Auditoría de Sistemas

Módulo 4: IT governance

Dra. Marcela Capobianco

Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur

Copyright

Gobierno corporativo

- El gobierno corporativo es el sistema de reglas, prácticas y procesos mediante el cual una empresa es dirigida y controlada. El gobierno corporativo esencialmente implica equilibrar los intereses de los muchos interesados de una empresa, como los accionistas, la administración, los clientes, los proveedores, los financistas, el gobierno y la comunidad. Dado que el gobierno corporativo también proporciona el marco para alcanzar los objetivos de una empresa, abarca prácticamente todas las esferas de la gestión, desde los planes de acción y los controles internos hasta la medición del rendimiento y la divulgación corporativa.

Video Corporate Governance

Qué es IT governance?

- Es una parte del gobierno corporativo
- Concierne como se aplican las TI en la organización
- Alinear las TI con los objetivos de la organización para agregar valor al negocio
- Agregar accountability (responsabilidad) al negocio

Desafíos de IT governance

- Estudiar e incorporar tecnología de HW y SW permanentemente cambiante
- Determinar el impacto de estos cambios en la organización
- Desarrollar productos innovadores para competir

-5-

Desafíos de un CIO

(Chief Information Officer) u Oficial en jefatura de sistemas

- Conseguir financiamiento
- Cooperación del resto de los ejecutivos
- Poder participar en la elección de los proyectos y en priorizar
- Peso como líder en la planificación estratégica

IT governance

-6-

Desde el punto de vista del auditor

¿Cómo puede el auditor evaluar si el gerente desempeña bien su función?

Una forma es considerar las principales tareas que debe realizar:

- planificar: determinar objetivos y formas de lograrlos
- organizar: obtener, asignar y coordinar los recursos
- conducir: motivar, guiar y comunicar
- Controlar!!

-7-

Planificar

La alta gerencia debe elaborar un plan maestro sobre los sistemas de información.
Preparar el plan, incluye:

- reconocer oportunidades y problemas en los cuales los SI pueden ser aplicados efectivamente por costos
- identificar los recursos necesarios para proveer la tecnología y los sistemas requeridos
- formular estrategias y tácticas para obtener los recursos necesarios

-8-

Importancia de Planificar

- Una pobre planificación ocasiona que no haya recursos humanos, de hw, y de sw necesarios para desarrollar correctamente la función
- Perder posición competitiva.
- La planificación de los SI es de vital importancia.

-9-

Evaluar la Función de Planificar...

La alta gerencia debe preparar dos tipos de planes:

- **plan estratégico:** plan de largo plazo que cubre los próximos 3 a 5 años de operaciones
- **plan operacional:** plan de corto plazo que cubre los próximos 1 a 3 años

-10-

Plan Estratégico

- evaluación de la información actual
- direcciones estratégicas
- estrategia de desarrollo

-11-

Plan Operacional

El plan operacional incluye:

- informes de avances
- iniciativas a tomar
- cronograma de implementación

Cómo podemos evaluar la planificación ? ➔

-12-

Modelo de McFarlan

- Argumenta que la necesidad de planificación está en función de 2 factores:
- la importancia estratégica de la cartera de los sistemas de información existentes
- la importancia estratégica de la cartera de los sistemas de información propuestos

-13-

Modelo de McFarlan

- Identifica 4 tipos de organizaciones, con diferentes necesidades de planeamiento:
  - organización soporte
  - organización industrial
  - organización en reconversión
  - organización estratégica

-14-

Organización Soporte

- Los SI existentes y propuestos tienen poca importancia.
- Los sistemas de información son soporte para la organización.
- Sólo se necesita poca planificación.

-15-

Organización Industrial

- Los sistemas propuestos son relativamente sin importancia.
- Los sistemas existentes son críticos.
- Requiere moderada planificación, fundamentalmente sobre los recursos necesarios a corto plazo.

-16-

Organización en Reconversión

- Los sistemas existentes son relativamente sin importancia.
- Los sistemas propuestos son críticos.
- Se requiere planificación de moderada a extensa, fundamentalmente de necesidades a largo plazo.

-17-

Organizaciones Estratégicas

- Los sistemas existentes y propuestos son críticos.
- Se requiere planificación a corto y largo plazo de recursos y necesidades.

-18-

Modelo de McFarlan - Resumen

Importancia de los Sist.Actuales		*Importancia de los Sist.Futuros*	
		Baja	Alta
	Baja	Organizaciones de Soporte	Organizaciones en Reconversión
	Alta	Organizaciones Industriales	Organizaciones Estratégicas

-19-

Modelo de Sullivan

- Se focaliza en 2 dimensiones:
- infusión: el grado con el cual la tecnología y los SI han sido integrados a las operaciones diarias.
- difusión: el grado en el cual la tecnología y los SI han sido dispersados a través de la organización.

-20-

Modelo de Sullivan

- Identifica 4 tipos de organizaciones:
  - tradicional
  - federal
  - medular
  - compleja

-21-

Organización Tradicional

- Ha ocurrido poca infusión y poca difusión.
- Requiere poca planificación que puede ser realizada por un grupo centralizado.

-22-

Organización Federal

- Si bien ha ocurrido poca infusión, existe alta difusión.
- Se necesita moderada planificación.
- La planificación puede ser descentralizada, concentrándose en necesidades de usuarios finales y divisiones.
- Generalmente se resisten a planificaciones a lo largo de toda la organización.

-23-

Organización Medular

- Si bien ha ocurrido poca difusión, existe alta infusión.
- Se necesita moderada planificación a extensa planificación.
- La planificación es centralizada, concentrándose en las necesidades de los grupos de los sistemas de información centralizados.

-24-

Organización Compleja

- Ha ocurrido infusión y difusión en grado alto.
- Se requiere mucha planificación.
- Debe considerar todo el espectro:
  - divisiones con su correspondiente autonomía
  - usuarios finales
  - organización en su conjunto

-25-

Modelo de Sullivan - Resumen

		Infusión de Sistemas	
		Baja	Alta
Difusión de Sistemas	Baja	Organización Tradicional	Organización Medular
	Alta	Organización Federal	Organización Compleja

-26-

IT governance (volviendo...)

- Hoy en día se debe hacer un alineamiento estratégico entre los objetivos de IT y los de negocio
- Las tecnologías de la información son tan críticas que no pueden ser relegadas a especialistas en IT o IT management
- Shared management

-27-

Para pensar

- "A board needs to understand the-overall architecture of its company's IT applications portfolio ... The board must ensure that management knows what information resources are out there in what condition they are and what role they play in generating revenue ... " (Nolan, R., F.W McFarlan: “IT and the Board of Directors”. Harvard Bussiness Review, October 2005).

-28-

Ventajas de IT governance

- Involucrar a los users (nivel CXO) como dueños de los proyectos de IT
  - Estabilizar funding
  - End user involvement

A chief experience officer (CXO) is an executive responsible for the overall experience of an organization's products and services.

-29-

Frameworks

- Brindan prácticas que nos dan feedback en value delivery y en risk management
- Deben estar alineados con las mejores prácticas reconocidas
- No existe “un” framework que encaje perfectamente con una organización

-30-

Procesos (en gral)

- Manejo de recursos de IT: inventario detallado de todos los recursos de IT y los riesgos asociados
- Mediciones de performance: asegurar que los recursos de IT se desenvuelven como es esperado y dan beneficios a la organización
- Gestión de conformidad: implementar procesos que respeten leyes y regulaciones

-31-

IT governance

-32-

IT governance frameworks

- COBIT
- ISO 27001: implementación y gestión de programas de seguridad de la información
- IT infrastructure library (ITIL): framework con información práctica sobre como alcanzar un manejo operacional exitoso de IT

-33-

Rol del auditor

- El auditor juega un rol fundamental en la implementación de un framework
- Está bien posicionado para influenciar en la gerencia y ayudar a mejorar y efectivizar las iniciativas implementadas
- Puede asegurar compliance con iniciativas de IT governance

-34-

Aspectos a auditar

- Cómo está alineada la función de los SI con la misión, visión, valores, objetivos y estrategias de la organización
- Ver si se alcanzan los objetivos de performance establecidos por el negocio (efectividad y eficiencia) mediante la función de los SI

-35-

Aspectos a auditar

- Requisitos legales, ambientales, de calidad de la información, fiduciarios, de seguridad y de privacidad
- El entorno de control de la organización
- Los riesgos inherentes dentro del entorno de IS
- Inversión / gasto de TI

-36-

Information security governance

- Dentro de IT governance, IS governance se focaliza en: confidencialidad, integridad y disponibilidad de la información, continuidad de servicios y protección de assets de información
- Parte importante e integral de IT governance
- En muchas organizaciones la información es el negocio (ejemplos?)

-37-

IS governance

- Dada la importancia y complejidad debe tener un nivel alto en el organigrama
- Objetivo: preservar la información, no sólo el programa que la manipula (cambio de énfasis)
- Es responsabilidad de la junta de directores y de la gerencia ejecutiva

-38-

Beneficios

- Provee mayor confianza en la interacción con los socios
- También en la relación con los clientes
- Protege la reputación de la organización
- Permite nuevas y mejores formas de procesar transferencias electrónicas

-39-

Roles y responsabilidades

- Junta directiva: aprobar políticas, realizar monitoreo y métricas
- Alta gerencia: realizar una estrategia efectiva en costo
- Comite de conducción: un representante de cada departamento involucrado puede ser vital para un cambio cultural
- CISO: puede ser el CIO, CEO, CFO... o alguien mas

-40-

- El CISO (Chief Information Security Officer, o director de seguridad de la información)

Estrategia de los SI

- La planificación estratégica desde el punto de vista de los SI se relaciona con la dirección a largo plazo que la organización quiere tener en cuanto a nivelar IT para mejorar su proceso de negocio.
- Lo crean el CISO junto con comite ejecutivo y el comité estratégico

-41-

Estrategia de los SI

- Una planificación efectiva incluye considerar los requerimientos de nuevos sistemas y de actualización
- Junto con la capacidad de la organización para desarrollar nueva funcionalidad mediante proyectos bien gerenciados
- Balancear costo de mantenimiento vs nuevas iniciativas

-42-

Comite de conducción

- Supervisa la función de IS y sus responsabilidades
- El chair debería ser un miembro de la junta que entiende las implicancias de la seg de la inf
- Debe incluir representantes de la alta gerencia, de la gerencia de usuarios y del dpto de IT

-43-

Comite de conducción

- No debe involucrarse en operaciones rutinarias
  - Revisa los planes a corto y largo plazo de IS
  - Adquisiciones significativas
  - Aprueba estándares y procedim.
  - Decisiones sobre asig. de responsabilidades, centralización, descentralización

-44-

Políticas y procedimientos

- Reflejan la posición de la alta gerencia sobre controles para los sistemas de información, recursos relacionados y los procesos del departamento de seguridad de la información

-45-

Políticas

- Son documentos de alto nivel que reflejan la filosofía de la organización y el pensamiento estratégico de la alta gerencia
- Deben ser claras y concisas para ser efectivas
- Son responsabilidad de la gerencia (escribirlas, promulgarlas, etc)

-46-

Políticas

- Los empleados afectados por una política deben recibir una explicación de la misma y entenderla
- Se pueden extender a terceros quienes deben ser ligados mediante un contrato de servicios en congruencia

-47-

Políticas

- Los departamentos definen políticas de bajo nivel
- Se usa un acercamiento top-down para facilitar la consistencia
- Se deben revisar y actualizar con cierta frecuencia
- Necesitan estar alineadas con los objetivos de negocio

-48-

Políticas

- Los controles se obtienen de alguna manera de las políticas
- Deben ser auditadas por compliance
- Las políticas de seguridad de la información brindan un estandar de seguridad coherente a usuarios, gerencia y técnicos
- Balancear control con productividad
- El costo del control no debe exceder al beneficio esperado

-49-

Política de Seg de la Inf

- Definición de Seg de la Inf, sus objetivos alcance e importancia
- Una declaración de la intención de la gerencia, apoyando los objetivos y ppio de seg de la inf en línea con los objetivos de negocio
- Framework para setear objetivos de control y controles

-50-

Seguridad de la Inf.

- Breve explicación de las políticas de seguridad, ppios, estándares y req de compliance de importancia para la organización
- Definir responsabilidades, como por ej reporte de incidentes
- Referencias a documentación de soporte

-51-

Revisión de la política de SI

- Debe ser revisada
- Debe tener un responsable
- Se debe responder ante distintos pedidos y revisar la política
- Debe haber un proceso para hacer cambio y un registro de los mismos

-52-

El auditor debe saber:

- Base por la cual fue definida
- Contenidos
- Excepciones
- Proceso para aprobar e implementar la política
- Entrenamiento del personal
- Revisiones periódicas y actualizaciones

-53-

Procedimientos

- Pasos detallados definidos y documentados para implementar políticas
- Deben ser derivados de las políticas
- Deben ser claros y concisos
- Son formulados por los dueños de los procesos como una traducción efectiva de las políticas

-54-

Procedimientos

- Son más dinámicos que las políticas
- Si las prácticas operacionales no se corresponden con procedimientos el auditor está en problemas...
- Y la gerencia también, es difícil identificar controles y ver si están en operación

-55-

Procedimientos

- Deben ser bien conocidos por la gente a la que afectan
- Importante guardarlos, distribuirlos y darlos a conocer, sino no sirven
- Se debe realizar una revisión independiente para ver si se siguen los procecimientos

-56-

Gerenciamiento del riesgo

- Proceso de identificar riesgos y amenazas a los recursos de información usados por una organización
- Se debe decidir que medidas tomar para reducir el riesgo a un nivel aceptable basado en el valor de los activos de información de la organización
- Se debe tener en claro cual es el nivel de riesgo que quiere la compañia

-57-

Gerenciamiento del riesgo

- En el contexto de IT esto impacta todas las inversiones futuras en tecnología
- También hasta que punto se protegen los activos de IT y el nivel de seguridad requerido
- El gerenciamiento del riesgo involucra identificar, analizar, evaluar, tratar, comunicar el impacto del riesgo en los proyectos de IT

-58-

Gerenciamiento del riesgo

- Se deben decidir las estategias que se usarán y dejar en claro las responsabilidades de cada actor
- Dependiendo del tipo de riesgo y de su importancia para el negocio la gerencia y la junta pueden elegir realizar alguna de las siguientes acciones:

-59-

Qué hacer con el riesgo

- Evitarlo: eliminar el riesgo eliminando su causa
- Mitigarlo: disminuir la probabilidad o impacto del riesgo (controles)
- Transferirlo: compartir el riesgo con partner o transferirlo mediante seguros
- Aceptarlo: reconocer formalmente la existencia del riesgo y monitorearlo

-60-

Qué hacer con el riesgo

- Otra alternativa (muy mala) es ignorar el riesgo (rechazarlo).
- Esto debe ser una bandera roja para el auditor

-61-

Desarrollar un programa de manejo de riesgo

- **Establecer el objetivo del programa**: por ej reducir el costo de asegurar o reducir el número de incidentes
- Se pueden definir KPI antes de iniciar el plan para luego usarlos para evaluar los resultados
- Responsable: alta gerencia y junta de directores

-62-

Desarrollar un programa de manejo de riesgo

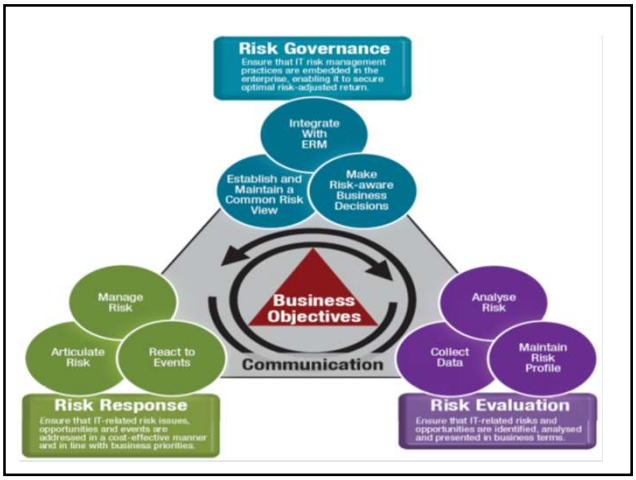
- **Asignar responsables del programa**: designar un individuo o equipo responsible de diseñar e implementar el programa
- También de su adopción en la organización

-63-

Risk IT

- La organización debe establecer un proceso repetible de manejo de riesgos
- Risk IT es un modelo basado en las normas COBIT
- Tres dominios: risk governance, risk evaluation y risk response

-64-



Risk governance

- El objetivo es asegurar que las prácticas de manejo de riesgos de IT están embebidas en la organización
- Esto permite a la organización asegurar un retorno optimo ajustado al riesgo

-66-

Establecer y mantener una visión común de riesgos -RG1

- Asegurar que las actividades de gestión de riesgos se alinean con la capacidad objetiva de la organización para las pérdidas relacionadas con IT y la tolerancia subjetiva de IT que posee el liderazgo

-67-

Integrar con ERM - RG2

- Integrar la estrategia y operaciones de IT con decisiones estratégicas del negocio

-68-

Hacer decisiones de negocios basadas en riesgo - RG3

- Asegurar que las decisiones de la organización consideren el rango completo de oportunidades y consecuencias que surgen de confiar en IT

-69-

Risk response

- Asegurar que los eventos de riesgo relacionados con IT son abordados en una forma efectiva en costo y en línea con las prioridades de negocio

-70-

Articular riesgos (RR1)

- Asegurar que la información sobre el verdadero estado de las exposiciones y oportunidades relacionadas con IT está disponible en tiempo y forma para la gente apropiada

-71-

Gestionar riesgos (RR2)

- Asegurar que las medidas para aprovechar oportunidades estratégicas y reducir riesgos a un nivel aceptable son manejadas como un portfolio

-72-

Reaccionar a eventos (RR3)

- Asegurar que las medidas para aprovechar oportunidades inmediatas o limitar la magnitud de las pérdidas de eventos relacionados con IT se activan en tiempo y forma y son efectivas

-73-

Risk evaluation

- Asegurar que todos los riesgos relacionados con IT están identificados, analizados y presentados en términos del negocio

-74-

Recolectar datos (RE1)

- Identificar datos relevantes para permitir una identificación, análisis y reporte de los riesgos efectiva

-75-

Analizar riesgos (RE2)

- Crear información util para soportar decisiones de riesgo que toman en cuenta la relevancia para el negocio de los factores de riesgo

-76-

Mantener un profile de riesgos (RE3)

- Mantener un inventario actualizado y completo de riesgos conocidos y atributos, recursos de IT, capacidades y controles como se los entiende en el contexto de los productos, servicios y procesos del negocio

-77-

Prácticas de gestión de IS

- Reflejan las políticas y procedimientos desarrollados para varias actividades y gerenciamiento relacionadas con SI
- En muchas organizaciones el departamento de SI es de soporte
- Un departamento de soporte ayuda a que los otros departamento desarrollen sus operaciones diarias de forma efectiva y eficiente

-78-

Prácticas de gestión de IS

- Hoy en día los SI se han vuelto esenciales en las operaciones diarias
- La tendencia dicta que sean cada día más importantes
- Auditores de SI deben entender y apreciar lo crucial que resulta un departamento de SI bien gerenciado

-79-

Manejo de RRHH

- Se relaciona con las políticas y procedimientos de la organización para reclutar, entrenar, seleccionar y promover el personal
- La efectividad de estas operaciones impacta en la calidad del personal y por tanto en el área de IT

-80-

Selección de Personal - Control

- control de referencias
- selección en base a salud física y mental
- obligación contractual para personal clave
- explicación de protocolos organizacionales a observar. Ej: confidencialidad, cuidado de equipos, etc.
- doctrinas propias de la organización

-81-

Selección de Personal - Control

- Acuerdos de confidencialidad
- Códigos de ética
- Acuerdos de conflictos de intereses

-82-

Riesgos de control

- El personal puede no ser el adecuado para la posición en que fue contratado
- Puede que no se realicen los chequeos de referencias
- Los servicios tercerizados pueden introducir riesgos que no son tenidos en cuenta!
- No considerar acuerdos requerimientos de confidencialidad

-83-

Desarrollo del Personal – Control

- Se deben realizar evaluaciones periódicas al personal para:
  - evaluar si el personal merece una promoción
  - identificar oportunidades para el crecimiento personal de los empleados
  - identificar las debilidades y fortalezas del personal
- Los empleados deben comprender claramente las reglas de la evaluación.

-84-

Desarrollo del Personal – Control

- El personal debe:
- ser informado de la evaluación,
- tener posibilidades de discutir la evaluación con su superior
- apelar la evaluación en caso de discordancia

-85-

Finalización de Servicios

- La terminación de servicios puede ser:
  - voluntaria
  - involuntaria
- Cuando un empleado se va:
  - la alta gerencia debe ser informada de inmediato
  - el supervisor deberá reportar las razones por las que el empleado se va.

-86-

Finalización de Servicios - Control

- Recuperar llaves y tarjetas de identificación
- Cancelar sus claves de acceso
- Modificar las listas de distribución
- Devolver libros, documentación, informes, etc
- Devolver cualquier equipo utilizado

-87-

Finalización de Servicios - Tareas

- Si el empleado que se va no está descontento debe capacitar a su reemplazo.
- Si el empleado que se va está descontento se lo debe separar de las áreas críticas o se le debe requerir que abandone la organización inmediatamente.

-88-