UNIVERSIDAD DE LIMA | 60 años

AUDITORÍA Y CONTROL DE SISTEMAS

UNIVERSIDAD DE LIMA

FACULTAD DE INGENIERÍA Y ARQUITECTURA
CARRERA DE INGENIERÍA DE SISTEMAS

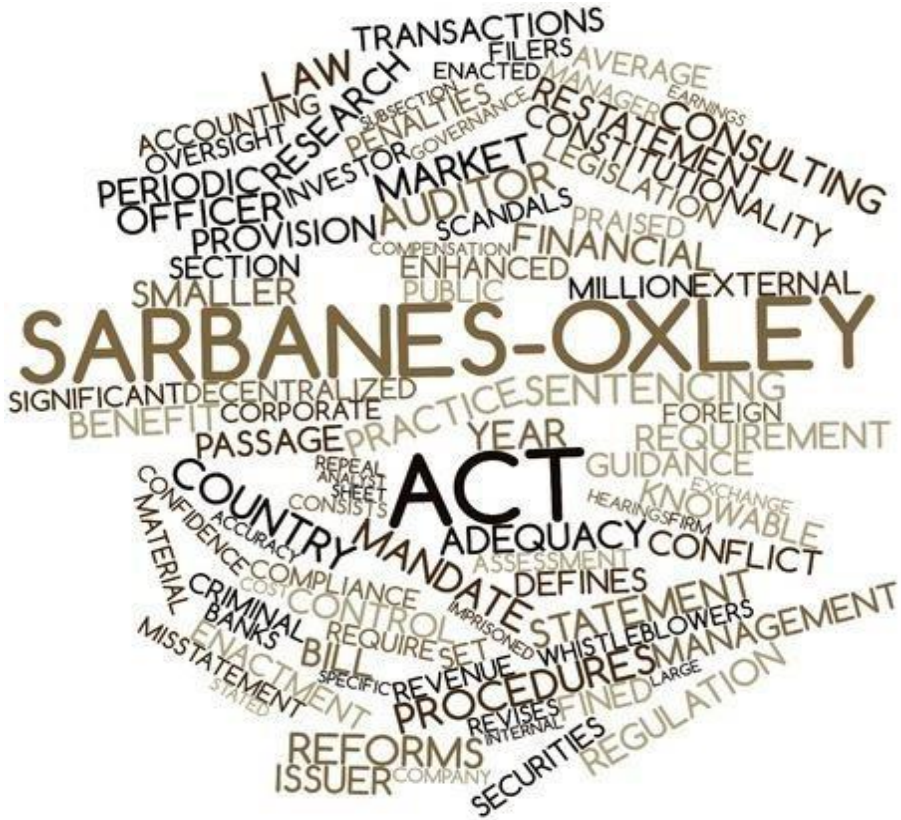
CONTROL INTERNO Y DE TECNOLOGÍA DE INFORMACIÓN

AUDITORÍA Y CONTROL DE SISTEMAS

Agenda

- Control Interno y tecnologías de información
- Tipología del control
- Controles de TI
- Normas, estándares y buenas práctica sobre control

¿Qué es Control Interno?



Según **COSO** el **Control Interno** es un proceso llevado a cabo por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un **grado de seguridad razonable** en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- ✓ **Eficacia y eficiencia de las operaciones,**
- ✓ **Veracidad de la información y**
- ✓ **Conseguir el cumplimiento regulatorio.**

Fuente: Committee of Sponsoring Organizations of the Treadway Comission (COSO)

Objetivos del Control Interno

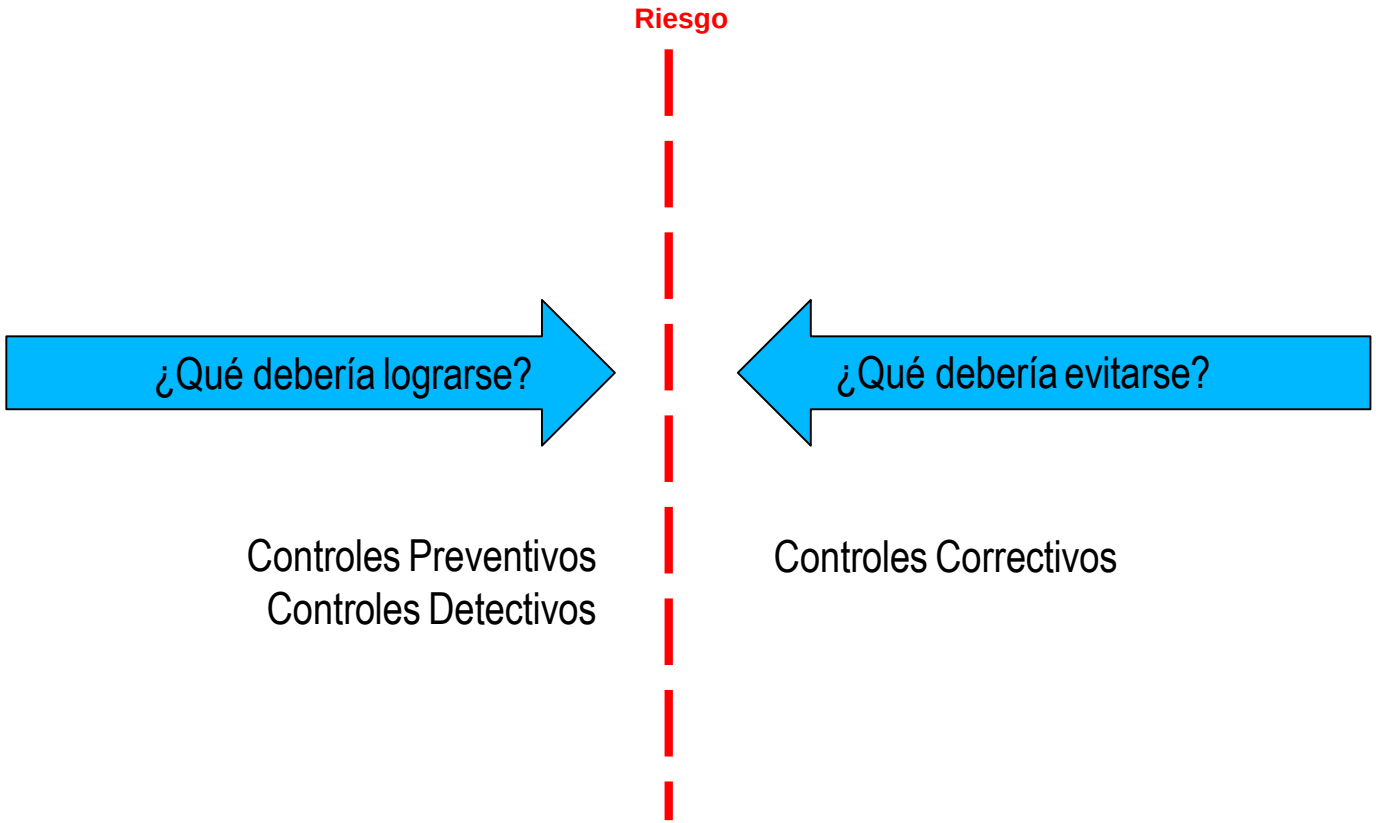
Verificar que los procesos de una organización están diseñados de tal forma que permiten alcanzar:

UNIVERSIDAD DE LIMA

60 años

TIPOLOGÍA DEL CONTROL

Controles Internos



Controles Internos

Controles Preventivos

Función

- Identifican los problemas antes de que aparezcan.
- Previenen que ocurran eventos no deseados
- Intentan entender los problemas potenciales antes de que ocurran y realizan ajustes.

Ejemplos

- Emplear sólo personal calificado.
- Segregar funciones (factor disuasivo).
- Establecer el acceso a instalaciones físicas.
- Utilizar plantillas de documentos bien diseñados (evita errores).
- Encriptar los datos para evitar la divulgación no autorizada de los mismos.

Controles Internos

Controles Detectivos

Función

- Descubren e informan la ocurrencia de un error, omisión o acto no autorizado en un proceso.
- **El error u omisión ocurre**.

Ejemplos

- Realizar totales de comprobación (hash totals).
- Realizar controles de eco en telecomunicaciones.
- Verificar cálculos duplicados.
- Revisar registros (logs) de actividad para detectar intentos de acceso no autorizado.

Controles Internos

- **Controles Correctivos**

- **Función**

  - Minimizar el impacto **negativo** de una amenaza.
  - **Remediar** problemas descubiertos por controles detectivos.
  - **Identificar la causa** de un problema.
  - Corregir errores que surgen de un problema.
  - Modificar los sistemas de procesamiento para minimizar futuras ocurrencias del problema.

Ejemplos

- Ejecutar Planificación de contingencia por no funcionamiento de centro de cómputo.
- Recuperar respaldo para reprocesar proceso fallido de cuentas corrientes.
- Realizar reproceso de sistema de cuentas corrientes del 28 de febrero.

UNIVERSIDAD DE LIMA

60 años

CONTROLES DE TI

Controles de TI

Los controles de TI proveen aseguramientos para la información y los servicios manejados Tecnología. Abarcan dos componentes:

- ❑ Controles Generales (ITGC)
- ❑ Controles de Aplicación

Importancia	Si se implementan
• Alcanzar los objetivos del negocio mediante soporte adecuado. • Protege los activos de información. • Cumplimiento con Leyes y Regulaciones	• Mejoran la eficiencia • Incrementan la confiabilidad • Provee flexibilidad • Incrementa la disponibilidad y asegura la evidencia

Controles de TI

Controles Generales de TI

Estos controles **aplican a todos** los sistemas, controles y datos.

Los más comunes controles ITGC son:

- ✓ Acceso lógico sobre infraestructura, aplicaciones y datos,
- ✓ Controles sobre el desarrollo y ciclo de vida de los aplicativos,
- ✓ Controles sobre cambios a programas,
- ✓ Controles sobre seguridad física en los centros de cómputos,
- ✓ Backup de sistemas y controles de recuperación de datos,
- ✓ Controles relacionados con operaciones computarizadas.

Controles de Aplicación

Son aquellos controles que son aplicables para un **determinado proceso de negocio soportado por una aplicación específica**, entre ellos podemos encontrar la edición de registros, segregación de funciones, totales de control, logs de transacciones y reportes de errores. El objetivo principal de los controles de aplicación es asegurar:

- ✓ Que el ingreso de los datos sea exacto, completo, autorizado y correcto
- ✓ Que los datos se procesen en tiempo oportuno
- ✓ Que los datos sean almacenados de forma adecuada y completa
- ✓ Que las salidas del sistema sean adecuadas y completas
- ✓ Que los registros sean mantenidos para realizar un seguimiento de las entradas y eventuales salidas del sistema.

Referencias bibliográficas

- COSO (2017). Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management Integrating with Strategy and Performance (COSO-ERM). COSO Board Publishing, Suiza.
- ISACA (2018). ISACA. COBIT 2019. ISACA Publishing, USA.
- Piattini (2009). Auditoría de Tecnologías y Sistemas de Información. Editorial RAMA, España (2009).
- Tupia (2011). Principios de auditoría de sistemas y tecnologías de información. Tupia Consultores Y Auditores S.A.C., Perú.

¿Consultas?

UNIVERSIDAD DE LIMA

60 años

CONTROL INTERNO Y DE TECNOLOGÍA DE INFORMACIÓN