



Universidad de Buenos Aires  
Facultad de Ciencias Económicas



# Riesgos, Probabilidad e Impacto

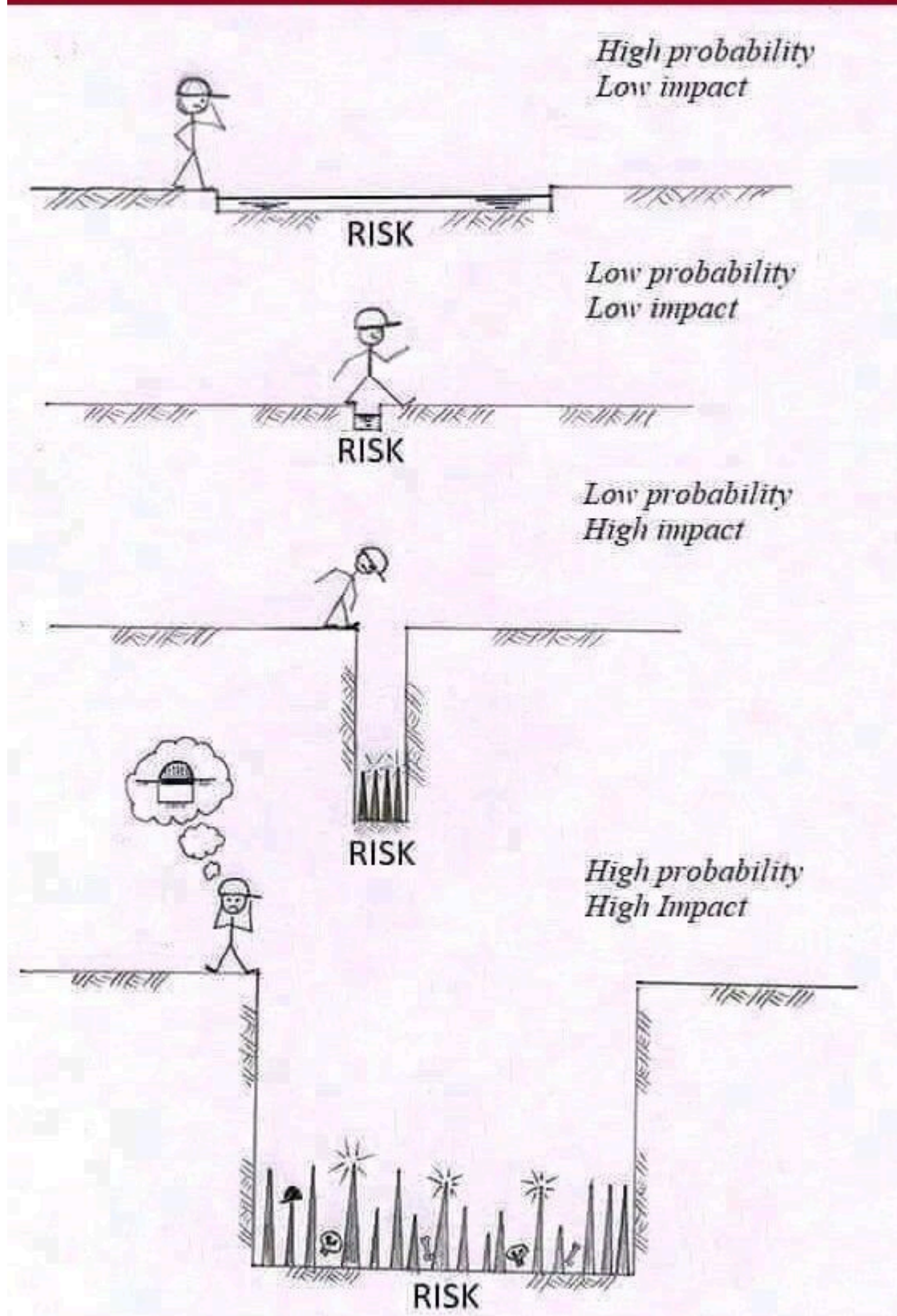


Material de Estudio

---

# Explain Risk, Probability and Impact

<http://pm-templates.info>





## Traducción y Comentarios

---

La imagen representa de manera gráfica cómo el **riesgo** depende de dos variables fundamentales:

- **Probabilidad (Probability)**: qué tan probable es que ocurra un evento.
- **Impacto (Impact)**: qué tan grave es la consecuencia si ocurre.

En términos de gestión de Tecnologías de la Información (TI), el riesgo puede expresarse conceptualmente como:

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

---

## Escenarios

### 1 Alta Probabilidad – Bajo Impacto

#### High probability – Low impact

Representa eventos que ocurren con frecuencia, pero cuyo efecto es limitado.

Ejemplo en TI:

- Pequeñas caídas momentáneas del sistema.
- Errores menores de usuario.
- Alertas falsas de seguridad.

En la matriz de riesgos, suelen clasificarse como **riesgos bajos o moderados**, dependiendo del contexto.

Gestión recomendada:

- Controles preventivos simples.

- Automatización de corrección.
- 

## **2** Baja Probabilidad – Bajo Impacto

### **Low probability – Low impact**

Eventos poco frecuentes y de impacto reducido.

Ejemplo:

- Fallo ocasional de una impresora.
- Error menor en reporte interno sin consecuencias estratégicas.

En la matriz de riesgos:

- Se ubican en la zona verde (riesgo bajo).
  - Pueden aceptarse con monitoreo básico.
- 

## **3** Baja Probabilidad – Alto Impacto

### **Low probability – High impact**

Eventos poco frecuentes pero potencialmente devastadores.

Ejemplo en TI:

- Incendio en el data center.
- Ataque sofisticado que comprometa información estratégica.
- Caída total del ERP en cierre contable.

En la matriz:

- Se ubican en zona naranja o roja.
- Requieren planes de contingencia (BCP – Business Continuity Plan / Plan de Continuidad del Negocio).
- DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres).

Este tipo de riesgo es crítico para la alta dirección.

---

## **4** Alta Probabilidad – Alto Impacto

### **High probability – High impact**

Es el escenario más peligroso.

Ejemplo:

- Vulnerabilidad conocida sin parchear.
- Phishing recurrente sin capacitación.
- Falta de backups en entorno con alto volumen de transacciones.

En la matriz:

- Zona roja (riesgo muy alto).
- Requiere acción inmediata.

Desde la administración:

- No puede aceptarse.
- Debe mitigarse o eliminarse.

---

## Comparación con una Matriz de Riesgos

La representación gráfica del "pozo" en la imagen es una metáfora visual del nivel de riesgo. Cuanto más profundo y peligroso el pozo, mayor el riesgo.

En gestión formal, esto se traduce en una:

### Matriz de Riesgos




La matriz cruza:

- Eje vertical: **Impacto**
- Eje horizontal: **Probabilidad**

	Probabilidad Baja	Probabilidad Media	Probabilidad Alta
Impacto Alto	Alto	Muy Alto	Crítico
Impacto Medio	Medio	Alto	Muy Alto
Impacto Bajo	Bajo	Medio	Alto

Colores típicos:

-  Verde: Riesgo bajo

-  Amarillo: Riesgo moderado
  -  Naranja: Riesgo alto
  -  Rojo: Riesgo crítico
- 

## Enfoque para Estudiantes de Administración en TI

En Sistemas de Información, la evaluación de riesgo permite:

- Priorizar inversiones en seguridad.
- Justificar presupuesto ante dirección.
- Definir controles preventivos.
- Diseñar arquitectura resiliente.
- Evaluar continuidad operativa.

Ejemplo práctico:

Un servidor sin actualización:

- Probabilidad: Alta.
- Impacto: Alto.  
→ Riesgo crítico → Acción inmediata.

Un error menor en formulario interno:

- Probabilidad: Alta.
  - Impacto: Bajo.  
→ Riesgo moderado → Mejora progresiva.
- 

## Elementos de TI que deben considerar

1. Infraestructura (servidores, redes).
2. Aplicaciones críticas (ERP, CRM).

3. Bases de datos.
4. Comunicaciones.
5. Seguridad de acceso.
6. Proveedores cloud.
7. Factor humano.

La evaluación sistemática del riesgo es base de:

- ISO 27001.
  - COBIT (Control Objectives for Information and Related Technologies / Objetivos de Control para Tecnologías de la Información y Relacionadas).
  - Gestión de continuidad.
- 

## Conceptos Clave Explicados

- **Probabilidad (Probability):** frecuencia estimada de ocurrencia.
  - **Impacto (Impact):** magnitud del daño.
  - **Riesgo (Risk):** combinación de ambas variables.
  - **Mitigación (Mitigation):** reducción del riesgo.
  - **Aceptación (Risk Acceptance):** decisión de tolerar el riesgo.
  - **Transferencia (Risk Transfer):** traslado mediante seguros o contratos.
- 

## Conclusión Conceptual

La imagen utiliza un recurso visual sencillo para explicar que el riesgo no depende únicamente de la probabilidad ni solo del impacto, sino de la combinación de ambos. En el contexto de Tecnologías de la Información, esta relación es fundamental para la toma de decisiones estratégicas.

La matriz de riesgos formaliza esta idea y permite a la administración priorizar recursos, justificar controles y diseñar arquitecturas seguras y resilientes. La

gestión profesional del riesgo transforma la incertidumbre en decisiones informadas.

---

## Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

---

## Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos)**, los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.

**La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.**

**Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.**

---

## Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.

**Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.**

**Queda expresamente excluido cualquier uso con fines comerciales.**

