Guía de Auditoría y Aseguramiento de SI
2205 Evidencia

La naturaleza especializada de la auditoría y aseguramiento de los sistemas de la información (SI) y de las habilidades necesarias para realizar este tipo de compromisos requiere estándares que apliquen especialmente a las auditorías y aseguramiento de SI. El desarrollo y diseminación de los estándares de auditoría y aseguramiento de SI son la piedra angular de la contribución profesional de ISACA® a la comunidad de auditoría.

Los estándares de auditoría y aseguramiento de SI definen requerimientos obligatorios para la auditoría de SI y presentación de informes e informan a:

- Los profesionales de auditoría y aseguramiento de SI de profesionales del nivel mínimo de desempeño aceptable requerido para cumplir las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- Expectativas de la gerencia y otras partes interesadas de la profesión respecto al trabajo de los profesionales.
- Los poseedores de la Certificación de Auditoría de Sistemas de la Información en Ingles Certified Information Systems Auditor® (CISA®) la designación de requisitos. El incumplimiento de estos estándares puede dar lugar a una investigación sobre la conducta del poseedor del certificado CISA por la Junta Directiva de ISACA o el comité apropiado y, en última instancia, en una acción disciplinaria.

Los profesionales de auditoría y aseguramiento de SI deben incluir una declaración en sus trabajos, donde sea apropiado, indicando que el trabajo ha sido realizado de acuerdo con los estándares de auditoría y aseguramiento de los SI de ISACA o de otros posibles estándares aplicables.

ITAF™, un marco de trabajo de prácticas profesionales para auditoría y aseguramiento de SI, proporciona múltiples niveles de dirección:

- **Estándares**, divididos en tres categorías:
  - Estándares generales (series 1000)-Son los principios rectores bajo los que opera la profesión de auditoría y aseguramiento de SI. Aplican a la realización de todas las tareas, y hacen frente a la ética, independencia, objetividad y debida diligencia del profesional de auditoría y aseguramiento de SI, así como los conocimientos, competencia y habilidades. Las declaraciones de los estándares (en **negrita**) son obligatorias.
  - Estándares de desempeño(series 1200)-Tienen que ver con la forma en que se conduce la asignación, tales como planificación y supervisión, definición del alcance, riesgos y materialidad, la movilización de recursos, supervisión y administración de asignaciones, evidencias de auditoría y aseguramiento, y el ejercicio de su juicio profesional y debida diligencia.
  - Estándares de presentación de informes (series 1400)-Direccionan los tipos de informes, medios de comunicación y la información comunicada.
- **Guías**, apoyan a los estándares y también se dividen en tres categorías:
  - Guías generales (series 2000).
  - Guías de rendimiento (series 2200).
  - Guías de presentación de informes (series 2400).
- **Herramientas y técnicas**, proporcionan una guía adicional para los profesionales de auditoría y aseguramiento de SI, por ej., documento técnico (white paper), programas de auditoría / aseguramiento de SI, los productos de la familia de COBIT® 5.

Se proporciona un glosario en línea de los términos utilizados en ITAF en *www.isaca.org/glossary*.

Aclaración: ISACA ha diseñado esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado exitoso. La publicación no debe considerarse como incluyente de cualquier procedimiento y pruebas o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a obtener los mismos resultados. Para determinar la conveniencia de cualquier procedimiento o prueba específica, los profesionales de controles deben aplicar su propio juicio profesional a las circunstancias de control específicas presentadas por los sistemas particulares o entorno de SI.

El Comitéde Estándares Profesionales y Administración de Carreras de ISACA, en Inglés “ISACA Professional Standards and Career Management Committee” (PSCMC) se ha comprometido a una amplia consulta en la preparación de estándares y guías. Antes de emitir cualquier documento, se emite internacionalmente un borrador de la norma para comentar por el público general. Los comentarios pueden también presentarse a la atención del director de desarrollo de estándares profesionales por correo electrónico (*standards@isaca.org*), fax (+1.847. 253.1443) o correo postal (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

Guía de Auditoría y Aseguramiento de SI 2205 Evidencia

La guía se presenta en las siguientes secciones:

1. Propósito de la guía y vinculación con estándares.
2. Contenido de la guía.
3. Relación con estándares y procesos de COBIT 5.
4. Terminología.
5. Fecha de vigencia.

1.Propósito de la Guía y Vinculación con Estándares

1.0 Introducción

Esta sección clarifica:

1.1 Propósito de la guía
1.2 Vinculación con estándares
1.3 Uso de términos 'función de auditoría' y 'profesionales'

1.1 Propósito

1.1.1 El propósito de esta guía es proporcionar ayuda a los profesionales de auditoría y aseguramiento de SI a obtener evidencia suficiente y apropiada, evaluar la evidencia recibida y preparar la documentación de auditoría apropiada.

1.1.2 Los profesionales de auditoría y aseguramiento de SI deben considerar esta guía para determinar cómo implementar el estándar, uso de su juicio profesional en su aplicación, estar preparado para justificar cualquier desvío y buscar guías adicionales si se considera necesario.

1.2 Vinculación con estándares

1.2.1 Estándar 1203 Desempeño y supervisión
1.2.2 Estándar 1205 Evidencia
1.2.3 Estándar 1206 Uso del Trabajo de Otros Expertos

1.3 Uso de términos

1.3.1 De aquí en adelante:

- 'Función de auditoría y aseguramiento de SI' esta referenciada como 'función de auditoría'
- 'Profesionales de auditoría y aseguramiento de SI' esta referenciada como 'profesionales'

2.Contenido de la Guía

2.0 Introducción

La sección del contenido de la guía está estructurada para proporcionar información sobre los siguientes temas de compromiso clave de auditoría y aseguramiento:

1.1 Tipos de evidencia
1.2 Obtener evidencia
1.3 Evaluar la evidencia
1.4 Preparar documentación de auditoría

Guía de Auditoría y Aseguramiento de SI 2205 Evidencia

2.1 Tipos de Evidencia

2.1.1 Cuando se planifica y desarrolla un trabajo, los profesionales deben considerar los tipos de evidencia a obtener, su uso para cumplir los objetivos del trabajo y sus diferentes niveles de confiabilidad. Los diferentes tipos de evidencia que los profesionales deben considerar usar se incluyen:

- Procesos observados y existencia de elementos físicos
- Evidencia documental
- Representaciones
- Análisis

2.1.2 Los procesos observados y la existencia de elementos físicos puede incluir observaciones de actividades, propiedad y funciones de SI, como:

- Un sistema de monitoreo de la seguridad de la red en desempeño
- Un inventario de medios en un lugar de almacenamiento externo

2.1.3 Evidencia documental, grabada en papel u otro medio, puede incluir:

- Políticas y procedimientos escritos
- Resultados de extracciones de datos
- Registros de transacciones
- Listados de programas
- Otros documentos y registros producidos en el curso del negocio ordinario

2.1.4 Representaciones escritas y orales de los auditados que pueden incluir:

- Declaración por escrito por la gerencia, ejemplo, representaciones acerca del la existencia y efectividad de controles internos o planes para la implementación de un nuevo sistema financiero.
- Representación oral de cosas tales como el desempeño de un proceso o un plan de seguimiento para la gerencia de acciones relacionadas con el programa de concienciación de la seguridad

2.1.5 Los resultados de analizar la información a través de comparaciones, simulaciones, cálculos y razonamiento que pueden también ser usadas como evidencia. Algunos ejemplos:

- Comparación de rendimiento de SI con otras empresas o periodos pasados
- Comparación de ratios de error entre aplicaciones, transacciones y usuarios
- Repetición de los procesos o controles

2.2 Obtener Evidencia

2.2.1 Los profesionales deben obtener evidencia suficiente y apropiada para permitirles definir conclusiones de auditoría razonable. Esta evidencia incluye:

- Procedimientos realizados
- Resultados de los procedimientos realizados
- Documentos fuente (en formato electrónico o papel), registros e información utilizada para apoyar el trabajo de auditoría.
- Documentación de que se realizo el trabajo y cumple con leyes aplicables, regulaciones y políticas.

2.2.2 Cuando la evidencia obtenida en forma de representación oral es crítica para la opinión o conclusión de auditoría, los profesionales deben considerar obtener la confirmación de las representaciones, por escrito o

2.2 Obtener Evidencia cont.

electrónicamente (por ejemplo por correo electrónico). Los profesionales deben considerar también evidencia alternativa para corroborar estas representaciones para asegurar su fiabilidad.

2.2.3 Cuando obtiene las evidencias, el profesional debe considerar:

- El tiempo, nivel de esfuerzo y coste de obtener la evidencia comparado a la suficiencia de evidencia en la reducción de riesgo de auditoría.
- Importancia de la materia evaluada y del procedimiento de auditoría que requiere la evidencia en el logro de los objetivos de auditoría y reducir el riesgo de auditoría.
- Evidencia electrónica que no puede ser recuperable en su totalidad o parte después del paso del tiempo

2.2.4 Los Procedimientos utilizados para obtener evidencias varían dependiendo de las características de los SI auditados, tiempos de la auditoría, alcance y objetivos de la auditoría, y juicio profesional. La evidencia puede ser obtenida a trabes del so de procedimientos de auditoría manual, técnicas de auditoría asistidas por ordenador (CAATs) o una combinación de ambos. Los profesionales deben seleccionar el procedimiento más apropiado en relación al objetivo de auditoría de SI. Se deben considerar los siguientes procedimientos:

- **Investigación y confirmación**—El proceso de búsqueda de información de personas con experiencia que están familiarizados con la materia. Las personas experimentadas no necesitan ser miembros de la empresa auditada. Este procedimiento puede ir desde investigaciones formales por escrito a orales informales.
- **Observación**—La observación de un procedimiento o proceso realizado por los individuos que típicamente son responsables de su realización, u observar elementos físicos como locales, ordenadores o ajustes o configuraciones de SI. Este tipo de evidencia está limitado al punto de tiempo en que se llevo a cabo. Los profesionales deben tener en cuenta que observar la realización de un proceso o procedimiento puede afectar a como se realiza ese procedimiento o proceso.
- **Inspección**—Examen de documentos y registros internos o externos. Los elementos a inspeccionar pueden suministrarse en papel o formato electrónico. La inspección puede también incluir examen de activos físicos.
- **Procedimientos analíticos**—Evaluar datos (financieros o no) mediante examen de las posibles relaciones entre los datos o entre los datos y otra información importante. Esto también incluye el examen de fluctuaciones, tendencias y relaciones inconsistentes.
- **Nuevo cálculo / computación**—El proceso de comprobar la exactitud aritmética y matemática de los documentos o registros. Puede realizarse manualmente o a través del uso de CAATs.
- **Realización de nuevo**—Realización independiente de procedimientos y / o controles que fueron ejecutados originalmente por los SI o por la propia empresa.
- **Otros métodos aceptados generalmente**—Otros procedimientos aceptados generalmente que pueden seguir los profesionales para obtener evidencias suficientes y apropiadas. Por ejemplo, pueden

2.2 Obtener Evidencia cont.

realizar ingeniería social, actuar como un invitado misterioso o realizar pruebas éticas de intrusión.

2.2.5 Cuando obtienen evidencias, los profesionales deben considerar la independencia y competencia del proveedor de la evidencia de auditoría. Por ejemplo, la evidencia de auditoría corroborativa de un tercero independiente puede ser más confiable que la evidencia de auditoría obtenida de la empresa auditada. La evidencia de auditoría física generalmente es más confiable que las representaciones de un individuo.

2.2.6 Si hay una posibilidad que la evidencia obtenida forme parte de un procedimiento legal, los profesionales deben consultar con el consultor legal apropiado para determinar si existen requisitos especiales que afectaran en la forma en que la evidencia necesita ser obtenida, presentada y revelada.

2.2.7 En situaciones donde los profesionales no son capaces de obtener suficiente evidencia de auditoría, como cuando los individuos o la gerencia rehúsan a proporcionar evidencia suficiente y apropiada necesaria para conseguir los objetivos de auditoría de SI, los profesionales deben revelar la situación a los gerentes de auditoría, y si es necesario a los encargados del Gobierno. Los profesionales deben revelar este hecho también de acuerdo con los procedimientos de auditoría establecidos en la organización. Las restricciones o limitaciones del alcance de la auditoría y el logro de los objetivos de auditoría deben darse a conocer en el comunicado de los resultados de la auditoría.

2.2.8 Los profesionales deben conservar las evidencias después de completar el trabajo de auditoría para asegurar que la evidencia es:

- Disponible para un periodo de tiempo y en un formato que cumple con las políticas de auditoría de la organización y estándares, leyes y regulaciones profesionales relevantes,
- Protección contra la divulgación o modificación no autorizada durante su preparación y retención
- Correctamente eliminados al final del periodo de retención

2.3 Evaluar Evidencia

2.3.1 La evidencia es suficiente y apropiada cuando proporciona una base razonable para apoyar los hallazgos o conclusiones dentro del contexto de los objetivos de auditoría. Si, en juicio de los profesionales, la evidencia no cumple esos criterios, deben obtener evidencia adicional o realizar procedimientos adicionales para reducir las limitaciones o incertidumbres relacionadas con la evidencia. Por ejemplo, un listado fuente del programa no puede ser evidencia adecuada hasta que se obtiene otra evidencia que verifique que representa el programa actual utilizado en el proceso de producción.

2.3.2 Al evaluar la fiabilidad de las evidencias obtenidas durante la auditoría, los profesionales deben considerar las características y propiedades de la evidencia, como su origen, naturaleza (escrita, oral, visual o electrónica), autenticidad (presencia de firma digital o manual, sellado de fecha / hora), y relaciones entre la evidencia que proporciona la evidencia corroborativa de

2.3 Evaluar Evidencia cont.

múltiples fuentes. En general, la confiabilidad de la evidencia se categoriza de baja a alta basándose en los procedimientos utilizados para obtener la evidencia como sigue:

- Investigación y confirmación
- Observación
- Inspección
- Procedimientos analíticos
- Repetir el cálculo o computación
- Repetir la realización

Para cada procedimiento anterior, la confiabilidad de la evidencia es mayor generalmente cuando:

- Forma escrita, en lugar de obtenerse de representaciones orales
- Obtenida directamente por los profesionales en lugar de indirectamente por la entidad auditada
- Obtenida de fuentes independientes
- Certificada por una tercero independiente
- Mantenida por un tercero independiente

2.3.3 Los profesionales deben considerar el periodo de tiempo durante el que existe o está disponible la información para determinar la naturaleza, tiempos y alcance de las pruebas sustantivas y, si es aplicable, pruebas de cumplimiento. Por ejemplo, la evidencia procesada por intercambio electrónico de datos (EDI), procesamiento de documentos de imágenes (DIP) y sistemas dinámicos como hojas de cálculo puede no ser recuperable tras un periodo de tiempo especifico si los cambios a los ficheros no están controlados o no los archivos no están respaldados. La disponibilidad de la documentación puede verse impactada por las políticas de retención de documentos de la empresa.

2.3.4 Si hay un tercero auditor independiente, los profesionales deben considerar si las pruebas de controles relevantes para el sujeto de la auditoría fueron realizadas y si se puede confiar en los resultados de las pruebas.

2.3.5 Los profesionales deben obtener evidencia suficiente y apropiada para permitir a un tercero independiente cualificado realizar las pruebas y obtener el mismo resultado y conclusiones.

2.4 Preparar Documentación de Auditoría

2.4.1 Durante la realización de la auditoría, los profesionales deben preparar documentación de la evidencia obtenida para retener y estar disponible durante un periodo de tiempo predefinido y en un formato que cumple las políticas de la empresa y estándares, leyes y regulaciones profesionales relevantes.

2.4.2 La evidencia obtenida durante el desarrollo de la auditoría debe ser adecuadamente identificada, con referencias cruzadas, y catálogos para facilitar la determinación de la suficiencia global y adecuación de la evidencia para apoyar de forma razonable los hallazgos y conclusiones dentro del contexto de los objetivos de la auditoría y permitir fácilmente la recuperación por otros miembros del equipo de auditoría de SI o terceros independientes.

2.4 Preparar Documentación de Auditoría cont.

2.4.3 Los profesionales deben asegurarse que la documentación de la evidencia está protegida de acceso, divulgación o modificación no autorizados durante su preparación y retención.

2.4.4 Los profesionales deben disponer de documentación de la evidencia al final del periodo de retención establecido.

3. Relación con Estándares y Procesos de COBIT 5

3.0 Introducción

Esta sección proporciona una visión general relevante de:
3.1 Relación con Estándares
3.2 Relación con los procesos de COBIT 5
3.3 Otras guías

3.1 Relación con Estándares

La tabla proporciona una visión general de:
- Los estándares más relevantes de ISACA que están directamente soportados por esta guía
- Las declaraciones estándar más relevantes para esta guía

Nota: Solo se enumeran las declaraciones estándar más relevantes para esta guía.

Titulo del Estándar	Declaración Estándar Relevante
1203 Desempeño y Supervisión	Los profesionales de auditoría y aseguramiento de SI deberán obtener evidencias suficientes, confiables, relevantes y a tiempo para conseguir los objetivos de auditoría. Los hallazgos y conclusiones de auditoría deben estar soportados por análisis e interpretación apropiados de estas evidencias. Los profesionales de auditoría y aseguramiento deberán documentar el proceso de auditoría, describiendo el trabajo de auditoría y la evidencia de auditoría que soporta los hallazgos y conclusiones.
1205 Evidencia de Auditoría	Los profesionales de auditoría y aseguramiento deberán obtener evidencia suficiente y adecuada para llegar a conclusiones razonables sobre las qué basar los resultados del trabajo. Los profesionales de auditoría y aseguramiento de SI deberán evaluar la suficiencia de la evidencia obtenida para apoyar las conclusiones y lograr los objetivos del trabajo.
1206 Uso del Trabajo de Otros Expertos	Los profesionales de auditoría y aseguramiento de SI deberán aplicar procedimientos de pruebas adicionales para obtener evidencia suficiente y adecuada en las circunstancias donde el trabajo de otros expertos no provea evidencia suficiente y adecuada.

3.2 Relación con los procesos de COBIT 5

La tabla proporciona una visión general de los más relevantes:

- Procesos de COBIT 5
- Propósito de los procesos de COBIT 5

Se encuentran actividades específicas realizadas como parte de la ejecución de estos procesos en *COBIT 5: Habilitación de Procesos*.

Procesos de COBIT 5	Propósito de los Procesos
MEA02 Monitorear y evaluar el sistema de controles internos.	Obtener transparencia para los interesados clave en la adecuación de los sistemas de control interno y, por tanto, proporcionar confianza en las operaciones, confianza en el logro de objetivos empresariales y una adecuada comprensión del riesgo residual.

3.3 Otras Guías

En la implementación de estándares y guías, se insta a los profesionales a buscar otras guías cuando se considere necesario. Esto podría ser desde auditoría y aseguramiento de SI:

- Colegas dentro de la empresa
- Gerentes
- Órganos de Gobierno dentro de la empresa, ejemplo, comité de auditoría
- Organizaciones profesionales o grupos de redes sociales profesionales
- Otras guías profesionales (por ejemplo, libros, papeles, otras guías)

4. Terminología

Término	Definición
Evidencia apropiada	La medida de calidad de la evidencia
Evidencia suficiente	La medida de la cantidad de evidencia; apoya todas las cuestiones materiales al objetivo y alcance de la auditoría. Ver evidencia.
Representación	Una declaración firmada u oral emitida por la gerencia a los profesionales, donde la gerencia declara que un hecho actual o futuro (por ejemplo, proceso, sistema, procedimiento, política) esta o estará en cierto estado, para el mejor conocimiento de la gerencia

5. Fecha de Vigencia

5.1 Fecha de Vigencia

Esta guía revisada es efectiva para todo compromiso de auditoría y aseguramiento de SI con fecha de inicio igual o posterior al 1 de Septiembre de 2014.

