UNIVERSIDAD DE LIMA | 60 años

AUDITORÍA Y CONTROL DE SISTEMAS

UNIVERSIDAD DE LIMA

FACULTAD DE INGENIERÍA Y ARQUITECTURA
CARRERA DE INGENIERÍA DE SISTEMAS

LA FUNCIÓN DE AUDITORÍA

Agenda

UNIVERSIDAD DE LIMA

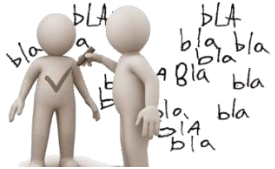
60 años

GENERALIDADES

Definición

Auditar es emitir un juicio profesional, **independiente, confiable, argumentado y evidenciable** sobre el funcionamiento de algún producto, servicio y/o procedimientos de tal manera que se puedan revisar sus comportamientos y resultados generados. Esta actividad se **debe(ría)** basar en *normas y procedimientos, marcos y estándares de calidad, mejores prácticas, entre otros.*

Independencia del auditor



Código de ética profesional del auditor (ISACA)

1. Respaldar la implementación y promover el cumplimiento con estándares y procedimientos apropiados del gobierno y gestión efectiva de los sistemas de información y la tecnología de la empresa, incluyendo la gestión de auditoría, control, seguridad y riesgos.
2. Llevar a cabo sus labores con objetividad, debida diligencia y rigor/cuidado profesional, de acuerdo con estándares de la profesión.
3. Servir en beneficio de las partes interesadas de un modo legal y honesto y, al mismo tiempo, mantener altos niveles de conducta y carácter, y no involucrarse en actos que desacrediten su profesión.
4. Mantener la privacidad y confidencialidad de la información obtenida en el curso de sus deberes a menos que la divulgación sea requerida por una autoridad legal. Dicha información no debe ser utilizada para beneficio personal ni revelada a partes inapropiadas.
5. Mantener la aptitud en sus respectivos campos y asumir sólo aquellas actividades que razonablemente esperen completar con las habilidades, conocimiento y competencias necesarias.
6. Informar los resultados del trabajo realizado a las partes apropiadas, incluyendo la revelación de todos los hechos significativos sobre los cuales tengan conocimiento que, de no ser divulgados, pueden distorsionar el reporte de los resultados.
7. Respaldar la educación profesional de las partes interesadas para que tengan una mejor comprensión del gobierno y la gestión de los sistemas de información y la tecnología de la empresa, incluyendo la gestión de la auditoría, control, seguridad y riesgos.

https://iaiperu.org/codigo-de-etica/

El juicio profesional

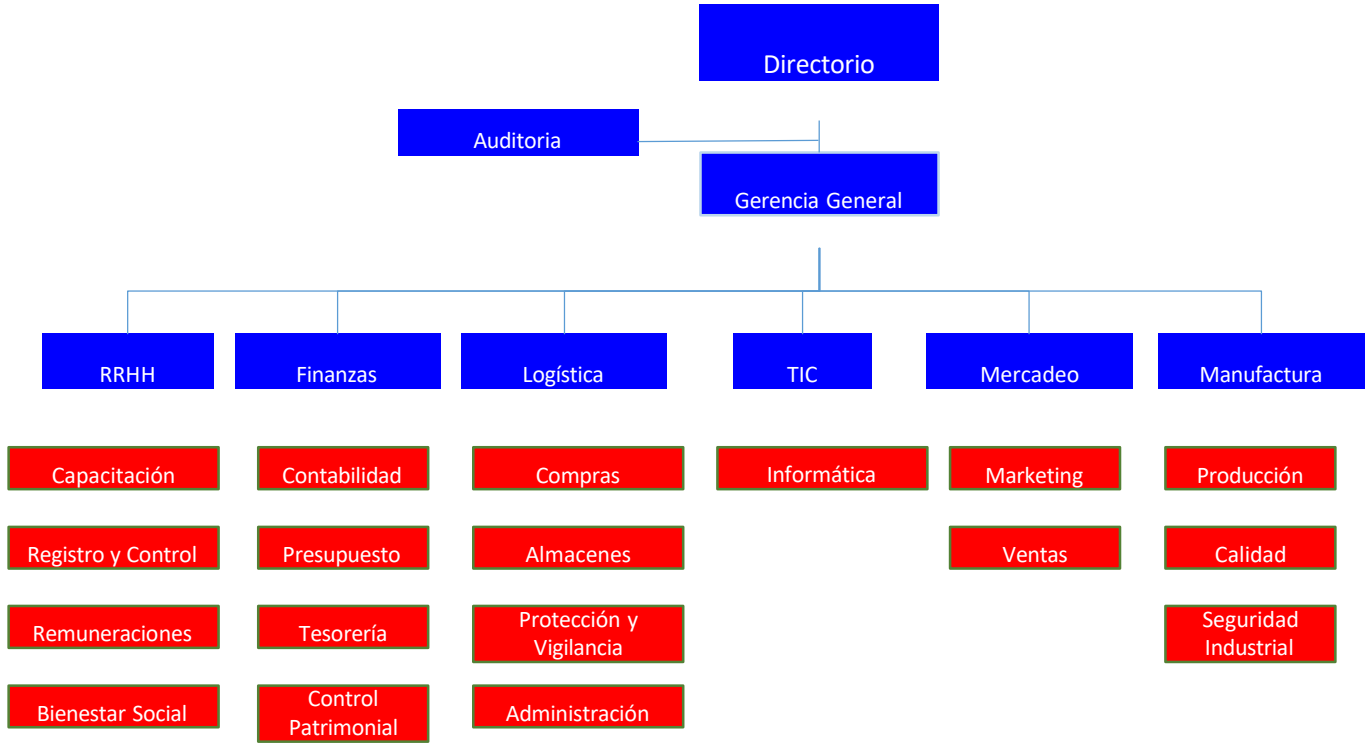
La aplicación del **conocimiento y experiencia** relevante de un profesional dentro un contexto determinado, para tomar decisiones informadas sobre los cursos de acción que son apropiados durante el trabajo de auditoría (Manual de la IFAC 2010)

¿Qué no es la Auditoría?

- EVALUACIÓN DE PERSONAL
- DETECCIÓN DE DELITOS
- RECABAMIENTO DE CAUSALES DE DESPIDO
- INVESTIGACIÓN FORENSE

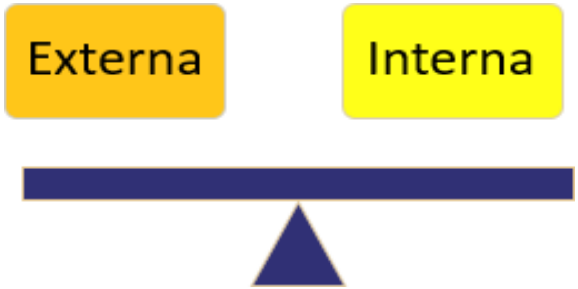
Concepto erróneo

Rol Ideal de Auditoría en la Empresa



Clasificación de Auditoría

POR EL ORIGEN DE LOS AUDITORES



POR EL ÁREA DE APLICACIÓN

Cumplimiento	Financieras	Sistemas y TICs
Operativas	Integradas	Administrativas

Auditoría Interna

Es el examen crítico, sistemático y detallado de un **sujeto de auditoría** (proceso, producto, sistema, entre otros) de una empresa específica, **realizado por un profesional con vínculos laborales con la misma,** utilizando técnicas determinadas y con el objeto de emitir informes y formular sugerencias para el mejoramiento del mencionado sujeto.

Auditoría Interna

Ventajas:

- Revisión más a profundidad por ser empleado de la propia empresa
- Esta auditoría consume sólo recursos internos.

Desventajas:

- Su veracidad, alcance y confiabilidad pueden ser limitados, porque puede haber injerencia por parte de las autoridades de la Organización sobre el auditor.
- En ocasiones, la opinión del auditor puede ser limitada en virtud a la objetividad.

Auditoría Externa

Definición:

Es el examen crítico, sistemático y detallado de un **sujeto de auditoría**, **realizado por un auditor sin vínculos laborales con la misma,** utilizando técnicas determinadas y con el objeto de emitir una opinión independiente sobre la forma cómo opera dicho sujeto y formular sugerencias para su mejoramiento.

UNIVERSIDAD DE LIMA

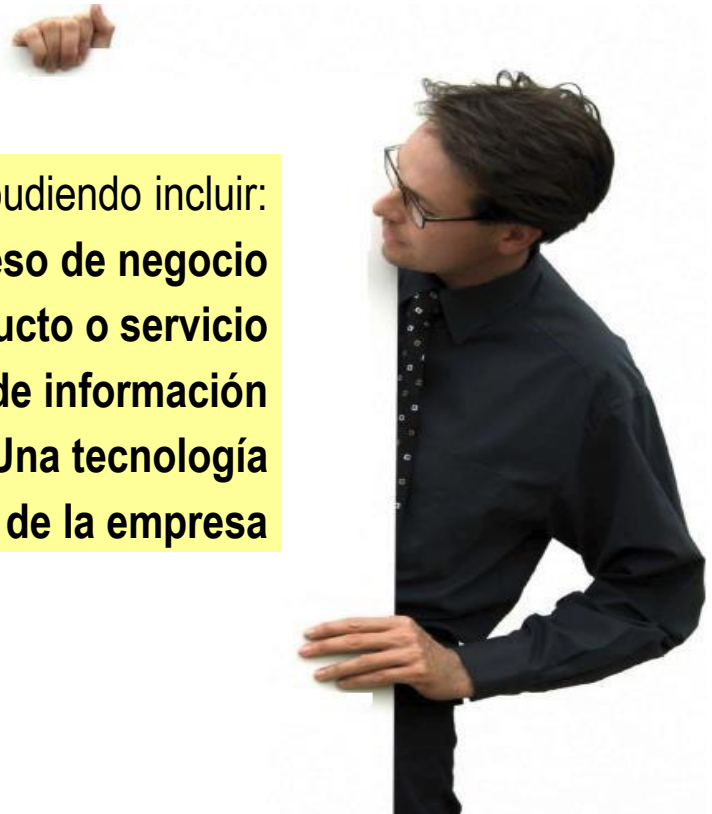
60 años

CONCEPTOS BÁSICOS

Sujeto de una auditoría

Es lo que se va a auditar, pudiendo incluir:

- **Un proceso de negocio**
- **Un producto o servicio**
- **Un sistema de información**
- **Una tecnología**
- **Los estados financieros de la empresa**



Tipos de una auditoría

Son los distintos aspectos a los que pertenece el sujeto de auditoría previamente planteado

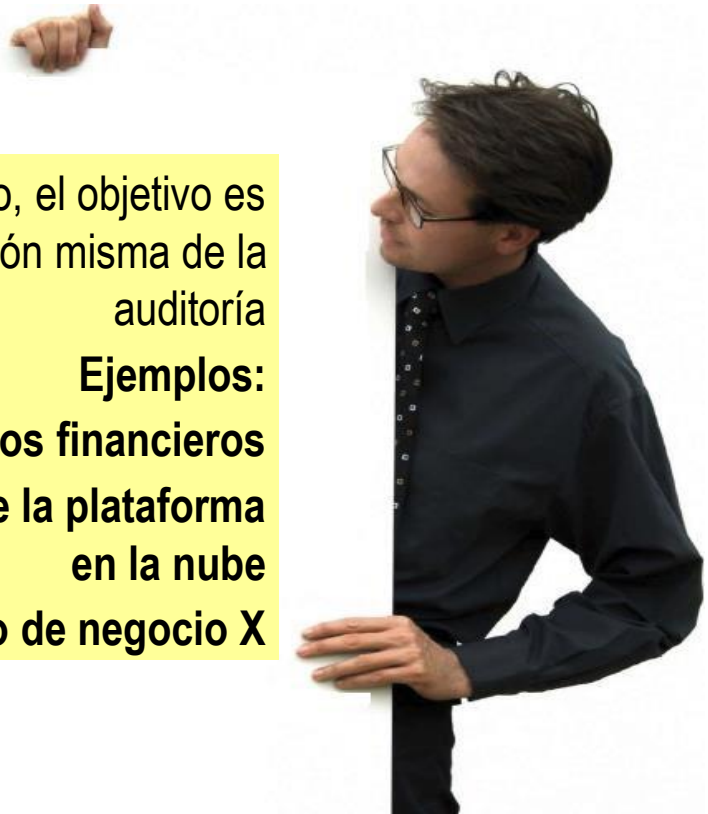
- ***Auditoría de procesos***
- ***Auditoría de calidad de productos***
- ***Auditoría de sistemas de información***
- ***Auditoría de redes, auditoría de base de datos, auditoría de seguridad, auditoría de privacidad.***
- ***Auditoría contable y financiera***

Objetivo general de una auditoría

Dentro de un tipo de auditoría determinado, el objetivo es lo que se pretende lograr con la ejecución misma de la auditoría

Ejemplos:

- **Revisar la exactitud de los estados financieros**
- **Verificar el correcto funcionamiento de la plataforma en la nube**
- **Verificar la correctitud del proceso de negocio X**

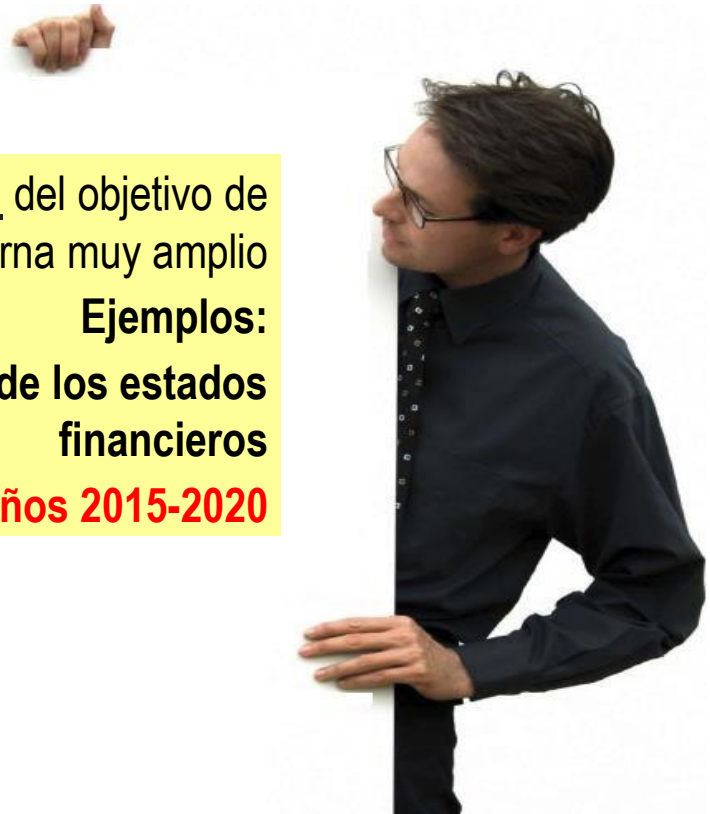


Alcance de una auditoría

El alcance funciona como **acotación** del objetivo de auditoría cuando éste se torna muy amplio

Ejemplos:

- **Objetivo: Revisar la correctitud de los estados financieros**
- **Alcance: Solamente cubrir los años 2015-2020**



Criterios de auditoría *(Estándar de auditoría y aseguramiento de SI 1008)*

Entiéndase, lo que hay que verificar durante una auditoría.

Es un **conjunto de requisitos** que el auditor tiene que verificar su cumplimiento, existencia, idoneidad en el sujeto de auditoría.

Ejemplos:

- **Norma ISO 27001 – Control de acceso**
- **Objetivos de negocio A y B**
- **Niveles de seguridad requeridos**

Objetivos específicos de auditoría

Se refiere a verificar el **cumplimiento de los criterios** en el sujeto de auditoría.

Ejemplos:

- **Verificar el cumplimiento de norma ISO 27001, control de acceso**
- **Verificar el cumplimiento de objetivos de negocio A y B**
- **Revisar los niveles de seguridad o calidad requeridos**

Evidencias de auditoría *(Estándar de auditoría y aseguramiento de SI 1205)*

Son todas aquellas informaciones que el auditor obtiene (releva), **con el fin de verificar el cumplimiento de los criterios de auditoría** y sustentar más adelante, su opinión profesional a manera de conclusiones. Tienen que ser verificables, no asumidas ni presupuestas.

Según la ISO 19011 son “registros, declaraciones de hecho u otra información que son relevantes para los criterios de auditoría y que son verificables” [ISO, 2018].

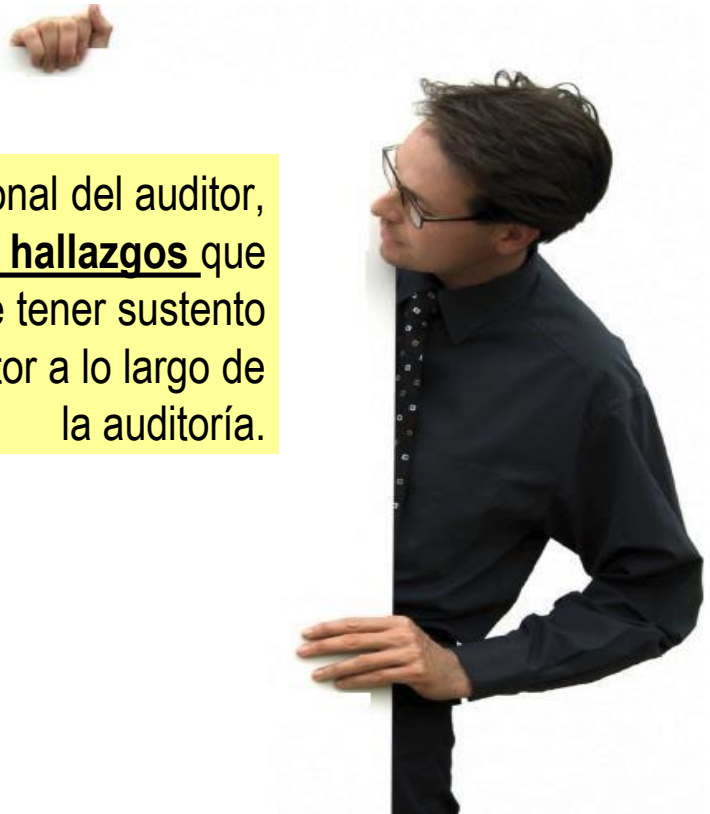
Hallazgos *(Estándar de auditoría y aseguramiento de SI 1204 - Materialidad)*

Resultados del análisis y la evaluación de las evidencias recolectadas por el auditor frente a los criterios que debe verificar, pudiéndose establecer **no conformidades de dichos criterios en cuyo caso estamos ante un hallazgo.**

AUNQUE UN HALLAZGO ES ALGO "MALO", NO IMPLICA NECESARIAMENTE LA BÚSQUEDA Y DETECCIÓN DE UN DELITO.

Conclusiones *(Estándar de auditoría y aseguramiento de SI 1401 Reportes)*

Son las expresiones de la opinión profesional del auditor, al terminar su labor **sobre la base de los hallazgos** que pudiera haber encontrado. Todas tienen que tener sustento en la propia actividad desplegada por el auditor a lo largo de la auditoría.



Recomendaciones

Manteniendo la independencia, y dependiendo si es parte de una auditoría interna o externa, el auditor puede brindar un **conjunto de sugerencias para poder levantar los hallazgos** encontrados o recalcar la importancia del pronto levantamiento de dichos hallazgos.

NO IMPLICA LA FORMA COMPLETA Y DETALLADA DE LEVANTAR LOS HALLAZGOS

¿Consultas?

Referencias bibliográficas

- Committee of Sponsoring Organizations (2017). Enterprise Risk Management Integrating with Strategy and Performance, EEUU.
- Contraloría General de la Republica. (2014). Directiva de Auditoría de Cumplimiento y modificatorias. Lima, Perú.
- Fonseca Luna, O. (2007). *Auditoría gubernamental moderna* (1st ed.). Lima: Instituto de Investigación en Accountability y Control (IICO).
- International Standar Organization (2018). *ISO 19011*. *Directrices de auditoría de Sistemas de Gestión.* Ginebra: ISO INTERNATIONAL.
- ISACA (2020). *Certified Information Systems Auditor (CISA) Exam Preparation Guide,* USA.

UNIVERSIDAD DE LIMA

60 años

LA FUNCIÓN DE AUDITORÍA