Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación

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 2202 Análisis de Riesgos en la Planificación

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 nivel de trabajo de auditoría requerido para conseguir los objetivos de auditoría es una decisión subjetiva realizada por los profesionales de auditoría y aseguramiento de SI. El propósito de esta guía es reducir el riesgo de alcanzar una conclusión incorrecta basada en los hallazgos de auditoría y reducir la existencia de errores en el área auditada.

1.1.2 La guía proporciona ayuda en aplicar una aproximación de análisis de riesgos para desarrollar:

- Plan de auditoría de SI que cubre todos los trabajos de auditoría anuales.
- Plan de proyecto del trabajo de auditoría que se enfoca en un trabajo de auditoría especifico.

1.1.3 La guía proporciona los detalles de los diferentes tipos de riesgo que se encuentran los profesionales de auditoría y aseguramiento de SI se encontrara.

1.1.4 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 1201 Planificación de la asignación.
1.2.2 Estándar 1202 Evaluación de riesgo en planificación.
1.2.3 Estándar 1203 Desempeño y supervisión.
1.2.4 Estándar 1204 Materialidad.
1.2.5 Estándar 1207 Irregularidades y actos ilegales.

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 Análisis de riesgos del plan de auditoría de SI.
1.2 Metodología de análisis de riesgos.
1.3 Análisis de riesgos de trabajos de auditoría individuales.
1.4 Riesgo de auditoría.
1.5 Riesgo inherente.
1.6 Riesgo de control.
1.7 Riesgo de detección.

2.1 Análisis de Riesgos del Plan de Auditoría de SI

2.1.1 Al desarrollar un plan de auditoría de SI completo, se debe seguir un enfoque de análisis de riesgos adecuado. Se debe realizar y documentar un análisis de riesgos al menos una vez al año para facilitar el procedo de desarrollo del plan de auditoría de SI. Debe tener en cuenta los planes y objetivos estratégicos organizacionales y el marco e iniciativas de gerencia del riesgo de la empresa.

2.1.2 Para evaluar correcta y completamente que el riesgo está relacionado al alcance del área de auditoría de SI, los profesionales deben considerar los siguientes elementos al desarrollar el plan de auditoría de SI:

- Cubrir completamente todas las áreas del alcance del universo de auditoría de SI, que representa el rango de toda posible actividad de auditoría.
- Fiabilidad y adecuación del análisis de riesgos proporcionado por la gerencia.
- Los procesos seguidos por la gerencia para supervisar, examinar e informar posibles riesgos o problemas.
- Cubrir el riesgo en actividades conexas relacionadas a las actividades bajo revisión.

2.1.3 El enfoque de análisis de riesgos aplicado debe ayudar a priorizar y planificar los procesos de auditoría de SI y el trabajo de aseguramiento. Debe apoyar la selección de áreas y temas de interés para la auditoría y la decisión del proceso para diseñar y llevar a cabo los trabajos de auditoría de SI particulares.

2.1.4 Los profesionales deben asegurarse que el enfoque de análisis de riesgos aplicado esta aprobado por los encargados del Gobierno y distribuido a los diferentes interesados del trabajo.

2.1.5 Los profesionales deben usar el análisis de riesgos para cuantificar y justificar la cantidad de recursos de auditoría de SI necesarios para completar el plan de auditoría de SI y los requerimientos para los trabajos específicos.

2.1.6 Basándose en el análisis de riesgos, los profesionales deben desarrollar un plan de auditoría de SI que actúe como marco de trabajo para las actividades de auditoría y aseguramiento de SI. Debe:

2.1 Análisis de Riesgos del Plan de Auditoría de SI cont.

- Considerar requerimientos y actividades distintos de auditoría y aseguramiento.
- Actualizarse al menos anualmente.
- Estar aprobado por los encargados del Gobierno.
- Direccionar las responsabilidades establecidas por la carta de auditoría.

Para más información referirse al Estándar 1201 Planificación de la asignación.

2.2 Metodología de Análisis de Riesgos

2.2.1 Los profesionales deben considerar la metodología de análisis de riesgos apropiada para asegurar que se cubre completa y exactamente los trabajos de auditoría en el plan de auditoría de SI.

2.2.2 Los profesionales deben al menos incluir un análisis, dentro de la metodología, del riesgo para la empresa relacionado con la disponibilidad de los sistemas, integridad de los datos y confidencialidad de la información del negocio.

2.2.3 Existen muchas metodologías de análisis de riesgos que apoyan el proceso de análisis de riesgos. Estas van desde simples clasificaciones de alto, medo y bajo, basadas en juicio profesional, a cálculos más cuantitativos y científicos proporcionando una clasificación de riesgo numérico, y otras que son una combinación de ambas. Los profesionales deben considerar el nivel de complejidad y detalle apropiado para la empresa o materia auditada. Se puede encontrar ayuda específica en el desarrollo del análisis de riesgos en la publicación de ISACA *COBIT 5 para el Riesgo*.

2.2.4 Todas las metodologías de análisis de riesgos se basan en juicios subjetivos en algún punto del proceso (ejemplo, para asignar pesos a los diferentes parámetros). Los profesionales deben identificar la decisión subjetiva requerida para utilizar una metodología particular y considerar si estos juicios pueden hacerse y validarse en un nivel adecuado de precisión.

2.2.5 Para decidir cuál es la metodología de análisis de riesgos más adecuada, los profesionales deben considerar:

- Tipo de información requerida a recoger (algunos sistemas utilizan efectos financieros como la única medida – esto no siempre es adecuado para los trabajos de auditoría de SI).
- Coste del software o de otras licencias requeridas para utilizar la metodología.
- Grado en que la información requerida esta siempre disponible.
- Cantidad de información adicional requerida para recoger antes de que se pueda obtener una salida confiable, y los costes de recoger esta información (incluyendo el tiempo necesario a invertir en el ejercicio de recopilación).
- Opiniones de otros usuarios de la metodología, y su visión de cómo les ha ayudado en la mejora de la eficiencia y/o efectividad de sus auditorías.
- Disposición de los encargados del Gobierno del área de auditoría de SI para aceptar la metodología como los medios para determinar el tipo y

2.2 Metodología de Análisis de Riesgos cont.

nivel del trabajo de auditoría llevado a cabo.

2.2.6 No existe una metodología única de análisis de riesgos que sea apropiada para todas las situaciones. Las condiciones que afectan a la auditoría pueden cambiar en el tiempo. Periódicamente, los profesionales deben reevaluar la adecuación de la metodología de análisis de riesgos elegida.

2.2.7 Los profesionales deben utilizar las técnicas de análisis de riesgos seleccionadas en el desarrollo del plan de auditoría de SI completo y en la planificación de los trabajos de auditoría específicos. El análisis de riesgos, en combinación con otras técnicas de auditoría, debe ser considerado en la toma de decisiones de planificación como:

- Áreas o funciones de negocio a auditar.
- Cantidad de tiempo y recursos a asignar a una auditoría.
- Naturaleza, alcance y tiempos de los procedimientos de auditoría.

2.2.8 La metodología de análisis de riesgos adoptada debe producir resultados consistentes, validos, comparables y repetibles. El análisis de riesgos que surge de la metodología debe ser coherente (durante un periodo), valida, comparable (con evaluaciones anteriores / posteriores usando la misma metodología de análisis) y repetible (dado un conjunto de hechos similar, utilizando la misma metodología de análisis producirá una salida similar).

2.3 Análisis de Riesgos de Trabajos de Auditoría Individuales

2.3.1 Cuando se planifica un trabajo individual, los profesionales deben identificar y analizar el riesgo relevante para el área bajo revisión. Los resultados de este análisis de riesgos deben estar reflejados en los objetivos del trabajo de auditoría. Durante el análisis de riesgos, los profesionales deben considerar:

1. Los resultados de un trabajo de auditoría anterior, las revisiones y hallazgos, incluyendo cualquier actividad correctiva.
2. El proceso de análisis de riesgos global de la empresa.
3. La probabilidad de suceso de un riesgo particular.
4. El impacto de un riesgo particular (en medida monetaria u otro valor) si ocurre.

2.3.2 Los profesionales deben garantizar la comprensión completa de las actividades en el alcance antes del análisis de riesgos. Deben solicitar comentarios y sugerencias de interesados y otras partes adecuadas. Es necesario determinar y examinar correctamente el impacto del posible riesgo en los trabajos de auditoría.

2.3.3 El objetivo del análisis de riesgos es la reducción del riesgo de auditoría a un nivel bajo aceptable, e identificar esas partes de una actividad que deben recibir más foco de auditoría. Esto necesita realizarse por un análisis adecuado de la materia de SI y controles relacionados, mientras que se planifica y realiza la auditoría de SI.

2.3.4 Cuando se planifica un procedimiento de auditoría y aseguramiento de SI especifica, los profesionales deben reconocer el hecho que cuando menor es el nivel de la materialidad, las expectativas de la auditoría serán más precisas y mayor el riesgo de auditoría.

2.3 Análisis de Riesgos de Trabajos de Auditoría Individuales cont.

2.3.5 Cuando se planifica un procedimiento de auditoría y aseguramiento de SI especifico, los profesionales deben considerar los posibles actos ilegales que pueden requerir una modificación de la naturaleza, tiempos o extensión de los procedimientos existentes. Para más información, consulte el Estándar 1207 Irregularidades y actos ilegales y la Guía 2207.

2.3.6 Para tener seguridad adicional en los casos donde hay elevado riesgo de auditoría o un umbral de materialidad menor, los profesionales deben compensar por cualquier extensión al alcance o naturaleza de las pruebas de auditoría de SI o incrementar o extender las pruebas sustantivas.

2.4 Riesgo de Auditoría

2.4.1 El riesgo de auditoría se refiere al riesgo de alcanzar una conclusión incorrecta basada en los resultados de la auditoría. Los tres componentes del riesgo de auditoría son:

- Riesgo de Control.
- Riesgo de Detección.
- Riesgo Inherente.

2.4.2 Los profesionales deben considerar cada componente del riesgo para determinar el nivel de riesgo general. Esto incluye el riesgo de la materia, que incluye el riesgo inherente y el riesgo de control; juntos con el riesgo de detección se referencian como riesgo de auditoría. Puede encontrar más información de los diferentes componentes del riesgo de auditoría en las secciones 2.5 a 2.7.

2.5 Riesgo Inherente

2.5.1 El riesgo inherente es la susceptibilidad de errar un área de auditoría de forma que puede ser importante, individual o en combinación con otros errores, asumiendo que no hubo controles internos relacionados. Por ejemplo, el riesgo inherente asociado con sistemas operativos sin controles apropiados es generalmente alto, ya que los cambios, o incluso la divulgación, de datos o programas a través de los fallos de seguridad del sistema operativo podrían llevar a información de administración falsa o desventaja competitiva. Por contraste, el riesgo inherente asociado con la seguridad para un PC independiente sin controles es bajo generalmente, cuando un análisis adecuado demuestra que no se usa para fines de negocio críticos.

2.5.2 Los riesgos inherentes para la mayoría de las áreas de auditoría es alto ya que los efectos potenciales de errores generalmente abarca varios sistemas de negocio y muchos usuarios.

2.6 Riesgo de Control

2.6.1 El riesgo de control es el riesgo que pueda suceder un error en un área de auditoría y podría ser material, individual o una combinación con otros errores, no será prevenido, detectado ni corregido oportunamente por el sistema de control interno. Por ejemplo, el riesgo de control asociado con

2.6 Riesgo de Control cont.

revisiones manuales de logs de ordenador puede ser alto por el volumen de la información de log. El riesgo de control asociado con los procedimientos de validación de datos por ordenador generalmente es bajo porque los procesos se aplican coherentemente.

2.6.2 Los profesionales deberán evaluar el riesgo de control como alto a menos existan controles internos relevantes:

- Identificados.
- Evaluados como efectivos.
- Se prueba y demuestra que funcionan adecuadamente.

2.6.3 Los profesionales deben considerar tanto los controles de SI generalizados como los controles de SI detallados:

- Controles de SI generalizados considerados un subconjunto de controles generales; son controles que se centran en la gerencia y monitorización del entorno de SI. Por lo tanto afectan a todas las actividades relacionadas con SI. El efecto de los controles de SI generalizados en el trabajo de los profesionales no se limita a la fiabilidad de los controles de aplicación en el sistema de proceso del negocio. También afectan a la fiabilidad de los controles de SI detallados sobre, por ejemplo, desarrollo de programas, implementación de sistemas, administración de seguridad y procedimientos de backup. Los controles de SI generalizados débiles, y por lo tanto la gerencia y monitorización débil del entorno de SI, debe alertar a los profesionales a la posibilidad de un alto riesgo que los controles diseñados a operar en el nivel detallado pueden ser inefectivos.
- Los controles de SI detallados se componen de los controles de aplicación más aquellos controles generales no incluidos en los generalizados. Siguiendo el marco de trabajo COBIT, son los controles sobre los sistemas y servicios de SI de adquisición, implementación, entrega y soporte.

2.6.4 Un riesgo que deben considerar los profesionales es la limitaciones y deficiencias en los controles de SI detallados que son inducidos por insuficiencias de los controles de SI generalistas.

2.7 Riesgo de Detección

2.7.1 El riesgo de detección es el riesgo de que los procedimientos sustantivos de los profesionales no detecten un error que podría ser material, individual o una combinación con otros errores. Por ejemplo, el riesgo de detección asociado con la identificación de brechas de seguridad en una aplicación generalmente es alto porque los logs para el periodo completo de la auditoría no están disponibles en el momento de la auditoría. El riesgo de detección asociado con la identificación de la falta de planes de recuperación de desastres generalmente es bajo, ya que se comprueba fácilmente.

2.7.2 Para determinar el nivel de pruebas sustantivas requeridas, los profesionales deben considerar:

2.7 Riesgo de Detección cont.

•Análisis del riesgo inherente.
•Conclusiones sobre el riesgo de control tras las pruebas de cumplimiento.

2.7.3 Cuando mayor sea la evaluación del riesgo inherente y de control, el profesional deberá obtener normalmente mas evidencia de auditoría de la realización de los procedimientos de auditoría sustantivos.

3. Relación con Estándares y Procesos de COBIT 5

3.0 Introducción

Esta sección proporciona una visión general relevante de:
3.1Relación con Estándares.
3.2Relación con los procesos de COBIT 5.
3.3Otras 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
1201 Planificación de la asignación.	Los profesionales de auditoría y aseguramiento de SI deben planear cada trabajo de auditoría y aseguramiento de SI para dirigir: • Objetivo(s), alcance, línea de tiempo y entregables. • Cumplimiento con leyes aplicables y estándares de auditoría profesionales. • Uso de enfoque basado en riesgos, cuando sea adecuado • Cuestiones especificas del trabajo. • Requisitos de documentación y presentación de informes.
1202 Evaluación de Riesgos en la Planificación de Auditoría.	La función de auditoría y aseguramiento de SI deberá utilizar un enfoque apropiado y el apoyo de metodología de análisis de riesgos para desarrollar el plan de auditoría de SI general y determinar las prioridades para la asignación efectiva de recursos de auditoría de SI. Los profesionales de auditoría y aseguramiento de SI deberán identificar y analizar los riesgos relevantes al área bajo revisión, en la planificación de trabajos individuales. Los profesionales de auditoría y aseguramiento deberán considerar el riesgo de la materia, riesgo de auditoría y exposiciones relacionadas con la empresa.

Titulo del Estándar	Declaración Estándar Relevante
1203 Desempeño y Supervisión.	Los profesionales de auditoría y aseguramiento de SI deberán conducir el trabajo de acuerdo al plan de auditoría de SI aprobado para cubrir los riesgos identificados y dentro del plan acordado.
1204 Materialidad.	Los profesionales de auditoría y aseguramiento de SI deberán considerar las debilidades o ausencias de controles potenciales mientras planifican un trabajo, y si tal debilidad o ausencia de control podría resultar en una deficiencia significativa o debilidad material. Los profesionales de auditoría y aseguramiento de SI deberán considerar la materialidad y su relación con el riesgo de auditoría mientras determinan la naturaleza, tiempos y extensión de los procedimientos de auditoría. Los profesionales de auditoría y aseguramiento de SI deberán considerar el efecto acumulativo de las deficiencias o debilidades de control menor y si la ausencia de controles se traduce en una deficiencia significativa o debilidad material. Los profesionales de auditoría y aseguramiento revelaran lo siguiente en el informe de auditoría: • Ausencia de controles o controles inefectivos. • Importancia de la deficiencia de los controles. • Probabilidad de estas debilidades resulten en una deficiencia significativa o debilidad material.
1207 Irregularidades y actos ilegales.	Los profesionales de auditoría y aseguramiento de SI deberán considerar el riesgo de actos irregulares e ilegales durante el trabajo.

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
EDM01 Asegurar el establecimiento y mantenimiento del marco de Gobierno.	Proporcionar un enfoque consistente integrado y alineado con el enfoque de Gobierno de la empresa. Para asegurar que las decisiones relacionadas con TI se hacen en línea con las estrategias y objetivos de la empresa, asegurando que los procesos relacionados con TI son

Procesos de COBIT 5	Propósito de los Procesos
	supervisados de forma efectiva y transparente, se confirma el cumplimiento con los requerimientos legales y regulatorios, y se cumplen los requerimientos de Gobierno de los miembros del consejo.
EDM03 Asegurar la optimización del riesgo.	Asegurar que el riesgo empresarial relacionado con TI no excede el riesgo aceptado y la tolerancia de riesgo, el impacto de riesgo de TI al valor de la empresa está identificado y gestionado, y la posibilidad de fallos de cumplimiento esta minimizada.
APO12 Gestionar el riesgo.	Integrar la gerencia de riesgos empresariales relacionados con TI con el ERM en general, y el balance de costes y beneficios de la gerencia de riesgos empresariales relacionados con TI.
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.
MEA03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos.	Asegurar que la empresa cumple con todos los requerimientos externos.

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 y fuera de la empresa, por ejemplo, a través de asociaciones profesionales o grupos de redes sociales profesionales.
- Gerentes.
- Órganos de Gobierno dentro de la empresa, ejemplo, comité de auditoría
- Otras guías profesionales (por ejemplo, libros, papeles, otras guías).

4. Terminología

Término	Definición
Análisis de Riesgos	Un proceso utilizado para identificar y evaluar riesgos y sus efectos potenciales. Los análisis de riesgos se utilizan para identificar aquellos elementos o áreas que presentan el riesgo, vulnerabilidad o exposición más altos para la empresa para incluirlos en el plan de auditoría anual de SI. Los análisis de riesgos se utilizan también para gestionar la ejecución de los proyectos y el riesgo en beneficio del proyecto.

Término	Definición
Carta de Auditoría	Un documento aprobado por los encargados de Gobierno que define el propósito, autoridad y responsabilidad de la actividad de auditoría y aseguramiento de SI interna. La carta debe: • Establecer la posición de la función de auditoría y aseguramiento de SI interna dentro de la empresa. • Autorizar acceso a registros, personal y los bienes relevantes para la realización del encargo de auditoría y aseguramiento de SI. • Definir el alcance de las actividades de la función de auditoría y aseguramiento de SI.
Controles de SI Detallados	Controles sobre las adquisición, implementación, entrega y soporte de sistemas y servicios de SI formado por los controles de aplicación más aquellos controles generales no incluidos en los controles generales.
Controles de SI Generalizados	Controles generales diseñados para gestionar y monitorear el entorno de SI y que, por tanto, afecta a todas las actividades relacionadas con SI.
Materialidad	Un concepto de auditoría respecto de la importancia de una información respecto a su impacto o efecto en el sujeto auditado. Una expresión del significado o importancia relativa de una materia particular en el contexto del encargo o la empresa en su conjunto.
Prueba Sustantiva	La obtención de evidencia de auditoría sobre la integridad, exactitud o existencia de actividades o transacciones durante el periodo de la auditoría.
Riesgo de Auditoría	El riesgo de llegar a una conclusión incorrecta basada en los resultados de la auditoría. Los tres componentes de riesgo de auditoría son: • Riesgo de control. • Riesgo de detección. • Riesgo inherente.
Riesgo de Control	El riesgo que exista un error material que no se evite o detectado de forma oportuna por el sistema de control interno. Ver riesgo inherente.
Riesgo de Detección	El riesgo que los procedimientos sustantivos del profesional de auditoría y aseguramiento de SI no detectara un error que podría ser material, individual o en combinación con otros errores. Ver riesgo de auditoría.
Riesgo Inherente	El nivel de riesgo o exposición sin tener en cuenta las acciones que la gerencia ha tomado o ha podido tomar (ejemplo, implementar controles). Ven riesgo de control.

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.

