UPC
UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS
Laureate International Universities®

SI-38 Seguridad y Auditoría de Sistemas

Profesor: Ing. Ronald Mejía Tarazona

Presentación del Curso

- Profesor:
  - Ing. Ronald Mejía
  - rmejiat@rimac.com.pe
  - mejiat.ronald@gmail.com
  - pcsirmej@upc.edu.pe

Presentación del Curso

CURSO : SI-38 SEGURIDAD Y AUDITORÍA DE SISTEMAS
SEMESTRE : 2007-02
CRÉDITOS : 3
HORAS : 3 horas / semana de teoría
PROFESOR : Ronald Mejía Tarazona
ÁREA : Sistemas de Información

I. SUMILLA

El curso comprende el estudio de técnicas de auditoría y control orientados hacia los sistemas informáticos de una empresa. Adicionalmente, desarrolla tópicos de seguridad de información y elementos de evaluación y administración de riesgos de Tecnología de Información, basándose en estándares de aceptación mundial como son: ISO 17799, COBIT, entre otros.

II. LOGROS DEL CURSO

1. Conocer como se desarrolla el proceso de auditoría de Sistemas de Información en una empresa.
2. Conocer los aspectos administrativos y técnicos fundamentales a ser evaluados en un proceso de auditoría de Sistemas de Información.
3. Identificar las vulnerabilidades de un Sistema de Información y desarrollar planes de reversión.
4. Evaluar aspectos de protección de activos, recuperación de desastres y continuidad del negocio.
5. Evaluar aspectos de desarrollo, adquisición, implementación y mantenimiento de los Sistemas de Información.
6. Proponer un modelo de auditoría y controles de aplicación.

1. Sistema de Evaluación
   - 04 Prácticas calificadas (PC)
   - 01 Examen Parcial (EA)
   - 01 Examen Final (EB)
   - 01 Trabajo del curso (T)

PF = 0,03*EA1 + 0,07*EA2 + 0,08*EA3 + 0,08*EB1 + 0,04*EB2 + 0,1*EB3 + 0,08*PC1 + 0.08*PC2 + 0.08*PC3 + 0.08*PC4 + 0.28T

2. Formación de Grupos / Elección de delegado

SI-38 Seguridad y Auditoría de Sistemas

Cap. 1: El Proceso de Auditoría de Sistemas de Información

El contexto internacional: Riesgos y amenazas

- En la última década, una serie de grandes escándalos financieros en grandes empresas globales, han evidenciado la fragilidad de los controles operativos y financieros en las empresas.

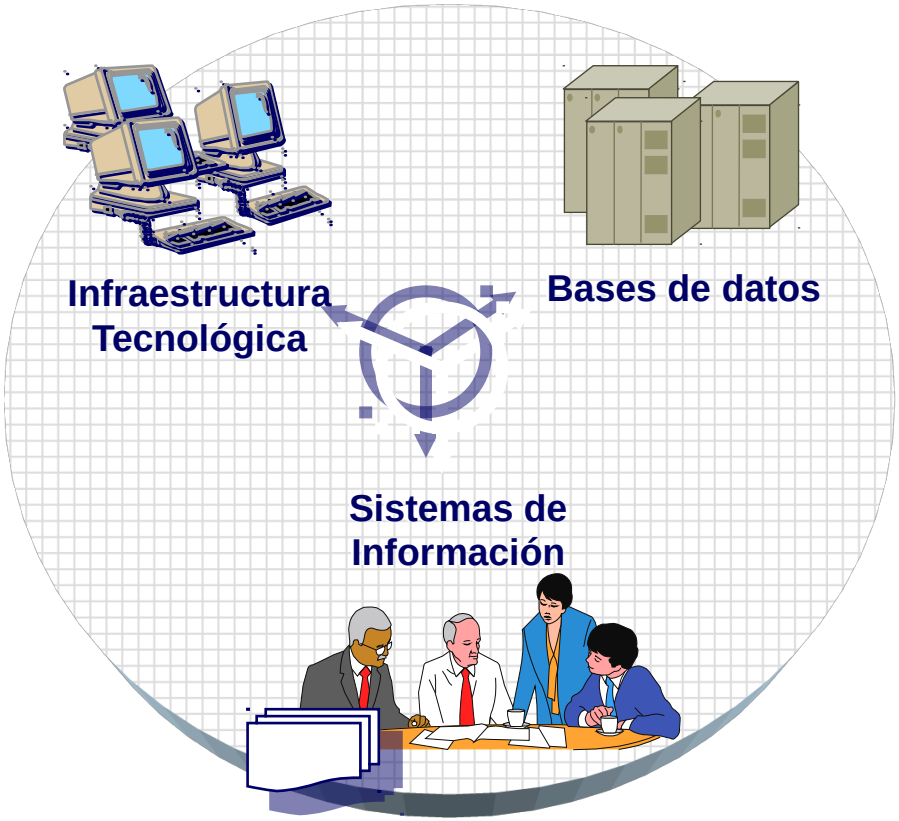
- Grandes empresas de auditoría internacionales se han visto envueltas por acción u omisión en estos escándalos.

- Como consecuencia, se ha reforzado a nivel internacional la exigencia de que las empresas cumplan una serie de procedimientos y prácticas de control, a fin de garantizar la transparencia y veracidad de sus operaciones y manejo financiero. Ej: Sarbanes-Oxley Act (USA, 2002).

- El soporte de tecnología es clave para las operaciones y manejo financiero de las empresas, la exigencia regulatoria sobre los controles de TI se ha incrementado grandemente: COSO, COBIT, etc.

- En Perú la SBS ha establecido normativa para el control del riesgo operativo y de TI en las empresas financieras (2003)

El Capital de Información



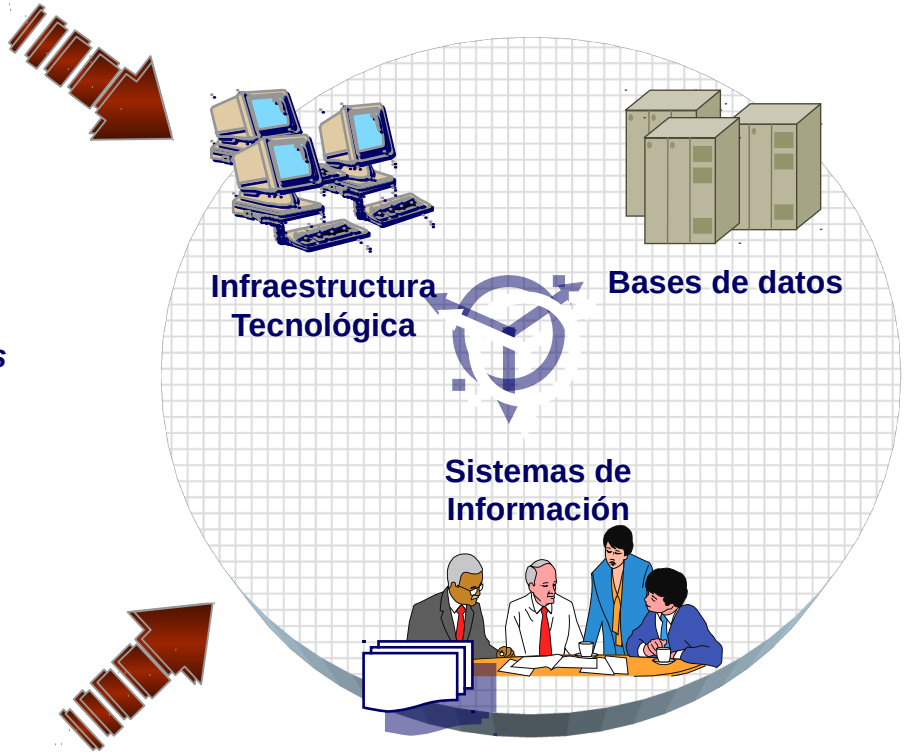
El capital de información junto con los demás activos intangibles influyen en el desempeño de la empresa al mejorar los procesos internos más importantes en la creación de valor para clientes y accionistas

Kaplan y Norton, Strategic Maps - 2004

Principales Amenazas al Capital de Información

Divulgación no autorizada de información confidencial

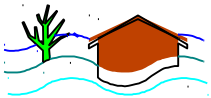
- ***Alteración no autorizada de información.***
- ***Accesos por proveedores***
- ***Fraudes por empleados***
- ***Espionaje por competidores***
- ***Violación de derechos de propiedad***
- ***Gestión deficiente de la tecnología***



Amenazas de origen tecnológico

Inoperatividad de tecnología

- ***Virus, worms, spyware***
- ***Ataques de hackers.***
- ***Saturación de servicios***
- ***Spam***



Amenazas de origen natural

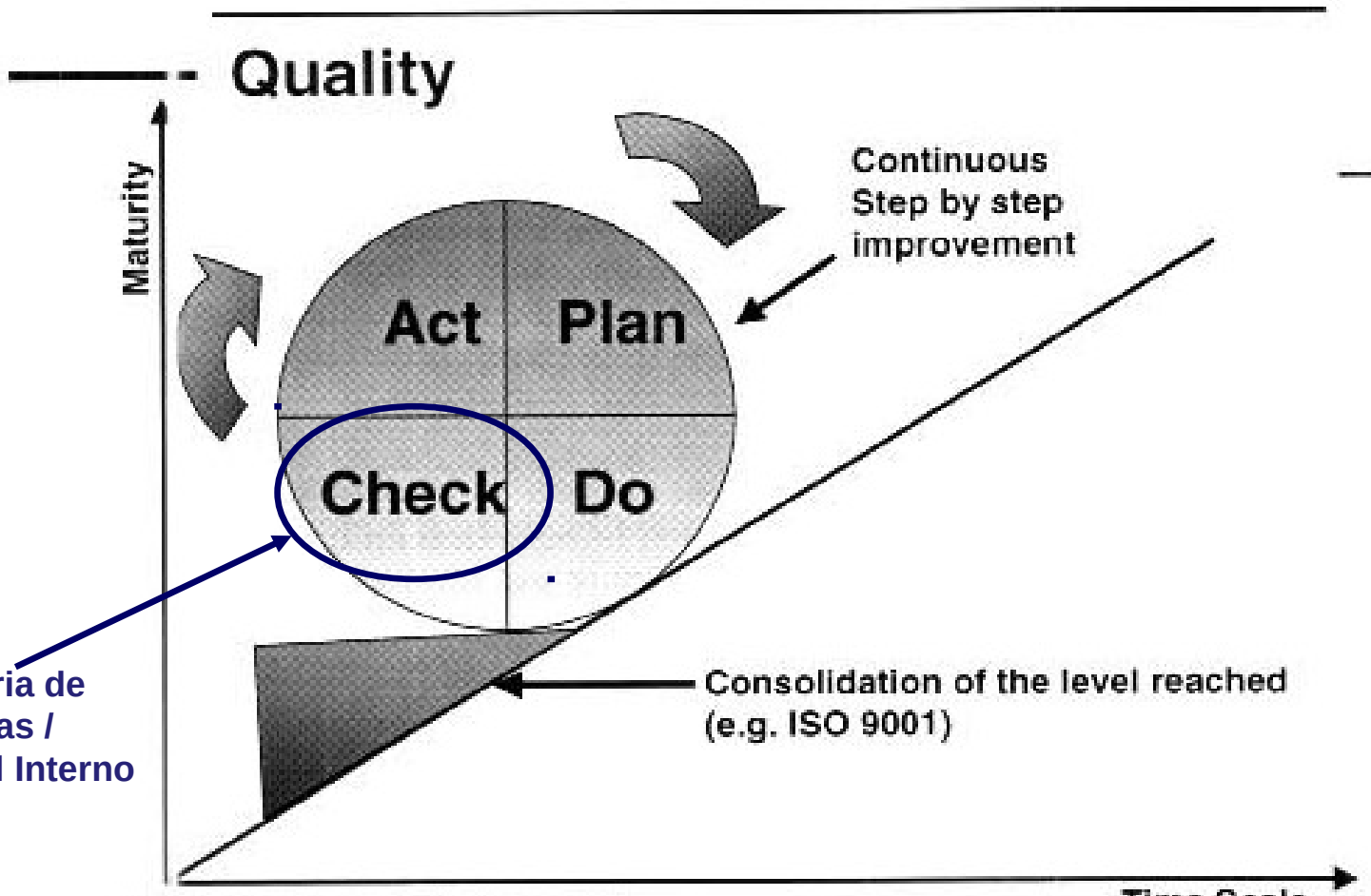
Terremotos

- ***Inundaciones***
- ***Incendios***

El contexto internacional: Riesgos y amenazas

- Atentado contra el World Trade Center, Washington (11/09/01): 8,000 servidores Intel, 5,000 servidores UNIX, 34,000 PC's, US$ 32 billones para recuperar equipos y sistemas, 3500 víctimas y destrucción de sedes corporativas de diversas empresas globales.
- En 1998 se produjo una interrupción de servicios de comunicaciones de AT&T por fallas en un switch (software y procedimientos). Por 18 horas, a nivel mundial, usuarios de tarjetas de crédito no pudieron usarlas.
- Terremoto de Kobe, Japón (17/01/95): duró 20 seg., intensidad de 6.8 Richter. 40,000 victimas, 148 incendios y 6.513 edificios destruidos.
- Empresa de Telecomunicaciones: Incendio daña instalaciones del centro de cómputo, el cual es inundado por la acción de los bomberos. Varios sistemas críticos quedan fuera de servicio por tres días.
- Empresa de Cosméticos: Por cercanía de su local a la Embajada de Japón, el centro de cómputo queda inutilizable por 23 días. (11/12/96)

El mejoramiento contínuo: el Ciclo Deming



Auditoria de Sistemas / Control Interno

Service Improvement Program:
A formal project undertaken within an organization to identify and introduce measurable improvements within a specified work area or, work process

Definición de Auditoría

Auditoría es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Contenido	Una **opinión**
Condición	**Profesional**
Justificación	Sustentada en determinados **procedimientos**
Objeto	Determinada información obtenida de ciertas fuentes
Finalidad	Determinar si representa adecuadamente la realidad o responde a las expectativas que le son atribuídas, es decir, su **fiabilidad**

Clases de Auditoría

El objeto y la finalidad de una auditoría definen su tipo, los principales son:

Clase	Contenido	Objeto	Finalidad
Financiera	Opinión	Cuentas anuales	Presentan realidad
Informática o de Sistemas	Opinión	Sistemas de información, recursos informáticos, planes de contingencia, etc.	Operatividad eficiente y según normas establecidas
Gestión	Opinión	Dirección	Eficacia, eficiencia.
Cumplimiento	Opinión	Normas establecidas	Las operaciones se adecúan a estas normas

El sector Financiero ha sido el principal usuario de los procedimientos de auditoría

Clases de Auditoría

Algunos ejemplos:

Clase	Ejemplo
Financiera	Auditoría de Estados Financieros de las empresas. Exigencia de entidades reguladoras y financieras. Debe verificar que los EE.FF. muestren la realidad de la empresa
Informática o de Sistemas	Auditoría de controles de sistemas, requerida por las Auditorías Financieras y entidades reguladoras
Gestión	Auditoría de las gestión de una entidad pública o privada, luego de un cambio de los Directivos.
Cumplimiento	Cumplimiento de estándares de gestión de la calidad (ISO 9000), estándares de gestión ambiental (ISO 14000), estándares de gestión de la seguridad de información (ISO 27000)

Procedimientos de Auditoría

- La opinión expresada en una auditoría se fundamenta en el cumplimiento de procedimientos específicos que deben proporcionar una seguridad razonable de lo que se afirma
- Existen auditorías altamente reglamentadas (las financieras) donde es obligatorio aplicar Normas Técnicas y procedimientos detallados.
- En general, una auditoría debe cumplir:
  - El trabajo debe ser planificado y supervisado adecuadamente
  - Se estudiará y evaluará el sistema de control interno
  - Se obtendrá evidencia suficiente y adecuada
  - La evidencia debe colectarse en los documentos de trabajo del auditor. Como justificación y soporte del trabajo y de la opinión emitida.

Definición de Consultoría

Consultoría es dar asesoramiento o consejo sobre lo que se ha de hacer o cómo llevar adecuadamente una determinada actividad para obtener los fines deseados.

Contenido	Dar **asesoramiento o consejo**
Condición	De carácter **especializado**
Justificación	En base a un **exámen o análisis**
Objeto	**La actividad o cuestión** sometida a consideración
Finalidad	Establecer la **manera de llevarla** a cabo adecuadamente

Necesidad de la Auditoría de Sistemas

- Hoy día, el procesamiento automatizado de la información a través de las computadoras, es indispensable en las empresas.
- El alto desarrollo tecnológico y la intensa competencia entre las empresas las hace cada vez más dependientes de los sistemas.
- La información y, en general, todos los activos tecnológicos son los recursos o activos más importantes de una empresa.
- La información procesada es utilizada para tomar decisiones operativas, tácticas y estratégicas.
- La información debe ser preservada de cualquier mal uso que afecte su integridad, privacidad o disponibilidad.
- Las fallas o el mal uso de los sistemas puede afectar grandemente a la sociedad (empresas y personas): mala asignación de recursos, fraudes, pérdida de privacidad, etc.

Necesidad de la Auditoría de Sistemas

Factores que influencian hacia el control y auditoría del uso de las computadoras

Necesidad de la Auditoría de Sistemas

Pérdida de datos	Daño o pérdida de información: archivos de cuentas por cobrar, cuentas por pagar, etc.
Mala toma de decisiones	La información se utiliza para la toma de decisiones. Dependiendo de si las decisiones son estratégicas, táctica u operativas, el impacto de la calidad de los datos y la información provista por los sistemas puede ser de mayor o menor impacto.
Uso indebido de la tecnología	Virus, hacking, acceso físico ilegal, abuso de privilegios de acceso a sistemas, etc. pueden originar pérdidas importantes a las organizaciones: destrucción o robo de activos o información, alteración indebida de datos, pérdida de confidencialidad o privacidad, interrupción de operaciones, uso indebido de activos, daño físico del personal, etc.
Protección de la inversión en tecnología y personal	Los montos invertidos en hardware y software son importantes. Su daño o robo puede originar una pérdida económica importante, interrupción de operaciones, pérdida de confidencialidad, pérdida de ingresos, etc.
Errores en procesamiento de la información	El mal funcionamiento de los sistemas puede originar fallas en los procesos productivos, merma de la calidad, accidentes, incremento de costos o pérdida de ingresos, etc.
Confidencialidad y privacidad	La liberación de información confidencial puede originar importantes pérdidas económicas y ventaja frente a la competencia, también puede originar pérdidas por denuncias de clientes afectados.

Definición de Auditoría de Sistemas o Auditoría Informática

- *Es el proceso de recolectar, agrupar y evaluar evidencias para determinar si un sistema informático salvaguarda los activos de cómputo, mantiene la integridad de los datos, utiliza eficientemente los recursos de la organización y contribuye eficazmente a los objetivos de la organización.*

- La auditoría de sistemas cumple dos clases de objetivos principales:
  - ✓ Objetivos de protección de activos e integridad de datos
  - ✓ Objetivos de gestión: eficacia y eficiencia en el cumplimiento de metas empresariales

Objetivos de la Auditoría de Sistemas

Protección de activos	Hardware, software, instalaciones, personas (conocimiento), archivos de datos, documentación de sistemas, formularios oficiales, suministros, Riesgos: daños físico, robo, uso indebido, etc.
Integridad de datos	Mantener atributos de los datos: deben ser completos, veraces, confiables. Riesgos: incertidumbre sobre las operaciones de la empresa, pérdida de competitividad
Efectividad de sistemas	Los sistemas deben cumplir/atender los objetivos/necesidades para los que fueron implementados. Riesgos: sistemas incompletos, no funcionales, complicados, costosos.
Eficiencia de Sistemas	Un sistema eficiente utiliza la menor cantidad posible de recursos para alcanzar sus objetivos: capacidad de procesamiento, software de base, dispositivos de entrada/salida, operación del sistema, etc.

Definición de Auditoría de Sistemas o Auditoría Informática

- El auditor informático evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos existentes, desarrollando y aplicando técnicas de auditoría, incluyendo de ser necesario el uso de software especializado.

- El auditor informático es responsable de revisar e informar a la Dirección de la organización sobre el diseño y funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

- El Informe de Auditoría es el documento formal donde se comunican los resultados de una auditoría informática.

La Auditoría y el control interno

Para cumplir los objetivos de protección de activos, integridad de datos, efectividad y eficiencia de sistemas, se requiere que la organización establezca un sistema de control interno (procesos y actividades) cuyos principales elementos son:

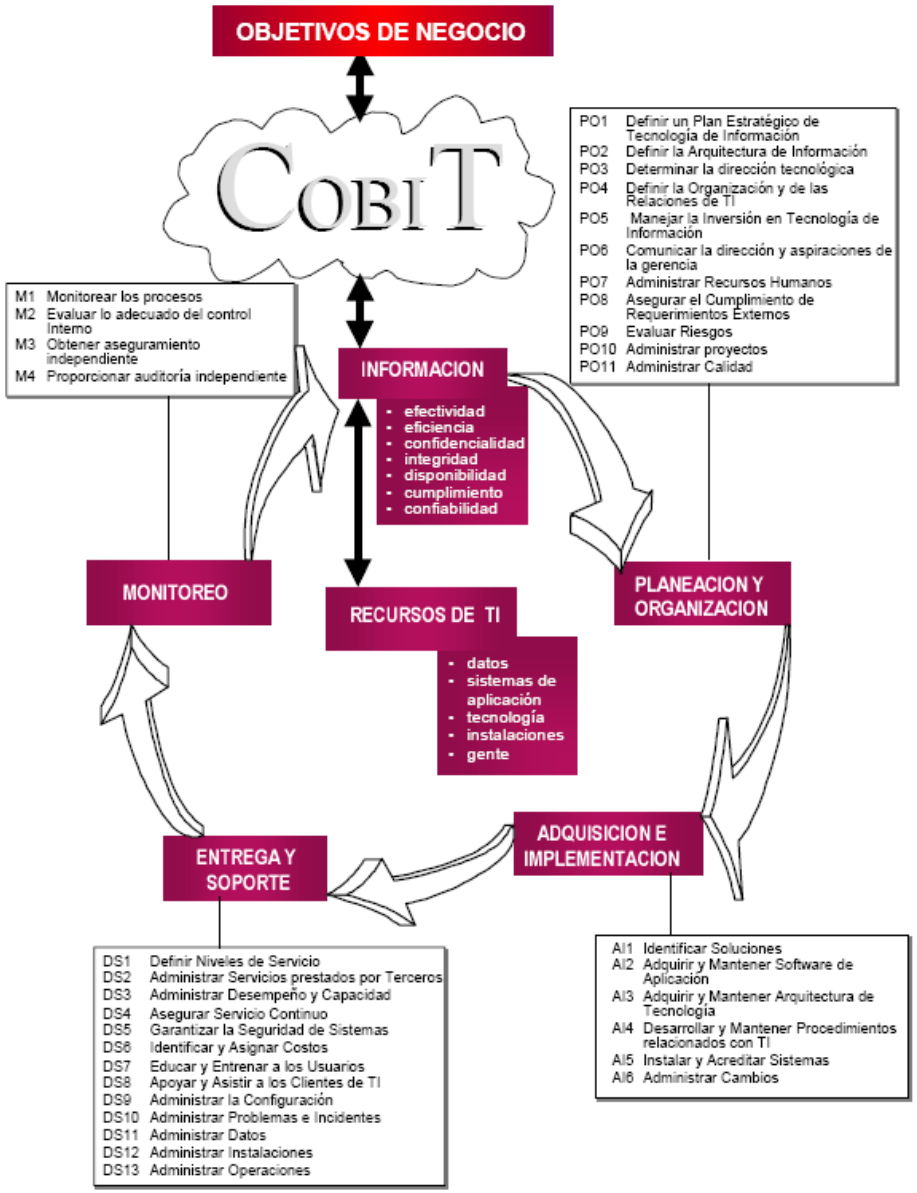
- Separación de actividades.
- Delegación de autoridad y responsabilidad.
- Personal competente y confiable
- Sistema de autorizaciones.
- Adecuados mecanismos de documentación y registro de actividades.
- Control físico sobre activos y registros.
- Adecuada supervisión
- Revisiones independientes de resultados.
- Verificación periódica de exactitud de la información contra los registros físicos.

COBIT

- Control Objetives for Information and Related Tecnologies es un marco metodológico de buenas prácticas para la administración de las tecnologías de la información. Fue desarrollado por ISACA e ITGI en 1996 y ya se encuentra en su cuarta versión (2005)

- COBIT provee a los Gerentes, auditores y usuarios de TI de un conjunto de métricas, indicadores, procesos y mejores prácticas generalmente aceptados como ayuda para alcanzar el mayor beneficio posible del uso de las TI, asegurar que estas apoyen los objetivos y estrategias de la organización y que cuenten con un marco apropiado de control.

PROCESOS DE IT DE COBIT DEFINIDOS DENTRO DE LOS CUATRO DOMINOS



ISACA

- Information System Audit and Control Asociation (ISACA) es una asociación internacional de profesionales relacionados a las tareas de auditoría de TI.

- Se fundó en 1967, cuando un conjunto de profesionales reconoció que debido a la criticidad de la función de auditoría de sistemas en las organizaciones requería una fuente centralizada de información, guías de trabajo y estándares. Tiene más de 50,000 miembros en 140 países.

- ISACA provee una serie de estándares, guías y procedimientos que deben seguirse para realizar auditorías de sistemas.

- ISACA provee dos certificaciones internacionales a los profesionales que cumplen los requisitos que establece:
  - CISA: Certified Information Systems Auditor
  - CISM: Certified Information Security Manager

Caso de estudio

Lectura y discusión en clase de caso Union Dime Savings Bank.

Gracias por su atención