Administración de Riesgos de TI

Auditoría Informática
Administración de riesgos

Dr en.A. Dulce María Morán Linares

Elaborado en Septiembre del 2015

Horas de teoría:	Horas de práctica:	Créditos:
2	2	4
Núcleo de formación	Carácter de la Unidad de Aprendizaje	
Integral	Obligatoria	

Bibliografía

1. Echenique, J.A. (2007). *Auditoría en Informática* (2ª ed). México: McGraw-Hill,
2. Li D.(1991).*Auditoría en centros de cómputo*. México:Trillas
3. Piattini, M. & Del Peso E.(*2ª ed)*.(2001).*Auditoría Informática un enfoque práctico*. México: Alfa Omega RA-MA
4. Piattini, M. & Del Peso (2008). *Auditoría de tecnologías y sistemas de información*. México : Alfaomega Ra-Ma
5.- Gómez A.(2011).Enciclopedia de la Seguridad Informática. (2ª ed).México: Alfaomega RA-MA

6.- Del Peso Navarro E.(2012).*Vocabulario español actualizado de Ias tecnologías de la información: Bibliografías de las TICS por tem*as: Ediciones Díaz de Santos

7.- Franklin, Enrique Benjamín.(2007).*Auditoria Administrativa: Gestión estratégica del cambio*: Pearson Education

8.- ISACA & ITGI. (2012). *Manual de Preparación al Examen CISA 2013*. U.S.A: ISACA & ITGI

9.- http://www.itil-officialsite.com/ http://www.isaca.org/COBIT

10.-Solís Montes G. A. (2002). *Reingeniería a la Auditoría Informática*. México: Trillas

Guión explicativo

- Este material puede ser empleado en la materia de Auditoría informática en la unidad de competencia 4 para exponer la teoría de un análisis de riegos
- Integrar un Análisis de Riesgos con la información obtenida en cada una de las áreas evaluadas en la auditoría informática.
- Elaborar un dictamen de la auditoría informática que permita la adecuada toma de decisiones en cuanto al uso de los recursos informáticos dentro de la organización.

Marco Conceptual de Administración de Riesgos

Administración de Riesgos

Definición

Es un **proceso interactivo** e **iterativo** basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales.

Aplicable a cualquier situación donde un resultado no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades.

Administración de Riesgos

Beneficios para la Organización

- Facilita el logro de los objetivos de la organización.
- Hace a la organización más segura y consciente de sus riesgos.
- Mejoramiento continuo del Sistema de Control Interno.
- Optimiza la asignación de recursos.
- Aprovechamiento de oportunidades de negocio.
- Fortalece la cultura de autocontrol.
- Mayor estabilidad ante cambios del entorno.

Administración de Riesgos

Beneficios para el Dpto. de Auditoría

- Soporta el logro de los objetivos de la auditoría.
- Estandarización en el método de trabajo.
- Integración del concepto de control en las políticas organizacionales.
- Mayor efectividad en la planeación general de Auditoría.
- Evaluaciones enfocadas en riesgos.
- Mayor cobertura de la administración de riesgos.
- Auditorías más efectivas y con mayor valor agregado.

Proceso de administración de Riesgos

Proceso de administración de Riesgos

1. Establecer Marco General

1.1. Establecer el Contexto Estratégico

Definir la relación entre la organización y el ambiente en el que opera.

1.2. Establecer el Contexto Organizacional

Entender la organización, sus capacidades y habilidades
Conocer sus objetivos y estrategias.

1.3. Identificar Objetos Críticos

Entendiendo por objeto, el área, proceso o actividad o cualquier otro elemento en que se pueda subdividir la organización y sobre el cual se pueda efectuar administración de riesgos.
Definir los criterios bajo los cuales se pueda establecer la criticidad de un objeto respecto de otro.

Este paso del proceso es importante para evaluar y priorizar los riesgos posteriormente en el paso No. 4

Proceso de administración de Riesgos

1. Establecer Marco General

Cómo Hacerlo?

1.1. Establecer el Contexto Estratégico

Aspectos financieros, operacionales, competitivos, políticos, imagen, sociales, clientes, culturales y legales, Stakeholders -Organización, propietarios, personal, clientes, proveedores, comunidad local y sociedad-.

1.2. Establecer el Contexto Organizacional

Objetivos del negocio:
Apoyados en COSO (de operaciones, de Información Financiera y de cumplimiento legal).
Otros: la rentabilidad, el crecimiento institucional, posicionamiento competitivo, imagen, servicio al cliente, productividad, calidad, recursos humanos, impacto en la comunidad.

1.3. Identificar Objetos Críticos

Definiendo los criterios Pérdida Financiera, Pérdida de Imagen, Incumplimiento de la misión, etc., que nos permitan elaborar una clasificación de las áreas, proyectos, procesos, sistemas o actividades sobre los cuales se llevará a cabo la administración de riesgos.

Proceso de administración de Riesgos

2. Identificar Riesgos

2.1. Establecer un marco específico de administración de riesgos

Entender la actividad o parte de la organización para la cual se aplicará el proceso de administración de riesgos.

2.2. Desarrollar criterios de evaluación de riesgos

Definir e identificar los criterios de análisis y el nivel de aceptación de los riesgos

2.3. Identificar la estructura

Separar la actividad o proyecto en un conjunto de elementos que facilite su comprensión y análisis.

Proceso de administración de Riesgos

2. Identificar Riesgos

2.4. Identificar riesgos

Responder ¿qué puede ocurrir? Identificar los eventos que puedan afectar los elementos de la estructura identificada en el numeral 2.3.

2.5. Identificar causas

¿Cómo y por qué pueden ocurrir los eventos identificados como riesgos? Identificar lo que motiva, dispara o genera los eventos y los escenarios más significativos.

Proceso de administración de Riesgos

2. Identificar Riesgos

Cómo Hacerlo?

2.1. Establecer un marco de administración de riesgos

Definiendo los objetivos, estrategias, alcance y parámetros de la evaluación de riesgos a realizar.

2.2. Desarrollar criterios de evaluación de riesgos

Definiendo los aspectos en los cuales va a centrar su atención durante la evaluación – operativos, técnicos, legales, sociales, financieros, humanos.

2.3. Identificar estructura

Descomponer el todo en sus partes, de tal manera que le facilite entender el objeto de análisis y le brinde un marco lógico de acción. Por ejemplo:

- **Basado en procesos (para TI, Cobit nos propone 34 procesos).**
- **Basado en Sistemas de Información (aplicaciones, programas, archivos, proceso, comunicaciones, entradas, salidas).**
- **Basado en Proyectos (ciclo de vida de desarrollo de SW, el proceso de administración, etapas, entregables).**
- **Basado en recursos (para TI, Cobit nos propone: Datos, Aplicaciones, Tecnología, Instalaciones y Recurso Humano).**

Proceso de administración de Riesgos

2. Identificar Riesgos

Cómo Hacerlo?

2.4. Identificar riesgos

Lo común en las definiciones de riesgo son algunas palabras claves como: eventos, deseables, no deseables, positivos, negativos, probabilidad, impacto, objetivos, consecuencia, inciertos, inesperados, eventuales, etc.

Riesgo: son incidentes o situaciones, que ocurren en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos.

2.5. Identificar causas

Factores que podrían materializar el riesgo, es importante establecer relaciones con otros riesgos una causa pude generar uno o más riesgos y un riesgo puede ser generado por una o más causas.

Por lo tanto exprese los riesgos en términos de consecuencia y considere las causas que pueden generarlo. Ejemplo:

Pérdida de confidencialidad debida a interceptación de la línea de comunicación.

Proceso de administración de Riesgos

3. Análisis de Riesgos

3.1. Valorar el riesgo inherente

Asignar valor al evento de materialización del riesgo propio del objeto de análisis.

3.2. Determinar Controles Existentes

Identificar las actividades o mecanismos de control implementados para mitigar los riesgos inherentes.

3.3. Identificar Nivel de Exposición

Resultante de aplicar la fórmula:
Nivel de Exposición = Riesgo inherente - Controles

Proceso de administración de Riesgos

3. Análisis de Riesgos

Cómo Hacerlo?

3.1. Valorar el riesgo inherente

Requiere que se defina una escala de valoración:
Cualitativa: Alto, Medio, Bajo
Cuantitativa: Escala numérica (el cálculo de P.A.E es un ejemplo)
Semicuantitativa: asigna rangos numéricos a las características Alto, Medio, Bajo

La valoración se puede hacer mediante el uso de históricos para los métodos cuantitativos, utilizando la fórmula Riesgo= Impacto X Probabilidad y mediante las técnicas de valoración en grupos de trabajo (delphy) para métodos cualitativos

3.2. Determinar Controles Existentes

Se requiere conocer que control es una propiedad emergente del Sistema de Control Interno, que son los mecanismos (dispositivos y procedimientos) implementados para prevenir, detectar o corregir la materialización de los riesgos.
¡Tenga presente que la negación del control no es el riesgo!

3.3. Identificar Nivel de Exposición

Nivel de Exposición = Riesgo inherente - Controles

Proceso de administración de Riesgos

4. Evaluar y Priorizar Riesgos

4.1. Comparar contra Criterios y Definir prioridades de riesgo

Comparar el resultado del análisis de riesgo realizado contra los criterios establecidos en el numeral 1. Marco general de referencia.

Las comparaciones de análisis de riesgo realizadas sobre diferentes áreas de la organización o sobre los diferentes procesos le permitirán priorizar los riesgos sobre los cuales ha de centrar la atención para definir una opción de tratamiento.

Proceso de administración de Riesgos

4. Evaluar y Priorizar Riesgos

Cómo Hacerlo?

4.1. Comparar contra Criterios y Definir prioridades de riesgo

Elabore una lista ordenada de mayor a menor, por la valoración del nivel de exposición.

Esto le permitirá definir los riesgos de mayor grado de importancia sobre los cuales deberá definir las opciones de tratamiento.

Centre su atención en lo crítico, de acuerdo a los niveles de aceptación que tenga definidos

Proceso de administración de Riesgos

5. Tratamiento del Riesgo

5.1. Identificar opciones de tratamiento

Para la actividad o componente al cual aplicó el proceso de administración de riesgos, determine las posibles formas de reducir o mitigar el riesgo.

5.2. Evaluar opciones de tratamiento

Bajo las consideraciones del marco de referencia definido, establecer cuáles de las opciones de tratamiento identificadas se ajustan a la organización y reducen el riesgo a un nivel de exposición aceptable.

5.3. Preparar planes de tratamiento

Elaborar los planes que le permitan poner en práctica las opciones de tratamiento del riesgo seleccionadas.

5.4. Implementar Plan de tratamiento

Poner en marcha el plan definido.

Proceso de administración de Riesgos

5. Tratamiento del Riesgo

Cómo Hacerlo?

5.1. Identificar opciones de tratamiento

Existen las siguientes:

Evitar: Se reduce la probabilidad de pérdida al mínimo; dejar de ejercer la actividad o proceso.

Reducir: Se consigue mediante la optimización de los procedimientos y la implementación de controles tendientes a disminuir la probabilidad de ocurrencia o el impacto.

Atomizar: Distribuir la localización del riesgo, segmentando el objeto sobre el cual se puede materializar el riesgo.

Transferir: Pasar el riesgo de un lugar a otro, compartir con otro el riesgo, esta técnica no reduce la probabilidad ni el impacto, involucra a otro en la responsabilidad.

Asumir: Se acepta la pérdida residual probable, con la aceptación del riesgo las estrategias de prevención se vuelven esenciales.

Proceso de administración de Riesgos

5. Tratamiento del Riesgo

Cómo Hacerlo?

5.2. Evaluar opciones de tratamiento

Las opciones de tratamiento deben evaluarse con base en el alcance de la reducción de riesgo (de su probabilidad o de su impacto), la evaluación debe extenderse a los beneficios u oportunidades que la opción de tratamiento pueda crear.

Tenga presente considerar varias opciones y que éstas pueden aplicarse individualmente o de manera combinada.

Considere los siguientes factores al momento de evaluar las opciones de tratamiento

Eficacia: Efectividad de la propuesta de propuesta de tratamiento para reducir el riesgos

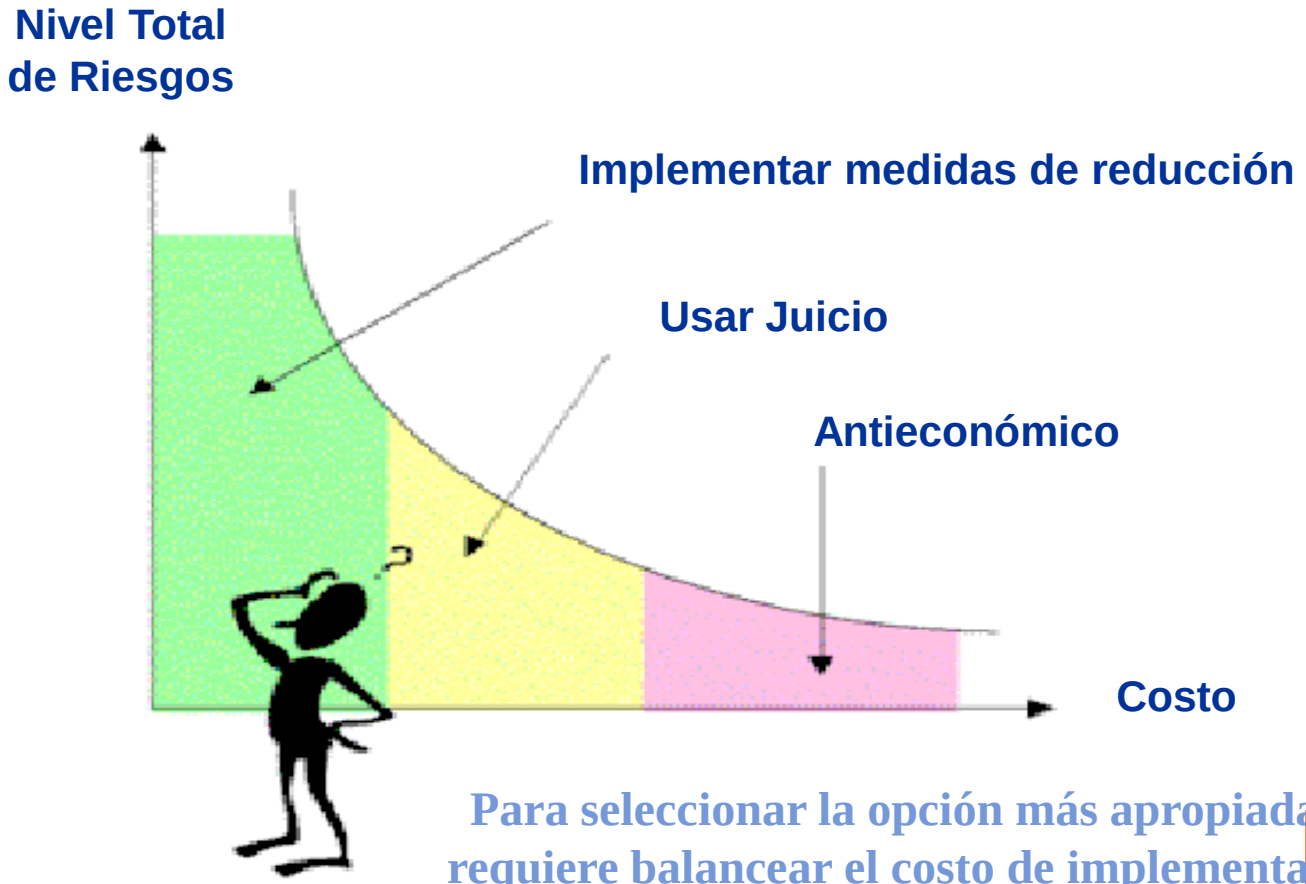
Factibilidad: La probabilidad de aceptar la opción propuesta

Eficiencia : Uso óptimo de los recursos ,Costo efectividad de la opción

Proceso de administración de Riesgos

5. Tratamiento del Riesgo

Cómo Hacerlo?



Para seleccionar la opción más apropiada se requiere balancear el costo de implementación contra los beneficios derivados.

Proceso de administración de Riesgos

5. Tratamiento del Riesgo

Cómo Hacerlo?

5.3. Preparar planes de tratamiento

Documentando cómo se implementarán las opciones elegidas:

- **Identificando responsabilidades**
- **Programas, resultados esperados, presupuesto**
- **Medir el desempeño y la revisión del proceso en su conjunto.**

El plan debería incluir también un mecanismo para evaluar la implementación de las opciones contra criterios de desempeño y responsabilidades individuales y otros objetivos, y para controlar hitos críticos de implementación.

5.4. Implementar el plan

Idealmente, la responsabilidad para el tratamiento de riesgo debería ser ejercida por los mejor capacitados de controlar el riesgo. Las responsabilidades de implementación se conciertan según la disponibilidad de tiempo de las partes.

La implementación exitosa del plan de tratamiento de riesgo requiere de un sistema efectivo de gestión:

- **Que especifique los métodos elegidos**
- **Asignación de responsabilidades, acciones individuales**
- **Controles contra criterios específicos.**

Administrando Riesgos de TI

Administración de Riesgos de TI

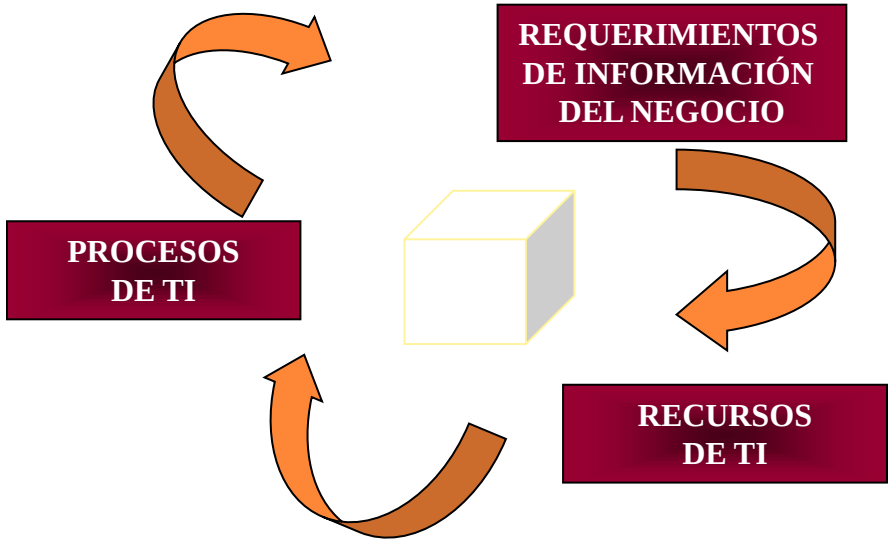
Por qué ?

- Hoy en día la mayoría de las empresas soportan sus procesos operativos con TI.
- Se ha generado un alto grado de dependencia de la tecnología informática.
- Las organizaciones tienen una elevada inversión en tecnología, por su adquisición, mantenimiento y seguridad.
- Se ha incrementado el número de ataques externos a las instalaciones de TI.
- Porque es un medio por el cual la administración puede concretar los objetivos de control sobre la T.I.

Administración de Riesgos de TI

Recordemos los principios del Modelo CobiT

- Requerimientos de la información del negocio.
- Recursos de Tecnología Informática
- Procesos de Tecnología Informática



CobiT

Requerimientos de la Información del Negocio

- **Efectividad**: La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable .
- **Eficiencia**: Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).
- **Confidencialidad**: Protección de la información sensitiva contra divulgación no autorizada.
- **Integridad**: Refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la empresa.

CobiT

Requerimientos de la Información del Negocio

- **Disponibilidad**: accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a los mismos.
- **Cumplimiento**: de las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.
- **Confiabilidad**: proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con las responsabilidades de los reportes financieros y de cumplimiento normativo.

CobiT

Recursos de Tecnología Informática

- **Datos**: Los objetos de información. Información interna y externa, estructurada o no, gráficas, sonidos, etc.
- **Aplicaciones**: Entendido como los sistemas de información, que integran procedimientos manuales y sistematizados.
- **Tecnología**: Incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.
- **Instalaciones**: Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.
- **Recurso Humano**: Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información.

Objetivos del Negocio

IT. Governance

CobiT

1. Seguimiento de los procesos
2. Evaluar lo adecuado del control Interno
3. Obtener aseguramiento independiente
4. Proveer una auditoría independiente

Seguimiento

1. Definir un plan estratégico de TI
2. Definir la arquitectura de información
3. Determinar la dirección tecnológica
4. Definir la organización y relaciones de TI
5. Manejo de la inversión en TI
6. Comunicación de la directrices Gerenciales
7. Administración del Recurso Humano
8. Asegurar el cumplir requerimientos externos
9. **Evaluación de Riesgos**
10. Administración de Proyectos
11. Administración de Calidad

Planeación y Organización

Req. Información
Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento, Confiabilidad

Recursos de TI
Datos, Aplicaciones Tecnología, Instalaciones, Recurso Humano

Adquisición e Implementación

1. Identificación de soluciones
2. Adquisición y mantenimiento de SW aplicativo
3. Adquisición y mantenimiento de arquitectura TI
4. Desarrollo y mantenimiento de Procedimientos de TI
5. Instalación y Acreditación de sistemas
6. Administración de Cambios

Prestación de Servicio y Soporte

1.Definición del nivel de servicio
2.Administración del servicio de terceros
3.Admon de la capacidad y el desempeño
4.Asegurar el servicio continuo
5.Garantizar la seguridad del sistema
6.Identificación y asignación de costos
7.Capacitación de usuarios
8.Soporte a los clientes de TI
9.Administración de la configuración
10.Administración de problemas e incidentes
11.Administración de datos
12.Administración de Instalaciones
13.Administración de Operaciones

Administrando Riesgos de TI

1. Establecer Marco General
1.1 Contexto Estratégico
1.2 Contexto Organizacional
1.3 Objetos Críticos

Leyes y Regulaciones

Ambiente Social

Entorno Económico

Ambiente Tecnológico

Clientes

Competencia

Objetivos del Negocio

Rendimiento Financiero, Crecimiento Institucional, Crecimiento competitivo, Calidad, Servicio al Cliente, Eficiencia operacional, Productividad, Etc.

Estructura Organizacional

Líneas de negocio

Procesos

Actividades

Productos

Impacto Económico - Reputación organizacional
Imagen de productos o servicios

Administrando Riesgos de TI

2. Identificar Riesgos
2.1 Marco Especifico,
2.2 Criterios de Evaluación,
2.3 Identificar Estructura,

Específicamente en la administración de TI.
y de procesos operativos apoyados con TI.

Tecnológicos y de Información
Integridad, Confidencialidad y Disponibilidad
\+ Efectividad, Eficiencia, Cumplimiento de Normas
\+ De negocio

Procesos de TI (Ejemplo COBIT) ➔ Subprocesos
Ej: Manejo y Administración de Proyectos
Adquisición y mantenimiento de sistemas de aplicación
Administración de la configuración
Prestación de servicio continuo
Proyecto de TI ➔ Etapas o actividades
Sistema de Información ➔ Módulos, Interfase, E/P/S

Administrando Riesgos de TI

2. Identificar Riesgos
2.4 Identificar Riesgos
2.5 Identificar Causas

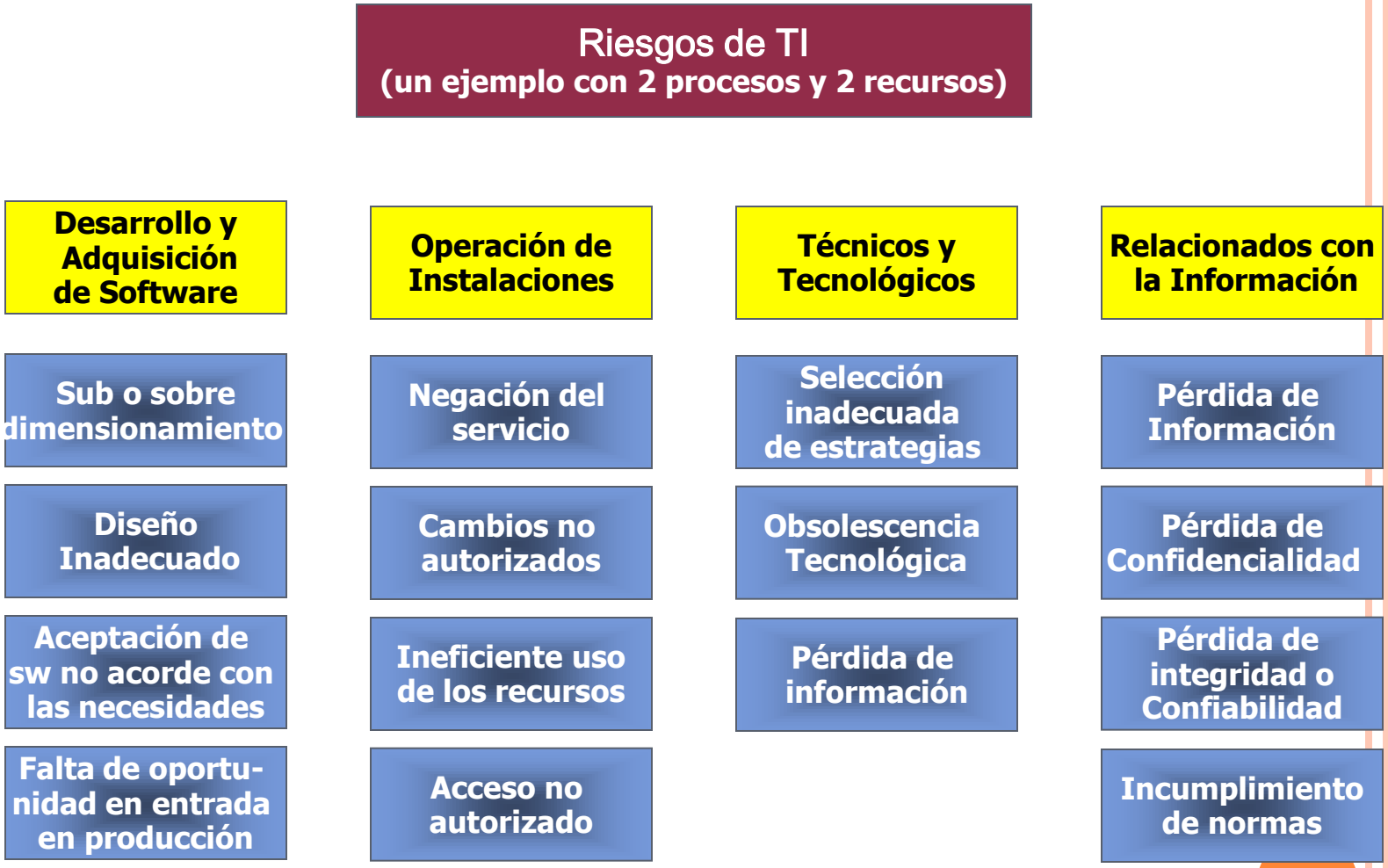
Algunos Riesgos

Ineficiencia en el uso de los recursos
Pérdida de confidencialidad
Pérdida de Integridad de información
Interrupción en la continuidad del servicio
Acceso no autorizado
Pérdida económica

Algunas Causas

Heterogeneidad en la ejecución de procesos
Ausencia de metodologías de procesos
Inadecuada clasificación de la información
Error u omisión en el procesamiento
Cambios no autorizados
Hurto de activos (recursos informáticos)
Incertidumbre para atender incidentes
Ausencia de planes de continuidad de Negocio
Suplantación de usuarios

Administrando Riesgos de TI



Administrando Riesgos de TI

3. Análisis de Riesgos
- 3.1 Valorar Riesgo Inherente
- 3.2 Determinar Controles existentes
- 3.3 Identificar el nivel de Exposición

Haga uso de la información histórica que tenga disponible.
Aplique un método cuantitativo (ej. P.A.E)

Vr. Riesgo (Causa) = Probabilidad x Impacto

Cuando lo requiera elabore sus propias escalas de medición
Aplique métodos semi-cuantitativos

Relacionados con la Probabilidad	Relacionada con el Impacto		
	Pérdida Financiera	Pérdida de Imagen	Pérdida de Disponibilidad
1 Rara vez ocurre	0 No hay pérdida	0 No se afecta la imagen	0 No se afecta
2 Poco probable	1 de 1 a 10.000	1 ante los empleados	1 por algunos segundos
3 Algunas Veces	2 de 10.000 a 50.000	2 ante un cliente	2 por algunos minutos
4 probable	3 de 50.000 a 100.000	3 ante una ciudad	3 por algunas horas
5 muy probable	4 de 100.000 a 500.000	4 ante el país	4 por un día/semana
	5 más de 500.000	5 ante el mundo	5 por una semana/mes

Administrando Riesgos de TI

3. Análisis de Riesgos
- 3.1 Valorar Riesgo Inherente
- 3.2 Determinar Controles existentes
- 3.3 Identificar el nivel de Exposición

Elabore la lista de los mecanismos de control que aplican a cada uno de los componentes de su objeto analizado

Procedimientos formales de planeación.
uso de estándares de programación, identificación, codificación.
uso de mecanismos de autenticación.
procedimientos documentados, divulgados y aplicados.
uso de metodologías de desarrollo de sw.
uso metodologías de definición de requerimientos.
procedimientos para el control de cambios.
acuerdos explícitos de niveles de servicio.
mecanismos de encripción
redundancia en dispositivos y recursos críticos.
clasificación de la información
procedimientos de respaldo
sensores y alarmas de factores ambientales (humo, humedad, temperatura)
toma física de inventarios de recursos computacionales
verificadores de licencias

Administrando Riesgos de TI

Nivel de Exposición = Riesgo – Controles aplicados

Definir el nivel de exposición le permitirá conocer la efectividad de los controles.

Sin embargo, tenga presente en relación con la efectividad de los controles los siguientes aspectos:

Internos	frente a los	Externos
Manuales	frente a los	Automáticos
Previos	frente a los	Posterior
Preventivos	frente a los	Correctivos y Detectivos
Generales	frente a los	Específicos
Continuos	frente a los	Discretos (aplicación)
Periódicos	frente a los	Esporádicos

Administrando Riesgos de TI

4. Evaluar y Priorizar Riesgos
4.1 Comparar contra criterios
4.2 Definir prioridades

Heterogeneidad en la ejecución de procesos	785
Inadecuada clasificación de la información	750
Desarrollo informal (sin metodología) de sw	675
Ausencia de planes de continuidad de Negocio	585
Incertidumbre para atender incidentes	400
Cambios no autorizados	310
Error u omisión en el procesamiento	250
Hurto de activos (recursos informáticos)	230
Suplantación de usuarios	175

Administrando Riesgos de TI

5. Tratamiento del Riesgo
- **Identificar y evaluar opciones**
- **Preparar e implementar planes**

- La identificación de opciones de tratamiento del riesgo puede conducirle a:
  - Implementación de nuevos mecanismos de control.
  - Cambiar, modificar o eliminar controles existentes.
  - Combinar mecanismos de control.
- Dependiendo del grado de complejidad de la opción elegida su implementación puede llegar al punto de convertirse en un proyecto.
  - Obligatoriedad del cambio de claves
  - Definición de pistas de auditoría
  - Documentación de Procesos
  - Plan de Continuidad Tecnológico
  - Función de aseguramiento de la calidad

Administrando Riesgos de TI

5. Tratamiento del Riesgo
- **Identificar y evaluar opciones**
- **Preparar e implementar planes**

- En los planes de Implementación es conveniente considerar:
  - Respaldo de la gerencia
  - Responsables
  - Presupuestos
  - Compromiso con la fecha de finalización

Administrando Riesgos de TI

Reflexión sobre el proceso de Administración de Riesgos

- Seguimiento a los compromisos en el plan de implementación de opciones de tratamiento.
- Revisión y ajuste de métodos y técnicas aplicadas.
- Análisis de los beneficios alcanzados (en el negocio, en la administración de TI, en la auditoría, en los usuarios).
- Es posible y conveniente continuar con otros objetos? (procesos, proyectos, áreas).
- Nivel de aprendizaje de la organización en relación con la administración de sus riesgos.

Monitorear y Revisar

Gracias!