**Clase 6**

**Auditoria en Sistemas**

La auditoría informática es el proceso que consiste en recoger, analizar y evaluar evidencias para determinar si un sistema informático protege el activo empresarial, mantiene la integridad de datos, utiliza eficientemente los recursos, cumple con las leyes y normas establecidas.

Los mecanismos de control que se utilizan en la informática para determinar una auditoría son

-        Directivos

-        Preventivos

-        De detección

-        Correctivos

-        De recuperación ante cualquier contingencia.

[**Objetivos**](https://ultra.content.blackboardcdn.com/ultra/uiv3900.125.0-rel.36_ba06598)

●      Análisis de la actividad de los sistemas informáticos

●      Verificación del cumplimiento de la normativa preestablecida.

●      Revisión de la eficaz gestión de los recursos.

[**Tipos de auditoria informática**](https://ultra.content.blackboardcdn.com/ultra/uiv3900.125.0-rel.36_ba06598)

Existen muchos tipos de auditorías informáticas, a continuación se mencionan los dos más importantes

●      Auditoría interna: Es el proceso de auditoría que se realiza dentro de la empresa, son los empleados los que realizan esta auditoría.

●      Auditoría externa: Este es realizado por una persona o personas que contrata la empresa para que realice la auditoría.

[**Control interno y auditoria informática**](https://ultra.content.blackboardcdn.com/ultra/uiv3900.125.0-rel.36_ba06598)

La auditoría cambió mucho con el paso del tiempo, sobre todo con el avance informático en el mundo empresarial. Ahora los controles se hacen en sistemas informáticos o se realizan por parte de la función informática de la empresa, y esto es representado por el control Interno Informático. Este enfoque centrado en controles exige conocimientos informáticos, es decir, personal capacitado en tecnología o en el área.

[**Las funciones de control interno y auditoria informática**](https://ultra.content.blackboardcdn.com/ultra/uiv3900.125.0-rel.36_ba06598)

[**Control interno informático**](https://ultra.content.blackboardcdn.com/ultra/uiv3900.125.0-rel.36_ba06598)

El Control Interno Informático es el proceso por el cual se controlan todas las actividades de los sistemas informáticos, específicamente controla que sean desarrolladas cumpliendo los procedimientos, estándares y normas fijadas por la dirección.

Se pueden indicar los siguientes objetivos del control interno informático

-        Controlar que el sistema informático se desarrolle cumpliendo los procedimientos y normas legales.

-        Asesorar sobre el conocimiento de las normas.

-        Colaborar y apoyar al trabajo de la auditoría informática.

-        Definir, implantar

Sobre los diferentes sistemas y entornos informáticos se debe realizar el control de las actividades operativos sobre:

-        Cumplimiento de procedimientos, normas y controles establecidos.

-        Controles sobre la producción diaria.

-        Controles sobre la calidad y eficiencia del desarrollo y mantenimiento del sistema.

-        Controles en las redes de comunicación

-        Control sobre el software base.

-        Seguridad informática

-        Licencias y relaciones contractuales con terceros

-        Asesorar y educar sobre el riesgo informático

[**Auditoria informática**](https://ultra.content.blackboardcdn.com/ultra/uiv3900.125.0-rel.36_ba06598)

La auditoría informática es el proceso de recoger, analizar y evaluar evidencia para determinar si un sistema informático protege los activos, mantiene integridad de datos, lleva a cabo de manera exitosa los objetivos de la organización y utiliza de manera eficaz los recursos. Se puede decir que la auditoría informática sustenta y confirma los objetivos de la auditoría tradicional.

El auditor analiza, evalúa y comprueba los controles y procedimientos informáticos más complejos, incorporando técnicas mecanizadas de auditoría. No siempre se realizan de manera manual, ya que es casi imposible cubrir todos los escenarios, por lo cual utilizan procedimientos informatizados que resumen, calculan y clasifican datos.

El auditor es responsable de revisar e informar a la dirección sobre el diseño y el funcionamiento de los controles implantados sobre la fiabilidad de la información.

Un auditor informático realiza muchas funciones que se pueden agrupar en 3 grupos:

●      Participa de las revisiones durante y después del diseño, realización, implementación y explotación de sistemas, así como en los cambios importantes.

●      Revisa y juzga los controles implantados en los sistemas para verificar su adecuación a las instrucciones de la dirección (requisitos legales, protección de datos y coberturas ante fraudes y errores)

●      Revisa y juzga el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos , sistemas y de la información.

[**Sistema de control interno informático**](https://ultra.content.blackboardcdn.com/ultra/uiv3900.125.0-rel.36_ba06598)

[**Definición y tipos de controles internos**](https://ultra.content.blackboardcdn.com/ultra/uiv3900.125.0-rel.36_ba06598)

El control interno es cualquier actividad que se realiza de manera manual y/o automática para evitar, corregir errores que pueden afectar al sistema. Cuando estos son diseñados y desarrollados deben ser completos, simples, fiables, revisables y rentables.

Existen distintas categorías que definen los objetivos de los controles informáticos

●      **Controles preventivos**: Es para evitar el error.

●      **Controles detectivos:** Estos se usan para cuando fallan los controles preventivos, tratan de conocer el error cuanto antes.

●      **Controles correctivos**: Cuando ocurre un error, este control hace más fácil el rollback. Ej: restore.

[**Implantación de un sistema de controles internos informáticos**](https://ultra.content.blackboardcdn.com/ultra/uiv3900.125.0-rel.36_ba06598)

Es de vital importancia conocer la configuración del sistema a evaluar para así poder identificar riesgos que puedan surgir. Los elementos o componentes que se deben considerar para este análisis son:

●      **Entorno de red:** esquema de red, descripción de hardware y software para acceso a la red, controles y seguridad, estado de situación de aplicaciones críticas, etc.

●      **Configuración de la computadora base:** soporte físico, sistema operativo, software con particiones, ambientes (prueba y productivo), bibliotecas de programas y conjunto de datos.

●      **Entorno de aplicaciones:** gestión de bases de datos, transacciones y procesos distribuidos.

●      **Productos y herramientas:**   software para desarrollo de programas, software para gestión de bibliotecas y para operaciones automáticas.

●      **Seguridad de computadora base:** identificación y verificación de usuarios, controles de acceso, registros, integridad del sistema, controles de supervisión, etc.

Una vez relevados los mencionados componentes, para la implantación de un sistema de control interno es necesario definir:

●      **Gestión de sistemas de Información:** políticas, pautas y normas que sirvan para el diseño y la implementación.

●      **Administración de sistemas:** controles sobre la actividad de centros de datos y funciones soporte, incluyendo redes.

●      **Seguridad:** integridad, confidencialidad y disponibilidad del sistema.

●      **Gestión del cambio:** separación de los ambientes de testing y productivo y controles para la migración de programas probados y aprobados.

La implantación de un sistema de control interno debe realizarse en fases, en la cual cada uno de los siguientes actores juega un papel importante:

●      **Dirección de Negocio o Dirección de Sistemas Informáticos:** definen la política y/o directrices para los sistemas de información en base a las exigencias internas y externas del negocio.

●      **Dirección de Informática:** definen la creación y publicación de procedimientos, estándares, metodologías y normas aplicables a todas las áreas de informática y usuarios para establecer un marco de funcionamiento.

●      **Control Interno Informático:** definen los diferentes controles periódicos a realizar en cada una de las funciones informáticas, de acuerdo al nivel de riesgo de cada una y considerando los objetivos del negocio y el marco legal.

También deben revisar periódicamente los controles establecidos, informando a la Dirección de Informática los desvíos encontrados y sugiriendo los cambios sobre los controles que crean convenientes.

**Auditor interno/externo informático:** revisa los diferentes controles internos definidos, la normativa interna y externa, de acuerdo al nivel de riego, corroborando que los objetivos establecidos por la Dirección de Negocio y la Dirección de Informática se cumplan. Informará a la Alta Dirección los hallazgos y en caso de detectar deficiencias o ausencia de controles, sugerirá acciones que minimicen el riesgo relacionado.