Gestión del Riesgo

Análisis y Tratamiento del Riesgo

RIESGO

Objetivos de la Gestión de Riesgo

Análisis de Riesgos: Comprende la Identificación de vulnerabilidades y amenazas, como también el análisis de probabilidad de ocurrencia y su impacto.

Tratamiento de Riesgos: Comprende las tareas de priorizar, presupuestar, implementar y mantener las medidas seleccionadas para mitigar los riesgos.

El principal objetivo de la Gestión del Riesgo, es el de reducir los riesgos hasta niveles de tolerancia aceptables para la organización.

RIESGO

El análisis de riesgos implica determinar lo siguiente:

- ***Qué necesito proteger:*** Evaluación de los activos y su importancia.

- ***De quién debo protegerlo***: Evaluación de amenazas y vulnerabilidades.

- ***Cómo protegerlo:*** Evaluación de contramedidas.

Gestión del RIESGO

Centrada en Seguridad de la Información, por lo tanto hay que observar los siguientes riesgos:

- **Daño Físico**: Fuego, agua, vandalismo, perdida de energía y desastres naturales.
- **Acciones Humanas**: Acción intencional o accidental que pueda atentar contra la productividad.
- **Fallas del Equipamiento**: Fallas del sistema o dispositivos periféricos.
- **Ataques Internos o Externos**: Hackeo y/o cualquier otro tipo de ataque.
- **Pérdida de Datos**: Divulgación de secretos comerciales, fraude, espionaje y robo.

Gestión del RIESGO

Resulta más sencillo comprender el alcance de **los procesos relacionados con la Gestión del Riesgo**, viendo los componentes que intervienen en dicho proceso, como una serie de preguntas:

¿Qué puede pasar? (Amenaza)

¿Si Pasa, qué tan malo puede ser? (Impacto de la amenaza)

¿Qué tan seguido puede pasar? (Frecuencia de la amenaza)

¿Qué tan seguro estoy de las respuestas anteriores? (Falta de Certeza, Incertidumbre)

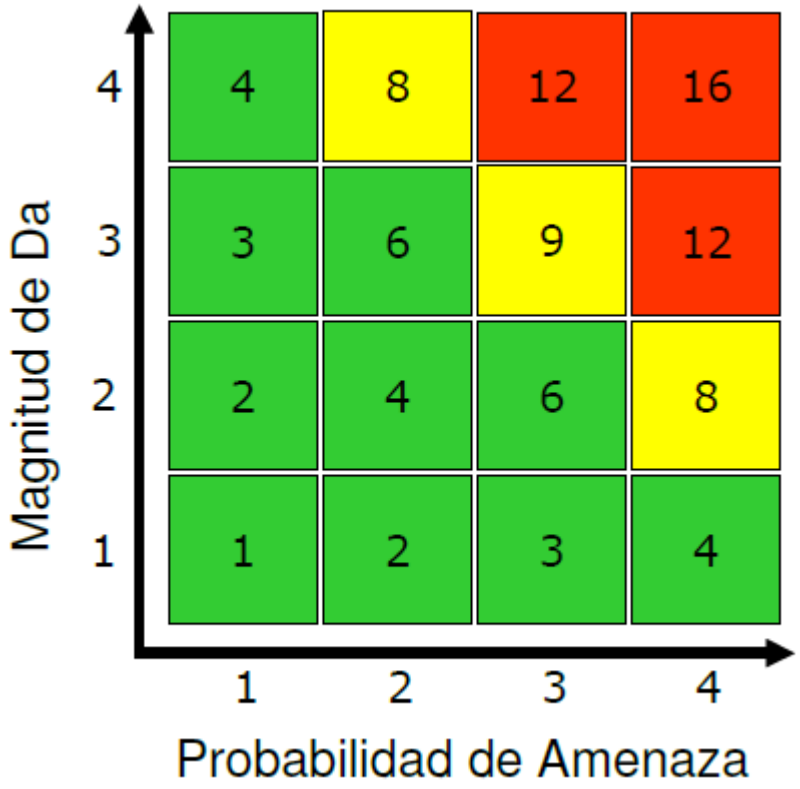
¿Qué puedo hacer? (Mitigar el riesgo)

¿Cuánto me costará? (Siempre calculado en forma anualizado)

¿Dicho costo es efectivo? (Relación costo beneficio)

Análisis de Riesgo

Riesgo = Probabilidad de Amenaza * Magnitud de Daño



Alto Riesgo (12-16)

Medio Riesgo (8-9)

Bajo Riesgo (1-6)

Valores:
1 = Insignificante
2 = Baja
3 = Mediana
4 = Alta

¿Cómo valorar la Probabilidad de Amenaza?

- Consideraciones
  - Interés o la atracción por parte de individuos externos
  - Nivel de vulnerabilidad
  - Frecuencia en que ocurren los incidentes
- Valoración de probabilidad de amenaza
  - Baja: Existen condiciones que hacen muy lejana la posibilidad del ataque
  - Mediana: Existen condiciones que hacen poco probable un ataque en corto plazo, pero no son suficientes para evitarlo en el largo plazo
  - Alta: Ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque

¿Cómo valorar la Magnitud de Daño?

- Consideración sobre las consecuencias de un impacto
  - ¿Quién sufrirá el daño?
  - Incumplimiento de confidencialidad (interna y externa)
  - Costo de recuperación

- Valoración de magnitud de daño
  - Bajo: Daño aislado, no perjudica ningún componentes de organización
  - Mediano: Provoca la desarticulación de un componente
  - Alto: En corto plazo desmoviliza o desarticula a la organización

¿Cuándo hablamos de un Impacto?

- Se pierde la información/conocimiento
- Terceros tienen acceso a la información/conocimiento
- Información ha sido manipulada o está incompleta
- Información/conocimiento o persona no está disponible
- Cambio de legitimidad de la fuente de información

Reducción de Riesgo

- Medidas físicas y técnicas
  - Construcciones de edificio, Control de acceso, Planta eléctrica, Antivirus, Datos cifrados,
- Medidas personales
  - Contratación, Capacitación
- Medidas organizativas
  - Normas y reglas, Seguimiento de control

Actividad 3: Seguridad

"Identificación de vulnerabilidades y sus amenazas sobre la Seguridad Física y Seguridad Lógica"

1.- Indicar 10 vulnerabilidades sobre **Seguridad Física** y sus consecuentes amenazas. (para cada vulnerabilidad puede existir una o más amenazas).

2.- Indicar 7 vulnerabilidades sobre **Seguridad Lógicas** y sus consecuentes amenazas. (para cada vulnerabilidad puede existir una o más amenazas).

Ejemplo:

IDENTIFICACIÓN DE VULNERABILIDADES Y AMENAZAS ANALISIS DE RIESGOS		
ITEM	**VULNERABILIDADES**	**AMENAZAS**
1	El cuarto de telecomunicaciones no está protegido del acceso de personas no autorizadas.	Robo de información
		Daños a los equipos
		Intrusión de software malicioso
		Manipulación de la información