Gestión de riesgos

Principales fases

- La gestión de riesgos es un proceso que consta de seis actividades o subprocesos:
  - Identificación del riesgo.
  - Evaluación y clasificación del riesgo.
  - Toma de decisiones.
  - Implementación de acciones.
  - Verificación de reducción del riesgo.
  - Aceptación o rechazo del riesgo residual.

1)
Criterios y limitantes

» Probabilidades de amenaza.

Para definir los criterios hay que identificar los activos: información, infraestructura y usuarios del sistema.

Pasos para obtener las entradas del subproceso 1

- Identificar activos
- Identificar limitantes: gubernamental (legales), organizacional, arquitectura (técnica)
- Valorar los activos en contraste con las limitantes, para tomar los activos más importantes: que usuarios (p ejem: vicepresidente), …

- Salida: Lista de causas y consecuencias, con riesgos potenciales.
- También identificar cuáles amenazas son las más probables, y cuáles las menos probables
- Subproceso: Luego de definidas las entradas, se procede a la identificación de riesgos, de acuerdo a las entradas.

2) Evaluación y clasificación del riesgo

- Cálculo mediante métodos probabilísticos del riesgo asociado a la amenaza.
- Basado en la observación de empresas similares o sistemas similares.

- Se clasifican las amenazas con base a los valores de riesgos, de los más probables a menos probables y según criticidad (importancia)

Salidas

- Riesgos clasificados de acuerdo a criticidad
- Políticas para evitar riesgos (primer borrador)

Roles: Los subprocesos 1 y 2 se deben realizar por el auditor de sistemas, revisando la documentación y realizando pruebas.

¿Roles en la vida real?

3) Toma de decisiones

- Enviar salida del proceso 2 a aquella(s) persona(s) con el poder de toma de decisiones.
- ¿Quiénes asumen el riesgo?
- ¿El informático es el dueño de la información?
- Salidas: Acciones puntuales y políticas

4) Implementación de acciones

- Las acciones que puede realizar el auditor o el departamento de IT, en general, se puede dividir en 4 grandes aspectos:
  - > Controlar el riesgo
  - > Eliminar el riesgo
  - > Compartir el riesgo
  - > Aceptar el riesgo.

- Salida: posible reducción del riesgo

5) Verificación

- Con base a observaciones: volver a calcular el riesgo, con las acciones y políticas implementadas.

- Salida: Validación de un nuevo riesgo calculado, pueden pasar tres cosas:
  - Reducción
  - Igualdad
  - Aumento

6) Riesgos residuales aceptados/rechazados

- Los nuevos cálculos de riesgos son presentados a los encargados de la toma de decisiones.
- Se toma la decisión de si se acepta o no el riesgo residual.
- Salida: Riesgos residuales aceptados o rechazados.

Notas

- Los riesgos residuales rechazados vuelven al inicio del proceso o a alguna de la fases anteriores. Se pueden presentar los siguientes casos:
  - El riesgo sigue siendo significativo
  - La solución no sirvió realmente.
  - Un riesgo pequeño se ha vuelto grande, porque se han dado cambios en la empresa.