UNIVERSIDAD DE LIMA | 60 años

AUDITORÍA Y CONTROL DE SISTEMAS

UNIVERSIDAD DE LIMA

FACULTAD DE INGENIERÍA Y ARQUITECTURA
CARRERA DE INGENIERÍA DE SISTEMAS

AUDITORÍAS DEL GOBIERNO DE TI, DEL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN Y DE LA GESTIÓN DE SERVICIOS

AUDITORÍA Y CONTROL DE SISTEMAS

AGENDA

- Ejecución de Auditoria al Gobierno de Tecnología de la Información, al Gobierno de la Seguridad de la información y la Gestión de Servicios de Tecnologías de la Información.
- Caso práctico
- Referencias

UNIVERSIDAD DE LIMA

60 años

CONCEPTOS GENERALES

Antecedente

- **Gobierno Corporativo**
- Conjunto de responsabilidades y prácticas ejercidas por la alta dirección de una organización con el fin de:
  - Dirigir, gestionar y monitorear sus actividades hacia la consecución de sus objetivos [ISACA, 2018b]

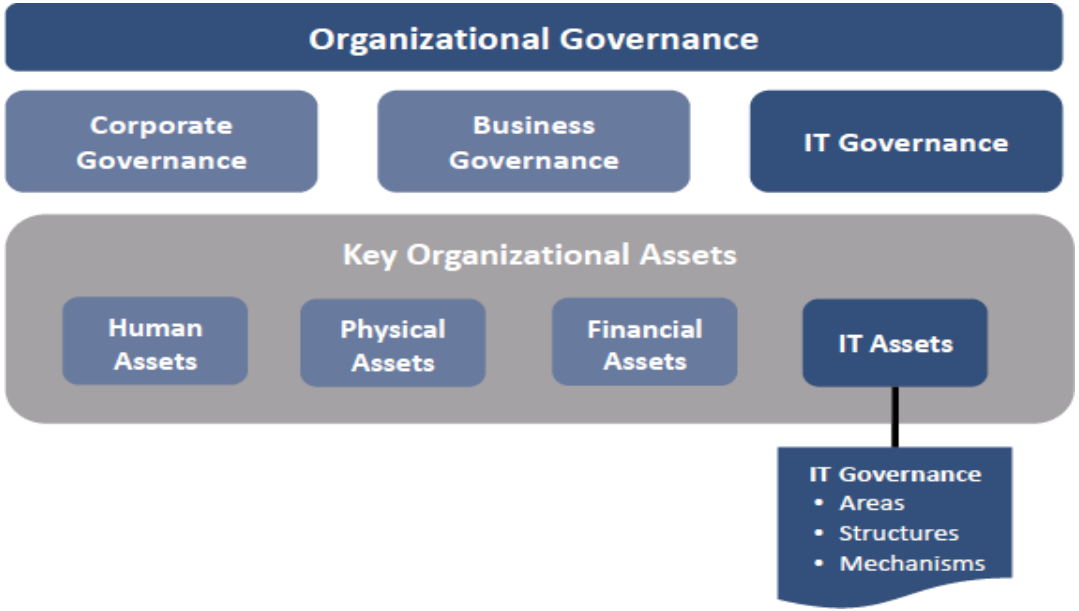
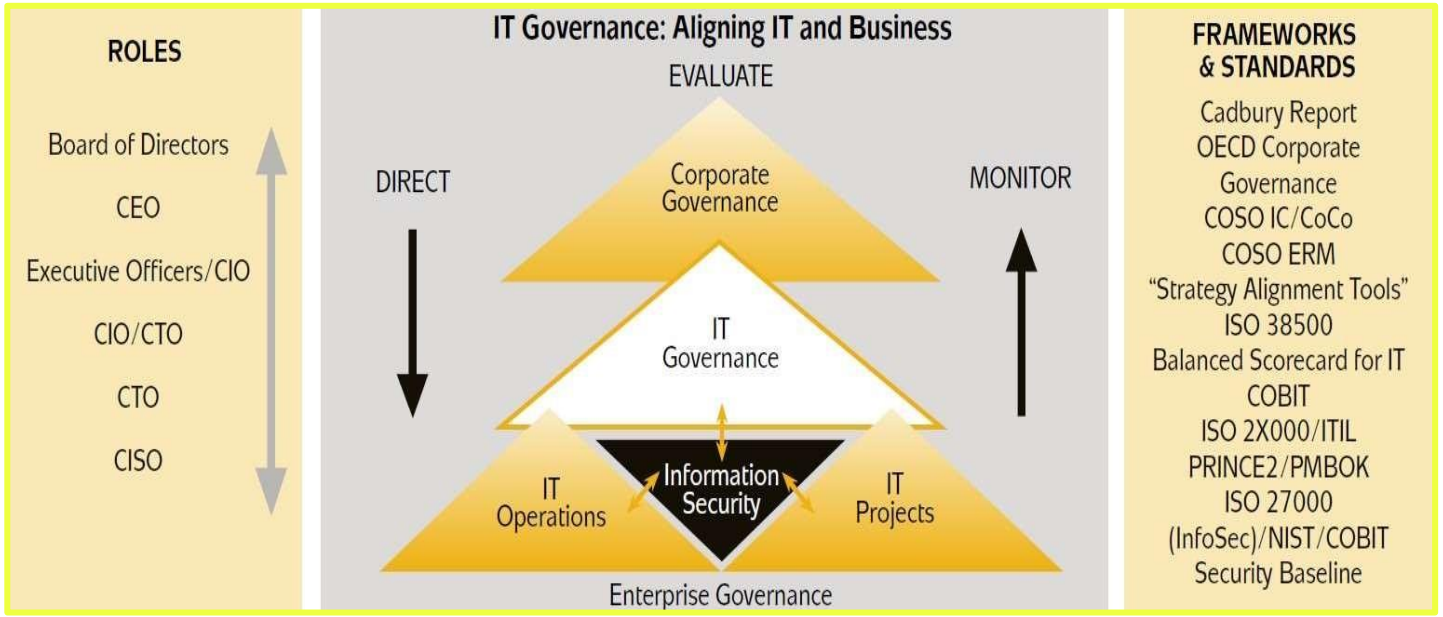


Figura 1: Gobernanza organizacional y relación de gobernanza de TI

Adaptado de: Institute of the Gouvernance des Systems d'Information, The place of IT Governance in the Enterprise Governance, 2005.

Definiciones

- **Gobierno de TI:** conjunto de responsabilidades y prácticas ejercidas por la alta dirección de una organización con el fin de proporcionar un uso adecuado de las TI alineadas al negocio, otorgando valor y facilitando la consecución de sus objetivos [ISACA, 2018b].



Definiciones

- **Gobierno de seguridad de la información:** Conjunto de responsabilidades y prácticas ejercidas por la alta dirección de una organización para proteger de los activos de información y la información relacionada, y garantizar el cumplimiento de los objetivos del negocio [ISACA, 2018a]

Definiciones

- **Gestión de servicios de TI:**
  Conjunto de responsabilidades y prácticas con el fin de diseñar **servicios de TIC, alineados con las necesidades** de las empresas, haciendo hincapié claramente en los beneficios que se van a obtener por el uso de dichas tecnologías, considerando[ISACA, 2018b]:
  - ✓ Eficacia y eficiencia
  - ✓ Concepto de valor
  - ✓ Concepto de servicios

Auditorías al gobierno de TI/seguridad

- Es el proceso de evaluación por medio del cual se verifica tanto para el gobierno de TI como para el gobierno de seguridad :
  - ✓ Que la alta dirección conoce y ejecuta sus responsabilidades de gobierno, otorgando liderazgo en estas iniciativas
  - ✓ Que se tiene y sigue una dirección basada en una estrategia (de TI, de seguridad)
  - ✓ Que se tiene un mecanismo de toma de decisiones (relacionadas con las TIC, con la seguridad, la privacidad y la ciberseguridad)
  - ✓ Que se optimizan beneficios, recursos y riesgos

UNIVERSIDAD DE LIMA | 60 años

EJECUCIÓN DE AUDITORÍAS AL GOBIERNO DE TI, DEL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN Y DE LA GESTIÓN SERVICIOS

Alcance

- Hay que incluir en la auditoría únicamente aspectos relevantes a las **responsabilidades del gobierno**, cualquiera que este sea:
  - ✓ Corporativo
  - ✓ De TI
  - ✓ De seguridad
- El principal error como se ha indicado previamente, es mezclar aspectos ajenos a estas responsabilidades.
  - Típico error: incluir “revisar un software”

Criterios para auditorías de Gobierno de TI / Seguridad de la información

- **Gobierno de TI / Seguridad**
- Estrategia de TI o SI
- Actividades del Comité de TI o SI
- Estructura del departamento de TI y funciones (segregación)
- Gestión de presupuestos de TI / SI
- Gestión de recursos humanos de TI / SI

- **Gobierno de Seguridad de la información**
- Política y plan de seguridad de la información
- Comité de seguridad de la información
- Estructura y funciones del área de seguridad de la información

Criterios para auditorías de Gestión de Servicios de TI

- Políticas y prácticas para implementar, entregar y gestionar servicios de TI a usuarios finales para satisfacer tanto sus necesidades y los objetivos establecidos por la empresa.
- Marco ITIL (biblioteca de infraestructura de tecnología de la información) – Estrategia y Diseño del Servicio.
- Norma ISO/IEC 20000.
- COBIT – Estrategia de Gestión del Servicio

Fuentes de evidencia

- El equipo auditor encontrará evidencias revisando:

- **Estructura organizacional de la empresa**:
  - ✓ Organigrama
  - ✓ ROF, MOF, documentación de los procesos de negocio.
  - ✓ Contratos con empleados y con proveedores
  - ✓ Actas de reuniones de los comités
  - ✓ Informes de auditorías internas o externas anteriores.

Fuentes de evidencia

- El equipo auditor encontrará evidencias revisando:

- Documentación relacionada con los procedimientos y políticas de seguridad de la información y la actividad de los comités respectivos:
  - ✓ Auditorías
  - ✓ Acciones correctivas y de mejora
  - ✓ Revisiones gerenciales
- Recordar que por un tema de alcance, estas auditorías **no deberían cubrir aspectos operativos**

Fuentes de evidencia

La siguiente lista de políticas relevantes es ilustrativa y no exhaustiva:

- ✓ Política de seguridad de la información
- ✓ Política de control de acceso
- ✓ Política de seguridad de la información del personal
- ✓ Política de seguridad física y ambiental
- ✓ Política de gestión de incidentes
- ✓ Política de continuidad de negocio y recuperación ante desastres
- ✓ Política de gestión de activos
- ✓ Reglas de comportamiento (uso aceptable)
- ✓ Política de adquisición, desarrollo de software y mantenimiento de sistemas de información
- ✓ Política de gestión de proveedores
- ✓ Política de gestión de comunicaciones y operaciones
- ✓ Política de cumplimiento
- ✓ Política de gestión de riesgos

Fuentes de evidencia

- El equipo auditor encontrará evidencias revisando:

- Documentación relacionada con la prestación de servicios de TI
  - ✓ Mesa de ayuda
  - ✓ Procedimientos de atención
  - ✓ Procedimientos relacionados a cambios
  - ✓ Evaluaciones y autorizaciones de servicios.
  - ✓ Políticas y procesos para la creación de servicios de TI
  - ✓ Relaciones con los proveerdores

Resultados esperados habituales

- La organización que conduce una auditoría de gobierno normalmente pretende encontrar como resultados lo siguiente:

- Alineación estratégica TI-NEGOCIO
- Gestión de riesgos adecuada
- Entrega de valor en forma de servicios de TI
- Gestión de recursos adecuada
- Medición del desempeño adecuada y sostenible en el tiempo.

UNIVERSIDAD DE LIMA

60 años

CASO PRÁCTICO

Contexto

- Institución estatal
- Registro público de bienes muebles, inmuebles, empresas.
- Decide realizar la adquisición de un sistema de balanceo de carga en tablas de bases de datos
  - Optimización del almacenamiento y el acceso a la información de los sistemas registrales.
- Lo instalan durante el feriado largo de fiestas patrias 2021
- Problemas presentados:
  - Falta de atención al público (2 días no se atendió)
  - Corrupción de la información
- Solicitud de una auditoría

Preguntas

1. Determine el objetivo más adecuado para la auditoría
2. Plantee el alcance de la auditoría
3. Enumere los criterios más adecuados para la auditoría
4. Indique las fuentes de evidencia más adecuadas.
5. Describa las pruebas que llevaría a cabo indicando los controles sobre los que las realizaría.

Referencias bibliográficas

- ISACA (2018a). ISACA. Certified Information Systems Auditor (CISA) Exam Preparation Guide. ISACA Publishing, USA.
- ISACA (2018b). ISACA. COBIT 2019. ISACA Publishing, USA.
- 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

AUDITORÍAS DEL GOBIERNO DE TI, DEL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN Y DE LA GESTIÓN SERVICIOS