auditoría cuya utilización debe tener en cuenta el auditor de SI comprenden :

- Procesos observados y existencia de ítems físicos
- Evidencia documental de auditoría
- Declaraciones
- Análisis

2.1.3 La evidencia física de auditoría puede incluir observaciones de actividades, características y funciones de sistemas de información, por ejemplo :

- Un inventario de los medios magnéticos ubicados en un centro de almacenamiento externo
- Un sistema de seguridad de un centro de cómputos en funcionamiento

2.1.4 La evidencia documental de auditoría, registrada en papel u otros medios, puede incluir :

- Resultados de extracciones de datos
- Registros de transacciones
- Listados de programas
- Facturas
- Registros (logs) de actividad y control
- Documentación de desarrollo de sistemas

2.1.5 Las declaraciones de las personas auditadas pueden constituir evidencia de auditoría, por ejemplo :

- Políticas y procedimientos escritos
- Diagramas de flujo de sistema
- Declaraciones escritas u orales

2.1.6 Los resultados del análisis de información mediante comparaciones, simulaciones, cálculos y razonamiento también pueden utilizarse como evidencia de auditoría. Son ejemplos :

- La realización de pruebas de rendimiento de los SI con el fin de compararlo con períodos anteriores u otras organizaciones
- La comparación de tasas de error entre aplicaciones, transacciones y usuarios

2.2 Disponibilidad de Evidencia de Auditoría

2.2.1 El Auditor de SI debe tener en cuenta el período durante el cual existe o está disponible la información al determinar la naturaleza, oportunidad y alcance de las pruebas sustantivas y, si corresponde, de las pruebas de cumplimiento. Por ejemplo, es probable que la evidencia de auditoría procesada por Intercambio Electrónico de Datos (Electronic Data Interchange), Procesamiento de Documentos por Imágenes (Document Image Processing) y sistemas dinámicos como planillas de cálculo no sea recuperable después de un período determinado si no se resguardan los archivos o no se controlan los cambios en los mismos.

2.3 Selección de Evidencia de Auditoría

2.3.1 El Auditor de SI debe planificar la utilización de la mejor evidencia de auditoría que pueda obtenerse de acuerdo con la importancia del objetivo de la auditoría y el tiempo y esfuerzo requeridos para la obtención de la evidencia.

2.3.2 Cuando la evidencia obtenida en forma de descripciones orales es crítica para la opinión o conclusión de la auditoría, el Auditor de SI debe considerar la posibilidad de obtener una confirmación documentada de las mismas, ya sea en papel o en otros medios.

3. REALIZACIÓN DE LAS TAREAS DE AUDITORÍA

3.1 Naturaleza de la Evidencia de Auditoría

3.1.1 La evidencia de auditoría debe ser suficiente, confiable, pertinente y útil para formar una opinión o respaldar los hallazgos y conclusiones del Auditor de SI. Si, a juicio del auditor, la evidencia de auditoría obtenida no cumple con estos criterios, éste debe obtener evidencia de auditoría adicional. Por ejemplo, es probable que un listado de programas no constituya suficiente evidencia de auditoría hasta que se recopile evidencia adicional para verificar que éste representa el programa concreto que se utiliza en el proceso de producción.

3.2 Recopilación de Evidencia de Auditoría

3.2.1 Los procedimientos utilizados para recopilar evidencia de auditoría varían de acuerdo con el sistema de información auditado. El Auditor de SI debe seleccionar el procedimiento más conveniente para el objetivo de auditoría. Deben tenerse en cuenta los siguientes :

- Solicitud de información
- Observación
- Inspección
- Confirmación
- Repetición de Desempeño (Reperformance)
- Monitoreo

3.2.2 Los procedimientos citados pueden aplicarse mediante la ejecución de procedimientos de auditoría manuales, técnicas de auditoría asistida por computadora o una combinación de ambos. Por ejemplo :

- Un sistema que utiliza totales de control manual para conciliar operaciones de entrada de datos podría proporcionar evidencia de auditoría de que se implementó el procedimiento de control mediante un informe adecuadamente conciliado y detallado. El Auditor de SI debe obtener evidencia de auditoría revisando y probando este informe ;
- Los registros detallados de las transacciones pueden estar disponibles solamente en formato computadorizado, requiriéndose que el Auditor de SI obtenga evidencia de auditoría mediante técnicas de auditoría asistida por computadora.

3.3 Documentación de Auditoría

3.3.1 La evidencia de auditoría reunida por el Auditor de SI debe ser adecuadamente documentada y organizada para respaldar sus hallazgos y conclusiones.

4. PRESENTACIÓN DE INFORMES

4.1 Limitación del Alcance

4.1.1 Si el Auditor de SI cree que no puede obtenerse suficiente evidencia de auditoría debe divulgarlo de manera consistente con la comunicación de los resultados de la misma.

5. FECHA DE VIGENCIA

5.1 Este Lineamiento rige para todas las auditorías de sistemas de información a partir del 1° de diciembre de 1998.

APÉNDICE – GLOSARIO

Evidencia de Auditoría – el Auditor de Sistemas de Información (Auditor de SI) recopila información en el transcurso de la auditoría de SI. La información utilizada por el Auditor de SI para alcanzar los objetivos de auditoría se denomina evidencia de auditoría (evidencia).

Evidencia de Auditoría Pertinente – la evidencia de auditoría es pertinente si se relaciona con los objetivos de auditoría y tiene una relación lógica con los hallazgos y conclusiones que sustenta.

Evidencia de Auditoría Confiable – la evidencia de auditoría es confiable si, a juicio del Auditor de SI, es válida, real, objetiva y sostenible.

Evidencia de Auditoría Suficiente – la evidencia de auditoría es suficiente si es completa, adecuada, convincente y si induce a otro Auditor de SI a sacar las mismas conclusiones.

Evidencia de Auditoría Útil – la evidencia de auditoría es útil si asiste a los Auditores de SI en el cumplimiento de los objetivos de auditoría.

Copyright 1998
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows,IL 60008 USA
Web Site:http://www.isaca.org

Information Systems Audit and Control Association

LINEAMIENTO DE AUDITORIA DE SI

DOCUMENTACION DE AUDITORIA

1. ANTECEDENTES

1.1 Articulación con Normas

1.1.1 La Norma 060.020 (Evidencia) establece que "En el transcurso de la auditoría, el auditor de sistemas de información debe obtener evidencia suficiente, confiable, pertinente y útil a fin de que se alcancen los objetivos de auditoría con eficacia. Los hallazgos y las conclusiones de la auditoría deben ser sustentados mediante el análisis y la interpretación adecuados de dicha evidencia."

1.1.2 La Norma 070.010 (Contenido y Estructura de Informes) determina que "El auditor de sistemas de información debe proporcionar a los destinatarios correspondientes un informe – con una estructura apropiada –sobre la realización de las tareas de auditoría. En dicho informe deben constar el campo de aplicación, los objetivos, el período de aplicación y la naturaleza y alcance de las tareas de auditoría realizadas. El informe debe identificar la organización, los destinatarios correspondientes y cualquier restricción a su difusión; asimismo, debe exponer los hallazgos, las conclusiones y recomendaciones y cualquier reserva o restricción que tenga el auditor con respecto a la auditoría."

1.2 Necesidad de un Lineamiento

1.2.1 El propósito de este Lineamiento es describir la documentación que debe preparar y retener el Auditor de SI para respaldar los resultados de la auditoría.

1.2.2 Este Lineamiento brinda orientación para la aplicación de las normas de auditoría de SI. El Auditor de SI debe tenerlo en cuenta al determinar cómo lograr la implementación de las Normas citadas, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto del mismo.

2. PLANIFICACIÓN

2.1 Contenido de la Documentación

2.1.1 La documentación de auditoría de sistemas de información es el registro de las tareas de auditoría realizadas y de la evidencia de auditoría que respalda los hallazgos y conclusiones del Auditor de SI. La documentación puede utilizarse con el fin de:

- Demostrar el grado de cumplimiento de las Normas de Auditoría de Sistemas de Información por parte del Auditor de SI
- Asistir en la planificación, realización y revisión de auditorías
- Facilitar las revisiones de terceros
- Evaluar el programa de garantía de calidad de la función de auditoría de SI
- Brindar apoyo en circunstancias tales como reclamos de indemnizaciones por seguros, casos de fraude y demandas judiciales
- Asistir en el desarrollo profesional del personal

2.1.2 La documentación debe incluir, como mínimo, un registro de :

- La planificación y preparación del alcance y los objetivos de auditoría
- El programa de auditoría
- Los pasos de auditoría ejecutados y la evidencia recopilada
- Los hallazgos, conclusiones y recomendaciones de auditoría
- Todo informe emitido como resultado de las tareas de auditoría
- La revisión de supervisión

2.1.3 El alcance de la documentación del Auditor de SI dependerá de las necesidades específicas de la auditoría. Ésta debe incluir :

- La comprensión del área a auditar y su ambiente por parte del Auditor de SI
- La comprensión de los sistemas de procesamiento de información y el ambiente de control interno por parte del Auditor de SI
- El autor y la fuente de la documentación de auditoría con la fecha de su finalización
- La evidencia de auditoría y la fuente de la documentación con la fecha de su finalización
- La respuesta a las recomendaciones por parte del auditado

2.1.4 La documentación debe incluir la información de auditoría requerida por ley, reglamentaciones gubernamentales o normas profesionales aplicables. La documentación debe ser clara, completa y comprensible para el revisor.

2.2 Custodia, Retención y Recuperación de Documentación

2.2.1 Deben implementarse políticas y procedimientos que garanticen la custodia y la retención apropiadas de la documentación que respalda los hallazgos y conclusiones de auditoría durante un período suficiente como para satisfacer los requisitos legales, profesionales y organizacionales.

2.2.2 La documentación debe ser ordenada, almacenada y protegida de un modo apropiado para los medios en que se retiene; asimismo, debe permanecer recuperable durante un período suficiente como para cumplir con las políticas y los procedimientos definidos anteriormente.

3. FECHA DE VIGENCIA

3.1 Este Lineamiento rige para todas las auditorías de sistemas de información a partir del 1° de Septiembre de 1999.

LINEAMIENTO DE AUDITORIA DE SI

EFECTO DE LOS CONTROLES ESENCIALES DE SI

1. ANTECEDENTES

1.1 Articulación con Normas

1.1.1 La Norma 060.020 (Evidencia) establece que “En el transcurso de la auditoría, el auditor de sistemas de información debe obtener evidencia suficiente, confiable, pertinente y útil a fin de que se alcancen los objetivos de auditoría con eficacia. Los hallazgos y las conclusiones de la auditoría deben ser sustentados mediante el análisis y la interpretación adecuados de dicha evidencia.”

1.1.1 Necesidad de un Lineamiento

1.2.1 La administración y el monitoreo de una organización, departamento o función tiene repercusiones en el modo en que funciona dicha organización, departamento o función, incluyendo la manera en que se aplican los controles. Este principio se aplica tanto al uso de SI como a una organización industrial, un departamento de cuentas a pagar o una función de tesorería.

1.2.2 La eficacia de los controles detallados de SI que se operan dentro de una organización está limitada por la eficacia de la administración y el monitoreo del uso de los sistemas de información de la organización en su totalidad. Esto es reconocido frecuentemente en los lineamientos para auditorías financieras, donde se reconoce el efecto de los controles “generales” del ambiente de SI en los controles de “aplicación” de los sistemas financieros. Por ejemplo, el Lineamiento de Auditoría del Reino Unido 3.2.407 (Auditoría en un Ambiente Computadorizado) establece que “Los controles generales sólidos contribuyen a que el auditor pueda obtener una garantía en relación con la eficacia de los controles de aplicación. Los controles generales poco satisfactorios pueden menoscabar los controles de aplicación sólidos o empeorar los controles de aplicación poco satisfactorios.”

1.2.3 “Objetivos de Control de Información y Tecnologías relacionadas” (CobiT), publicado por la Fundación de Auditoría y Control de Sistemas de Información, suministra un marco que puede ayudar al Auditor de SI a distinguir entre:

- Los controles detallados de SI que están directamente relacionados con el alcance de auditoría de SI
- Las características de la administración y el monitoreo de SI que contribuyen a que el Auditor de SI pueda obtener una garantía con relación a la eficacia de esos controles

1.2.4 La división entre controles generales y de aplicación fue diseñada específicamente para ser aplicada a las auditorías cuyo objetivo es determinar si la información financiera está libre de errores materiales (auditorías financieras).

1.2.5 En los casos en que los auditores internos y los consultores independientes llevan a cabo auditorías de SI, el objetivo y el alcance de auditoría son normalmente diferentes de los establecidos para las auditorías financieras. Los sistemas en uso constituyen una combinación de procesos manuales y computadorizados y los objetivos de control deben establecerse para todo el proceso, que puede abarcar más o menos que los registros contables. Por consiguiente, el marco de controles utilizado para las auditorías financieras puede no resultar adecuado para algunas auditorías de SI.

1.2.6 A fin de determinar el grado de eficacia de los controles detallados auditados, el Auditor de SI debe considerar la necesidad de evaluar la eficacia de la administración y el monitoreo de los sistemas de información, aun cuando tales cuestiones estén fuera del alcance acordado para la auditoría. El resultado de tal consideración puede oscilar entre una ampliación del alcance acordado y un informe en el que se consignen las limitaciones pertinentes.

1.2.7 La población total de controles de administración y monitoreo es amplia, y es probable que parte de estos controles no estén relacionados con el objetivo de auditoría específico. A fin de evaluar el riesgo de auditoría y determinar el enfoque de auditoría apropiado, es preciso que el Auditor de SI cuente con un método estructurado para determinar:

- Los controles de administración y monitoreo que están relacionados con el alcance y los objetivos de auditoría
- Los controles de administración y monitoreo que deben ser probados
- El efecto de los controles de administración y monitoreo pertinentes para la opinión de auditoría

Esto puede lograrse mediante un marco de controles específico para el uso de SI y la tecnología relacionada, que ayude al Auditor de SI a concentrarse en los controles clave que afectan las operaciones y los sistemas de información auditados.

1.2.8 Este Lineamiento brinda orientación para la aplicación de las normas de auditoría de SI. El Auditor de SI debe tenerlo en cuenta al determinar cómo lograr la implementación de la Norma citada, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación.

2. MARCO DE CONTROLES

2.1 Introducción

2.1.1 CobiT define “control” como “Las políticas, procedimientos, prácticas y estructuras organizacionales, diseñados para garantizar razonablemente que se alcanzarán los objetivos de negocio y se evitarán o detectarán y corregirán los eventos no deseados.” Para cada una de las auditorías de SI, el Auditor debe diferenciar entre aquellos controles

generales que afectan a todas las operaciones y sistemas de información (controles esenciales de SI) y los controles generales y de aplicación que operan en un nivel más específico (controles detallados de SI) a fin de concentrar el esfuerzo de auditoría en las áreas de riesgo relacionadas con el objetivo de auditoría de SI. El propósito del marco de controles descrito a continuación es asistir al Auditor de SI en la ejecución de este enfoque.

2.2 Controles Esenciales de SI

2.2.1 El término controles esenciales de SI está definido en el glosario. Son ejemplos de controles esenciales los controles de procesos de SI definidos en el dominio de Planificación y Organización y en el dominio de Monitoreo de CobiT, por ej., "PO1 – Definición de un Plan Estratégico de TI" y "M1 – Monitoreo de los Procesos". Los controles esenciales de SI constituyen un subconjunto de controles generales que se concentran en la administración y el monitoreo de los SI.

2.2.2 El efecto de los controles esenciales en las tareas del auditor de SI no está limitado a la confiabilidad de los controles de aplicación de los sistemas financieros. Los controles esenciales también afectan la confiabilidad de los controles detallados de SI sobre, por ejemplo, el desarrollo de programas, la implementación del sistema, la administración de la seguridad y los procedimientos de resguardo.

2.2.3 Una administración y un monitoreo de SI ineficaces (por ej., controles esenciales deficientes) debe alertar al Auditor de SI sobre la posibilidad de un alto riesgo de que los controles diseñados para operar en el nivel de detalle puedan ser ineficaces.

2.3 Controles Detallados de SI

2.3.1 El término controles detallados de SI está definido en el glosario. Están integrados por los controles de aplicación y aquellos controles generales no incluidos en los controles esenciales de SI. En el marco CobiT, éstos son los controles de adquisición, implementación, entrega y soporte de servicios y sistemas de información. Entre los diferentes ejemplos pueden citarse los controles referidos a los siguientes ítems:

- Implementación de paquetes de software
- Parámetros de seguridad del sistema
- Planificación de recuperación ante desastres
- Validación de la entrada de datos
- Preparación de informes de excepciones
- Cierre de cuentas de usuario posterior a una serie de tentativas nulas de acceso a las mismas.

Los controles de aplicación constituyen un subconjunto de controles detallados de SI. La validación de entrada de datos, por ejemplo, es tanto un control detallado de SI como un control de aplicación. La instalación y acreditación de sistemas (AI5) constituye un control detallado de SI, aunque no un control de aplicación.

2.3.2 Las relaciones entre los controles de SI están expuestas en el siguiente esquema:

Controles de SI
-Controles generales
-Controles esenciales de SI
-Controles detallados de SI
-Controles de aplicación

Asimismo, el Auditor de SI debe considerar el efecto de los controles que no se aplican a SI en el alcance y los procedimientos de auditoría.

2.4 Interacción de los Controles Esenciales y Detallados de SI

2.4.1 El marco CobiT divide los procesos de control de SI en cuatro dominios :

- Planificación y Organización
- Adquisición e Implementación
- Entrega y Soporte
- Monitoreo

2.4.2 La eficacia de los controles de los dominios de Planificación y Organización (PO) y Monitoreo (M) influye en la eficacia de los controles de los dominios de Adquisición e Implementación (AI) y Entrega y Soporte (ES). Una deficiente planificación, organización y monitoreo por parte de la gerencia conducirá a la ineficacia de los controles de adquisición, implementación y entrega y soporte de servicios. A la inversa, una buena planificación, organización y monitoreo puede identificar y corregir controles ineficaces de adquisición, implementación y entrega y soporte de servicios.

2.4.3 Por ejemplo, la eficacia de los controles detallados del proceso de "Adquisición y Mantenimiento de Software de Aplicación" (proceso AI2 de CobiT) depende del grado de suficiencia de los controles esenciales de SI de los siguientes procesos:

- "Definición de un Plan Estratégico de TI" (proceso PO1 de CobiT)
- "Administración de los Proyectos" (proceso PO10 de CobiT)
- "Administración de la Calidad" (proceso PO11 de CobiT)
- "Monitoreo de los Procesos" (proceso M1 de CobiT)

2.4.4 La auditoría de la adquisición de un sistema de aplicación debe incluir la identificación del efecto de la estrategia de SI, el enfoque de administración del proyecto, la administración de la calidad y el enfoque de monitoreo. En los casos en que, por ejemplo, la administración del proyecto sea deficiente, el Auditor de SI debe tener en cuenta:

- La planificación de tareas adicionales a fin de garantizar que el proyecto específico auditado se administre con eficacia
- La comunicación a la gerencia de los puntos débiles de los controles esenciales de SI

2.4.5 Otro ejemplo es que la eficacia de los controles detallados del proceso de "Garantía de la Seguridad de los Sistemas" (proceso DS5 de CobiT) depende del grado de suficiencia de los controles esenciales de los siguientes procesos:

- "Definición de la Organización y las Relaciones de TI" (proceso PO4 de CobiT)
- "Comunicación de los Objetivos y Directivas de la gerencia" (proceso PO6 de CobiT)
- "Evaluación de los Riesgos" (proceso PO9 de CobiT)
- "Monitoreo de los Procesos" (proceso M1 de CobiT)

2.4.6 La auditoría de la adecuación de los parámetros de seguridad de un sistema (por ej., UNIX, Windows NT, RACF, etc.) debe incluir el examen de las políticas de seguridad de la gerencia (PO6), la asignación de responsabilidades por la seguridad (PO4), los procedimientos de evaluación de riesgos (PO9) y los procedimientos para monitorear el cumplimiento de sus políticas de seguridad (M1). Aun cuando los parámetros no se ajusten a la opinión del Auditor de SI acerca de cuál es la "mejor práctica", éstos pueden considerarse adecuados a la luz del riesgo identificado por la gerencia y las políticas de gestión que rigen el modo en que debe abordarse dicho nivel de riesgo. En consecuencia, las recomendaciones de mejoras por parte de la auditoría deben referirse a la administración o a las políticas de riesgos, así como a los parámetros detallados.

3. PLANIFICACIÓN

3.1 Enfoque para los Controles Esenciales Pertinentes

3.1.1 El Lineamiento sobre Planificación de la Auditoría de SI

establece que el Auditor de SI debe llevar a cabo una evaluación preliminar de control de la función auditada." Esta evaluación preliminar debe incluir la identificación y evaluación de los controles esenciales pertinentes. Las pruebas de los controles esenciales de SI pueden tener lugar en un ciclo diferente de la auditoría específica que se esté llevando a cabo dado que por su naturaleza éstos abarcan diversos aspectos del uso de SI. El Auditor de SI debe por tanto considerar si puede dependerse de algún trabajo de auditoría anterior en esta área con el fin de identificar y evaluar estos controles.

3.1.2 Cuando las tareas de auditoría indican que los controles esenciales de SI son poco satisfactorios, el Auditor de SI debe tener en cuenta el efecto de este hallazgo en el enfoque planificado para alcanzar el objetivo de auditoría:

- Los controles esenciales sólidos pueden contribuir a que el Auditor de SI obtenga una garantía con relación a la eficacia de los controles detallados
- Los controles esenciales deficientes pueden menoscabar los controles detallados sólidos o empeorar los puntos débiles en el nivel detallado

3.2 Procedimientos de Auditoría Suficientes

3.2.1 Cuando los controles esenciales de SI tienen un efecto potencial significativo en el objetivo de auditoría, no basta planificar una auditoría que comprenda únicamente los controles detallados. Si no es posible o práctico auditar los controles esenciales debe comunicarse esta restricción del alcance.

3.2.2 El Auditor de SI debe planificar las pruebas de los controles esenciales pertinentes cuando esto contribuya a la consecución del objetivo de auditoría.

3.3 Controles Pertinentes

3.3.1 Los controles esenciales pertinentes son aquellos que influyen en los objetivos de auditoría específicos para la misión. Por ejemplo, cuando el objetivo de auditoría es informar sobre los controles de los cambios en una biblioteca de programas específica, los controles pertinentes serán los controles esenciales de SI relacionados con las políticas de seguridad (PO6) ; no obstante, es probable que no sean pertinentes los controles esenciales relacionados con la determinación de la orientación tecnológica (PO3).

3.3.2 Al planificar la auditoría, el Auditor de SI debe identificar qué parte de la población total de controles esenciales influye en los objetivos de auditoría específicos; asimismo, debe planificar la inclusión de los controles identificados en el alcance de auditoría. Los objetivos de control de CobiT para los dominios de "Planificación y Organización" y "Monitoreo" pueden ayudar al Auditor de SI a identificar los controles esenciales pertinentes.

3.4 Evidencia de Auditoría

3.4.1 Los controles esenciales de SI pueden no estar documentados; no obstante, el Auditor de SI debe planificar la obtención de evidencia de auditoría que corrobore que los controles pertinentes están operando con eficacia. Las pruebas que pueden realizarse están expuestas en la sección sobre Realización de las Tareas de Auditoría.

3.5 Enfoque para los Controles Detallados Pertinentes

3.5.1 En los casos en que el trabajo de auditoría de SI indique que los controles esenciales son satisfactorios, el Auditor de SI debe considerar la posibilidad de reducir el nivel de pruebas planificado para los controles detallados, dado que la evidencia de auditoría de los controles esenciales sólidos contribuirá a que el Auditor de SI pueda obtener una garantía con relación a la eficacia de los controles detallados de SI.

3.5.2 En los casos en que el trabajo de auditoría de SI indique que los controles esenciales no son satisfactorios, el Auditor de SI debe llevar a cabo pruebas suficientes de los controles detallados, a fin de suministrar evidencia de auditoría que corrobore que éstos están operando con eficacia pese a las deficiencias de los controles esenciales pertinentes.

4. REALIZACIÓN DE LAS TAREAS DE AUDITORÍA

4.1 Pruebas de Controles Esenciales de SI

4.1.1 El Auditor de SI debe llevar a cabo suficientes pruebas como para garantizar que los controles esenciales pertinentes operaron con eficacia durante el período de auditoría o en un momento determinado. Entre los procedimientos de pruebas que pueden resultar apropiados se encuentran los siguientes:

- Observación
- Averiguaciones corroborativas
- Revisión de documentación pertinente (políticas, normas, actas de reuniones, etc.)
- Nueva ejecución (por ejemplo utilizando CAATs)

4.1.2 Si las pruebas de los controles esenciales pertinentes indican que éstos son satisfactorios, el Auditor de SI debe proceder con la auditoría planificada de los controles detallados de SI que son directamente aplicables al objetivo de auditoría. El nivel de dichas pruebas puede ser menor que el que sería apropiado si los controles esenciales de SI no estuvieran operando satisfactoriamente.

5. PRESENTACIÓN DE INFORMES

5.1 Puntos Débiles de los Controles Esenciales de SI

5.1.1 En los casos en que el Auditor de SI identifique puntos débiles en los controles esenciales de SI, éstos deben ser comunicados a la gerencia, aun cuando el examen de tales áreas no hubiera sido identificado específicamente en el alcance de tareas acordado.

5.2 Limitaciones del Alcance

5.2.1 En los casos en que los controles esenciales de SI pudieran tener un efecto potencial significativo en el grado de eficacia de los controles detallados de SI, y estos controles esenciales no hubieran sido auditados, el Auditor de SI debe comunicar este hecho a la gerencia en el informe final, junto con una declaración acerca de su efecto potencial en los hallazgos, conclusiones y recomendaciones de auditoría. Por ejemplo, cuando prepara un informe sobre una auditoría de adquisición de software comercial, pero no conoce la estrategia de SI de la organización, el Auditor debe consignar que la estrategia de SI no fue puesta a su disposición o no existe. Cuando corresponda, el Auditor de SI debe asimismo informar del efecto potencial en los hallazgos, conclusiones y recomendaciones de auditoría, por ejemplo, indicando que debido a lo expuesto no es posible establecer si la adquisición del paquete de soluciones es consecuente con la estrategia de SI y si respaldará los futuros planes de negocio.

6. FECHA DE VIGENCIA

6.1 Este Lineamiento rige para todas las auditorías de sistemas de información a partir del 1° de marzo de 2000.

APÉNDICE – GLOSARIO

Controles de Aplicación –Estos controles se refieren a las transacciones y los datos permanentes relacionados con cada uno de los sistemas de aplicación computadorizados y, por consiguiente, son específicos para cada una de dichas aplicaciones. El objetivo de los controles de aplicación, que pueden ser manuales o programados, es garantizar la totalidad y exactitud de los registros y la validez de las entradas ejecutadas como resultado del procesamiento, tanto manual como programado. Entre los ejemplos de controles de aplicación se encuentran la validación del ingreso de datos, la conciliación de totales de lote y la encriptación de los datos transmitidos.

CAATs - (Técnicas de Auditoría Asistida por Computadora) – Son técnicas de auditoría automatizadas, por ejemplo el software de auditoría de propósitos generales, el software utilitario, los datos de prueba, el rastreo y registro de software de aplicación y los sistemas expertos de auditoría.

Controles Detallados de SI – Son los controles aplicados a la adquisición, implementación, entrega y soporte de servicios y sistemas de información. Están integrados por los controles de aplicación y aquellos controles generales no incluidos en los controles esenciales.

Controles Generales – Son controles que, además de los de aplicación, tienen que ver con el ambiente en el cual se desarrollan, mantienen y operan los sistemas de aplicación computadorizados y, en consecuencia, son aplicables a todas las aplicaciones. El objetivo de los controles generales es garantizar el desarrollo y la implementación adecuados de las aplicaciones y la integridad de los archivos de datos y programas y de las operaciones computadorizadas. Del mismo modo que los controles de aplicación, los controles generales pueden ser manuales o programados. Entre los diferentes ejemplos de controles generales se encuentran el desarrollo y la implementación de una estrategia y una política de seguridad de SI, la organización del personal de SI destinada a segregar funciones y la planificación de prevención y recuperación ante desastres.

Controles Esenciales de SI – Son aquellos controles generales diseñados para administrar y monitorear el ambiente de SI y, en consecuencia, afectan a todas las actividades relacionadas con los mismos.

Information Systems Audit and Control Association

LINEAMIENTO DE AUDITORIA DE SI

MUESTREO DE AUDITORIA

1. ANTECEDENTES

1.1 Articulación con Normas

1.1.1 La Norma 060.020 (Evidencia) establece que “En el transcurso de la auditoría, el auditor de sistemas de información debe obtener evidencia suficiente, confiable, pertinente y útil a fin de que se alcancen los objetivos de auditoría con eficacia. Los hallazgos y las conclusiones de la auditoría deben ser sustentados mediante el análisis y la interpretación adecuados de dicha evidencia.”

1.2 Necesidad de un Lineamiento

1.2.1 El propósito de este Lineamiento es brindar orientación al Auditor de SI a fin de diseñar y seleccionar una muestra de auditoría y evaluar los resultados de la misma. El muestreo y la evaluación deberán cumplir con los requisitos de “evidencia suficiente, confiable, pertinente y útil” y deberán ser “respaldados por un análisis adecuado”.

1.2.2 El Auditor de SI debe tener en cuenta diferentes técnicas de selección a fin de obtener una muestra representativa basada en estadísticas para llevar a cabo pruebas de cumplimiento o sustantivas.

1.2.3 Entre los ejemplos de pruebas de cumplimiento de controles en las que puede tenerse en cuenta el muestreo se encuentran los derechos de acceso del usuario, los procedimientos de control de cambios en programas, la documentación de procedimientos, la documentación de programas, el seguimiento de excepciones, la revisión de registros, las auditorías de licencias de software, etc.

1.2.4 Entre los ejemplos de pruebas sustantivas en las que puede tenerse en cuenta el muestreo se encuentran la nueva ejecución de un cálculo complejo (por ej., interés) en una muestra de cuentas, una muestra de transacciones para refrendar una documentación de respaldo, etc.

1.2.5 Este Lineamiento brinda orientación para la aplicación de las normas de auditoría de SI. El Auditor de SI debe tenerlo en cuenta al determinar cómo lograr la implementación de la Norma citada, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto del mismo.

1.2.6 Otras referencias útiles sobre Muestreo de Auditoría incluyen la Norma Internacional sobre Auditoría N° 530, Muestreo de Auditoría y otros Procedimientos de Pruebas Selectivas, emitida por la Federación Internacional de Contadores (IFAC).

2. REALIZACIÓN DE LAS TAREAS DE AUDITORÍA

1.1 Muestreo de Auditoría

2.1.1 Al utilizar métodos de muestreo estadístico o no estadístico, el Auditor de SI debe diseñar y seleccionar una muestra de auditoría, ejecutar procedimientos de auditoría y evaluar los resultados de las muestras para obtener evidencia suficiente, confiable, pertinente y útil.

2.1.2 Al formarse una opinión, los Auditores de SI frecuentemente no examinan toda la información disponible ya que ésta puede ser poco práctica y se puede llegar a conclusiones válidas mediante el muestreo de auditoría.

2.1.3 El muestreo de auditoría se define como la aplicación de procedimientos de auditoría a menos del 100% de la población, a fin de permitir que el Auditor de SI evalúe la evidencia sobre alguna característica de los ítems seleccionados para llegar a una conclusión – o asistir en la obtención de una conclusión – referida a la población

2.1.4 El muestreo estadístico implica la utilización de técnicas mediante las cuales pueden obtenerse conclusiones fundamentadas matemáticamente con respecto a la población.

2.1.5 Los resultados del muestreo no estadístico no deben extrapolarse a la población puesto que es improbable que la muestra sea representativa de la misma.

1.2 Diseño de la Muestra

2.2.1 Al diseñar la amplitud y estructura de una muestra de auditoría, los Auditores de SI deben tener en cuenta los objetivos de auditoría específicos, la naturaleza de la población y los métodos de muestreo y selección.

2.2.2 El Auditor de SI debe considerar la necesidad de convocar a especialistas adecuados para el diseño y análisis de las muestras.

2.2.3 Unidad de Muestreo – La unidad de muestreo dependerá del propósito de la muestra. Para las pruebas de cumplimiento de los controles se utiliza normalmente el muestreo por atributo, donde la unidad de muestreo es un evento o transacción (por ej., un control como la autorización de una factura). Para las pruebas sustantivas se utiliza frecuentemente el muestreo de variables o por estimación, donde la unidad de muestreo es normalmente monetaria.

2.2.4 Objetivos de auditoría – El Auditor de SI debe tener en cuenta los objetivos específicos de la auditoría y los procedimientos más apropiados para alcanzar dichos objetivos. Asimismo, cuando el muestreo de auditoría es adecuado, debe considerarse la naturaleza de la evidencia de auditoría buscada y las posibles condiciones de error.

2.2.5 Población – La población es el conjunto de todos los datos a partir de los cuales el Auditor de SI desea obtener una muestra para llegar a una conclusión sobre la misma. Por consiguiente, la población de la cual se toma la muestra deberá ser adecuada y

verificarse como completa para el objetivo de auditoría específico.

2.2.6 Estratificación – La estratificación puede ser apropiada para asistir en el diseño eficiente y eficaz de la muestra. La estratificación es el proceso de división de una población en subpoblaciones con características similares definidas explícitamente de tal manera que cada unidad de muestreo pueda incluirse en un solo estrato.

2.2.7 Amplitud de la muestra – Al determinar la amplitud de la muestra, el Auditor de SI debe tener en cuenta el riesgo de muestreo, el grado de error aceptable y hasta qué punto están previstos los errores.

2.2.8 Riesgo de muestreo – El riesgo de muestreo surge de la posibilidad de que la conclusión del Auditor de SI difiera de la conclusión a la que se llegaría si toda la población estuviera sujeta al mismo procedimiento de auditoría. Hay dos tipos de riesgo de muestreo.

- El riesgo de aceptación incorrecta, que es el riesgo de que se considere improbable la ocurrencia de un error material cuando en realidad existe un error material en la población.
- El riesgo de rechazo incorrecto, que es el riesgo de que se considere probable la ocurrencia de un error material cuando en realidad no hay errores materiales en la población.

2.2.9 La amplitud de la muestra es afectada por el nivel de riesgo de muestreo que el Auditor de SI está dispuesto a aceptar. Asimismo, el riesgo de muestreo debe considerarse en relación con el modelo de riesgo de auditoría y sus componentes, el riesgo inherente, el riesgo de control y el riesgo de detección.

2.2.10 Error tolerable – El error tolerable es el máximo error que los Auditores de SI están dispuestos a aceptar en la población y a pesar del cual concluyen que se logró el objetivo de auditoría. En cuanto a las pruebas sustantivas, el error tolerable está relacionado con el juicio que emita el Auditor de SI con respecto a su materialidad. En lo que se refiere a las pruebas de cumplimiento, es el máximo índice de desviación que el Auditor de SI está dispuesto a aceptar con relación a un procedimiento de control prescrito.

2.2.11 Error esperado – Si el Auditor de SI prevé la ocurrencia de errores en la población normalmente deberá examinar una muestra más grande que en el caso de que no se prevean errores, a fin de concluir que el error real en la población no es mayor que el error tolerable proyectado. Se podrán utilizar muestras más pequeñas cuando se prevea que la población estará libre de errores. Al determinar el error esperado en una población, el Auditor de SI debe considerar asuntos tales como los niveles de error identificados en auditorías anteriores, los cambios en los procedimientos de la organización y la evidencia disponible a partir de una evaluación del sistema de control interno y los resultados de procedimientos de revisión analíticos.

2.3 Selección de la Muestra

2.3.1 Comúnmente se utilizan cuatro métodos de muestreo:

Métodos de Muestreo Estadístico

- Muestreo al azar – garantiza que todas las combinaciones de unidades de muestreo de la población tengan igual probabilidad de selección
- Muestreo sistemático – implica la selección de unidades de muestreo mediante un intervalo constante entre las selecciones, requiriéndose que el primer intervalo tenga un inicio al azar. Son ejemplos de muestreo sistemático el Muestreo de Unidades Monetarias o Selección Ponderada de Valores donde a cada uno de los valores monetarios (por ej., $1) de la población se le asigna la misma probabilidad de selección. Dado que normalmente no se puede analizar cada una de las unidades monetarias por separado, se selecciona y analiza el ítem que incluye la unidad monetaria. Este método inclina sistemáticamente la selección hacia las cantidades más grandes, no obstante asignando a cada valor monetario una idéntica probabilidad de selección. Otro ejemplo es la selección de unidades de muestreo a intervalos constantes.

Métodos de Muestreo no Estadístico

- Muestreo fortuito – en el cual el Auditor de SI selecciona la muestra sin seguir una técnica estructurada, no obstante evitando cualquier parámetro o previsión conscientes. Sin embargo, no se debe depender del análisis de una muestra fortuita para obtener una conclusión sobre la población.
- Muestreo discrecional – en la cual el Auditor de SI fija un parámetro para la muestra (por ej., todas las unidades de muestreo sobre un valor determinado, todas para un tipo específico de excepción, todas negativas, todas de nuevos usuarios, etc.). Debe observarse que una muestra discrecional no se basa en estadísticas y los resultados no deben extrapolarse a la población puesto que es improbable que la muestra sea representativa de la misma.

2.3.2 El Auditor de SI debe seleccionar ítems de muestra de tal manera que pueda esperarse que ésta sea representativa de la población con relación a las características probadas, por ej., utilizando métodos de muestreo estadístico. A fin de mantener la independencia de la auditoría, el Auditor de SI debe garantizar que la población sea completa y también debe controlar la selección de la muestra.

2.3.3 Para que una muestra sea representativa de la población, todas las unidades de muestreo de la misma deberán tener igual probabilidad – o una probabilidad conocida – de ser seleccionadas, por ej., en los métodos de muestreo estadístico.

2.3.4 Comúnmente se utilizan dos métodos de selección: la selección sobre registros y la selección sobre campos cuantitativos (por ej., unidades monetarias).

Para la selección sobre registros, los métodos más comunes son:

- Muestra al azar (muestra estadística)
- Muestra fortuita (no estadística)
- Muestra discrecional (no estadística; alta probabilidad de que no pueda llegarse a una conclusión objetiva)

Para la selección sobre campos cuantitativos, los métodos más comunes son:

- Muestra al azar (muestra estadística sobre unidades monetarias)
- Muestra a intervalos constantes (muestra estadística utilizando un intervalo constante)
- Muestra por celda (muestra estadística utilizando la selección al azar en un intervalo)

2.4 Documentación

2.4.1 Los documentos de trabajo de auditoría deben ser lo suficientemente detallados como para describir claramente el objetivo de muestreo y el proceso de muestreo utilizados. Los documentos de trabajo deben incluir la fuente de la población, el método de muestreo utilizado, los parámetros de muestreo (por ej., método o número de

inicio al azar por el cual se logró el inicio al azar, intervalo de muestreo), los ítems seleccionados, los detalles de las pruebas de auditoría realizadas, las conclusiones a las que se llegó.

2.5 Evaluación de los Resultados de la Muestra

2.5.1 Una vez ejecutados en cada uno de los ítems de muestra los procedimientos de auditoría apropiados para el objetivo de auditoría dado, el Auditor de SI debe analizar los eventuales errores detectados en la muestra para determinar si son realmente errores y, si corresponde, la naturaleza y causa de los mismos. Los errores así determinados deben ser extrapolados a la población, según corresponda, si el método de muestreo utilizado está basado en estadísticas.

2.5.2 Deben revisarse los errores detectados en la muestra para determinar si son realmente errores. El Auditor de SI debe tener en cuenta los aspectos cualitativos de los mismos. Éstos comprenden la naturaleza y causa del error y el probable efecto del mismo en las otras etapas de la auditoría. Los errores que se producen como consecuencia de la falla de un proceso automatizado normalmente tienen una mayor incidencia en los índices de error que el error humano.

2.5.3 Cuando no puede obtenerse la evidencia de auditoría prevista con respecto a un ítem específico de la muestra, es probable que el Auditor de SI pueda obtener suficiente evidencia adecuada mediante la ejecución de procedimientos alternativos con relación al ítem seleccionado.

2.5.4 El Auditor de SI debe considerar la posibilidad de proyectar los resultados de la muestra a la población con un método de proyección compatible con el método utilizado para seleccionar la unidad de muestreo. La proyección de la muestra podría implicar la estimación del error probable en la población y la estimación de otros errores que pudieran no haber sido detectados a causa de la imprecisión de la técnica conjuntamente con los aspectos cualitativos de los errores hallados.

2.5.6 El Auditor de SI deberá considerar si los errores en la población podrían exceder el nivel tolerable comparando éste con el error de población proyectado, teniendo en cuenta los resultados de otros procedimientos relacionados con el objetivo de auditoría. Cuando el error de población proyectado excede el nivel tolerable, el Auditor de SI debe realizar una nueva evaluación del riesgo de muestreo y, si dicho riesgo resulta inaceptable, debe considerar la posibilidad de ampliar el procedimiento de auditoría o ejecutar procedimientos alternativos.

3 FECHA DE VIGENCIA

3.1 Este Lineamiento rige para todas las auditorías de sistemas de información a partir del 1° de marzo de 2000.

APÉNDICE – GLOSARIO

Muestreo de Auditoría – la aplicación de procedimientos de auditoría a menos del 100% de los ítems de una población a fin de obtener evidencia de auditoría sobre una característica concreta de la población.

Error – desviaciones en el control (pruebas de cumplimiento) o errores (procedimientos sustantivos).

Materialidad – una expresión de la trascendencia o la importancia relativas de un asunto determinado en el contexto de la organización en su totalidad.

Población – el conjunto de todos los datos de los cuales se selecciona una muestra y a partir de los cuales el Auditor de SI desea obtener conclusiones.

Riesgo de Muestreo – la probabilidad de que el Auditor de SI haya llegado a una conclusión errónea debido a que se probó una muestra de auditoría en lugar de la población en su totalidad. Aunque el riesgo de muestreo puede reducirse a un nivel aceptablemente bajo utilizando una amplitud de muestra y un método de selección adecuados, éste nunca puede ser eliminado.

Information Systems Audit and Control Association

LINEAMIENTO DE AUDITORIA DE SI

USO DE TECNICAS DE AUDITORIA ASISTIDA POR COMPUTADORA (CAATs)

1. ANTECEDENTES

1.1. Articulación con normas

1.1.1 La norma 060.020 (Evidencia) establece que “En el transcurso de la auditoría, el auditor de sistemas de información debe obtener evidencia suficiente, confiable, pertinente y útil a fin de que se alcancen los objetivos de auditoría con eficacia. Los hallazgos y las conclusiones de la auditoría deben ser sustentados mediante el análisis y la interpretación adecuados de dicha evidencia.”

1.1.2 La norma 050.010 (Planificación de la Auditoría) establece que “El auditor de sistemas de información debe planificar las tareas de auditoría de tal manera que se aborden los objetivos y se cumpla con las normas aplicables de auditoría profesional.”

1.1.3 La norma 030.020 (Debido Cuidado Profesional) establece que “Se debe proceder con el debido cuidado profesional y deben observarse las normas aplicables de auditoría profesional en todos los aspectos del trabajo del auditor de sistemas de información.”

1.2. Necesidad de un lineamiento

1.2.1 Las Técnicas de Auditoría Asistida por Computadora (CAATs) constituyen herramientas importantes para el Auditor de SI en la realización de auditorías.

1.2.2 Las CAATs comprenden muchos tipos de herramientas y técnicas ; entre las más comunes figuran el software de auditoría de propósitos generales, el software utilitario, los datos de prueba, el rastreo y registro (tracing and mapping) del software de aplicaciones y los sistemas expertos de auditoría.

1.2.3 Las CAATs pueden utilizarse en la ejecución de diversos procedimientos de auditoría, entre ellos :

- Pruebas de los detalles de las transacciones y los balances ;
- Procedimientos de revisión analítica ;
- Pruebas de cumplimiento de los controles generales de SI ;
- Pruebas de cumplimiento de los controles de aplicación de SI
- Pruebas de penetración

1.2.4 Las CAATs pueden producir una gran parte de la evidencia de auditoría desarrollada en las auditorías de SI y, como consecuencia de ello, el auditor de SI debe planificar y dar muestras de un debido cuidado profesional en el uso de las CAATs.

1.2.5 Este lineamiento proporciona una orientación para la aplicación de las normas de auditoría de SI. El Auditor de SI debe tenerlo en cuenta al determinar cómo lograr la implementación de las Normas citadas, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto del mismo.

1.2.6 Este lineamiento debe aplicarse en la utilización de las CAATs sin tener en cuenta si el auditor participante es Auditor de SI.

2. PLANIFICACIÓN

2.1 Factores de decisión para el uso de CAATs

2.1.1 Al planificar la auditoría, el auditor de SI debe considerar una combinación apropiada de técnicas manuales y CAATs. A fin de determinar si se utilizan CAATs, deben tenerse en cuenta los siguientes factores :

- Competencia, experiencia y conocimiento informáticos del Auditor de SI
- Disponibilidad de instalaciones adecuadas de SI y CAATs
- Eficiencia y eficacia del uso de CAATs respecto de las técnicas manuales
- Restricciones de tiempo
- Integridad del sistema de información y el ambiente de TI
- Nivel de riesgo de auditoría

2.2 Etapas de planificación de CAATs

2.2.1 Las principales medidas que debe tomar el auditor de SI durante la preparación de la aplicación de las CAATs seleccionadas son :

- Fijar los objetivos de auditoría de las CAATs
- Determinar la accesibilidad y disponibilidad de los datos, los programas/sistema y las instalaciones de SI de la organización
- Definir los procedimientos a seguir (por ej., muestreo estadístico, nuevos cálculos, confirmación, etc.)
- Definir los requerimientos de salida
- Determinar los requerimientos de recursos, por ej., personal, CAATs, ambiente de procesamiento (instalaciones de SI de la organización o instalaciones de SI de auditoría)
- Obtener acceso a las instalaciones, los programas/sistema y los datos de SI de la organización, incluidas las definiciones de archivo
- Documentar las CAATs a utilizar, incluidos los objetivos, los diagramas de flujo de alto nivel y las instrucciones de ejecución

2.3 Disposiciones de auditor y auditado

2.3.1 Los archivos de datos, como los archivos de transacciones detalladas, a menudo se retienen sólo por un corto período ; por consiguiente, el auditor de SI debe disponer la retención de los datos correspondientes al período de auditoría pertinente.

2.3.2 El acceso a los datos, los programas/sistema y las instalaciones de SI de la organización deben disponerse con la debida anticipación a fin de minimizar el efecto en el ambiente de producción de la organización.
2.3.3 El auditor de SI debe evaluar el efecto que pueden tener los cambios de los programas/sistema de producción en el uso de las CAATs. Al hacer esto, debe considerar el efecto de estos cambios en la integridad y utilidad de las CAATs, así como en la integridad de los programas/sistema y los datos utilizados.

2.4 Prueba de las CAATs

2.4.1 El auditor de SI debe garantizar razonablemente la integridad, confiabilidad, utilidad y seguridad de las CAATs mediante la adecuada planificación, diseño, prueba, procesamiento y revisión de la documentación. Esto debe llevarse a cabo antes de depositar confianza en las CAATs. La naturaleza, la oportunidad y el alcance de las pruebas depende de la disponibilidad comercial y estabilidad de las CAATs.

2.5 Seguridad de datos y CAATs

2.5.1 Cuando las CAATs se utilizan para obtener información para el análisis de datos, el Auditor de SI debe verificar la integridad del sistema de información y el ambiente de TI de los cuales se obtienen los datos.
2.5.2 Las CAATs pueden utilizarse para obtener información crítica de programa/sistema y datos de producción confidenciales. El auditor de SI debe proteger la información de programa/sistema y los datos de producción con un nivel apropiado de confidencialidad y seguridad. Al realizar esta tarea, el Auditor de SI debe considerar el nivel de confidencialidad y seguridad que requiere la organización propietaria de los datos y toda legislación pertinente.
2.5.3 El auditor de SI debe utilizar y documentar los resultados de los procedimientos apropiados para mantener la integridad, confiabilidad, utilidad y seguridad de las CAATs. Esto debería incluir una revisión del mantenimiento de programas y de los controles de cambios de programas sobre el software de auditoría incorporado a fin de determinar si sólo se realizaron cambios autorizados en las CAATs.
2.5.4 Cuando las CAATs residen en un ambiente que no está bajo el control del auditor de SI, debe existir un adecuado nivel de control para identificar los cambios de las CAATs. Cuando éstas se modifican, el auditor de SI debe garantizar su integridad, confiabilidad, utilidad y seguridad mediante la adecuada planificación, diseño, prueba, procesamiento y revisión de la documentación antes de depositar confianza en ellas.

3. REALIZACIÓN DE LAS TAREAS DE AUDITORÍA

3.1 Reunión de evidencia de auditoría

3.1.1 El auditor de SI debe controlar el uso de las CAATs para garantizar razonablemente que se hayan cumplido los objetivos de auditoría y las especificaciones detalladas de las mismas. El auditor de SI debe :

- Realizar una conciliación de los totales de control, si corresponde
- Revisar la razonabilidad de la salida
- Llevar a cabo una revisión de la lógica, los parámetros u otras características de las CAATs
- Revisar los controles generales de SI de la organización que pueden contribuir a la integridad de las CAATs (por ej., controles de cambios de programas y acceso al sistema, programa y/o archivos de datos)

3.2 Software de auditoría de propósitos generales

3.2.1 Al utilizar software de auditoría de propósitos generales para acceder a los datos de producción, el auditor de SI debe tomar medidas adecuadas para proteger la integridad de los datos de la organización. En el caso del software de auditoría incorporado, es necesario que el auditor de SI participe en el diseño del sistema. Asimismo, las técnicas deberán desarrollarse y mantenerse dentro de los programas/sistemas de aplicación de la organización.

3.3 Software utilitario

3.3.1 Al utilizar software utilitario, el auditor de SI debe confirmar que no se hayan producido intervenciones imprevistas durante el procesamiento y que el software utilitario se haya obtenido en la adecuada biblioteca de sistema. El auditor de SI también debe tomar medidas apropiadas para proteger la integridad del sistema y los archivos de la organización ya que estos utilitarios pueden dañarlos fácilmente.

3.4 Datos de prueba

3.4.1 Al utilizar datos de prueba, el auditor de SI debe saber que éstos solamente señalan la posibilidad de procesamiento erróneo ; esta técnica no evalúa los datos de producción real. El auditor de SI también debe tener en cuenta que el análisis de los datos de prueba puede requerir mucho tiempo y resultar sumamente complejo según el número de transacciones procesadas, el número de programas probados y la complejidad de los programas/sistema. Antes de utilizar los datos de prueba, el Auditor de SI debe verificar que éstos no afectarán definitivamente la actividad del sistema (the live system).

3.5. Rastreo y registro del software de aplicaciones

3.5.1 Al utilizar el rastreo y registro del software de aplicaciones, el auditor de SI debe confirmar que el código fuente que se evalúa haya generado el programa objeto que se utiliza efectivamente en la producción. El auditor de SI debe tener en cuenta que el rastreo y registro del software de aplicaciones sólo señala la posibilidad de procesamiento erróneo ; no evalúa los datos de producción real.

3.6. Sistemas expertos de auditoría

3.6.1 Al utilizar sistemas expertos de auditoría, el auditor de SI debe estar perfectamente informado de las operaciones del sistema a fin de confirmar que las vías que se han tomado para llegar a las decisiones sean apropiadas para el ambiente/situación de auditoría correspondiente.

4. DOCUMENTACIÓN DE LAS CAATs

4.1 Documentos de trabajo

4.1.1 El proceso gradual de las CAATs debe estar suficientemente documentado como para proporcionar adecuada evidencia de auditoría.
4.1.2. Específicamente, los documentos de trabajo de la auditoría deben contener suficiente documentación como para describir la aplicación de las CAATs, incluidos los detalles expuestos en los siguientes párrafos.

4.2. Planificación

4.2.1 La documentación debe incluir :

- Los objetivos de las CAATs
- Las CAATs a utilizar
- Los controles a ejercer

- La contratación de personal y los plazos

4.3. Ejecución

4.3.1 La documentación debe incluir :

- La preparación y los procedimientos y controles de pruebas de las CAATs
- Los detalles de las pruebas realizadas por las CAATs
- Los detalles de las entradas (por ej., datos utilizados, despliegues [layouts] de archivos), del procesamiento (lógica y diagramas de flujo de alto nivel de las CAATs) y de las salidas (informes, archivos de registro [log files])
- Un listado de los parámetros pertinentes o código fuente

4.4. Evidencia de Auditoría

4.4.1 La documentación debe incluir :

- La salida generada
- La descripción del trabajo de análisis de auditoría realizado en base a la salida
- Los hallazgos de auditoría
- Las conclusiones de auditoría
- Las recomendaciones de auditoría

5. PRESENTACIÓN DEL INFORME

5.1. Descripción de las CAATs

5.1.1 La sección de metodología, alcance y objetivos del informe debe contener una descripción clara de las CAATs utilizadas. Esta descripción no debe ser demasiado detallada, pero debe brindar una adecuada idea de conjunto al lector.

5.1.2 La descripción de las CAATs utilizadas también debe incluirse en la parte principal del informe, donde se discute el hallazgo específico relacionado con el uso de las CAATs.

5.1.3 Si la descripción de las CAATs utilizadas es aplicable a diversos hallazgos, o es demasiado detallada, ésta debería discutirse brevemente en la sección de metodología, alcance y objetivos del informe y debería remitirse al lector un apéndice con una descripción más detallada.

6. FECHA DE VIGENCIA

6.1 Este lineamiento rige para todas las auditorías de sistemas de información a partir del 1° de diciembre de 1998**.**

APÉNDICE - GLOSARIO

Rastreo y Registro del Software de Aplicaciones - herramientas especializadas que pueden utilizarse para analizar el flujo de datos mediante la lógica del procesamiento del software de aplicaciones y documentar la lógica, los paths, las condiciones de control y las secuencias del procesamiento. Pueden analizarse tanto el lenguaje de mando o los enunciados de control de tareas como el lenguaje de programación. Esta técnica incluye el registro, el rastreo, las imágenes instantáneas, las simulaciones paralelas y las comparaciones de códigos.

Sistemas Expertos de Auditoría - sistemas expertos o de soporte de decisiones que pueden utilizarse para asistir a los auditores de SI en el proceso de toma de decisiones automatizando el conocimiento de los expertos en el campo correspondiente. Esta técnica incluye el análisis automatizado de riesgos, el software del sistema y los paquetes de software de objetivos de control.

Técnicas de Auditoría Asistida por Computadora (CAATs) - cualquier técnica automatizada de auditoría, como el software de auditoría de propósitos generales, el software utilitario, los datos de prueba, el rastreo y registro del software de aplicaciones y los sistemas expertos de auditoría.

Software de Auditoría de Propósitos Generales - un programa o serie de programas computadorizados diseñados para desempeñar ciertas funciones automatizadas. Estas funciones comprenden la lectura de archivos computadorizados ; la selección, manipulación, clasificación y resumen de datos ; la realización de cálculos, la selección de muestras y la impresión de informes o cartas en un formato especificado por el auditor de SI. Esta técnica incluye el software adquirido o escrito para auditoría y el software incorporado en los sistemas de producción.

Datos de Prueba - transacciones simuladas que pueden utilizarse para probar la lógica, los cálculos y los controles de procesamiento efectivamente programados en las aplicaciones computadorizadas. Pueden probarse los programas individuales o todo el sistema. Esta técnica incluye las Instalaciones de Prueba Integradas (ITFs) y las Evaluaciones Básicas de Sistema (Base Case System Evaluations ; BCSEs).

Software Utilitario - programas computadorizados suministrados por un fabricante de hardware o un proveedor de software y utilizados en la ejecución del sistema. Esta técnica puede utilizarse para examinar las actividades de procesamiento, probar las actividades y los procedimientos operacionales de los programas y el sistema, evaluar las actividades del archivo de datos y analizar los datos de registro de tareas.

Copyright 1998
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows,IL 60008 USA
Web Site:http://www.isaca.org

Information Systems Audit and Control Association

LINEAMIENTO DE AUDITORIA DE SI

UTILIZACION DEL TRABAJO DE OTROS AUDITORES Y EXPERTOS

1. ANTECEDENTES

1.1 Articulación con normas

1.1.1 La Norma 060.020 (Evidencia) determina que “En el transcurso de la auditoría, el auditor de sistemas de información debe obtener evidencia suficiente, confiable, pertinente y útil a fin de que se alcancen los objetivos de auditoría con eficacia. Los hallazgos y las conclusiones de la auditoría deben ser sustentados mediante el análisis y la interpretación adecuados de dicha evidencia.”

1.2 Necesidad de un lineamiento

1.2.1 La interdependencia del procesamiento de clientes y proveedores y la tercerización de las actividades no centrales implican que un auditor de SI (interno o externo) a menudo encontrará que algunas partes del ambiente auditado son controladas y auditadas por organizaciones o funciones independientes. Este lineamiento expone de qué manera el auditor de SI debe cumplir con la norma mencionada anteriormente en estas circunstancias. El cumplimiento de este lineamiento no es obligatorio; no obstante, el auditor de SI debería estar preparado para justificar cualquier desviación respecto del mismo.

2. MANDATO DE AUDITORÍA

2.1 Derechos de acceso al trabajo de otros auditores o expertos

2.1.1 El auditor de SI debe garantizar que, cuando el trabajo de otros auditores o expertos esté relacionado con los objetivos de la auditoría de SI, el mandato de auditoría o los términos de referencia especifiquen el derecho de acceso a dicho trabajo por parte del auditor de SI.

3. PLANIFICACIÓN

3.1 Consideraciones para la planificación

3.1.1 Cuando una auditoría de SI requiere la utilización del trabajo de otros auditores o expertos, el auditor de SI debe considerar sus actividades y su efecto en los objetivos de la auditoría de SI al planificar las tareas. El proceso de planificación debe incluir :

- la evaluación de la independencia y la objetividad de los otros auditores o expertos
- la evaluación de su aptitud profesional
- la comprensión del alcance de su trabajo y del enfoque
- la determinación del nivel de revisión requerido.

3.2 Independencia y objetividad

3.2.1 Los procesos de selección y designación, la posición dentro de la organización, la línea de comunicación y el efecto de sus recomendaciones en las prácticas gerenciales son indicadores de la independencia y objetividad de otros auditores y expertos.

3.3 Aptitud profesional

3.3.1 Las aptitudes, la experiencia y los recursos de otros auditores y expertos deben tenerse en cuenta al evaluar la competencia profesional.

3.4 Alcance del trabajo y enfoque

3.4.1 El alcance del trabajo y el enfoque normalmente constarán por escrito en el mandato de auditoría, los términos de referencia o el contrato de los otros auditores o expertos.

3.5 Nivel de revisión requerido

3.5.1 La naturaleza, la oportunidad y el alcance de la evidencia de auditoría requerida dependen de la importancia del trabajo de los otros auditores o expertos. El proceso de planificación del auditor de SI debe identificar el nivel de revisión requerido para proporcionar evidencia de auditoría suficiente, confiable, pertinente y útil para alcanzar con eficacia los objetivos globales de la auditoría de SI. El auditor debe considerar la posibilidad de revisar el informe final, el/los programa/s de auditoría y los documentos de trabajo de los otros auditores o expertos. El auditor de SI también debe considerar si se requieren pruebas adicionales del trabajo de otros auditores o expertos.

4. REALIZACIÓN DE LAS TAREAS DE AUDITORÍA

4.1 Revisión de documentos de trabajo de otros auditores o expertos

4.1.1 Si es preciso revisar los documentos de trabajo de otros auditores o expertos, el auditor de SI debe realizar un trabajo de auditoría suficiente para confirmar que las tareas de los otros auditores o expertos fueron adecuadamente planificadas, supervisadas, documentadas y revisadas y para considerar la conveniencia y suficiencia de la evidencia de auditoría proporcionada por ellos. También debe evaluarse el cumplimiento de las normas profesionales pertinentes.

4.2 Revisión de informes de otros auditores o expertos

4.2.1 El auditor de SI debe llevar a cabo suficientes revisiones de los informes finales de otros auditores o expertos para confirmar que se haya cumplido con el alcance especificado en el mandato de auditoría, los términos de referencia o el contrato; que se hayan identificado los supuestos significativos utilizados por los otros auditores o expertos y que la gerencia haya aceptado las conclusiones y los hallazgos comunicados.

4.2.2 Puede resultar adecuado que la gerencia proporcione su propio informe sobre las entidades auditadas, en reconocimiento de su responsabilidad primaria por los sistemas de control interno. En este caso el auditor de SI debe considerar el informe de la gerencia y el informe del auditor al mismo tiempo.

4.3.2 El auditor de SI debe evaluar la utilidad y conveniencia de los informes emitidos por los otros auditores y expertos y debe considerar los hallazgos significativos comunicados por ellos. Es responsabilidad del auditor de SI evaluar el efecto de los hallazgos y las conclusiones de los otros auditores o expertos en el objetivo global de la auditoría y verificar que se lleven a cabo las tareas adicionales necesarias para alcanzarlo.

5. ACTIVIDADES DE SEGUIMIENTO

5.1 Implementación de recomendaciones

5.1.1 Cuando corresponda, el auditor de SI debe considerar hasta qué punto la gerencia ha implementado las recomendaciones de los otros auditores o expertos.

6. FECHA DE VIGENCIA

6.1 Este Lineamiento rige para todas las auditorías de sistemas de información a partir del 1° de junio de 1998.

APENDICE – GLOSARIO

Independencia **–** auto-gobierno, ausencia de conflicto de intereses e influencia indebida.

Objetividad **–** capacidad de emitir juicios, expresar opiniones y presentar recomendaciones con imparcialidad.

Aptitud profesional – nivel de capacidad probado, frecuentemente vinculado con los requisitos emitidos por los cuerpos profesionales pertinentes y el cumplimiento de sus códigos de práctica y normas.

Copyright 1998
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows,IL 60008 USA
Web Site:http://www.isaca.org

LINEAMIENTO DE AUDITORIA DE SI

CONTENIDO Y ESTRUCTURA DE INFORMES

1 ANTECEDENTES

1.1 Articulación con Normas

1.1.1 La Norma 070.010 (Contenido y Estructura de Informes) determina que "El auditor de sistemas de información debe proporcionar a los destinatarios correspondientes un informe – con una estructura apropiada –sobre la realización de las tareas de auditoría. En dicho informe deben constar el campo de aplicación, los objetivos, el período de aplicación y la naturaleza y alcance de las tareas de auditoría realizadas. El informe debe identificar la organización, los destinatarios correspondientes y cualquier restricción a su difusión; asimismo, debe exponer los hallazgos, las conclusiones y recomendaciones y cualquier reserva o restricción que tenga el auditor con respecto a la auditoría."

1.2 Necesidad de un Lineamiento

1.2.1 El propósito de este lineamiento es describir las prácticas recomendadas para preparar y emitir un informe de auditoría de sistemas de información ("informe").

1.2.2 Este lineamiento proporciona una orientación para la aplicación de las normas de auditoría de SI. El Auditor de SI debe tenerlo en cuenta al determinar cómo lograr la implementación de la Norma citada, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto del mismo.

2. PRESENTACIÓN DE INFORMES

2.1 Propósito y Contenido del informe

2.2.1 El informe es el medio formal para comunicar los objetivos de la auditoría, las normas de auditoría aplicadas (si se requiere), el alcance de auditoría, la metodología utilizada (si se requiere) y los hallazgos, conclusiones y recomendaciones.

2.2 Destinatarios

2.2.1 Al preparar el informe, el auditor debe tener en cuenta las necesidades de los destinatarios previstos, entre los cuales pueden encontrarse el auditado, la gerencia ejecutiva, el directorio o su comité de auditoría, y el gobierno.

2.3 Estilo y Contenido

2.3.1 El estilo y el contenido del informe deben ser los adecuados para los destinatarios previstos ; éste puede presentarse en forma escrita, oral u otra.

2.3.2 Un informe escrito debe identificar la organización auditada e incluir título, firma y fecha.

2.3.3 Un informe en otro medio puede incluir una forma apropiada de autenticación en lugar de una firma escrita.

2.3.4 Los informes deben ser objetivos, claros, concisos, constructivos y oportunos.

2.4 Declaración de Objetivos

2.4.1 El informe debe incluir una declaración de los objetivos de la auditoría a fin de identificar su propósito. Si, a juicio del auditor, no se alcanzó alguno de los objetivos de auditoría establecidos en el informe, este hecho debe constar en el mismo.

2.5 Amplitud, Naturaleza, Oportunidad y Alcance de las Tareas de Auditoría Realizadas

2.5.1 El informe debe incluir una declaración del alcance de auditoría que describa la naturaleza, oportunidad y alcance de las tareas de auditoría realizadas. La declaración del alcance debe identificar el área funcional de la auditoría, el período de la misma y los sistemas de información, aplicaciones o ambientes de procesamiento auditados.

2.5.2 El informe debe identificar las circunstancias de limitación del alcance cuando, a juicio del auditor, no hayan podido llevarse a cabo las pruebas y los procedimientos adecuados para cumplir con las normas, o cuando las restricciones a las tareas de auditoría hayan sido impuestas por el auditado.

2.6 Restricciones a la Distribución

2.6.1 El informe debe identificar al auditado e indicar la fecha de emisión. Cuando corresponda, el informe debe especificar que está destinado únicamente a la información y el uso de las partes previstas, como el auditado, el directorio, la gerencia y cualquier destinatario ajeno a la organización que se haya previsto (por ej., una agencia gubernamental). El informe también debe establecer cualquier restricción a su distribución.

2.7 Hallazgos Significativos a Comunicar

2.7.1 El informe debe incluir todos los hallazgos de auditoría significativos. Cuando un hallazgo requiera explicación, el Auditor de SI debe describir el hallazgo, su causa y su riesgo. Cuando corresponda, el Auditor de SI debe suministrar la explicación en un documento separado y hacer referencia a éste en el informe. Asimismo, el Auditor de SI debe identificar los criterios organizacionales, profesionales y gubernamentales aplicados (como los Objetivos de Control para Información y Tecnologías Relacionadas – CobiT emitidos por ISACF).

2.8 Conclusión

2.8.1 Cuando corresponda, el informe debe incluir – a manera de conclusión – una evaluación del área auditada realizada por el Auditor de SI. La

conclusión puede ser una evaluación global o múltiples evaluaciones referidas a objetivos de auditoría específicos.

2.9 Recomendaciones

2.9.1 Cuando corresponda, el informe debe incluir recomendaciones de medidas correctivas. Las recomendaciones deben estar referidas a hallazgos específicos.

2.10 Reservas o Restricciones

2.10.1 El informe debe describir cualquier reserva o restricción significativa.

2.11 Presentación para Propiciar la Comprensión

2.11.1 El formato del informe debe reflejar una presentación lógica y organizada. El informe debe contener suficiente información como para ser comprendido por los destinatarios previstos.

2.12 Oportunidad de la Presentación de Informes

2.12.1 El informe debe ser emitido de manera oportuna para propiciar una inmediata acción correctiva. Cuando corresponda, el Auditor debe comunicar los hallazgos significativos a las personas adecuadas prontamente antes de la emisión del informe. La comunicación previa de los hallazgos significativos no debe alterar el propósito o contenido del informe.

2.13 Consideración de Eventos Posteriores

2.13.1 Antes de emitir la versión definitiva del informe, el Auditor de SI debe considerar la posibilidad de determinar si se produjeron cambios significativos en la organización o su entorno que pudieran afectar los hallazgos, conclusiones y recomendaciones comunicados. Si se identifican cambios de esta naturaleza el Auditor de SI debe tomar medidas adecuadas para alertar a los destinatarios del informe del efecto potencial de estos cambios en los hallazgos, conclusiones y recomendaciones comunicados.

2.13.2 Entre los ejemplos de eventos significativos de esta índole pueden encontrarse los siguientes :

- Un fraude descubierto después de una revisión de auditoría de los controles de un sistema de aplicación.
- Daños graves provocados por un incendio que se produzca después de una revisión de los controles generales de las instalaciones
- Tercerización de la función de SI auditada.
- Falla del sistema en la implementación, demora en la implementación o terminación del proyecto después de una revisión pre-implementación de la aplicación, sus pruebas o su planificación de proyecto
- Incumplimiento o quiebra de un cliente o proveedor importante, litigios graves o falla de producción que tenga como resultado modificaciones en los riesgos clave para el negocio.
- Redundancias comunicadas que afecten al personal que habría implementado las recomendaciones.

3. ÉTICA Y NORMAS PROFESIONALES

3.1 Identificación de Normas

3.1.1 Si se requiere, el informe debe identificar las normas o códigos organizacionales, profesionales y/o gubernamentales aplicados (por ej., Normas de ISACA para Auditoría de Sistemas de Información) en la realización de la auditoría. El informe debe identificar las excepciones significativas a la aplicación de estas normas, las razones para no utilizarlas y, cuando corresponda, el efecto potencial en los resultados de la auditoría.

4. ACTIVIDADES DE SEGUIMIENTO

4.1 Solicitud de Respuesta

4.1.1 Cuando sea conveniente, el Auditor de SI debe solicitar una respuesta que incluya las medidas que se proponga tomar la gerencia como resultado de las observaciones presentadas en el informe y las fechas previstas para su implementación.

5. FECHA DE VIGENCIA

5.1 Este lineamiento rige para todas las auditorías de sistemas de información a partir del 1° de diciembre de 1998.

Copyright 1998
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows,IL 60008 USA
Web Site:http://www.isaca.org

Capítulo Buenos Aires

E-mail: info@isaca.org
Web site: www.isaca.org