UNIVERSIDAD DE COSTA RICA

Administración de Riesgos

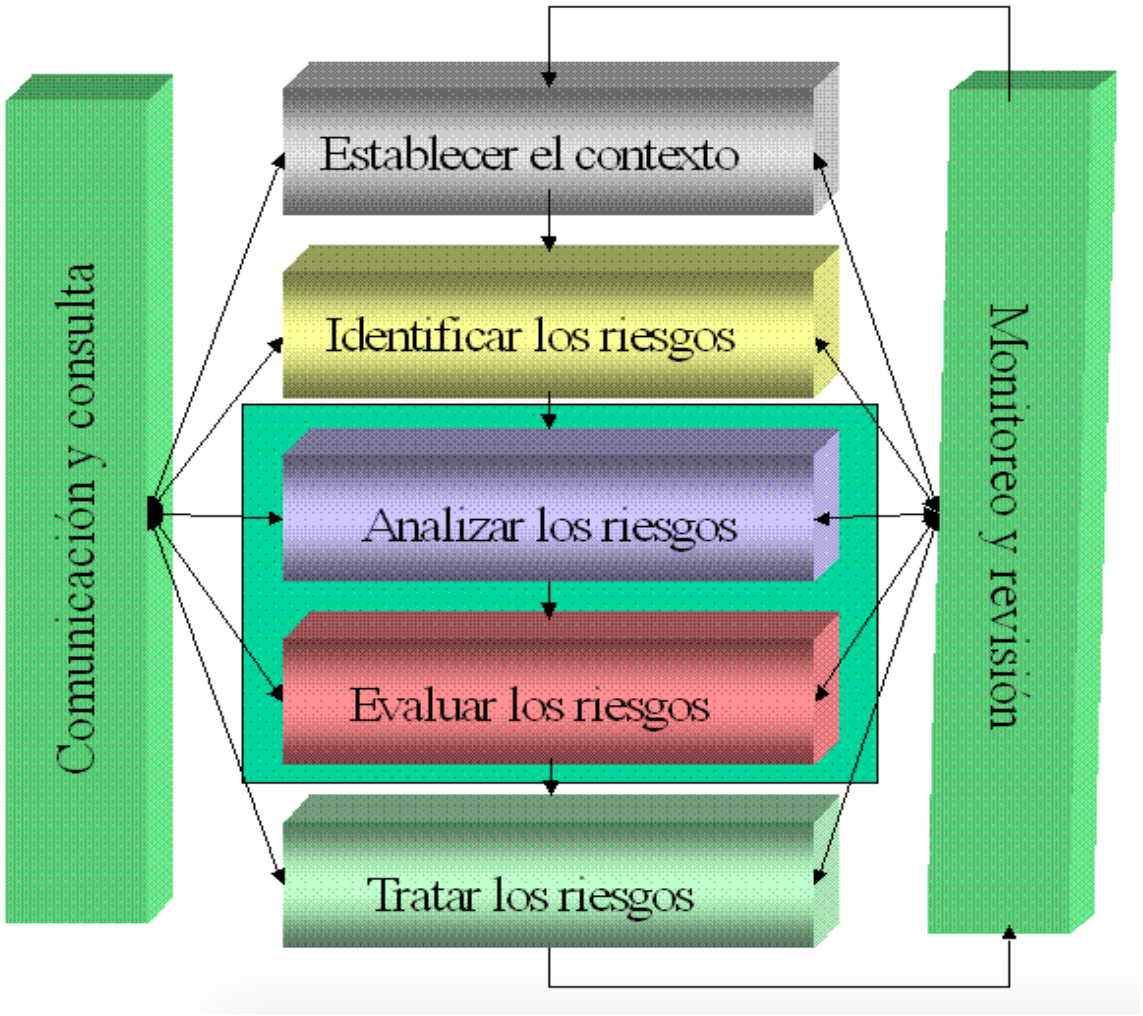
Prof. Carlos Vega Alvarado

Evaluación de Riesgos

Agenda

- Proceso de gestión de riesgos
- Criterios para la evaluación de riesgos
- Controles organizacionales

Proceso de gestión de riesgos



#1: Establecimiento del contexto

- **Propósito:** definir los parámetros básicos dentro de los que se gestionarán los riesgos para proveer una guía para la toma de decisiones.
- **Actividades:**
  - *Establecimiento del contexto estratégico*, definiendo la relación entre la organización y el entorno;
  - *Establecimiento del contexto organizacional*, comprendiendo la organización y sus capacidades;

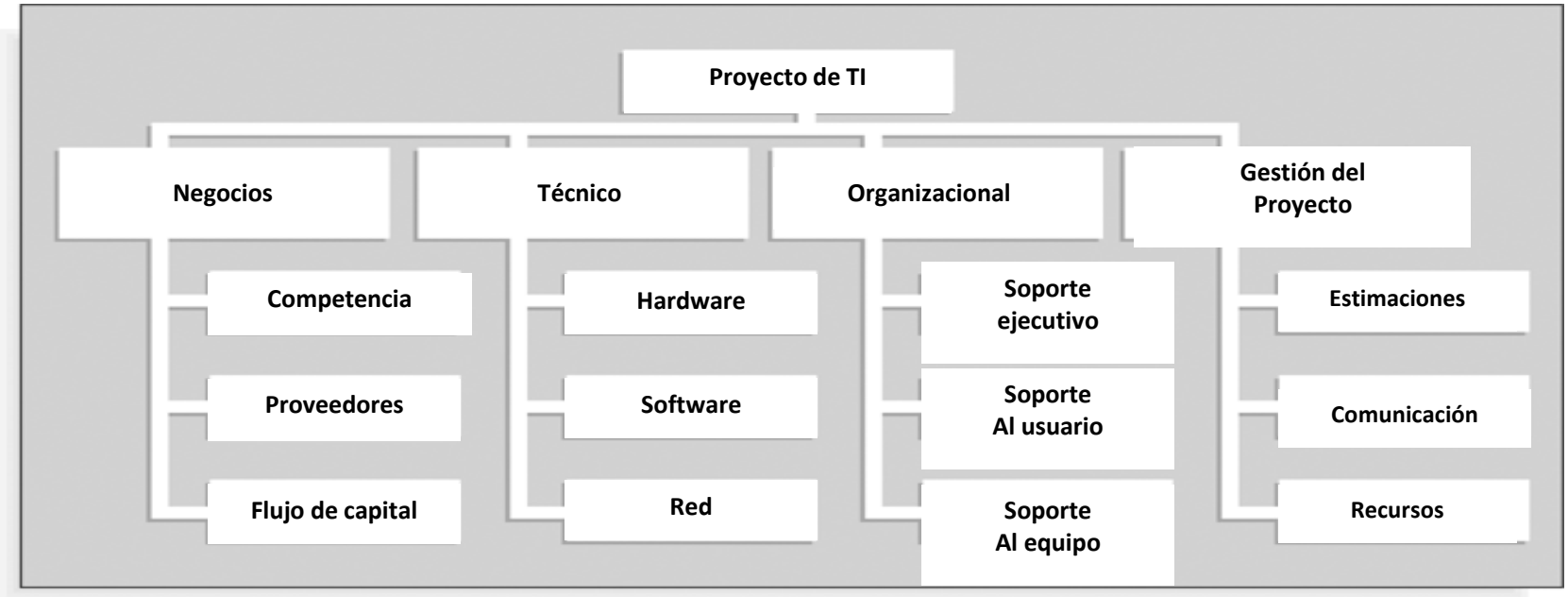
#1: Establecimiento del contexto (cont.)

- **Actividades:**
  - *Establecimiento del contexto de la gestión de riesgos,* analizando metas, alcance, parámetros, recursos, etc.;
  - *Desarrollo de criterios de evaluación,* definiendo decisiones relacionadas con la aceptación y tratamiento de riesgos a partir de criterios financieros, operativos, técnicos, etc.; y

CRITERIO DE MEDICIÓN DEL RIESGO:	Reputación y confianza del cliente		
	Bajo	Moderado	Alto
Afectación a la imagen de la organización.	La información relacionada con el incidente de seguridad solo se conoce dentro del área de TI.	La información relacionada con el incidente de seguridad se conoce dentro de la organización.	La información relacionada con el incidente de seguridad se conoce públicamente.

#1: Establecimiento del contexto (cont.)

- **Actividades:**
  - *Definición de la estructura de riesgos,* identificando los elementos que permiten analizar los riesgos significativos.



#2: Identificación de riesgos

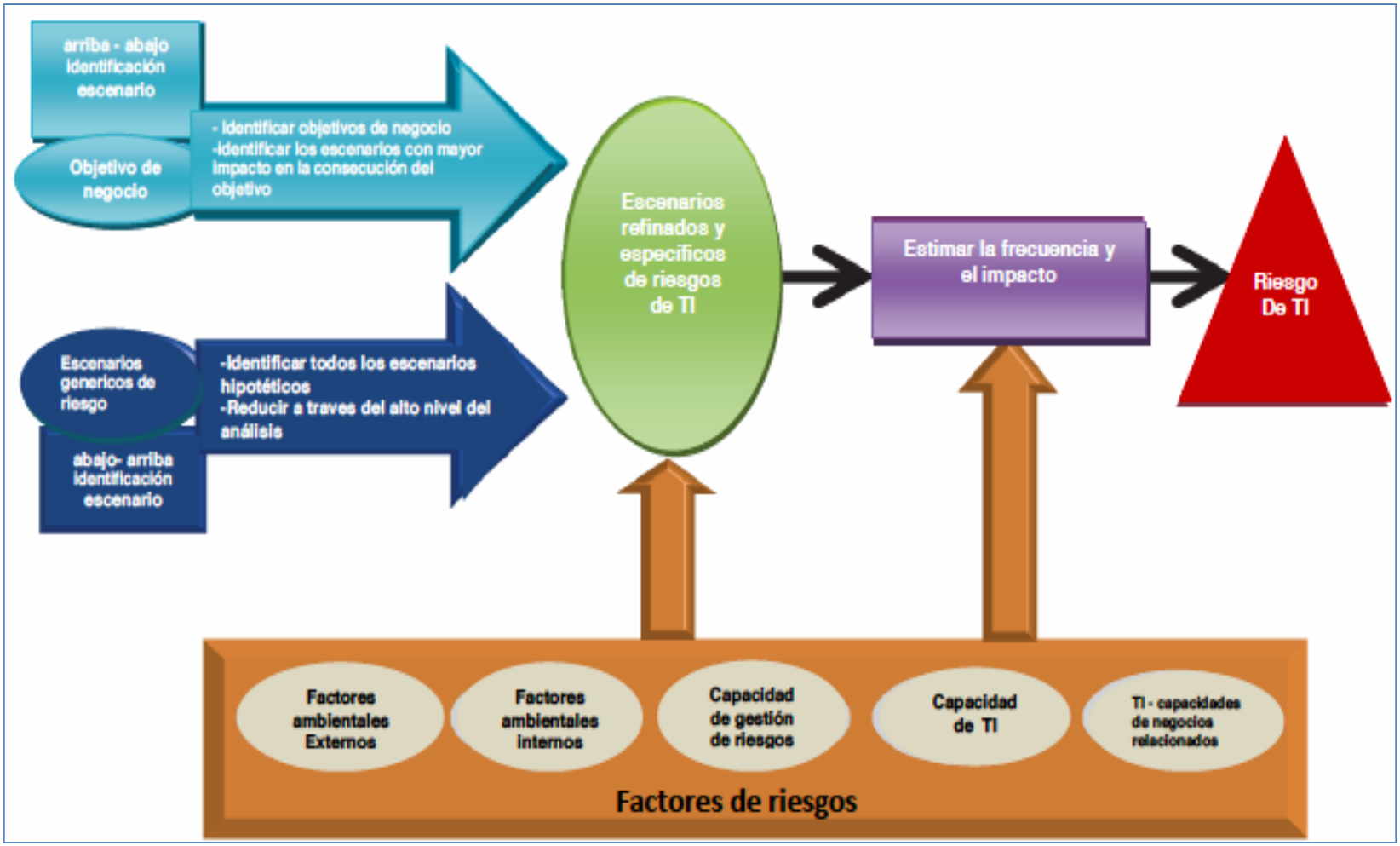
- **Propósito:** identificar ampliamente los riesgos por medio de un proceso bien estructurado.
- **Actividades:**
  - *Generación de listado de eventos potenciales,* indicando cómo afecta a cada elemento de la estructura;

PROCESO:				
Objetivo:				
Código	Descripción	Causas (factores internos y externos)	Agente Generador	Consecuencias

#2: Identificación de riesgos (cont.)

- **Actividades:**
  - *Identificación de causas y escenarios posibles,* mediante la identificación de los componentes del escenario:

#2: Identificación de riesgos (cont.)



#2: Identificación de riesgos (cont.)

- Tópicos de interés para identificar riesgos:
  - Deben impactar los objetivos;
  - No deben ser causales o factores;
  - Son las amenazas posibles, aunque no hayan ocurrido;
  - Se trata de identificar, no de valorar;
  - Deben ser de alto nivel y holísticos;
  - Consideran el ambiente interno así como el entorno; y
  - Deben revisarse las interrelaciones entre elementos.

#3: Análisis de riesgos

- **Propósito:** separar los riesgos menores aceptables de los riesgos mayores y proveer datos para asistir la evaluación y tratamiento de dichos riesgos.
- **Actividades:**
  - *Determinación de los controles existentes*, verificando la existencia y completitud de dichos controles;

#3: Análisis de riesgos (cont.)

- **Actividades:**
  - *Establecimiento de consecuencias y probabilidades, considerando los controles existentes;*

Probabilidad	Amenazas					Oportunidades				
0.90	0.05	0.09	0.18	0.36	0.72	0.72	0.36	0.18	0.09	0.05
0.70	0.04	0.07	0.14	0.28	0.56	0.56	0.28	0.14	0.07	0.04
0.50	0.03	0.05	0.10	0.20	0.40	0.40	0.20	0.10	0.05	0.03
0.30	0.02	0.03	0.06	0.12	0.24	0.24	0.12	0.06	0.03	0.02
0.10	0.01	0.01	0.02	0.04	0.08	0.08	0.04	0.02	0.01	0.01
	0.05	0.10	0.20	0.40	0.80	0.80	0.40	0.20	0.10	0.05

Riesgo Bajo **Riesgo Medio** **Riesgo Alto**

#3: Análisis de riesgos (cont.)

- **Actividades:**
  - *Estimación del nivel del riesgo:*

	Impacto / Consecuencia				
Probabilidad	1 Muy Bajo	2 Bajo	3 Moderado	4 Alto	5 Muy alto
1 – Improbable					
2 – Poco probable					
3 – Probable					
4 – Bastante Probable					
5 – Sumamente Probable					

#4: Evaluación de riesgos

- **Propósito:** efectuar una priorización de los riesgos.
- **Actividades:**

  - *Comparación del nivel de riesgo con los criterios previamente establecidos; y*
  - *Priorización del riesgo.*

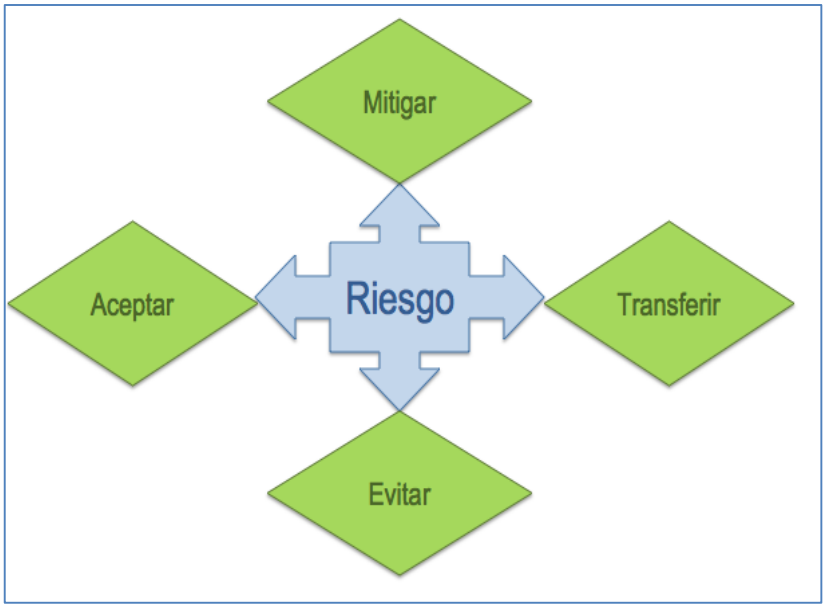
Nivel de Riesgo	Acciones
Crítico	Debe controlarse inmediatamente. Mientras se encuentra la solución definitiva, se adoptan acciones temporales para disminuir el nivel de riesgo.
Alto	Deben adoptarse medidas urgentes para controlar el riesgo.
Moderado	Requiere controles a mediano o largo plazo. Se consideran opciones que no supongan una carga económica importante
Aceptable	Validar que los controles mantienen su eficacia. No requiere ninguna acción al corto plazo.

#4: Evaluación de riesgos (cont.)

- Los tres estados de medición del riesgo son:

#5: Tratamiento/Respuesta a riesgos

- **Propósito:** analizar las diferentes opciones para tratar los riesgos e implementar la mejor opción posible.
- **Actividades:**
  - *Identificación de opciones;*
  - *Evaluación de las opciones;*
  - *Preparación del plan; e*
  - *Implementación del plan.*



#5: Tratamiento/Respuesta a riesgos (cont.)

- Los tipos de respuesta a los riesgos son:
  - *Evitar:* si se sabe de un evento que definitivamente va a ocurrir, deben tomarse todas las acciones para que no suceda.
  - *Transferir:* si se sabe de un evento que puede ocurrir, se le puede transferir la responsabilidad a otras entidades (personas o empresas).

#5: Tratamiento/Respuesta a riesgos (cont.)

- Los tipos de respuesta a los riesgos son:
  - *Mitigar:* si se sabe de un evento que **puede ocurrir pero no se puede transferir o evitar**, se toman acciones para minimizar su impacto.
  - *Aceptar:* si se sabe de un evento que **si ocurre no se puede tomar ninguna medida para evitarlo o mitigarlo**, no queda más que aceptarlo, por lo que debe tenerse una contingencia.

#6: Monitoreo y control

- **Propósito:** garantizar que el riesgo se mantiene debidamente controlado.
- **Actividades:**
  - *Monitoreo de los riesgos*, analizando si las condiciones han cambiado y si se mantiene o no en el mismo nivel;
  - *Monitoreo de las medidas de control*, verificando que siguen siendo efectivas; y
  - *Repetición del ciclo de gestión de riesgos*, detectando los cambios en los riesgos conocidos y los nuevos riesgos.

#6: Monitoreo y control (cont.)

- Consideraciones en cuanto al monitoreo y control:
  - Asegurar que los controles son eficaces y eficientes, tanto en diseño como en funcionamiento;
  - Buscar más información relacionada, de manera que se pueda ir mejorando el análisis y seguimiento;
  - Analizar y aprender de los acontecimientos;
  - Detectar cambios en el contexto tanto externo como interno;
  - Identificar riesgos emergentes.

#6: Monitoreo y control (cont.)

- El propósito de los **controles organizacionales** es disponer de controles adecuados para proteger los recursos que se vean comprometidos por un riesgo, de manera que se reduzca al máximo su grado de exposición al riesgo y que este último no se materialice.

#6: Monitoreo y control (cont.)

- Los principales tipos de controles son:
  - *De diseño:* preventivos, detectivos, correctivos;
  - *De implementación:* manuales o automatizados; y
  - *De ejecución:* discretos o continuos.

#7: Comunicación y consulta

- **Propósito:** garantizar que todos los involucrados conozcan los riesgos y los métodos para controlarlos.
- **Actividades:**
  - *Desarrollo del plan de comunicación de riesgos*;
  - *Documentación* de las percepciones de los involucrados en cuanto a riesgos y beneficios.

#7: Comunicación y consulta (cont.)

- Componentes de la comunicación de riesgos de TI:

Referencias Bibliográficas

- ISACA. **Marco de Riesgos de TI**. ISACA, 2009.
  - *Capítulo #5:* Fundamentos de Gobierno del Riesgo

- **Norma ISO 31000:2009 – Gestión de Riesgos**.

- ISACA. **The Risk-IT Practitioners Guide**. ISACA, 2009.