DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Unidad 3: Planeando la ciberseguridad

Gobierno de la seguridad de la información

Profesor
Juan Ignacio Iturbe A.

Objetivos de aprendizaje

- OA: Evaluar y planear la seguridad informática en las organizaciones.
  - Explicar el concepto de gobierno de la seguridad y como este difiere del concepto de gestión de la seguridad de la información.
  - Proveer una vista general de los elementos claves del gobierno de la seguridad de la información.
  - Discutir los tópicos que deben ser cubiertos en un plan estratégico de seguridad de la información.
  - Discutir los tópicos que deben ser cubiertos en un reporte de seguridad de la información a nivel de Gobernanza.

Gobierno de la Seguridad de la Información

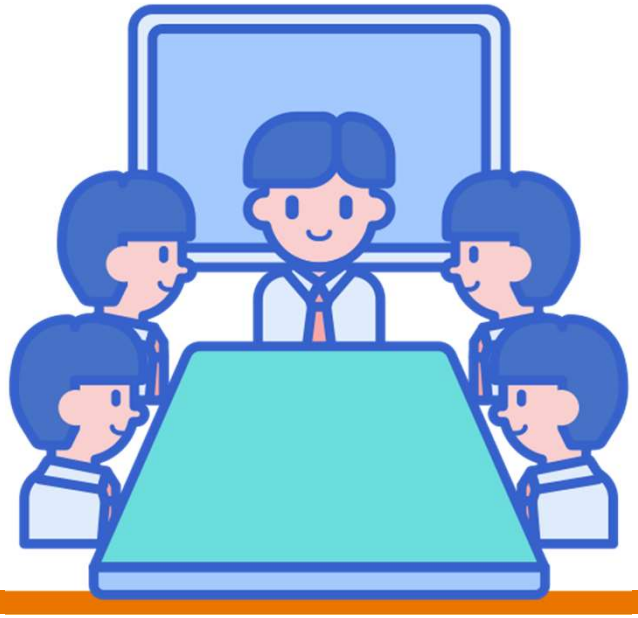
"El proceso de establecer y mantener un marco y una estructura y procesos de gestión de apoyo para garantizar que las estrategias de seguridad de la información se ajusten a los objetivos comerciales y los apoyen, sean coherentes con las leyes y reglamentos aplicables mediante la adhesión a las políticas y los controles internos, y proporcionen una asignación de responsabilidades, todo ello en un esfuerzo por gestionar el riesgo"

NIST SP 800-100

Gobierno de la Seguridad de la Información

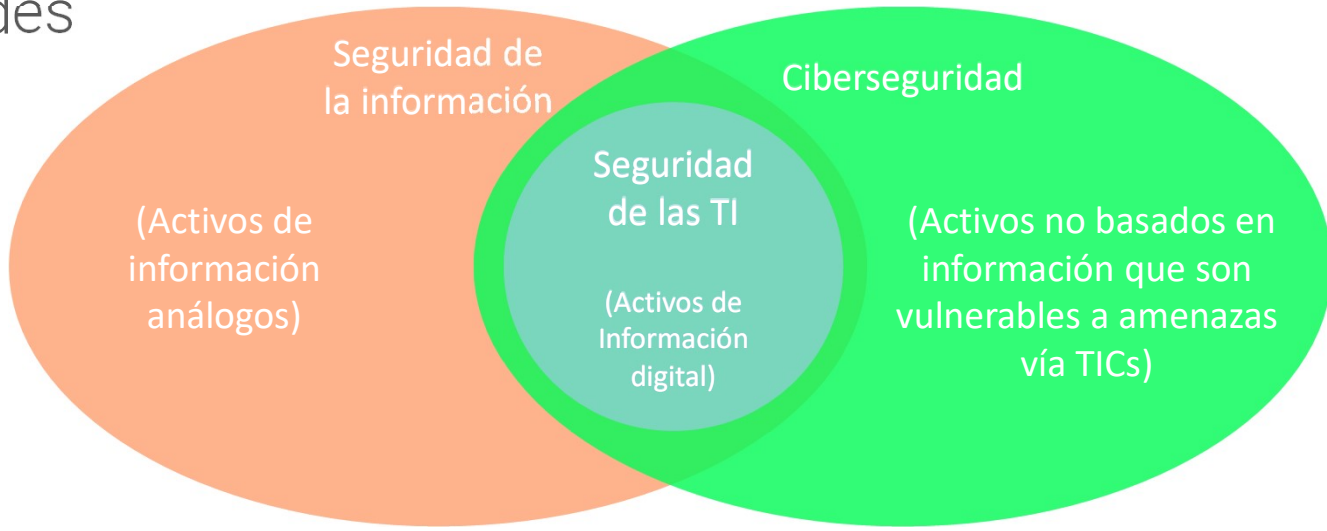
"El sistema por el que se dirigen y controlan las actividades de una organización relacionadas con la seguridad de la información"

ITU-T X.1054 e ISO 27014



Gobierno de la Seguridad de la Información

- El término Gobierno de la Seguridad abarca:
  - Ciberseguridad
  - Seguridad de la información
  - Seguridad de las redes



Gobernanza

- Establecimiento de políticas y vigilancia continua de su correcta aplicación por parte de los miembros del órgano rector de una organización.
- El gobierno incluye los mecanismos necesarios para equilibrar los poderes de los miembros (con la correspondiente rendición de cuentas).
- Su deber primordial de aumentar la prosperidad y la viabilidad de la organización.

Recordar

Política de seguridad

“Conjunto de normas y prácticas que especifican o regulan la forma en que un sistema u organización presta servicios de seguridad para proteger los recursos sensibles y críticos del sistema.”

Gobierno de la seguridad y gestión de la seguridad

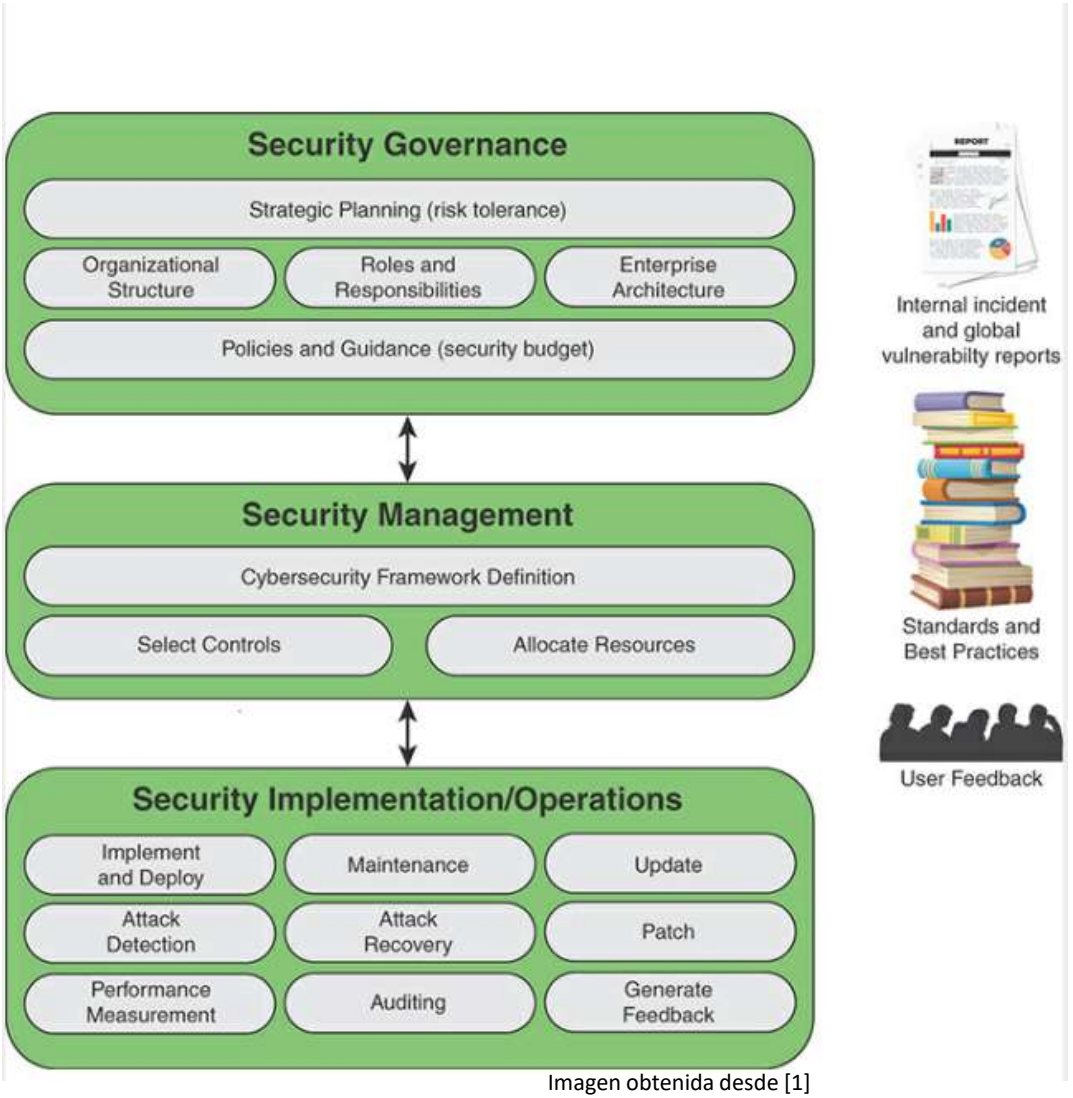


Imagen obtenida desde [1]

Principios

1. Establecer la seguridad de la información en toda la organización.
2. Adopte un enfoque basado en los riesgos.
3. Establecer la dirección de las decisiones de inversión.
4. Asegurar la conformidad con los requisitos internos y externos.
5. Fomentar un entorno positivo para la seguridad de todos los interesados.
6. Examinar el desempeño en relación con los resultados comerciales.

X.1054 e ISO 27014

Resultados deseados

El IT Governance Institute, define los siguientes 5 resultados básicos para la Gobernanza de la seguridad.

1. Alineación estratégica.
2. Gestión del riesgo.
3. Gestión de los recursos.
4. Entrega de valor.
5. Medición del rendimiento.

Componentes de la gobernanza de la seguridad

- En el SP 800-100 se enumeran las siguientes actividades clave, o componentes que constituyen gobernanza de la seguridad efectiva:
  - Planificación estratégica
  - Estructura organizativa
  - Establecimiento de funciones y responsabilidades
  - Integración con la arquitectura de la empresa
  - Documentación de los objetivos de seguridad en las políticas y la orientación.

Imagen obtenida desde [1]

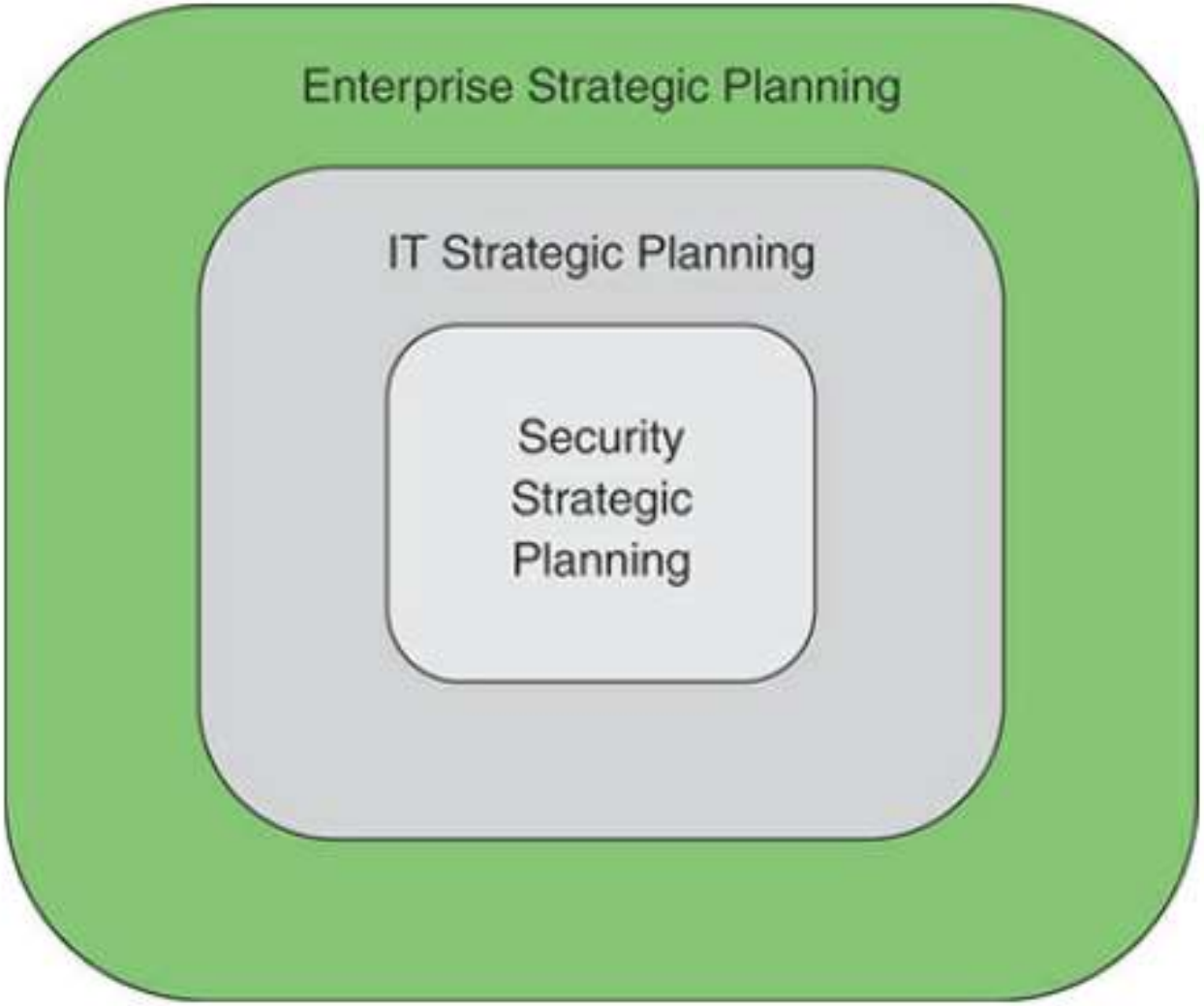


Imagen obtenida desde [1]

Proceso de planificación estratégica TI de Intel

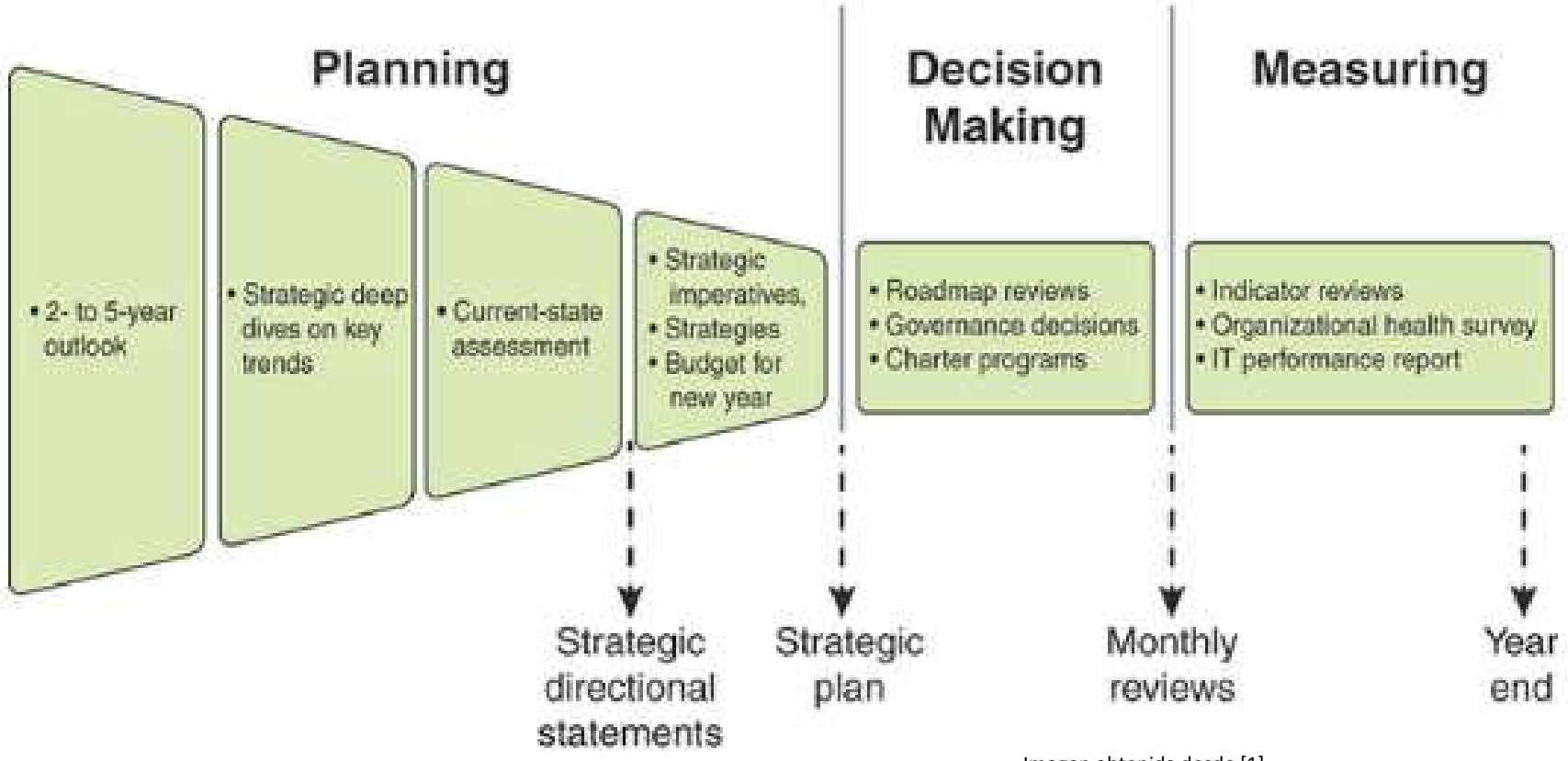


Imagen obtenida desde [1]

Planeamiento estratégico de la seguridad de la información

- La planificación estratégica de la seguridad de la información es la alineación de la gestión y el funcionamiento de la seguridad de la información con la planificación estratégica de la empresa y la tecnología de la información.
- Uso generalizado y el valor de la TI debe incluir la mitigación de los riesgos asociados.
- La planificación estratégica de la seguridad de la información es un componente esencial de la planificación estratégica.

Elementos de un documento de plan estratégico

Definición	Ejecución	Revisión
• Misión, visión y objetivos • Prioridades • Criterios de éxito • Integración • Defensa contra amenazas	• Plan operacional • Plan de monitoreo • Plan de ajustes	• Plan de revisión

Estructura organizacional
Gobierno de la Seguridad de la Información

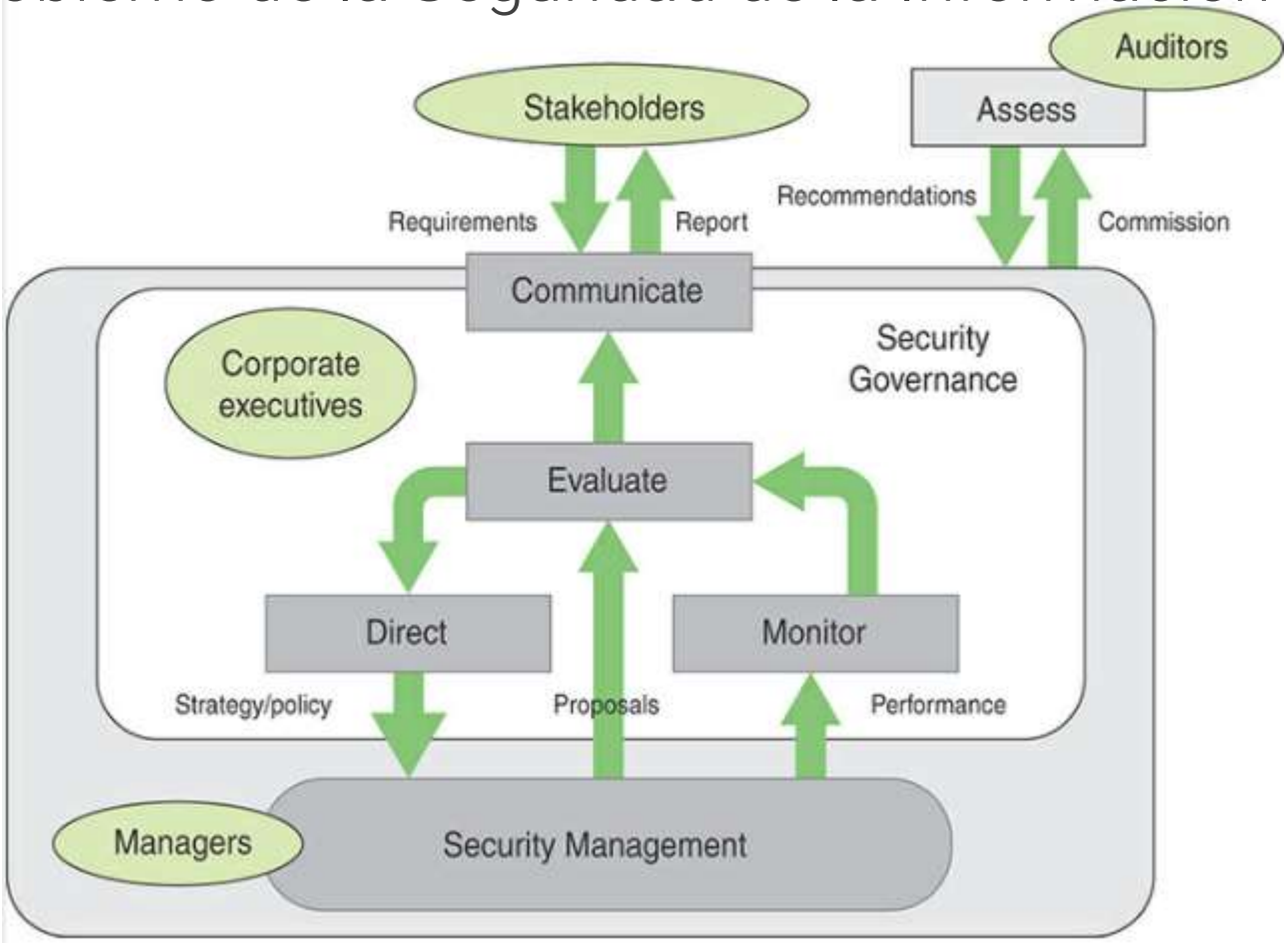


Imagen obtenida desde [1]

Reporte de la seguridad de la información

1. Información básica
2. Conceptos de gestión en materia de seguridad de la información
3. Gobernanza de la seguridad de la información
4. Planificación y objetivos de las medidas de seguridad de la información
5. Temas focales principales relacionados con la Seguridad de la Información
6. Temas focales principales relacionados con la Seguridad de la Información
7. Aprobación de terceros, acreditación, etc. (si es necesario)

Preguntas de revisión

1. ¿Cómo se define el concepto de gobierno de la seguridad?
2. ¿Cómo se define el concepto de gestión de la seguridad?
3. ¿Cómo se define el concepto de operación de la seguridad?
4. ¿Cómo estos difieren?
5. ¿Cuáles son los principios del gobierno de la seguridad de la información?
6. ¿Cuáles son los resultados esperados del gobierno de la seguridad?
7. ¿Qué debe cubrir un plan estratégico de seguridad?
8. ¿Qué debe cubrir un reporte seguridad de la información?

Revisión de lo visto

- Se explicó el concepto de gobierno de la seguridad y como este difiere del concepto de gestión de la seguridad.
- Se dio una vista general de los elementos claves del gobierno de la seguridad.
- Se indicaron los tópicos que deben ser cubiertos en un plan estratégico de seguridad y en reporte de seguridad de la información.

Actividad formativa

1. Revise el plan estratégico de la USACH,
2. Revise el plan estratégico de la Facultad de Ingeniería.
3. Proponga un lineamiento estratégico para TI alineado con un lineamiento anterior.
4. Acompañe al lineamiento estratégico con una política de seguridad.
5. Establezca controles asociados.
6. Indique como se implementaría operacionalmente dicho control.
7. Revise como lo anterior afectó a la estructura organizacional del Gobierno de seguridad de la información.
8. ¿En que parte se realizó Gobierno de la seguridad de la información? ¿Gestión de la seguridad de la información? ¿Operación?
9. ¿Se incorporaron los 6 principios? Sino, ¿Como los incorporaría?
10. ¿Cómo se podrían conseguir los 5 resultados básicos para la Gobernanza de la seguridad en este caso?

Bibliografía

1. Stallings, William. Effective Cybersecurity . Pearson Education. Kindle Edition.
2. ISO/IEC 27014:2013: Governance of information security
3. UNE-ISO/IEC 38500: Gobernanza corporativa de la Tecnología de la Información. Editorial: Aenor.
4. Fernández, A.; Llorens, F.; Juiz, C.; Maciá, F; y Aparicio, J.M. (2018). Cómo priorizar los proyectos TI estratégicos para tu universidad. Editorial: Publicaciones de la Universidad de Alicante.

Derechos de autor

- Iconos diseñados por Pixel perfect, https://www.flaticon.es

¿Preguntas?

Anexo: Gobierno de las TI

Modelo de Gobierno TI

Figura. Modelo para el Gobierno de las TI (adaptado desde [3])

Principios generales del buen Gobierno TI

1. Responsabilidad
2. Estrategia
3. Adquisición
4. Rendimiento
5. Cumplimiento
6. Comportamiento humano

Estudio de caso: FING

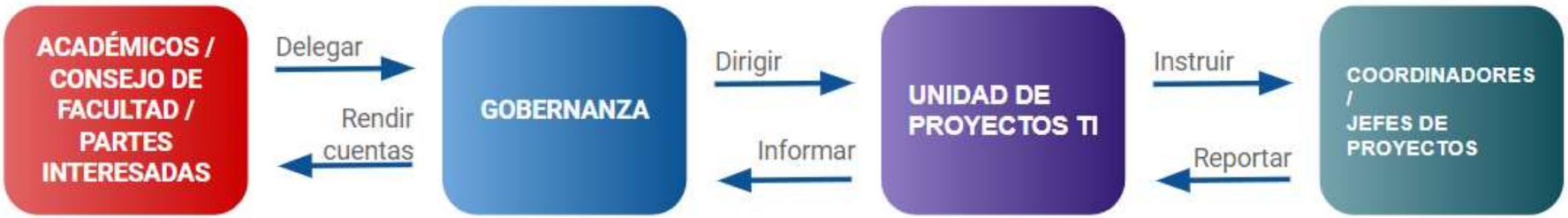


Figura. Procesos de alineamiento jerárquico (adaptado desde [4])

Modelo de cartera de proyectos

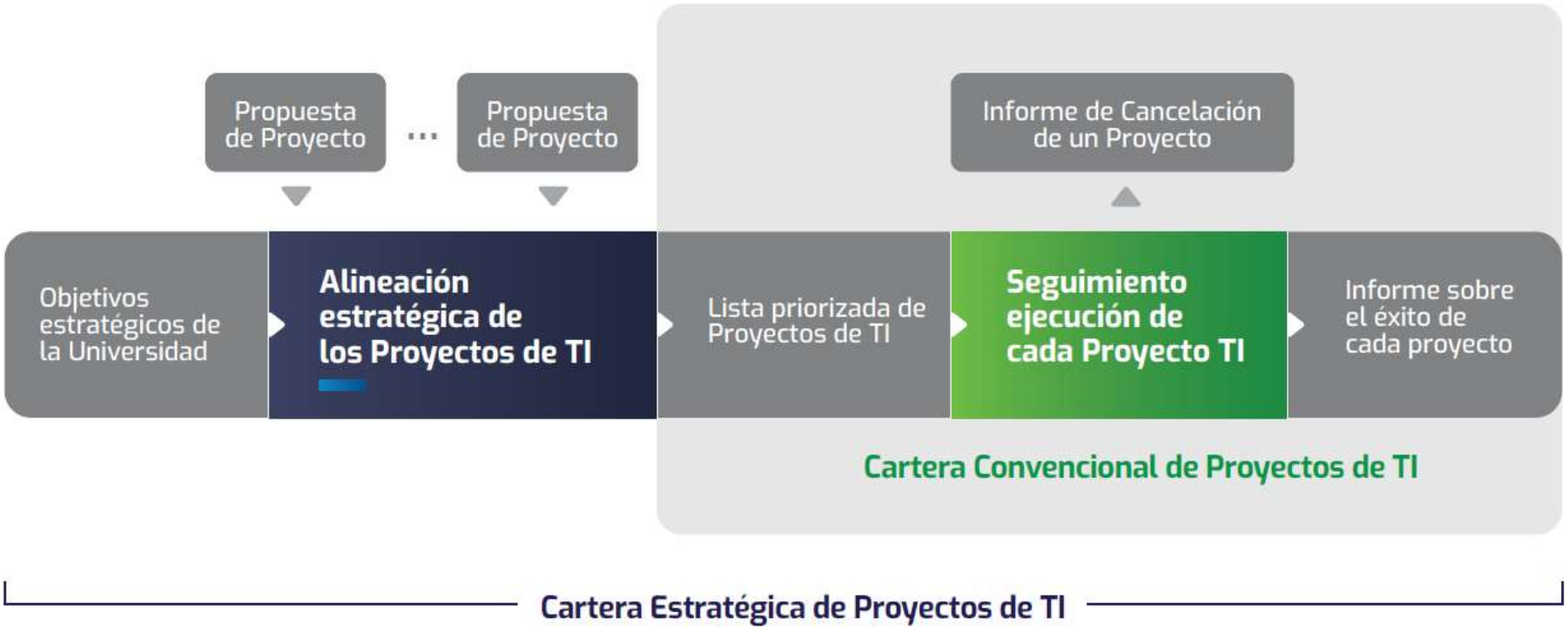


Figura. Modelo de Cartera estratégica de Proyectos TI (adaptado desde [4])

Fases y subfases de la cartera estratégica de Proyectos TI

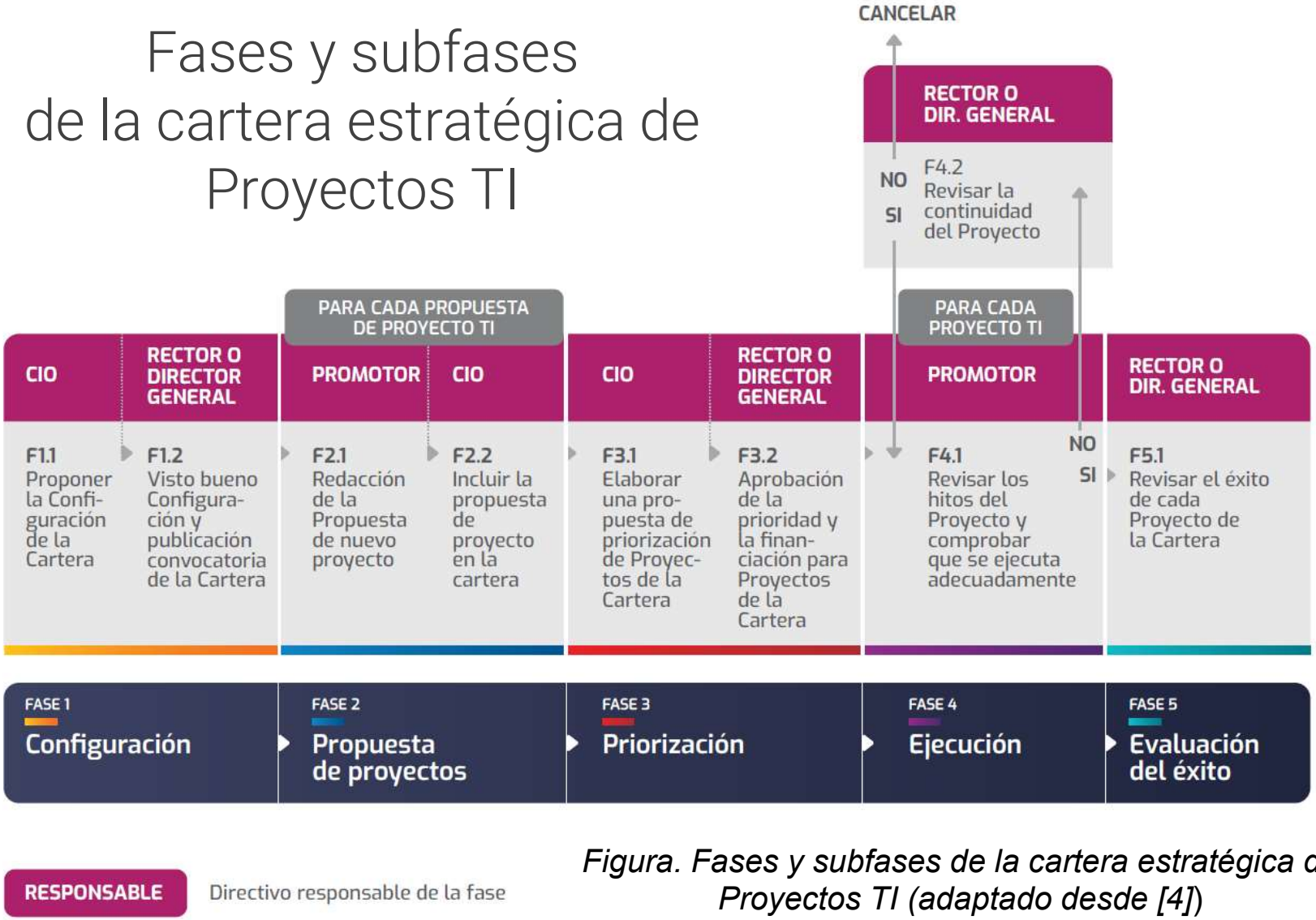


Figura. Fases y subfases de la cartera estratégica de Proyectos TI (adaptado desde [4])

Cartera de proyectos estratégicos de TI

Figura. Priorización de las decisiones sobre la cartera de proyectos (adaptado desde [4])

Priorización de proyectos

Para definir la prioridad se proponen los siguientes parámetros:

- Urgencia x Impacto = Prioridad

		Impacto				
		Muy Alto (5)	***Alto (4)***	***Medio (3)***	***Bajo (2)***	***Muy bajo (1)***
Urgencia	***Muy Urgente (5)***	Mayor (25)	Mayor (20)	Muy alta (15)	Medio (10)	Medio (5)
	Urgente (4)	Mayor (20)	Muy alta (16)	Medio (12)	Medio (8)	Baja (4)
	Media (3)	Muy alta (15)	Medio (12)	Medio (9)	Baja (6)	Muy baja (3)
	Poco urgente (2)	Medio (10)	Medio (8)	Baja (6)	Baja (4)	Muy baja (2)
	Muy poco urgente (1)	Medio (5)	Baja (4)	Baja (3)	Muy baja (2)	Muy baja (1)

Priorización de proyectos: Impacto

		Descripción
Impacto	Muy Alto	Proyecto que puede influir directamente en el cumplimiento de la misión, aumento patrimonial importante o mejora significativa de la imagen de la Facultad de Ingeniería. Afecta a toda la comunidad de la Facultad de Ingeniería. Que aumenta la eficiencia y eficacia de una gran cantidad de procesos internos y por consiguiente se mejora en gran medida la calidad del servicio. Se automatiza un proceso crítico.
	Alto	Proyecto que puede mejorar el patrimonio, imagen o conducir al logro de los objetivos institucionales. Que puede afectar a un estamento de la Facultad en un gran porcentaje. Que aumenta la eficiencia y eficacia de un conjunto de procesos internos de alta criticidad y por consiguiente se mejora la calidad del servicio. Se automatiza gran parte de un proceso crítico o se automatiza un proceso de alta criticidad.
	Medio	Proyecto que puede implicar un aumento en el patrimonio o mejora de la imagen de la Facultad de Ingeniería. Que puede afectar a un grupo significativo de personas. Que aumenta la eficiencia y eficacia de los procesos internos de un Vicedecanato o procesos de criticidad media. Se automatiza parte de un proceso de alta criticidad o se automatiza parte un proceso de criticidad media.
	Bajo	Proyecto que puede causar una pequeña mejoría en el patrimonio o imagen. Puede afectar a un grupo o agrupación de personas. Que podría aumentar la eficiencia y eficacia de algún proceso de criticidad baja y por consiguiente se mejora la calidad del servicio del mismo.
	Muy Bajo	Proyecto que puede tener un pequeño o nulo efecto en la Facultad. Afecta a un grupo reducido de personas.

Priorización de proyectos: Urgencia

		Descripción
Urgencia	Muy Urgente	Los plazos para comenzar con la ejecución del proyecto ya vencieron. Este proyecto debió haber comenzado hace mucho tiempo atrás.
	Urgente	El proyecto se debe comenzar a la brevedad.
	Media	El comienzo del proyecto debe ser durante el primer semestre del próximo año.
	Poco urgente	El comienzo del proyecto debe ser durante el segundo semestre del próximo año.
	Muy poco urgente	El proyecto podría esperar un año para comenzar.

Roles en la cartera de proyectos TI

- Decano:
  - Establece los criterios estratégicos de la cartera
  - Asigna financiación a los proyectos más estratégicos
- Gobernanza:
  - Aconsejan al Decano en:
    - Definir la estrategia de la Facultad
    - Configurar la cartera
    - Priorizar estratégicamente los proyectos
    - Asignar financiación a los proyectos más estratégicos

Roles en la cartera de proyectos TI

- Unidad de proyectos TI:
  - Debe promover la puesta en marcha y una explotación adecuada de la cartera
  - También supervisará el funcionamiento de la Oficina de la cartera y desde allí:
    - Asesorar a los promotores.
    - Colaborar en la coordinación de proyectos transversales
    - Elaborar la propuesta de priorización de la lista de proyectos y elevarla a Gobernanza.
    - Realizar el seguimiento de la ejecución de los proyectos e informar a Gobernanza sobre el éxito de los mismos.
    - Proponer la cancelación de un proyecto si lo estima conveniente.

Roles en la cartera de proyectos TI

- Promotor:
  - Persona que propone incluir un nuevo proyecto en la cartera.
  - Defiende la necesidad o conveniencia de su ejecución.
  - Debe ser un Vicedecano, Secretario o Decano.
- Solicitante:
  - Persona que solicita al promotor que apoye la puesta en marcha de un nuevo proyecto.
  - Encargado de justificar su necesidad y beneficios, elabora la propuesta de proyecto y define sus hitos.
  - Debe ser el encargado del área en donde se va implementar el proyecto.

Roles en la cartera de proyectos TI

- Director de proyecto:
  - Es la persona designada por el promotor del proyecto para la dirección y ejecución posterior del mismo y tendrá la responsabilidad de alcanzar los objetivos propuestos.
  - Debe ser un coordinador, o jefe de unidad o servicio. Puede ser el mismo que el solicitante.
- Apoyo técnico:
  - Revisar los aspectos tecnológicos de la propuesta de proyecto del Solicitante.
  - Dirigir la implantación tecnológica durante la ejecución del proyecto.

Roles en la cartera de proyectos TI

Oficina de la cartera de proyectos TI

- Coordina y gestiona la Cartera mediante:
  - Asesora a lo usuarios de la cartera en las diferentes fases del proceso, especialmente a la hora de redactar en términos estratégico una propuesta de proyecto.
  - Elaborar un primer informe de evaluación de las propuestas de proyecto y elevarlo a Gobernanza.
  - Supervisar el seguimiento de la ejecución de los proyectos.