

Guía de Auditoría de SI (Sistemas de Información)

Reportes

Documento G20

Introducción

La naturaleza especializada de la auditoría de los sistemas de Información (SI) y las habilidades necesarias para realizar las auditorías, requiere de estándares que se aplican específicamente a la auditoría de SI. Una de las metas de la Asociación de Auditoría y Control de Sistemas de Información (ISACA) - por sus siglas en inglés – es de presentar estándares globales aplicables para enfrentar esta necesidad. El desarrollo y diseminación de Estándares de Auditoría de SI son básicas dentro de la contribución profesional de ISACA para la comunidad de auditores.

Objetivos

Los objetivos de los Estándares de Auditoría de SI de ISACA son informar:

- A los auditores de SI sobre los niveles mínimos de desempeño aceptables requeridos para alcanzar las responsabilidades profesionales del *Código de Ética Profesional* de ISACA para auditores de SI
- A la Gerencia y otros grupos que se interesen sobre las expectativas profesionales relativas al trabajo de los practicantes

El objetivo de las Guías de Auditoría de SI, es proveer información adicional sobre cómo mantenerse en cumplimiento con los Estándares de Auditoría de SI.

Alcance y Autoridad de los Estándares de Auditoría de SI

La plantilla base para los Estándares de Auditoría de SI provee guía en muchos niveles:

- **Estándares** definen requerimientos mandatorios para auditar y hacer reportes de SI.
- **Guías** proveen pasos para aplicar los Estándares de Auditoría de SI. El auditor de SI debe considerar las guías al determinar cómo lograr la implementación de los estándares, utilizar el criterio profesional en su aplicación y estar preparado para justificar alguna salida.
- **Procedimientos** proveen ejemplos sobre cómo debe actuar un auditor de SI en una auditoría. Los procedimientos no deben ser considerados parte de cualquier procedimiento o prueba formal o fuera de otros procedimientos y pruebas que son razonablemente dirigidas a obtener los mismos resultados. Para determinar cuál procedimiento es más apropiado, o el grupo de procedimientos o pruebas, el auditor de SI debe utilizar su criterio profesional según la circunstancia específica presentada por el ambiente de los sistemas de información o tecnología. Los documentos del procedimiento contienen información sobre cómo alcanzar los estándares cuando se realiza un trabajo de auditoría de SI, pero no dan requerimientos.

Las palabras auditoría y revisión son intercambiables. Un glosario completo de términos puede ser encontrado en el sitio web de ISACA en www.isaca.org/standard/appendix.htm

Quienes cuenten con la designación de Auditor Certificado de Sistemas de Información (CISA) deben cumplir con los Estándares de Auditoría de SI adoptados por ISACA. Si no logran cumplir con estos estándares, pueden ser sujetos a investigación de la conducta del auditor CISA por parte de la Junta Directiva de ISACA o el comité apropiado y, si fuera requerido, una acción disciplinaria.

Desarrollo de Estándares, Guías y Procedimientos

La Junta de Estándares ISACA está comprometida a realizar consultas extensivas en la preparación de los Estándares, Guías y Procedimientos de Auditoría de SI. Antes de publicar cualquier documento, la Junta de Estándares, pone a disposición borradores de los documentos internacionalmente para la revisión y comentarios del

público en general. La Junta de Estándares, también busca a expertos específicos según el tema bajo consideración para consultas donde sea necesario.

La Junta de Estándares cuenta con un programa de desarrollo continuo y puede recibir contribuciones de los miembros de ISACA, aquellos con certificación CISA y otros grupos que se interesen en identificar temas emergentes que requieran nuevos productos estándar. Cualquier sugerencia debe ser enviada a través de correo electrónico (research@isaca.org), por fax (+1.847.253.1443) o por correo (dirección está al final de ésta guía) a ISACA en sus Oficinas Internacionales, a la atención del director de investigaciones, estándares y relaciones académicas.

Esta guía reemplaza la publicada anteriormente, Reporte de Formulario y Contenido, que será removida en la fecha en que esta guía se haga efectiva. Este material fue levantado el 1º de Octubre de 2002.

**Information Systems Audit and Control Association
2002-2003 STANDARDS BOARD**

Chair, Claudio Cilli, CISA, CIA, Ph.D KPMG, Italy
Claude Carter, CISA, CA Nova Scotia Auditor General's Office, Canada
Sergio Fleginsky, CISA PricewaterhouseCoopers, Uruguay
Alonso Hernandez, CISA, ROAC Colegio Economistas, Spain
Marcelo Hector Gonzalez, CISA Central Bank of Argentina Republic, Argentina
Andrew J. MacLeod, CISA, FCPA, MACS, PCP, CIA Brisbane City Council, Australia
Peter Niblett, CISA, CA, CIA, FCPA Day Neilson, Australia
John G. Ott, CISA, CPA Aetna, Inc., USA
Venkatakrisnhan Vatsaraman, CISA, ACA, AICWA, CISSP Emirates Airlines, United Arab Emirates

1. Antecedentes

1.1. Enlace al Estándar ISACA

1.1.1. El estándar S7 del Reportes dicta: “El auditor de SI debe proveer un reporte, en un formato apropiado, al finalizar la auditoría. El reporte debe identificar la organización, los receptores interesados y cualquier restricción en cuanto a la circulación. El reporte debe señalar el alcance, objetivos, período de cobertura y la naturaleza, tiempo, así como la dimensión del trabajo de auditoría realizado. El reporte debe mostrar los hallazgos, conclusiones y recomendaciones y cualquier reserva, calificación o limitación en el alcance que el auditor de SI tenga con respecto a la auditoría.”

1.2. Definiciones

1.2.1. La Evidencia o el área de actividad es la información específica, sujeta al reporte del auditor de SI y procedimientos relacionados. Puede incluir conceptos como el diseño o la operación de controles internos y cumplimiento con prácticas privadas o estándares o leyes específicas y regulaciones.

1.2.2. El compromiso de reportes sobre atestados, es un compromiso donde un auditor de SI examina las aseveraciones de la gerencia relacionadas con una evidencia en particular o la evidencia sujeta a estudio directamente. El reporte del auditor de SI consiste en una opinión sobre alguno de los siguientes temas:

- **La evidencia.** Estos reportes relacionan directamente a la evidencia más que a la aseveración. En algunas situaciones la gerencia no podrá realizar una aseveración sobre la evidencia del compromiso. Un ejemplo de esta situación, es cuando los servicios de TI los brinda un tercero. La gerencia no podrá hacer una aseveración de manera ordinaria sobre controles en los que un tercero es responsable. Entonces, un auditor de SI debe realizar un reporte directamente de la evidencia y no de la aseveración.
- La aseveración de la gerencia sobre la efectividad de los procedimientos de control
- Un compromiso de reportes de evaluación, donde un auditor de SI genera una opinión de una evidencia en particular. Estos compromisos pueden incluir reportes de controles implementados por la gerencia y sobre su efectividad operativa.

Esta guía está dirigida al primer tipo de opinión. Si los términos de referencia requieren de los últimos tipos de opinión, los requerimientos del reporte pueden necesitar ser adaptados.

1.2.3. Objetivos de control, que son los objetivos de la gerencia y son usados como base para desarrollar e implementar controles (Procedimientos de control)

1.2.4. Controles o procedimientos de control, significan aquellas políticas y procedimientos implementados para lograr un objetivo de control relativo

1.2.5. Debilidad en el control, significa una deficiencia en el diseño u operación de un procedimiento de control. Una debilidad en el control puede resultar potencialmente en riesgos relevantes a que el área de actividad no sea reducida a un nivel aceptable (los riesgos relevantes son aquellos que amenazan el incumplimiento de los objetivos relevantes al área de actividad que se está examinando). Las debilidades en el control, pueden ser materiales cuando el diseño o la operación de uno o más procedimientos de control no reduce a un nivel relativamente bajo, el riesgo de los hechos relevantes fallidos causados por actos ilegales o irregularidades que puedan ocurrir y no sean detectadas por procedimientos de control relacionados.

1.2.6. El criterio, son los estándares y rendimiento relativo utilizados para medir y presentar la evidencia y sobre lo que el auditor de SI evalúa la evidencia. El criterio debe ser:

- Objetivo – libre de influencias
- Medible – Fuente de medición consistente
- Completo – Incluir todos los factores relevantes para llegar a una conclusión
- Relevante – Relacionable a la evidencia

1.2.7. Compromisos de reportes directos, es un compromiso donde la gerencia no hace aseveraciones escritas sobre la efectividad de sus procedimientos de control y el auditor de SI provee una opinión, tanto de la efectividad de los procedimientos de control, como sobre la evidencia directamente.

1.2.8. Estructura de control interno (control interno), son los procesos dinámicos, integrados afectados por el cuerpo gobernante, la gerencia y otros departamentos. Son diseñados para proveer aseguramiento razonable acerca del cumplimiento de los siguientes objetivos generales:

- Efectividad, eficiencia y economía en las operaciones
- Confiabilidad de la gestión
- Procedimientos de control

1.2.9. Las estrategias de la gerencia para obtener estos objetivos generales son afectadas por el diseño y operación de los siguientes componentes:

- Ambiente controlado
- Sistema de información
- Procedimientos de control

1.3. Necesidad de Guía

1.3.1. Esta guía propone cómo el auditor de SI debe cumplir con los estándares de auditoría de ISACA y CobiT, cuando se reporta sobre los controles de sistemas de información y los objetivos de control relacionados de una organización.

2. Introducción

2.1. Propósito de esta Guía

2.1.1. El propósito de esta guía, es proveer dirección a los auditores de SI involucrados a reportar si los procedimientos de control de un área de actividad específica son efectivos para:

- La gestión de una organización al nivel gerencial y/o al nivel operativo
- Una tercera organización, por ejemplo un ente regulador u otro auditor

2.1.2. El auditor de SI puede estar involucrado para reportar sobre la efectividad de un diseño o su efectividad operativa.

3. Aseguramiento

3.1. Tipos de Servicios

3.1.1. Un auditor de SI puede realizar cualquier de las siguientes:

- Auditorías (directas o sobre atestados)
- Revisiones (directas o sobre atestados)
- Procedimientos pre-acordados

3.2. Auditorías y Revisiones

3.2.1. Una auditoría provee un nivel alto, pero no absoluto, de aseguramiento acerca de la efectividad de los procesos de control. Esto, ordinariamente es expresado como aseguramiento razonable en reconocimiento del hecho de que el aseguramiento absoluto es raramente obtenible debido a factores como la necesidad de juicio, el uso de pruebas, las limitaciones inherentes al control interno y porque mucha de la evidencia disponible al auditor de SI, es persuasiva más que conclusiva por naturaleza.

3.2.2. Una revisión provee un nivel moderado de aseguramiento sobre la efectividad de los procesos de control. El nivel de aseguramiento provisto es menor al de una auditoría, porque el alcance del trabajo es menos extensivo que el de una auditoría, y la naturaleza, duración y alcance de los procedimientos realizados no provee suficiente y apropiada evidencia auditada para permitir al auditor de SI a que exprese una opinión positiva. El objetivo de la revisión, es permitir al auditor de SI a decidir si, en base a los procedimientos, algo ha llamado la atención del auditor de SI que obligue a creer que los procedimientos de control no fueron basados efectivamente en criterios identificados (expresión de aseguramiento negativo)

3.2.3. Ambas auditorías y revisiones de los procedimientos de control involucran:

- Planear el compromiso
- Evaluar la efectividad del diseño de los procedimientos de control
- Probar la efectividad operativa de los procedimientos de control (la naturaleza, tiempo y extensión de la prueba varía según sea una auditoría o una revisión)
- Formar una conclusión y un reporte, sobre el diseño y la efectividad operativa de los procedimientos de control basados en criterios identificados:
 - ◆ La conclusión de una auditoría es expresada como una expresión de opinión positiva y provee un alto nivel de aseguramiento
 - ◆ La conclusión de una revisión es expresada como una expresión negativa de aseguramiento y provee sólo un nivel moderado de aseguramiento.

3.3. Procedimientos pre-acordados

3.3.1. Un compromiso de procedimientos pre-acordados, no resulta en una expresión de aseguramiento por el auditor de SI. El auditor de SI, se compromete a realizar procedimientos específicos para obtener la información necesaria para aquellos interesados que han acordado a que se realicen los procedimientos. El auditor de SI genera un reporte de hallazgos sobre hechos a aquellos interesados que han acordado que se realicen los procedimientos. Los interesados se forman sus propias conclusiones porque el auditor de SI no ha determinado la naturaleza, tiempo y alcance de los

procedimientos para que le permita expresar cualquier expresión de aseguramiento. El reporte está limitado a aquellos interesados (por ejemplo, un ente regulatorio) que ha acordado a que se realicen los procedimientos, ya que otros no cuentan con el conocimiento de las razones para los procedimientos y puede malinterpretar el resultado.

3.4. Reportes de Procedimientos pre-acordados

3.4.1. El reporte de procedimientos pre-acordados, debe estar en la forma de procedimientos y hallazgos. El reporte debe contener los siguientes elementos:

- Un título que incluya la palabra **independiente**
- Identificación de las partes específicas
- Identificación de la evidencia (o la aseveración escrita a la que se refiere) y el tipo de compromiso
- Identificación de la parte responsable
- Una declaración de que la evidencia es responsabilidad de la parte responsable
- Una declaración de que los procedimientos realizados fueron aquellos acordados por las partes identificadas en el reporte
- Una declaración de que la totalidad de los procedimientos, es responsabilidad única de las partes específicas y un levantamiento de responsabilidades por la suficiencia de esos procedimientos
- Una lista de los procedimientos realizados (o una referencia a estos) y hallazgos relacionados
- Una declaración de que el auditor de SI no estuvo comprometido y no condujo ninguna examinación de la evidencia
- Una declaración de que si el auditor de SI hubiera realizado procedimientos adicionales, otras evidencias pudieron haber llamado la atención del auditor de SI y hubieran sido reportadas.
- Una declaración de las restricciones en cuanto al uso del reporte, porque es dirigido exclusivamente a las partes específicas

3.5. Mandato de Compromiso

3.5.1. En donde deba ser llevado a cabo un compromiso para encontrar un requerimiento regulatorio o similar, es importante que el auditor de SI esté satisfecho de que el tipo de compromiso esté cumpliendo con la legislación relevante o con cualquier otra fuente del mandato del compromiso. Si existiera alguna incertidumbre, se recomienda que el auditor de SI y/o la parte señalada se comuniquen con el regulador relevante o cualquier otra parte responsable de establecer o regular el requerimiento y acuerden el tipo de compromiso y el aseguramiento a ser proveído.

3.5.2. Un auditor de SI, quien antes de la finalización de un compromiso se le solicite cambiar el compromiso de una auditoría a una revisión o unos procedimientos pre-acordados, necesita considerar si hacerlo es apropiado o no, y no puede aceptar el cambio donde no exista justificación razonable para el cambio. Por ejemplo, un cambio no es apropiado para evitar un reporte modificado.

4. Opinión de Auditoría de SI

4.1. Limitaciones

4.1.1. La opinión de un auditor de SI, está basada en los procedimientos que se han determinado como necesarios para la recolección de evidencia suficiente y apropiada, la evidencia siendo persuasiva más que conclusiva por naturaleza. El aseguramiento brindado por el auditor de SI en la efectividad de los controles internos. Sin embargo, es restringido por la naturaleza de los controles internos y de las limitaciones inherentes de cualquier colección de controles y sus operaciones. Estas limitaciones incluyen:

- Requerimiento usual de gerencia de que el costo de un control interno no exceda los beneficios que se deriven del mismo
- Muchos controles internos tienden a ser dirigidos hacia la rutina más que a transacciones/eventos que se salen de ella
- El potencial de errores humanos por descuido, distracción o fatiga, malentendidos de instrucciones y errores de juicio
- La posibilidad de evadir los controles internos a través de la colusión de empleados, entre ellos o con partes externas a la organización
- La posibilidad de que una persona responsable del ejercicio del control interno abuse esa responsabilidad, por ejemplo, un miembro de la gerencia evadiendo un procedimiento de control
- La posibilidad de que la gerencia no esté sujeta a los mismos controles internos aplicables al resto del personal
- La posibilidad de que los controles internos se vuelvan inadecuados debido a cambios en las condiciones y el cumplimiento con los procedimientos se deteriore.

4.1.2. Sistemas de gobernabilidad, (corporativa y de TI) la costumbre y la cultura, pueden inhibir irregularidades de la gerencia, pero no son formas de disuadir infalibles. Un ambiente efectivo de control puede ayudar a mitigar la probabilidad de estas irregularidades. Factores del ambiente de control como el de un ente gubernamental, el comité de auditorías y una función de auditoría interna puede limitar la conducta impropia de la gerencia. Alternativamente, un ambiente de control inefectivo puede negar la efectividad de los procedimientos de control en la estructura del control interno. Por ejemplo, aunque la organización tiene procedimientos de control de TI adecuados relacionado al cumplimiento de las regulaciones del ambiente, la gerencia puede tener una motivación fuerte para suprimir información acerca de cualquier información y/o cualquier brecha detectada que pueda reflejar adversamente en la imagen pública de la organización. La efectividad o relevancia de los controles internos también puede verse afectada por factores como el cambio de posesión o control, cambios en la gerencia u otro personal o desarrollos en el mercado o industria de la organización.

4.2. Eventos Subsecuentes

4.2.1. Los eventos, algunas veces ocurren luego del punto en el tiempo o período de tiempo en que la evidencia fue revisada pero antes de que el auditor de SI entregue el reporte, con lo que puede afectar materialmente la evidencia y requerir un ajuste o un comentario en la presentación de la evidencia o la aseveración. Estos eventos se les llaman eventos subsecuentes. Al efectuar un compromiso atestado, un auditor de SI debe considerar información acerca de eventos subsecuentes que le llamen la atención. Sin embargo, el auditor de SI no tiene la responsabilidad de detectar eventos subsecuentes.

4.2.2. El auditor de SI debe averiguar con la gerencia, si ellos están conscientes de algún evento subsecuente a la fecha del reporte del auditor de SI, que pueda tener un efecto material sobre la evidencia o la aseveración.

4.3. Conclusiones y Reporte

4.3.1. El auditor de SI debe revisar y asegurar las conclusiones derivadas de la evidencia obtenida, como la base para formar la opinión sobre la efectividad de los procesos de control basado en un criterio identificado.

4.3.2. Un reporte de un auditor de SI sobre la efectividad de los procedimientos de control debe incluir lo siguiente:

- Título
- Interesados
- Descripción del alcance de la auditoría, incluyendo:
 - ◆ Identificación o descripción del área de actividad
 - ◆ Criterio utilizado como la base para la conclusión del auditor de SI
 - ◆ Una declaración de que el mantenimiento de una estructura de control interno efectiva, incluyendo procedimientos de control para el área de actividad, es la responsabilidad de la gerencia.
- Donde el compromiso sea un compromiso atestado, una declaración identificando la fuente de la representación de la gerencia acerca de la efectividad de los procedimientos de control
- Una declaración de que el auditor de SI ha realizado el compromiso para expresar la opinión de la efectividad de los controles internos
- Identificación del propósito para el cual el reporte del auditor de SI ha sido preparado y aquellos autorizados para revisarla y una declaración de responsabilidad por el uso para cualquier otro propósito o por cualquier otra persona
- Descripción del criterio o descripción de la fuente del criterio
- Declaración de que la auditoría ha sido conducida de acuerdo con los Estándares de Auditoría SI de ISACA y otros profesionales
- Detalles que explican aún más acerca de las variables que afectan el aseguramiento provisto y otra información apropiada
- Donde sea apropiado, un reporte separado debe incluir recomendaciones para acciones correctivas e incluir respuesta de la gerencia
- Un párrafo detallando el por qué de las limitaciones inherentes de cualquier control interno, atestados fallidos debido a errores o fraudes que ocurran y no sean detectados. Adicionalmente, el párrafo debe declarar que las proyecciones de cualquier evaluación de control interno sobre reportes financieros de períodos futuros están sujetos al riesgo de que el control interno se vuelva inadecuado por cambios en las condiciones o que el nivel de cumplimiento con las políticas o procedimientos pueda deteriorarse

- ◆ Una auditoría no está diseñada para detectar todas las debilidades en los procedimientos de control ya que no se realiza continuamente a través del período y las pruebas realizadas sobre los procedimientos de control son de base simple
 - ◆ Cuando la opinión del auditor de SI sea calificada, un párrafo que describa la calificación debe de incluirse
- Una opinión de expresión acerca de si, en lo que respecta a materiales, el diseño y la operación de los procedimientos de control en relación con el área de actividad fueron efectivos
 - La firma del auditor de SI
 - La dirección del auditor de SI
 - La fecha del reporte de auditoría de SI. En muchas instancias, la fecha del reporte se basa en estándares profesionales aplicables. En otras instancias, la fecha del reporte debe ser basada en la conclusión del trabajo de campo.
- 4.3.3. En un compromiso de reporte directo, el auditor de SI reporta directamente sobre la evidencia que sobre la aseveración. El reporte debe hacer referencia sólo al tema del compromiso y no debe contener ninguna referencia a la aseveración de la gerencia sobre la evidencia.
- 4.3.4. Donde el auditor de SI tome un compromiso de revisión, el reporte indica que la conclusión del auditor de SI se relaciona con la efectividad del diseño y la operación y que el trabajo del auditor de SI con relación a la efectividad operativa, estaba limitada primordialmente a investigaciones, inspecciones, observaciones y pruebas mínimas de la operación de los controles internos. El reporte incluye una declaración de que la auditoría no se ha ejecutado, que los procedimientos realizados proveen menos aseguramiento que una auditoría y que una opinión de auditoría no fue expresada. La expresión de aseguramiento negativa, dicta que nada ha llamado la atención del auditor de SI que lleve al auditor de SI a creer que los procedimientos de control de la organización eran, en el aspecto material, inefectivos con relación al área de actividad, basado en el criterio identificado.
- 4.3.5. Durante el curso del compromiso, el auditor de SI puede identificar debilidades en el control. El auditor de SI debe reportar al apropiado nivel de gerencia en un período oportuno, cualquier deficiencia en el control. El procedimiento de compromiso está diseñado para obtener suficiente y apropiada evidencia, con el fin de formar una conclusión de acuerdo con los términos del compromiso. En la ausencia de un requerimiento específico en los términos del compromiso, el auditor de SI no tiene la responsabilidad de diseñar procedimientos para identificar evidencias que puedan ser apropiadas para el reporte a la gerencia.

5. Fecha Efectiva

- 5.1. Esta guía es efectiva para todas las auditorías de sistemas de información que comiencen en o después del 1 de enero de 2003. Un glosario completo de términos puede encontrarse en el sitio web de ISACA en www.isaca.org/standard/appendix.htm

Copyright 2002
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
E-mail: research@isaca.org
Web site: www.isaca.org