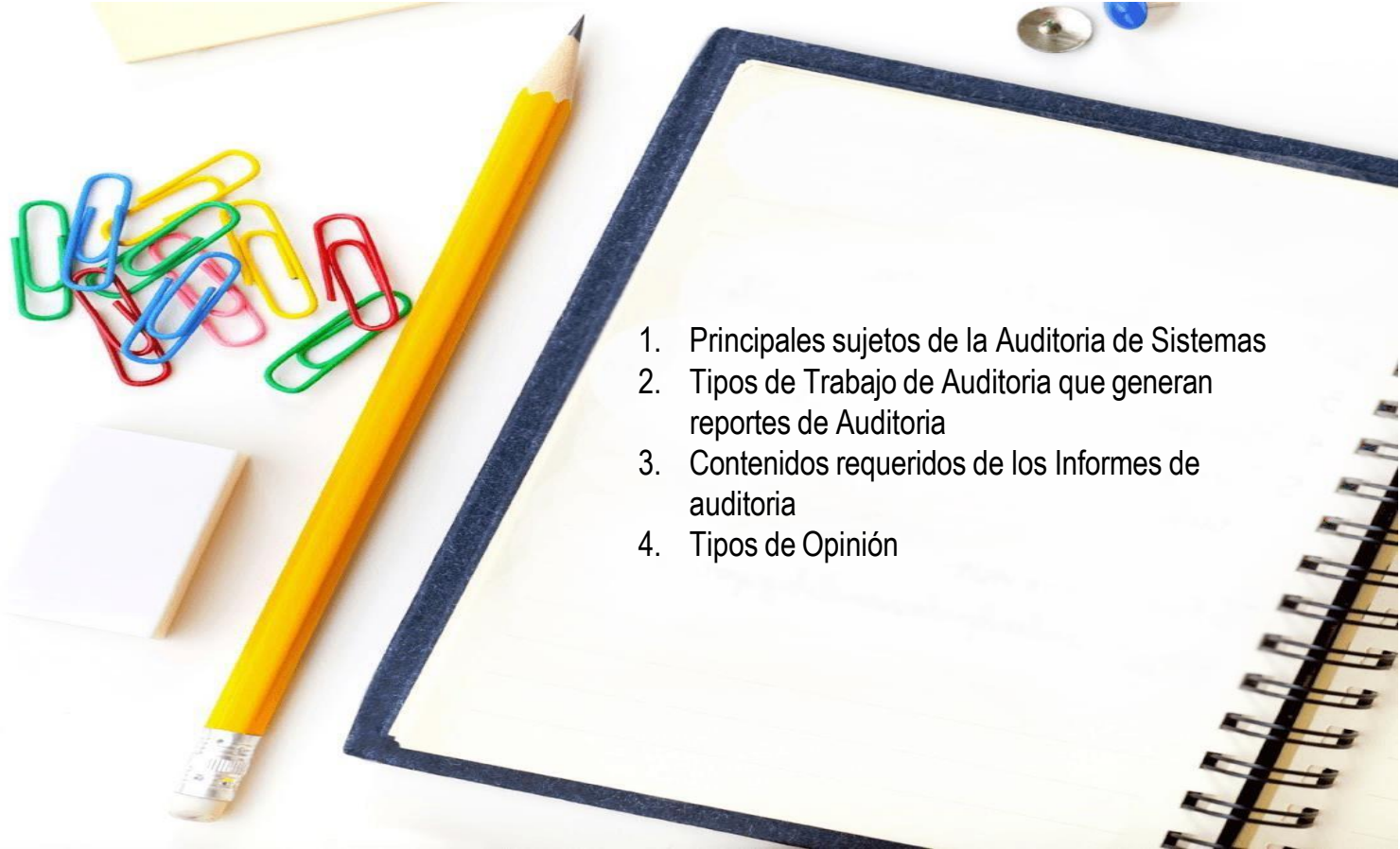


AUDITORÍA Y CONTROL DE SISTEMAS

INFORME DE AUDITORÍA

Agenda

- 
1. Principales sujetos de la Auditoria de Sistemas
 2. Tipos de Trabajo de Auditoria que generan reportes de Auditoria
 3. Contenidos requeridos de los Informes de auditoria
 4. Tipos de Opinión

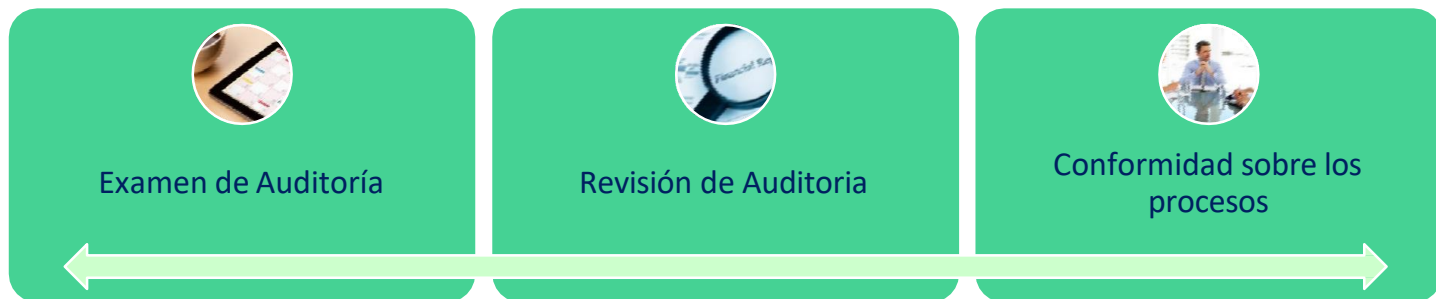
1. Principales sujetos de la Auditoría de Sistemas



- ☐ Revisiones al entorno físico
- ☐ Revisiones a la administración de sistemas
- ☐ Revisiones a los softwares
- ☐ Revisiones a la seguridad de las redes
- ☐ Revisiones a la continuidad de negocios
- ☐ Revisiones a la integridad de datos
- ☐ Revisiones a la privacidad de datos
- ☐ Revisiones a la ciberseguridad

NO TODO PUEDE SER AUDITADO. EL ALCANCE DE LOS PLANES ANUALES DE AUDITORIA Y DEL PLAN DE TRABAJO SE DETERMINA CON BASE A LOS CONCEPTOS DE MATERIALIDAD Y RIESGO DE AUDITORIA

2. Tipos de trabajo que generan reportes de Auditoría

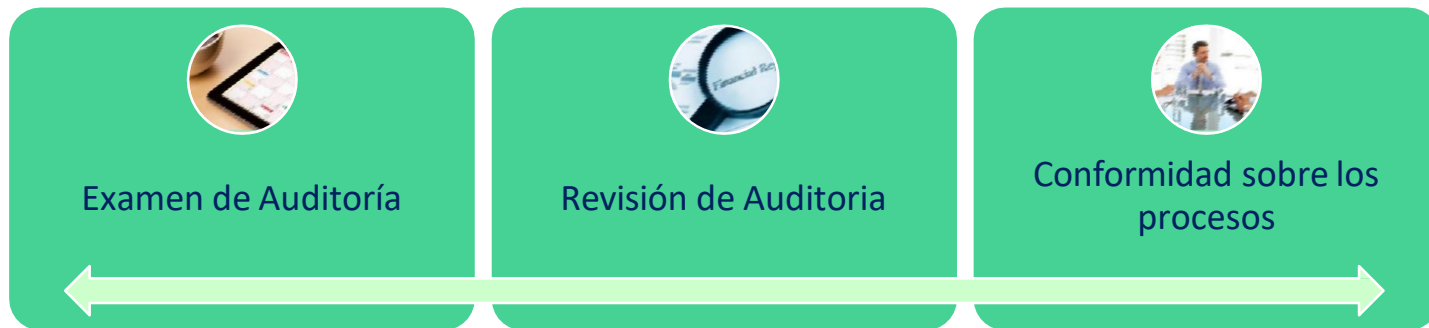


Tanto el **examen** como la **revisión** involucran:

- ☐ Planificación del trabajo
- ☐ Evaluar el diseño efectivo de procedimientos de control
- ☐ Probar la operatividad efectiva de los procedimientos de control
- ☐ Formar una conclusión, e informar, sobre el diseño y/o efectividad operativa de los procedimientos de control basándose en criterios identificados:

La conclusión para un **trabajo de aseguramiento razonable** se expresa como opinión positiva y ofrece un alto nivel de aseguramiento. La conclusión para un **trabajo de aseguramiento limitada** se expresa como opinión negativa y ofrece solo un nivel moderado de aseguramiento.

2. Tipos de trabajo que generan reportes de Auditoria



- ☐ Un trabajo de '**conformidad sobre procesos**' no dan lugar a la expresión de aseguramiento de los profesionales. Los profesionales se encargan de llevar a cabo procedimientos específicos para lograr las necesidades de la información de las partes que han aprobado realizar los procedimientos (ej.: gerencia ejecutiva, comité o encargados del Gobierno).
- ☐ Los profesionales emiten un informe de hallazgos verdaderos a las partes que han aprobado los procedimientos.

3. Contenidos requeridos en los Informes de Auditoria

- ❑ Se debe considerar toda evidencia relevante obtenida.
- ❑ Toda opinión, debe ser apoyada por los resultados de los procedimientos de control basados en los criterios identificados.
- ❑ Verificar que se ha obtenido evidencia suficiente y apropiada para apoyar las conclusiones en el informe de trabajo de auditoría. Se puede encontrar más ayuda detallada en el **Estándar 1205 Evidencia.**



3.1.1 Principales elementos del contenido requerido en los Informes de Auditoría



INFORME DE AUDITORIA

NOMBRE DEL PROCESO: Auditoría al Proceso de Infraestructura Tecnológica

INFORME DEFINITIVO: 18 de agosto de 2017

1. INTRODUCCIÓN

La Oficina de Control Interno, en ejercicio de las facultades legales otorgadas por la Ley 87 de 1993, modificada por la Ley 1474 de 2011, el Decreto 2145 de 1999 y sus modificaciones; Los Decretos 019, 2482 y 2641 de 2012, el Decreto 943 de 2014, Decreto 648 de 2017 y las Circulares Normativas establecidas por la Entidad, el estatuto de Auditoría Interna y la guía de auditoría para entidades públicas emitida por el DAFP en su versión No 2, tiene como función realizar la evaluación independiente y objetiva al Sistema de Control Interno, a los procesos, procedimientos, actividades y actuaciones de la administración, con el fin de determinar la efectividad del Control Interno, el cumplimiento de la gestión institucional y los objetivos de la Entidad, produciendo recomendaciones para asesorar al Representante Legal y al Comité de Coordinación de Control Interno y/o Comité de Auditoría y/o Junta Directiva, en busca del mejoramiento continuo del Sistema de Control Interno.

En cumplimiento al Programa General de Auditorías aprobado en el mes de enero de 2017, por el Comité Asesor de Junta Directiva de Auditoría, la Oficina de Control Interno suscribió el contrato 016-2017, con la firma Deloitte & Touche Ltda., para realizar la Auditoría al Proceso de Infraestructura Tecnológica, el cual incluyó, la evaluación de controles generales de TI, controles automáticos y gestión de cambios en la compañía. Este informe tiene como propósito resumir el trabajo efectuado y las conclusiones obtenidas, además de efectuar las recomendaciones necesarias en pro del mejoramiento continuo del proceso, lo cual redundará en el cumplimiento de la Misión y los Objetivos Institucionales.

1. **Título apropiado y distintivo.** Distinguir el informe de cualquier otro no sujeto a estándares de auditoría
2. **Destinatarios** a quien se dirige el informe, de acuerdo a los términos en la carta de auditoría o carta de encargo.
3. Identificar la **parte responsable**, incluyendo una declaración de la parte responsable para la materia.
4. Descripción del **alcance del trabajo de auditoría**, el nombre de la entidad o componente de la entidad que relata la materia, incluyendo: Identificación o descripción del área de actividad, **Criterios** usados como base para la conclusión de los profesionales, Fecha o periodo de tiempo en que el trabajo, evaluación o medida relata la materia, **Declaración** que el mantenimiento de una estructura de control interno efectiva, incluyendo procedimientos de control para el área de actividad, es responsabilidad de la gerencia
5. Identificación del **propósito** para lo que se han preparado los informes de los profesionales
6. Descripción del **criterio o rechazo** de la fuente del criterio.

3.1.1 Principales elementos del contenido requerido en los Informes de Auditoría

7. Declaración del **trabajo de auditoría** ha sido realizado de acuerdo con los estándares de auditoría y aseguramiento de SI de ISACA u otros estándares profesionales aplicables. Cualquier no cumplimiento debe ser mencionado explícitamente en el informe.
8. **Hallazgos, conclusiones y recomendaciones** para las acciones correctivas e incluir la respuesta de la gerencia. Para cada respuesta de la gerencia, los profesionales deben obtener información sobre las acciones propuestas para implementar o direccionar las recomendaciones informadas y la implementación planificada o fechas de acción.
9. Un párrafo indicando que debido a las **limitaciones inherentes** de cualquier control interno, pueden ocurrir y no ser detectadas declaraciones erróneas debido a errores o fraude.
10. Un **resumen** del trabajo realizado, que ayudará a los usuarios a comprender mejor la naturaleza de los resultados.
11. Una expresión de **opinión** acerca de si, en todos los aspectos materiales, el diseño y/o operación de los procedimientos de control en relación al área de actividad fueron efectivos. Cuando la opinión de los profesionales es cualificada, se debe incluir un párrafo describiendo las razones de la cualificación.
12. Cuando sea apropiado, **referenciar** cualquier otro informe separado que deba ser considerado.
13. **Fecha de emisión** del informe del trabajo de auditoría. En muchos casos la fecha del informe se basa en la fecha del evento. Es recomendable mencionar también las fechas en que fue realizado el trabajo de auditoría, si no se menciona ya en el resumen del trabajo realizado.
14. Nombres de las personas o entidad **responsable del informe**, firmas adecuadas y lugares.

3.1.2 Atributos de calidad de la información de los Informes de Auditoria



Información Relevante

- Relacionada con controles, le indica al evaluador algo significativo sobre la operación de los controles subyacentes o componente de control.
- Basado en las metas de calidad de la información de COBIT5



Información Confiable

- Información que es precisa, verificable y de una fuente objetiva. Consultar las metas de calidad de información COBIT5.



Información Suficiente

- La información es suficiente cuando los evaluadores han recolectado suficiente información para formular una conclusión razonable. Sin embargo, para que la información sea suficiente, primero debe ser adecuada



Información Adecuada

- Información relevante (es decir, se adapta para su propósito previsto), confiable (es decir, precisa, verificable y de una fuente objetiva) y oportuna (es decir, producida y utilizada en un marco de tiempo apropiado).



Información Oportuna

- Producida y utilizada en un marco de tiempo que permite prevenir o detectar las deficiencias de control antes de que sean materiales en una empresa.

3.2.1 Riesgo de Auditoria, Materiabilidad y debilidad material

Riesgo de Auditoria

- El riesgo de alcanzar una conclusión incorrecta en base a los hallazgos de auditoría. Los tres componentes del riesgo de auditoría son:
 - Riesgo de control
 - Riesgo de detección
 - Riesgo inherente

Materialidad

- **Una deficiencia o una combinación de deficiencias en un control interno**, por lo cual exista una posibilidad razonable de que una falsa declaración importante no sea evitada ni detectada de manera oportuna.

Debilidad Material

- La debilidad en el control se considera material si la ausencia del mismo ocasiona que no exista una garantía razonable de que se cumplirá con el objetivo de control.
- Una debilidad clasificada como material **implica que:**
 - * **controles no están establecidos y/o**
 - * **los controles no son utilizados y/o**
 - * **los controles son inadecuados.**

NIVEL DE MATERIALIDAD = EVIDENCIA DE AUDITORIA = RIESGO DE AUDITORIA

MATERIALIDAD = EVIDENCIA DE AUDITORIA = RIESGO DE AUDITORIA

3.2.1.. Riesgo de Auditoria

Riesgo inherente

- Son los riesgos que se encuentran presentes en la entidad, antes de considerar las actividades de control establecidas por la gerencia para mitigarlos.
- Es necesario que el auditor obtenga un conocimiento de la entidad.

Riesgo de Control

- Las entidades deben establecer actividades de control que les permitan prevenir, detectar y corregir las desviaciones que se presentan en sus procedimientos. Así, como mitigar los principales riesgos a los que se expone la entidad.
- El riesgo de control es la probabilidad que existe de que esos controles no permitan detectar y corregir los errores a tiempo.

Riesgo de Detección

- El riesgo de detección está relacionado con la posibilidad de que **los procedimientos de auditoría no detecten los errores**.
- El auditor debe establecer cuál es el riesgo mínimo de detección que va a aceptar

3.2.1 A Responsabilidades frente a la Materiabilidad



- ❑ Los profesionales de auditoría y aseguramiento de SI deben **considerar las debilidades potenciales o ausencias de controles** mientras planifican una asignación y si esas debilidades o ausencias de controles pudieran resultar en una deficiencia significativa o una debilidad material.
- ❑ Considerar las **definiciones de materialidad cuando son provistas por las autoridades regulatorias o legislativas**. Observar que la evaluación de la materialidad y el Riesgo de auditoría puede variar de vez en cuando, dependiendo de las circunstancias y el entorno cambiante
- ❑ **Evaluar el efecto de los controles compensatorios** y si dichos controles compensatorios son efectivos para determinar si una deficiencia de control o la combinación de las deficiencias de control es una Debilidad material.

https://www.pcihispano.com/controles-compensatorios-que-son-y-cuando-se-utilizan/#:~:text=Un%20%E2%80%9Ccontrol%20compensatorio%E2%80%9D%20es%20un_ser%20empleado%20bajo%20circunstancias%20excepcionales.

3.2.1 B Materialidad en los Sistemas Informáticos

❑ El auditor puede considerar:

- ✓ Sistemas que soportan procesos críticos contables
- ✓ Sistemas que han presentado fallas superiores a las tasas tolerables
- ✓ Aquellos que requieren cumplimientos regulatorios obligatorios y que necesitan de opiniones de auditoria recurrentes
- ✓ Nuevas implementaciones de sistemas informáticos.
- ✓ Migraciones de información, a fin de preservar la integridad.
- ✓ Procesos con susceptibilidad o sospecha de fraude
- ✓ Exista alto nivel de riesgos inherente (cambio en los sistemas, complejidad tecnológica, sistemas con alta probabilidad de pérdida o modificación intencional de datos), riesgos de control (alta dependencia de controles manuales) o riesgos de detección (procesos o transacciones donde sea posible que el auditor no haya detectado errores).

4. Tipos de Opinión

No cualificada (limpia)

- Los profesionales deben expresar una opinión no cualificada cuando concluyan que, **en todos los aspectos materiales**, el diseño y/o operación de los **procedimientos de control** en relación al área de actividad **fueron efectivos**, de acuerdo con los criterios aplicable

Cualificada (con advertencia)

- Hayan obtenido **evidencia suficiente y apropiada**, concluyan que la **debilidad del control**, individualmente o en grupo, **son materiales, pero no predominante en los objetivos de auditoría de SI**
- No son capaces de obtener evidencia suficiente y apropiada en que basar la opinión, pero concluyen que los efectos posibles sobre los objetivos de auditoría de SI de debilidades no detectadas, si hay, podrían ser materiales pero no predominantes

Adversa (negativa)

- Los profesionales deben expresar una opinión adversa cuando **una o más deficiencias significativas se une a una debilidad material y predominante**

Renuncia

- Los profesionales deben renunciar una opinión cuando **no son capaces de obtener evidencia suficiente y apropiada en que basar la opinión**, y concluyen que el posible efecto sobre los objetivos de auditoría de las debilidades no detectadas, si hay, podría ser tanto material como predominante.

<i>Naturaleza de la cuestión que origina la opinión modificada</i>	<i>Juicio del auditor sobre la generalización de los efectos o posibles efectos sobre los estados financieros</i>	
	<i>Material pero no generalizado</i>	<i>Material y generalizado</i>
Los estados financieros contienen incorrecciones materiales	Opinión con salvedades	Opinión desfavorable (adversa)
Imposibilidad de obtener evidencia de auditoría suficiente y adecuada.	Opinión con salvedades	Denegación (abstención) de opinión

Fuente: NIA 705

¿Consultas?



INFORME DE AUDITORÍA