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

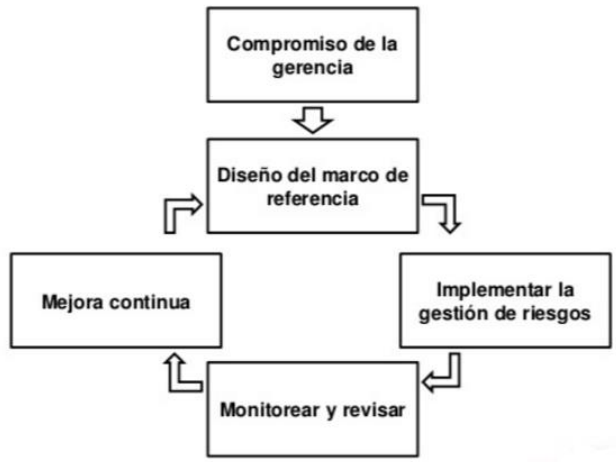
2

Parte 2

MARCO NORMATIVO

3

Marco de trabajo propuesto por la ISO 31000



4

Marco de trabajo propuesto por la ISO 31000

- **Compromiso de la Alta Dirección**
  - Avalar la política de gestión de riesgos, articulándola con la estrategia de la organización.
  - Identificar los indicadores de desempeño, y verificar que estos estén alineados con la estrategia de la organización.
  - Garantizar que los objetivos de la organización, y los objetivos de la gestión de riesgos estén alineados.
  - Asegurar las conformidades regulatorias y legales.
  - La asignación de responsabilidades en los diferentes niveles de la organización.
  - La asignación de recursos necesarios para el correcto funcionamiento del sistema.
  - La comunicación de los beneficios que aporta la gestión de riesgos, de tal forma que sean conocidos por todas las partes interesadas.
  - Asegurar el mantenimiento del marco de trabajo de ISO 31000

5

5

Marco de trabajo propuesto por la ISO 31000

- **Diseño del marco de trabajo**
  - Basado en el ciclo de Deming PDCA
  - La planificación (P): Es preciso tener un conocimiento profundo de la organización, tanto en el contexto externo como interno, la política de gestión de riesgos, la rendición de cuentas, los recursos para el funcionamiento del sistema, la integración y alineación con los procesos de la organización y las comunicaciones tanto internas como externas.
  - La implementación (D): supone tener claros dos aspectos: la implementación del marco de referencia para la gestión del riesgo, y la implementación de los procesos de gestión de riesgos.

6

6

Marco de trabajo propuesto por la ISO 31000

- **Diseño del marco de trabajo**
  - Monitorear
  - El monitoreo y la revisión de la eficacia del marco de referencia (C): teniendo en cuenta los periodos de evaluación, la elaboración de los informes, y el desempeño general del sistema

7

7

Marco de trabajo propuesto por la ISO 31000

- **Diseño del marco de trabajo**
  - Mejora
  - La mejora continua (A): como elemento esencial en todas las normas ISO, lo que contribuye a contar con elementos de juicio eficaces para la toma de decisiones acertadas.

8

8

Parte 3

PROCESO DE LA GESTION DE RIESGO

Proceso de la gestión de riesgos

1. Estableciendo el contexto

- El alcance está constituido por los parámetros globales de rendimiento que se espera cumplir, considerando los factores internos y externos en los que está inmersa la organización.
  - Qué sí y qué no se va a considerar

11

11

1. Estableciendo el contexto

- **Clasificación de activos**
  - Localizar e identificar los activos (inventariado).
  - Identificar los procesos de negocio a los que brindan soporte.
  - Establecer niveles de sensibilidad y criticidad.
  - Asignar clasificaciones a los activos de acuerdo a los niveles.
  - Identificar las medidas de seguridad adoptadas para cada uno de los activos identificados, caso existan

12

12

1. Estableciendo el contexto

- **Inventario y valoración de activos**
  - Para poder determinar los riesgos y amenazas a los que están expuestos los activos de la información de la empresa, es imperativo saber qué tan valiosos son precisamente para la empresa.

13

13

1. Estableciendo el contexto

Factores cuantitativos

- Costo del activo
- Costo de reposición del equipo, de la instalación o de los recursos humanos
- Costos por pérdida de productividad y de negocio
- Costo por el proceso de recuperación de la operatividad: tareas, tiempo y recursos involucrados
- Costo por incumplimiento legal, regulatorio o contractual

Factores cualitativos

- Capacidad de seguir produciendo o brindando un servicio
- Pérdida de competitividad
- Pérdida de confianza y credibilidad de parte de clientes, socios y demás *stakeholders*

14

14

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).

15

15