Conceptos Auditoría Sistemas de Información

Descripción

Una auditoría, es un proceso ejecutado por un auditor, que tiene la característica de ser sistemático, independiente y documentado, y que busca obtener a partir de la realización de pruebas de auditoría registros, declaraciones de hechos u otra información conocida como evidencias de auditoría.

Las evidencias de auditoría deben ser verificables, pertinentes y evaluables de manera objetiva para, en base a ellas, determinar la medida en la cual el hecho auditado cumple unos criterios de auditoría. Estos criterios están determinados por un conjunto de políticas, procedimientos o requisitos y son usados como referencia contra la que se compara la realidad.

Las pruebas de estas diferencias entre la realidad y la referencia son lo que se entiende como hallazgos de auditoría. Finalmente, el proceso concluye con el análisis de estos hallazgos para poder emitir unas conclusiones de la auditoría

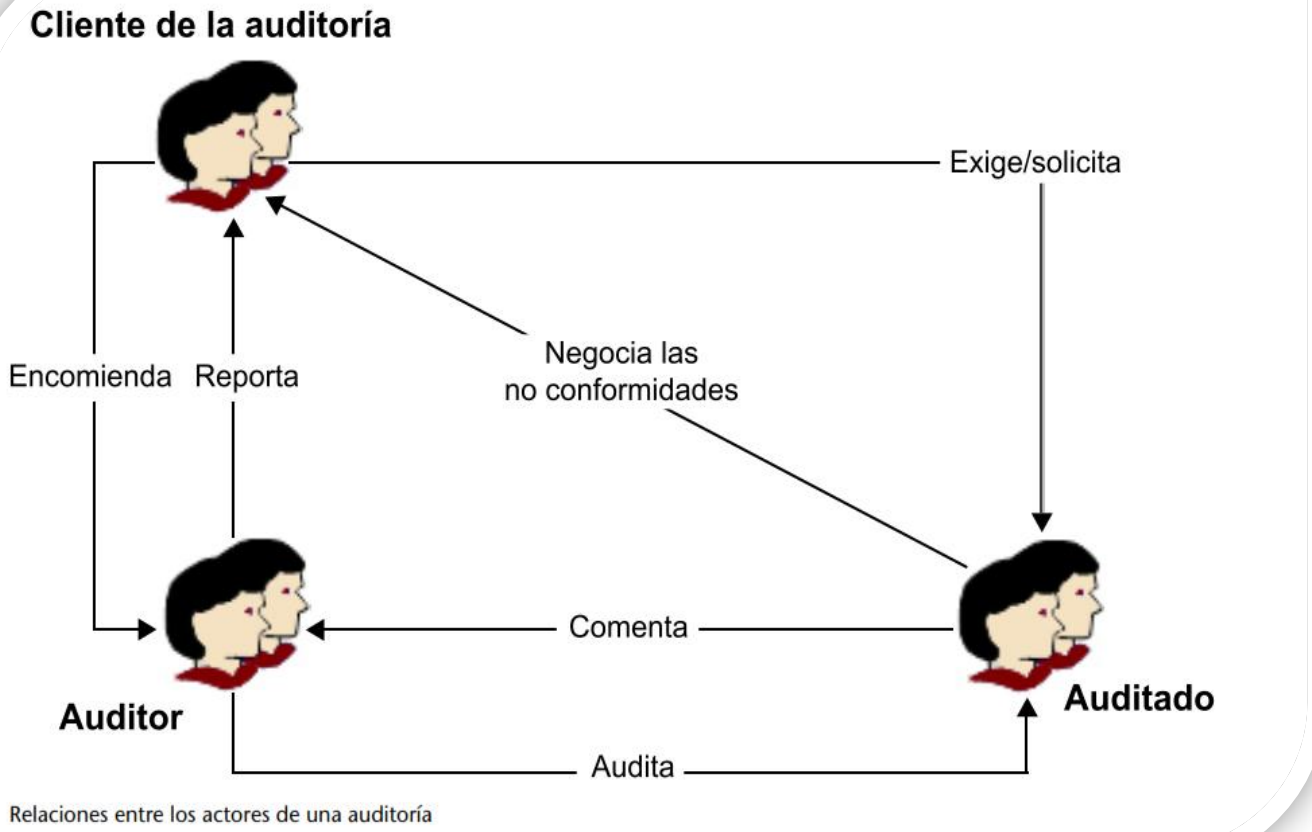
Metodología de trabajo de la Auditoría Informática

El **objetivo inicial** de la Auditoría Informática era evaluar el diseño y efectividad del sistema de control interno asociado a los sistemas de información que posee una organización.

Hoy en día también incluye:

- El análisis de la eficiencia y eficacia de los Sistemas de Información
- La verificación de la consistencia y cumplimiento de la Normativa general en ese ámbito
- La revisión de la eficaz gestión de los Recursos Informáticos.

Tipos de auditoria



Relaciones entre los actores de una auditoría

Relación del cliente

- **Auditoria de Primera Parte**
- **Auditorias de Segunda Parte**
- **Auditorias de Tercera Parte**

Relación del Auditor

- **Auditoria Interna**
- **Auditoria Externa**

Objetivos

- Es el examen del diseño y efectividad del sistema de control interno informático establecido en una organización.
- El análisis de la eficiencia y eficacia de los Sistemas de Información.
- La verificación de la consistencia y cumplimiento de la Normativa general en ese ámbito.
- La revisión de la eficaz gestión de los Recursos Informáticos.

Alcance

- ✓ Las organizaciones auditadas pueden tener múltiples procesos asociados, ejecutados en un área geográfica que puede ser muy amplia, con unos medios muy diversos y por personal también variado.
- ✓ El alcance de la auditoría describe la extensión y los límites de la auditoría. Por ejemplo, las localizaciones físicas, las unidades organizativas, las actividades o los procesos a ser auditados en el período de tiempo cubierto por la auditoría.
- ✓ Es decir, todos los parámetros que limitan física, temporal y lógicamente la
- ✓ actividad del auditor dentro de la organización auditada.

Tipos de Auditoría Informática

- Auditoría sobre los elementos que componen la Organización Informática y su definición dentro de la organización
- Auditoría sobre la elaboración, aprobación, implementación, actualización y seguimiento del Plan Estratégico de TI
- Auditoría sobre la Arquitectura de la Información, analizando la disponibilidad, oportunidad, integridad y exactitud de los datos
- Auditoría de la creación, documentación, comunicación y actualización de Políticas y Procedimientos sobre las actividades relacionadas con TI
- Auditoría sobre el cumplimiento de las Regulaciones Externas a la organización
- Auditorías sobre las actividades relacionadas con la Administración de Proyectos

Tipos de Auditoría Informática

•Auditorías sobre las actividades asociadas al Desarrollo, Adquisición y Mantenimiento de Software de Aplicación
•Auditorías sobre las actividades asociadas a la Adquisición y Mantenimiento de la Infraestructura Tecnológica
•Auditoría sobre la elaboración, aprobación, implementación, actualización y cumplimiento de la Política de Seguridad de la Información.
•Auditoría sobre contratación de servicios de Procesamiento y/o Soporte brindados por Terceros
•Auditoría sobre el monitoreo de los Procesos
•Auditoría sobre las Aplicaciones Informáticas

Tipos y Enfoques de Auditoría Informática

El enfoque en el cual basaremos nuestro análisis son:

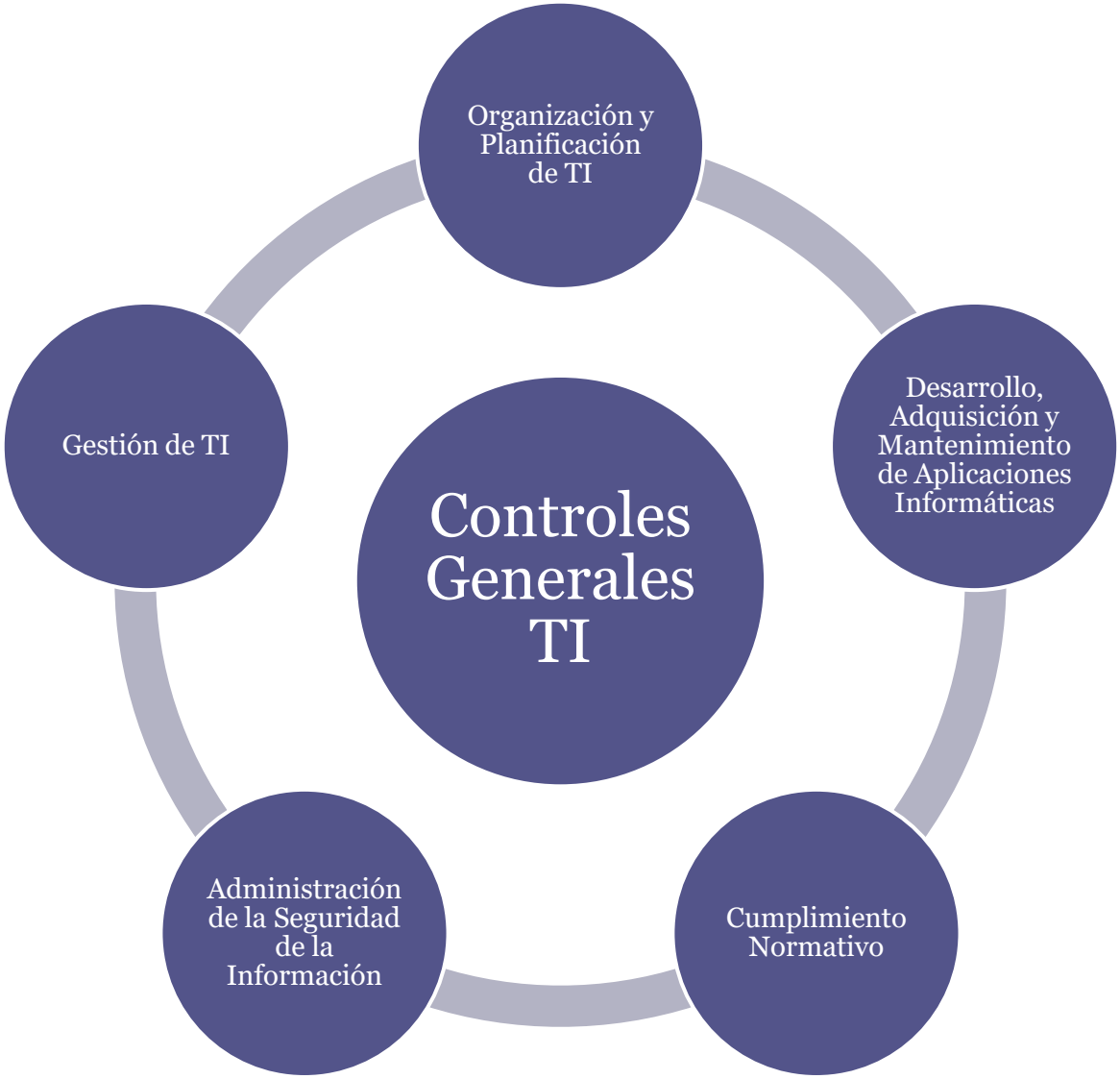
- Controles Aplicativos
- Controles Generales de TI

La efectividad de los Controles de Aplicación depende del grado de confiabilidad del ambiente donde se realizan las actividades de IT.

Controles Generales de TI

Se definen sobre las actividades de servicio de TI, están presentes sobre el ambiente que rodea a los sistemas de información.

- Cumplimiento de Políticas y Procedimientos
- Desarrollo, Adquisición y Mantenimiento de Aplicaciones Informáticas
- Monitoreo de las Operaciones
- Organización y Planificación de TI
- Administración de la Seguridad de la Información
- Otros

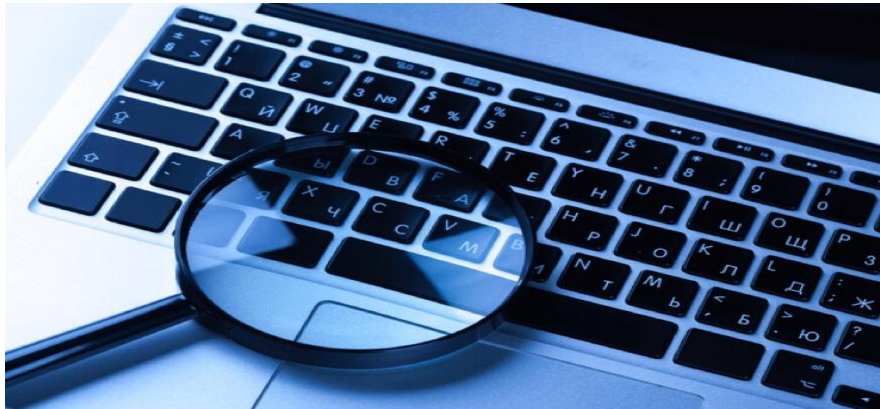

Controles Generales TI
Organización y Planificación de TI
Desarrollo, Adquisición y Mantenimiento de Aplicaciones Informáticas
Cumplimiento Normativo
Administración de la Seguridad de la Información
Gestión de TI

Controles Aplicativos

Se aplican a nivel de procesos, definidos para actividades específicas las cuales pueden estar automatizadas o integradas con los sistemas aplicativos.

Una clasificación general de los diferentes tipos de controles a implementar podría incluir:

- Controles Manuales sobre las aplicaciones
- Controles Programados en las aplicaciones
- Controles Lógicos de acceso a los sistemas aplicativos



Controles de Aplicación

- Eficiencia y Eficacia de la Aplicación
- Preparación y Autorización de Información de Origen
- Recolección e Ingreso de Información de Origen
- Chequeos de Exactitud, Integridad y Autenticidad
- Integridad y Validez del Procesamiento
- Revisión de Salidas, y Manejo de Errores
- Autenticación e Integridad de Transacciones Origen.