
**Facultad de Ciencias e Ingeniería**
**Ingeniería Informática**

**TEMAS AVANZADOS EN TECNOLOGÍAS DE INFORMACIÓN 1**
**Gestión de riesgos de Tecnologías de Información**

Cap. 2 – Principios y Marco Normativo

*Profesor: Ing. Dr. Manuel Tupia A.*
*2020-1*

1

# Contenido de la presentación

- **Principios normativos**
- Marco
- Proceso
- Referencias

2

2

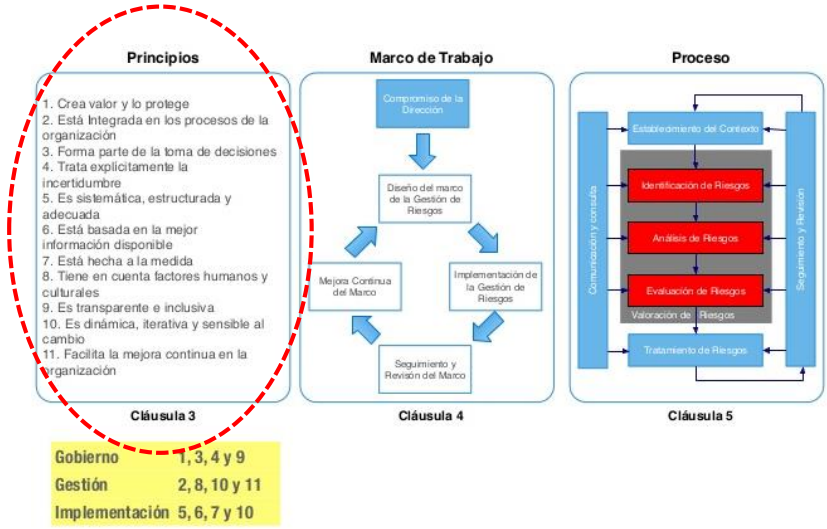
# Gestión de riesgos

- Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo [ISO, 2009].
  - Enfoque integral, sistémico y repetible.
  - Identificar necesidades de la organización en relación a los riesgos, sobre la base de los propios requisitos que ésta tenga.

3

3

# Gestión de riesgos




| | |
|---|---|
| Gobierno | 1, 3, 4 y 9 |
| Gestión | 2, 8, 10 y 11 |
| Implementación | 5, 6, 7 y 10 |

4

4

Parte 1

# PRINCIPIOS NORMATIVOS



5

## Principio 1

- **La gestión de riesgos crea y protege el valor para el negocio**
  - Contribución de manera tangible
  - Se puede saber qué puede “atacar” al negocio
  - Controles



6

# Principio 2

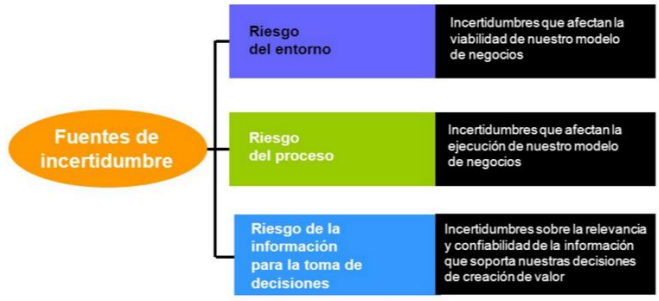
- **Es una parte integral de los procesos de cualquier organización**
  - Debería serlo
  - No importa el tipo de organización


7

7

# Principio 3

- **Es parte de la toma de decisiones**
  - O debería serlo
  - Elecciones informadas, priorizaciones.




8

8

# Principio 4

- **La gestión de riesgos trata explícitamente a la incertidumbre que aqueja al negocio**
  - La naturaleza de la incertidumbre
  - Cómo tratarla


9

9

# Principio 5

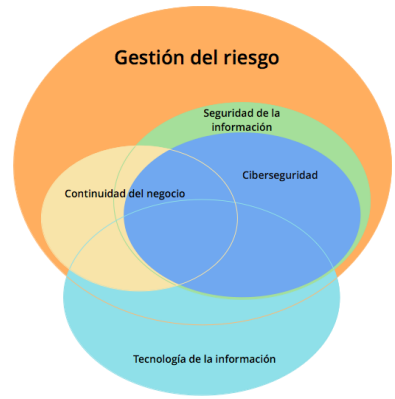
- **La gestión de riesgos es sistemática y estructurada.**
  - No es una actividad ad hoc
  - No es un esfuerzo “de un día, de una persona”
  - Integración
  - Resultados coherentes


10

10

# Principio 6

- **La gestión de riesgos se basa en la mejor información disponible**
  - Aquí se destaca la importancia de la conservación y protección de la información (seguridad de la información) por encima de la seguridad de cualquier otro activo en la empresa




11

11

# Principio 7

- **La gestión de riesgos es adaptable**
  - Hacer frente a entornos cambiantes
  - Entornos externos e internos
  - Perfil de riesgo actualizado


12

12

# Principio 8

- **Se integran factores humanos y culturales**
  - Cultura y ética organizacional
  - El individuo como fuente de riesgos
  - El proceso de negocio como fuente de riesgos
  - La tecnología como fuente de riesgos

13

13

# Principio 9

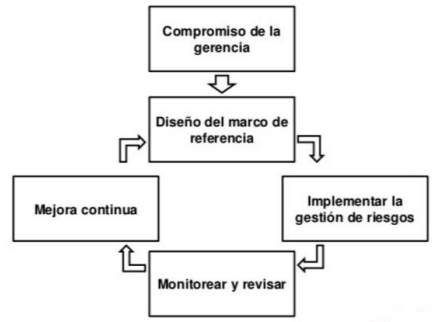
- **La gestión de riesgos es transparente y sirve para proporcionar transparencia**
  - Porque obliga a la participación activa de todas las partes interesadas.
  - Perfil de riesgo permanente y actualizado


14

14

# Principio 10

- **La gestión de riesgos es dinámica, iterativa y responde a los cambios**
  - Entorno cambiante
  - Continua




15

15

# Principio 11

- **Facilita la mejora continua de la organización**
  - Madurez de las empresas al integrar la gestión de riesgos.

16

16

# Bibliografía


- [ISACA, 2009] ISACA International. The Risk IT Framework. ISACA Publishing, USA (2009)
- [ISACA, 2016] ISACA Internacional. Manual de preparación para el examen de certificación CRISC (Certified in Risk and Information System Control) ISACA Publishing, USA (2016)
- [ISO, 2018] The International Organization for Standardization. ISO 31000:2018 Risk Management- Principles and Guidelines. ISO, Suiza (2018).


17

17