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.

Resultados de aprendizaje

- OA: Evaluar y planear la seguridad informática en las organizaciones.
  - Explicar el concepto de gobierno de la seguridad y cómo éste 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.
  - Identificar los diferentes roles de la ciberseguridad de acuerdo a ENISA CSF y al NIST NICE.

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

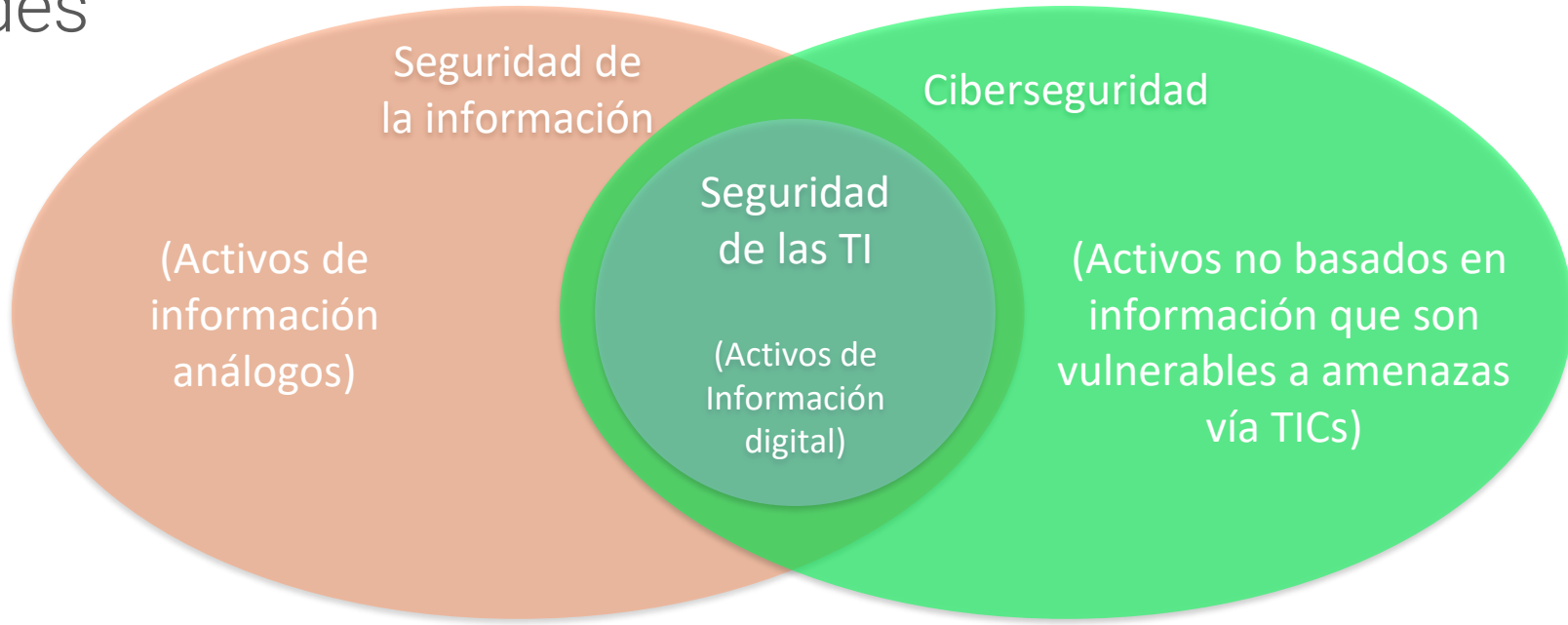
Gobierno de la Seguridad de la Información

"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

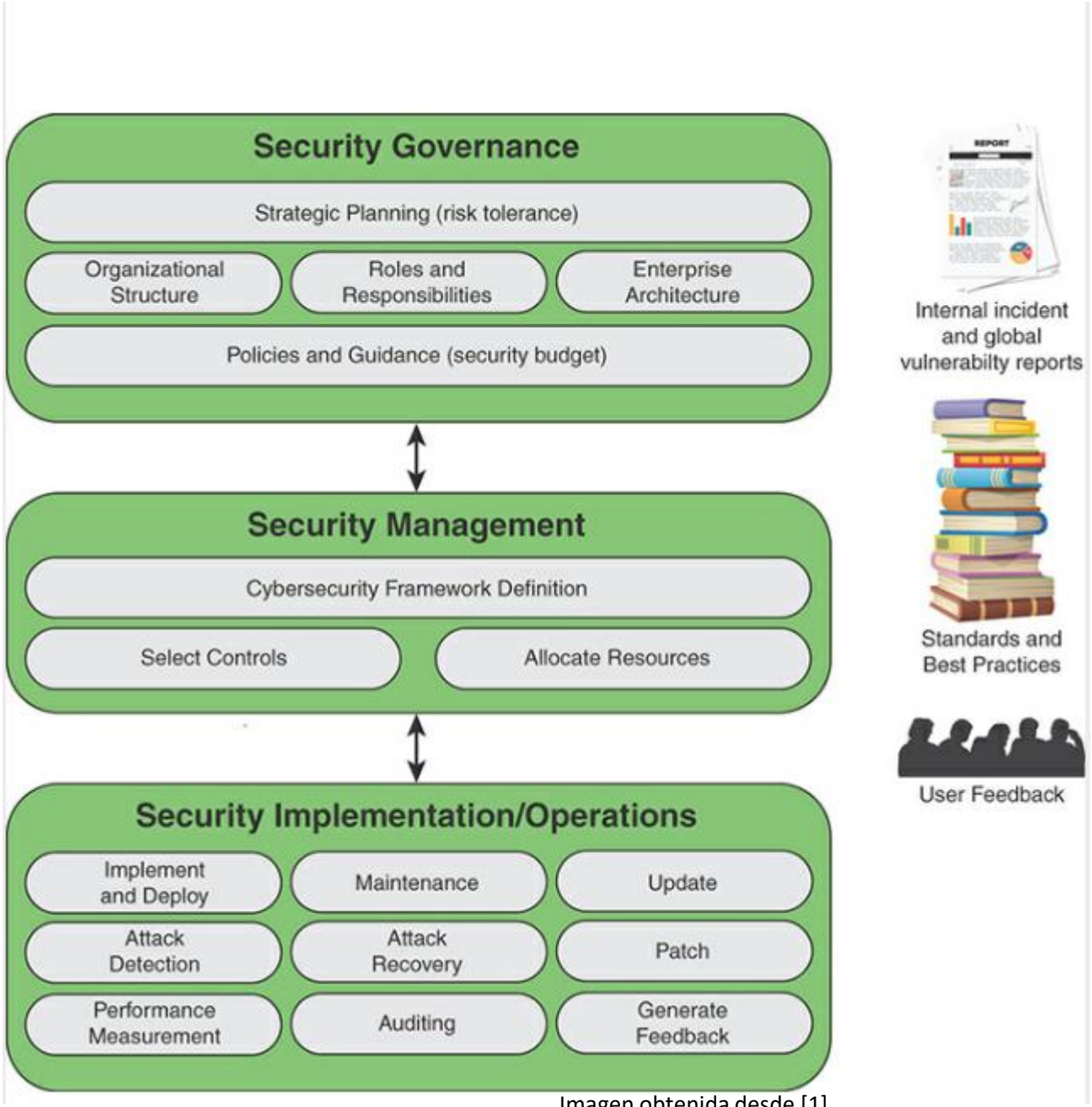


Imagen obtenida desde [1]

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 NIST 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]

¿Alguna/o de ustedes a revisado una política de seguridad de la información?
¿Qué debería contener una política de seguridad de la información en su organización?

Planeamiento estratégico de la ciberseguridad

- La planificación estratégica empresarial implica la definición de metas y objetivos a largo plazo para una organización.
- Es una actividad para establecer prioridades, centrar la energía y los recursos, fortalecer las operaciones, garantizar que los empleados y otras partes interesadas trabajen en pos de objetivos comunes.
- Todo ello implica la elaboración de un plan estratégico y la supervisión permanente de la aplicación de ese plan.

Imagen obtenida desde [1]

Proceso de planificación estratégica TI de Intel

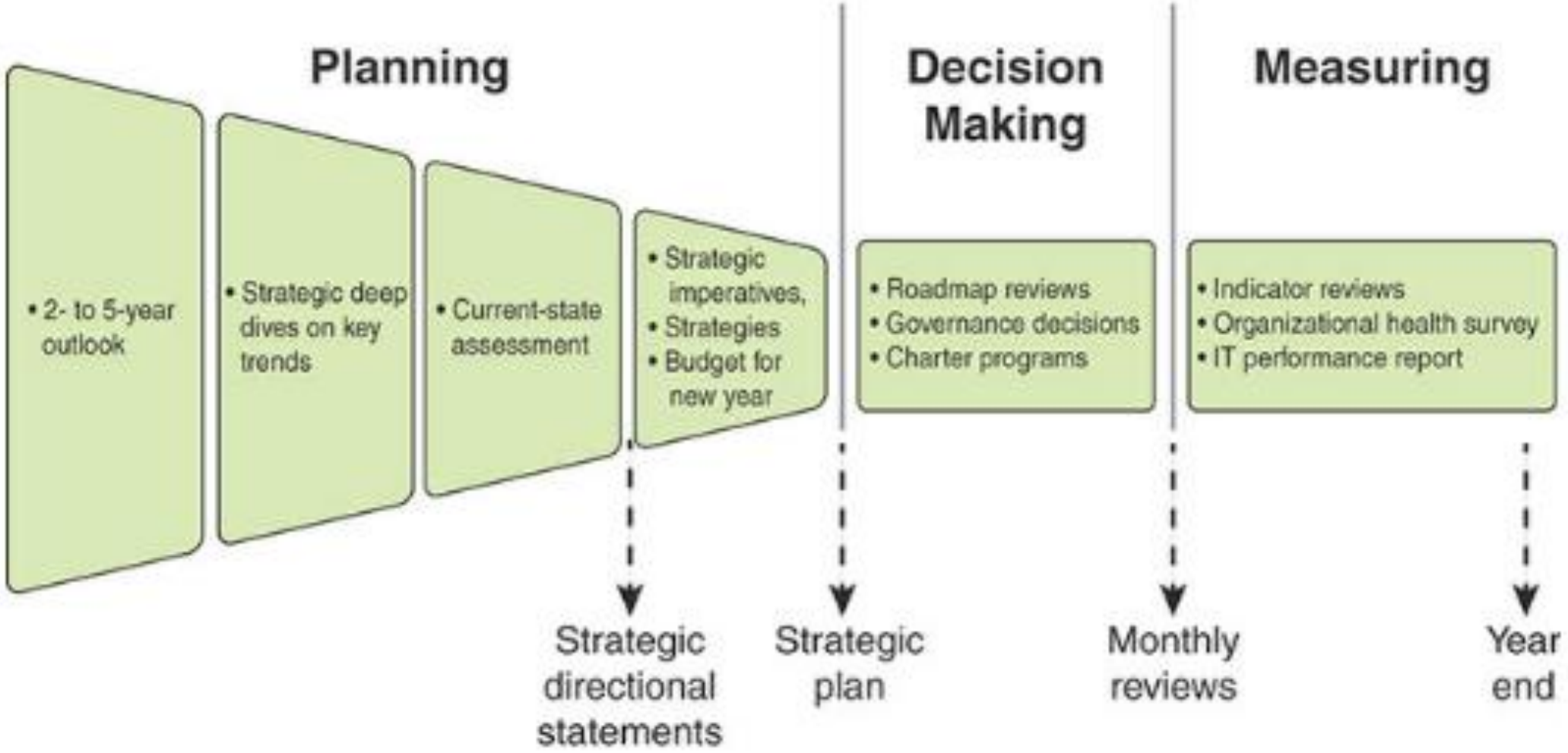


Imagen obtenida desde [1]

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 de seguridad de la información

Definición

- Misión, visión y objetivos
- Prioridades
- Criterios de éxito
- Integración
- Defensa contra amenazas

Ejecución

- Plan operacional
- Plan de monitoreo
- Plan de ajustes

Revisión

- Plan de revisión

¿Alguna/o de ustedes a revisado un plan estratégico? ¿Qué debería contener? Revisemos el de la USACH y proponga un lineamiento estratégico relacionado con TI y Ciberseguridad.

Estructura organizacional
Gobierno de la Seguridad de la Información

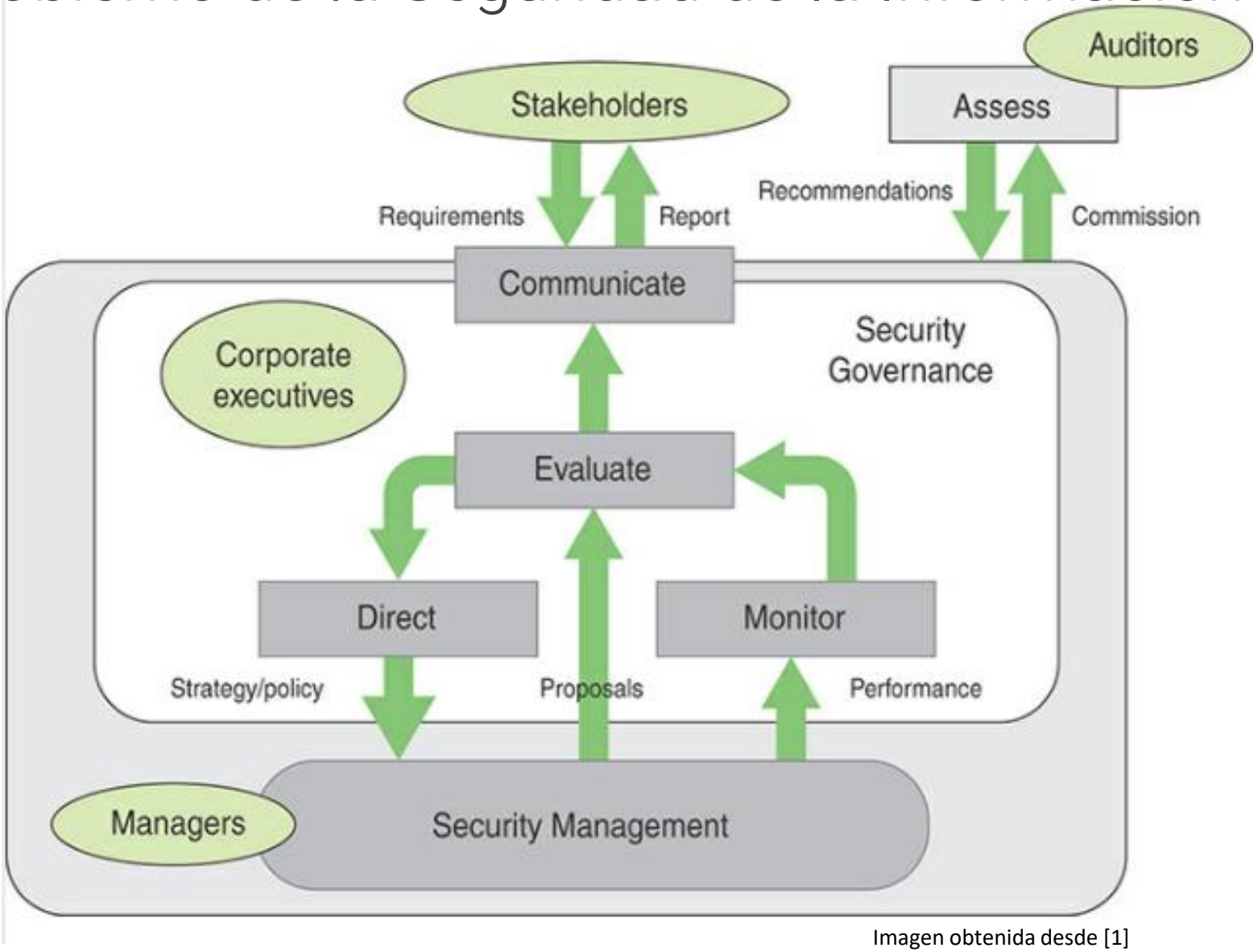
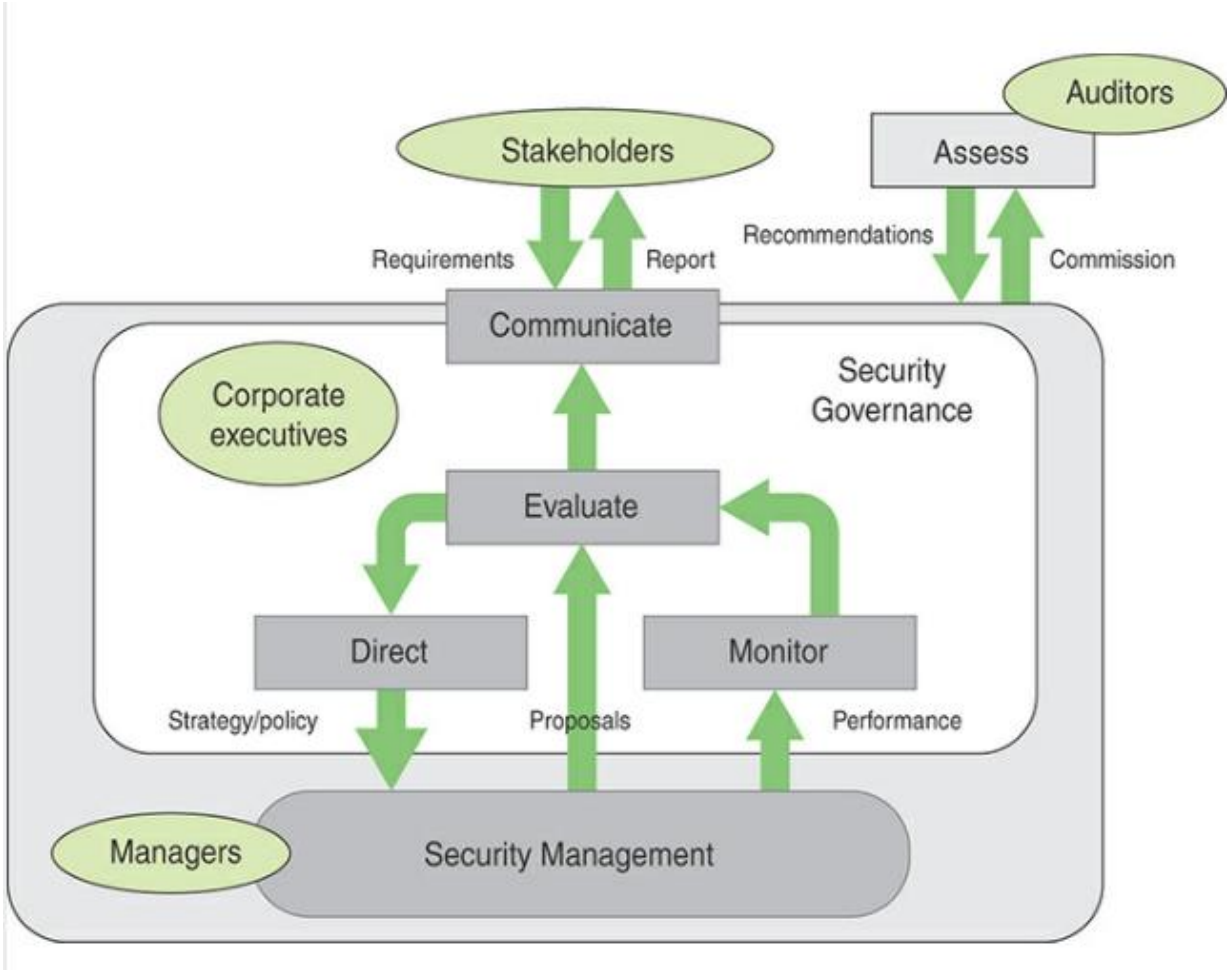
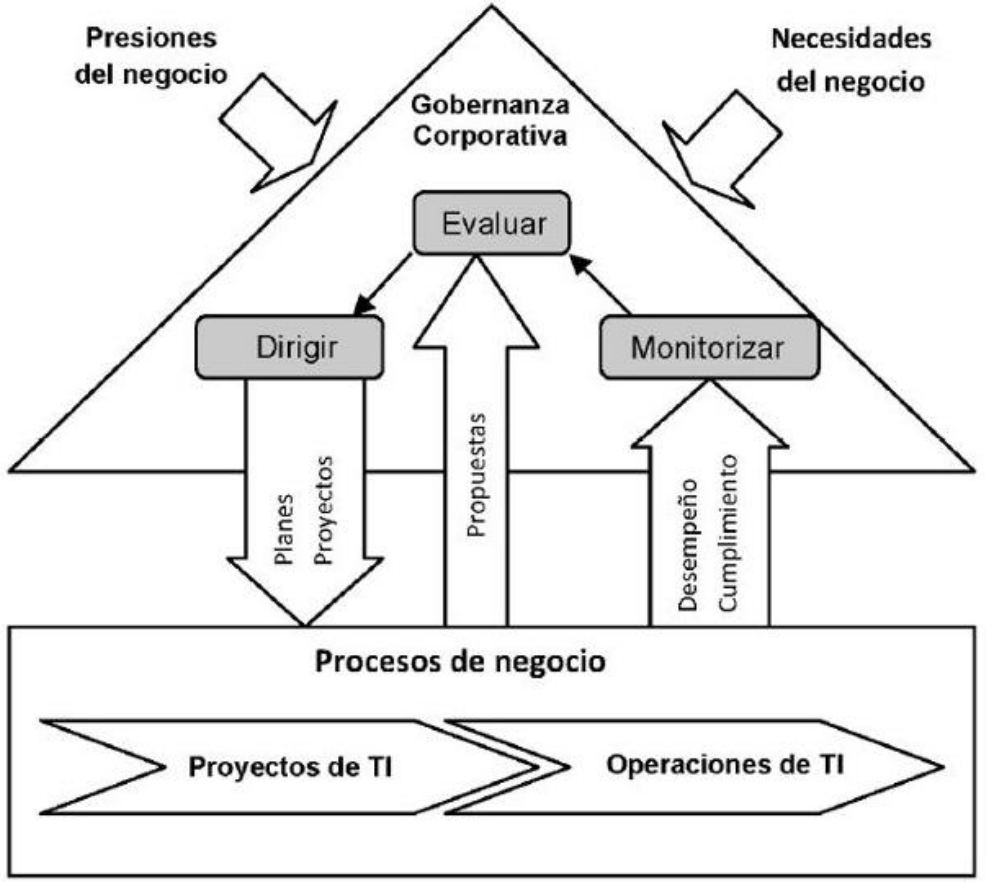


Imagen obtenida desde [1]

Gobierno de la seguridad de la información vs Gobierno TI





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)

Demanda de fuerza de trabajo en ciberseguridad (1/2)

GLOBALLY, the shortage of cybersecurity professionals is estimated to be

2.72 Million

Source: (ISC)² Cybersecurity Workforce Study, 2021

Over the last three years,

87%

of organizations reported actively seeking to meet diversity goals when hiring new graduates

Source: Fortinet 2022 Cybersecurity Skills Gap Global Research Report

The biggest skill gaps in today's cybersecurity professionals:

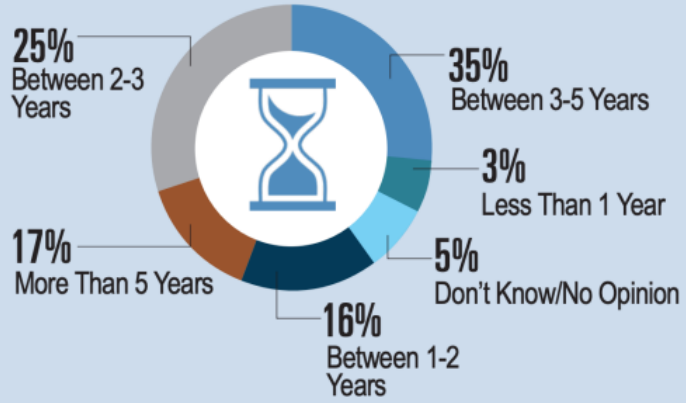
54% Soft Skills

52% Cloud Computing

34% Security Controls

Source: ISACA State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources, and Cyberoperations

How long does it take a cybersecurity professional to become proficient



Source: The Life and Times of Cybersecurity Professionals 2021

https://www.nist.gov/system/files/documents/2022/07/06/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf

Demanda de fuerza de trabajo en ciberseguridad (2/2)

714,548 total cybersecurity job openings

1,091,575 total employed cybersecurity workforce

Source: CyberSeek, June 2022

78% of decision makers indicate it's hard to find certified people, which is why 91% of organizations are willing to pay for the training and certification of their employees

Source: Fortinet 2022 Cybersecurity Skills Gap Global Research Report

Prior hands-on cybersecurity experience remains the primary factor **(73%)** in determining whether a candidate is considered qualified

Source: ISACA State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources, and Cyberoperations

13.5% Growth

Computer and mathematical occupations will grow much faster than the average job during 2016–2026

Source: Bureau of Labor Statistics, U.S. Department of Labor

Top cybersecurity job titles:

- Cybersecurity Analyst
- Software Developer
- Cybersecurity Consultant
- Penetration & Vulnerability Tester
- Cybersecurity Manager
- Network Engineer
- Systems Engineer
- Senior Software Developer
- Systems Administrator

Source: CyberSeek, June 2022

Top tasks identified for entry-level candidates include:

- Alert and Event Monitoring
- Documenting Processes and Procedures
- Incident Response
- Using Scripting Languages
- Reporting (Developing and Producing Reports)

Source: (ISC)² Cybersecurity Hiring Managers Guide: Best Practices for Hiring and Developing Entry and Junior-Level Cybersecurity Practitioners, 2022

https://www.nist.gov/system/files/documents/2022/07/06/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf

Roles de la Ciberseguridad
ENISA Cybersecurity Skill Framework

https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Roles de la Ciberseguridad
NICE Framework (NIST)

- Categorías (7)
- Áreas de especialidad (33)
- Roles de trabajo (52)

https://niccs.cisa.gov/workforce-development/nice-framework

Ejemplo

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
Securely Provision (SP)	Risk Management (RSK)	Authorizing Official/Designating Representative	SP-RSK-001	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).
		Security Control Assessor	SP-RSK-002	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
	Software Development (DEV)	Software Developer	SP-DEV-001	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
		Secure Software Assessor	SP-DEV-002	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
	Systems Architecture (ARC)	Enterprise Architect	SP-ARC-001	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
		Security Architect	SP-ARC-002	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.

Preguntas de conocimiento

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?
9. ¿Cuáles son los roles de ciberseguridad de acuerdo a ENISA? ¿NICE?

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.
- Se identificaron los diferentes roles de la ciberseguridad de acuerdo a ENISA CSF y al NIST NICE.

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?