UNIVERSIDAD TECNOLOGICA NACIONAL

Ingeniería en Sistemas de Información

Ciberseguridad

Docente: Ing. Gabriela Nicolao

Ayudantes: Ing. Luciano Sebastianelli, Matías Baghdassarian

UNIVERSIDAD TECNOLOGICA NACIONAL

Gestión de la Seguridad de la Información

UNIVERSIDAD TECNOLOGICA NACIONAL

Introducción a los Sistemas de Gestión de la Seguridad de la información

Objetivos

- Gestionar en forma efectiva la Seguridad de la Información dentro de una organización, enfocarse en las tareas y el conocimiento con los que debe contar el gerente de seguridad de la información.

Normas para la Gestión de la Seguridad de la Información

- Serie ISO 27000 (ex IRAM/ISO/IEC 17799, basada en BS 7799)
  - Establece una base común de buenas prácticas para desarrollar normas de seguridad.
  - Para certificar se usa la ISO 27001 que es menos detallada y define requisitos de auditoría (se basa en controles).
- Otros SGSI:
  - **ISO 22301** (Continuidad de negocio), **COBIT 2019** (Control Objectives for Information and related Technology), **MITRE**, **NIST 800-53, ITIL** (Information Technology Infrastructure Library), **COSO** (Committee of Sponsoring Organizations), **PCI**, etc.

Serie ISO 27000

- ISO/IEC 27001 es un estándar generado para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.
- Es consistente con las mejores prácticas descritas en IRAM/ISO/IEC 17799.
  - 27.001: Requisitos de los SGSI ← Certificable
  - 27.002: Objetivos de control y controles recomendables
  - 27.003: Guía de implementación del SGSI
  - 27.005: Gestión de riesgos

Estructura de la ISO 27001

UNIVERSIDAD TECNOLOGICA NACIONAL

- Objeto y campo de aplicación
- Referencias normativas
- Términos y definiciones
- Contexto de la organización
- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación de desempeño
- Mejora

Objeto y campo de la aplicación

UNIVERSIDAD TECNOLOGICA NACIONAL

Enfoque del proceso

UNIVERSIDAD TECNOLOGICA NACIONAL

- La adopción del SGSI debe ser una decisión estratégica dentro de la organización
- Debe tener apoyo de la alta gerencia.
- Enfatizar la importancia en:
  - Entender los requerimientos de Seguridad de la Información.
  - Establecer políticas y objetivos de Seguridad de la Información.
  - Implementar y operar controles.
  - Manejar los riesgos de la Seguridad de la Información.
  - Monitorear y revisas el desempeño.
  - Mejoramiento continuo en base a la medición del objetivo.

Alcance

- Abarca todos los tipos de organizaciones
  - Empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro, etc.

Referencias normativas

- ISO/IEC 17799:2005 Tecnología de la Información – Técnicas de Seguridad – Código de práctica para la Gestión de la Seguridad de la Información.

Establecer el SGSI

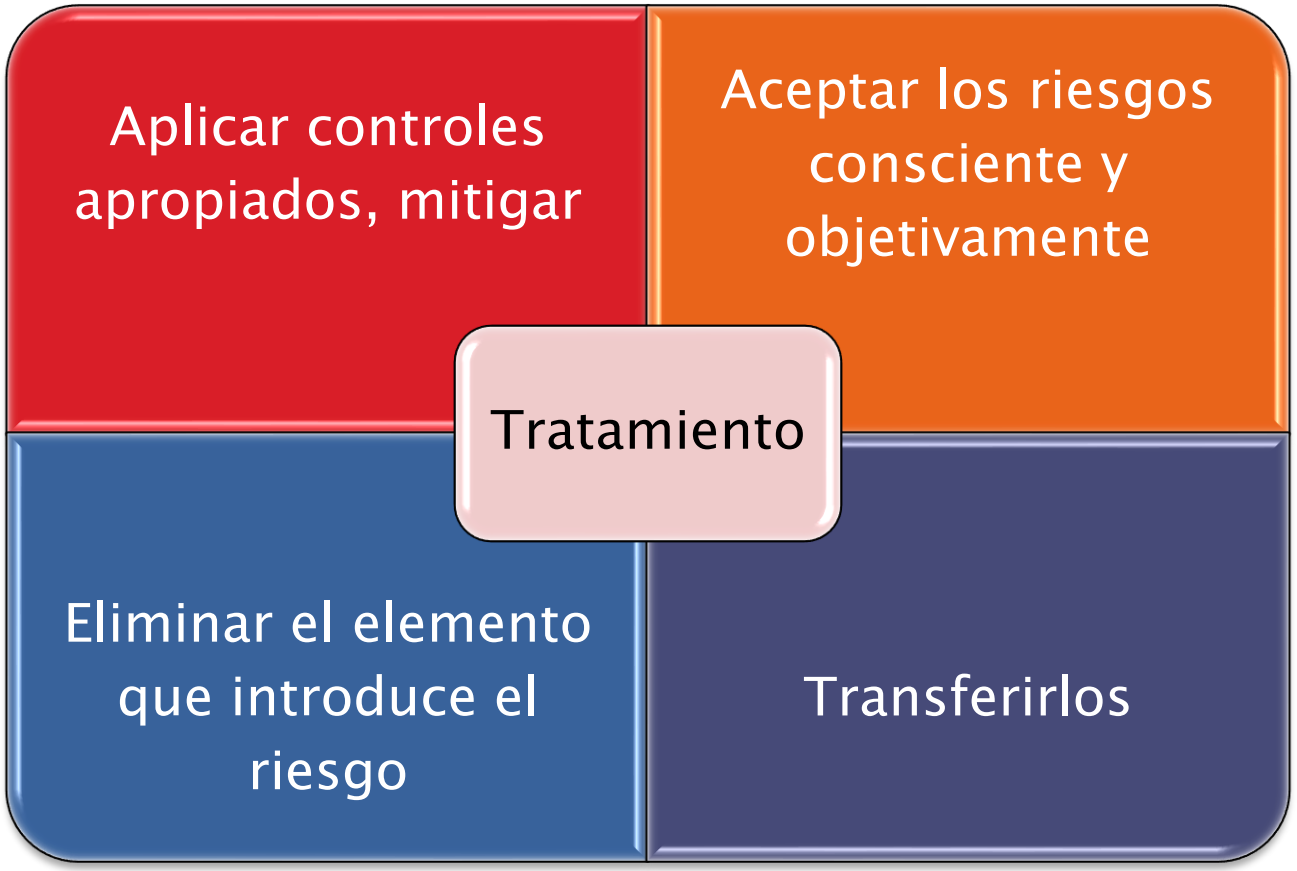
- Definir alcance/limites del SGSI en términos de las características del negocio.
- Definir la política:

Operación

- Identificar los riesgos:

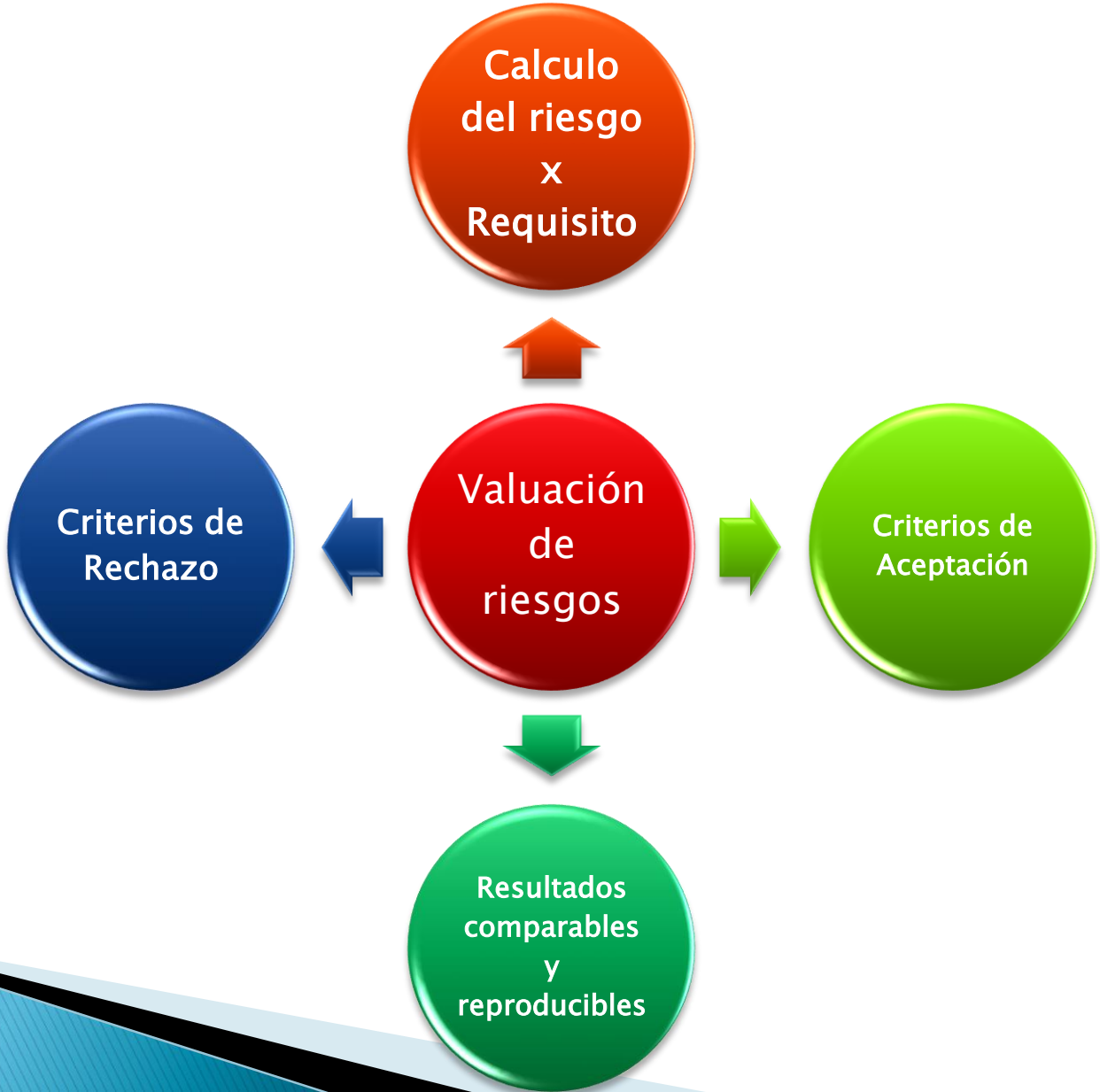
Operación

- Identificar y evaluar opciones de tratamiento:



Operación

- Definir la valuación de Riesgos:



Operación

- Seleccionar los objetivos de control y controles para el tratamiento de riesgos.
- Obtener la aprobación de la gerencia respecto de los riesgos residuales
- Obtener la autorización de la gerencia para implementar y operar el SGSI.
- Preparar enunciado de aplicabilidad respecto del tratamiento de los riesgos.

UNIVERSIDAD TECNOLOGICA NACIONAL

Implementar y operar SGSI

Monitorear y revisar el SGSI

Detectar errores en los resultados de procesamiento

Identificar

Incidentes

Revisar la segregación de funciones

Detectar eventos de Seguridad

Evitando los incidentes con el uso de indicadores

Determinar si son efectivas las acciones tomadas ante una violación de Seguridad

Monitorear y revisar el SGSI

- Realizar revisiones teniendo en cuenta la auditoría, incidentes y mediciones de seguridad.
- Realizar evaluaciones de riesgos a intervalos planeados tomando en cuenta los cambios.
- Realizar revisiones gerenciales periódicas del SGSI.
- Actualizar los planes de Seguridad.
- Registrar eventos y acciones que podrían tener impacto en el desempeño del SGI.

Mantener y mejorar el SGSI

UNIVERSIDAD TECNOLOGICA NACIONAL

Documentación del SGSI

- Política y objetivos del SGSI.
- Alcance del SGSI.
- Procedimientos y controles de soporte de SGSI.
- Descripción de la metodología de evaluación de riesgos.
- Informe de evaluación de riesgos.
- Plan de tratamiento del riesgo.
- Procedimientos documentados de planeación, operación y control.
- Enunciado de aplicabilidad.

Auditorías internas SGSI

- La organización debe realizar auditorías internas a intervalos planeados para determinar si los objetivos, controles, procesos y procedimientos:
  - Cumplen los requerimientos del estándar.
  - Cumplen con los requerimientos de Seguridad.
  - Se implementan y mantienen de manera efectiva.
  - Se realizan conforme a lo esperado.

Mejoramiento continuo

- La organización debe realizar acciones:
  - Correctiva: Para eliminar la causa de las no conformidades con los requerimientos de SGSI para evitar la recurrencia.
  - Preventiva: Para eliminar la causa de las potenciales no conformidades de los requerimientos SGSI para evitar la ocurrencia.

UNIVERSIDAD TECNOLOGICA NACIONAL

PREGUNTAS?