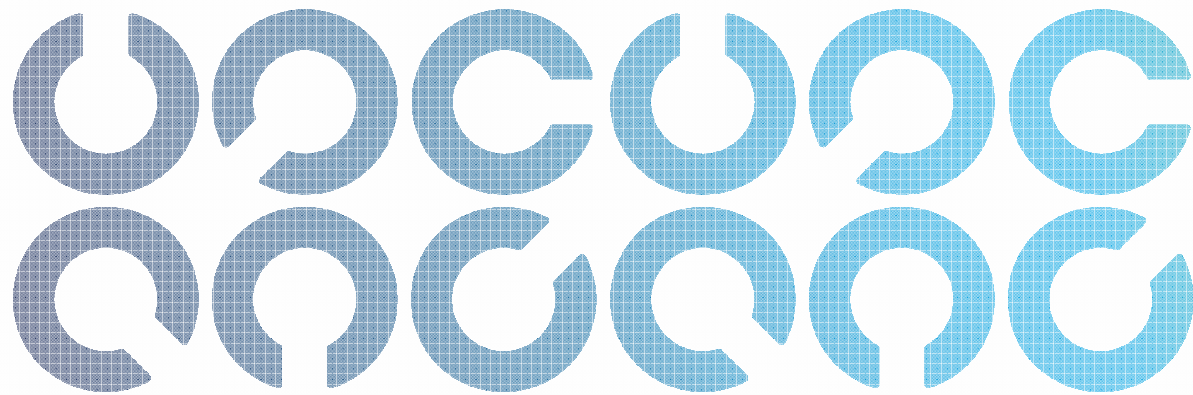


# Gobierno de Seguridad de la Información



Juan Carlos López,  
PMP, CISA, CGEIT,  
CRISC, CISM  
[presidencia@isaca.org.ec](mailto:presidencia@isaca.org.ec)  
[jclopez@exacta.com.ec](mailto:jclopez@exacta.com.ec)

## Juan Carlos López

---

Consultor con experiencia en definición, implementación y gestión de prácticas de gobierno, administración de riesgos, control interno planeación estratégica, auditoría y dirección de proyectos; del negocio y tecnología. Durante 5 años fue consultor de PricewaterhouseCoopers. Fue Gerente de Auditoría, de Tecnología y de la Oficina de Dirección de Proyectos del Banco Internacional, durante los ocho años que laboró en la Institución. Miembro de asociaciones profesionales como el Instituto de Dirección de Proyectos (PMI), de la Asociación para la Auditoría y Control de Sistemas de Información (ISACA) y del Instituto para la Gobernabilidad de Tecnología de Información (ITGI), de estos dos últimos fue Presidente y Director de Educación. Posee las Certificaciones CISA, CISM, CRISC, CGEIT, SMC, PMP, ITIL y COBIT. Es instructor COBIT 2019 acreditado por APMG. Docente en la Universidad de la Américas en las maestrías de Gerencia de Sistemas, Gerencia de Seguridad de la Información y Gerencia de Operaciones en las asignaturas de Gobierno de Información & Tecnología, Gobierno de Seguridad de la Información y Dirección de Proyectos.

# Internacional

- Más de 50 años
- Más de 145000 miembros alrededor del mundo.
- La organización más importante del mundo en GEIT:
  - Is Audit
  - IS Management
  - Cybersecurity Management
  - IT Risk
- Marcos de referencia referentes a nivel mundial (COBIT, Risk IT, ITAF, CMMI)
- Recursos y bases de conocimientos de calidad indiscutible.
- Eventos globales de alto reconocimiento internacional.
- Participe y promotor de iniciativas globales como GDPR, PCI, NIST Frameworks de Ciberseguridad.
- Certificaciones profesionales reconocidas y valoradas mundialmente.
- Estudios sobre el estado de la profesión.
- Foros , grupos de interés, oportunidades de crecimiento profesional, networking.



# Ecuador

- Más de 200 miembros
- 19 años de vida
- Entrenamientos en COBIT, CISA, CISM, CRISC. Csx
  
- CRISC: 27 de mayo




# GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

---

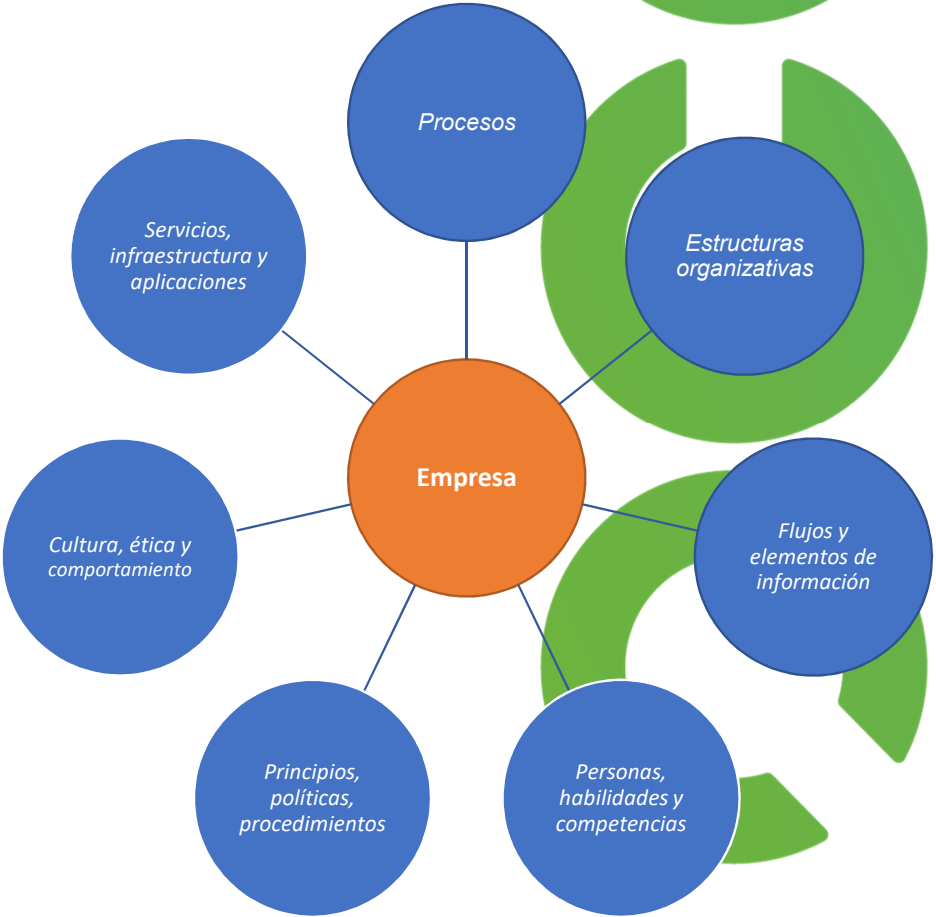
Visión General

- Que es un Sistema?

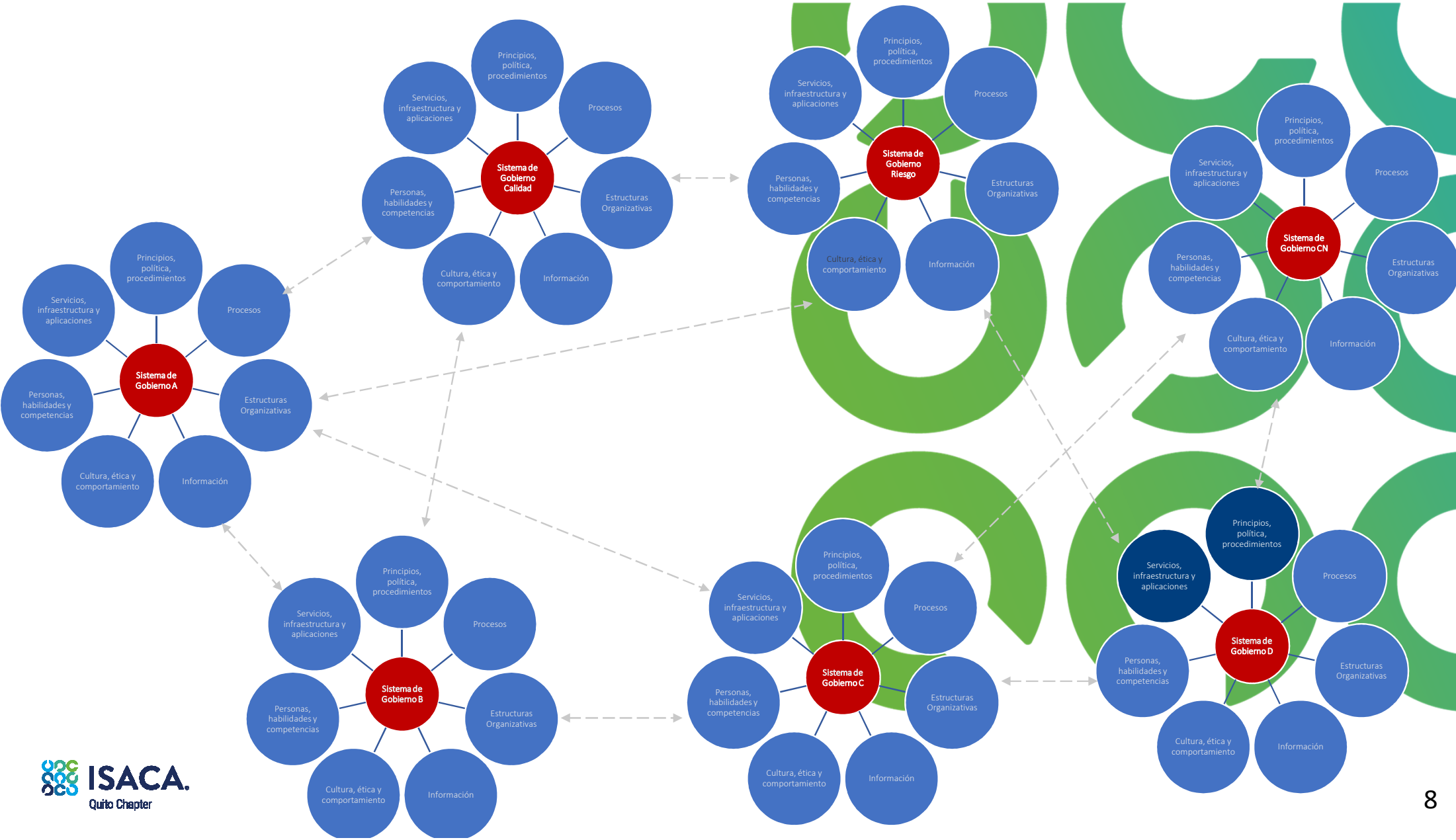


Es un conjunto de componentes que interactúan entre si para que, funcionando como un todo, lograr un objetivo

# Componentes de un sistema de gobierno









# GOBIERNO CORPORATIVO

**El Gobierno Empresarial o Corporativo** es un conjunto de responsabilidades y prácticas ejercidas por el personal y la dirección ejecutiva con el objetivo de :

- Proveer **dirección estratégica**
- Asegurar que los **objetivos** son alcanzados
- Controlar que los **riesgos** son manejados de manera apropiada
- Verificar que los **recursos de la empresa** son usados con responsabilidad



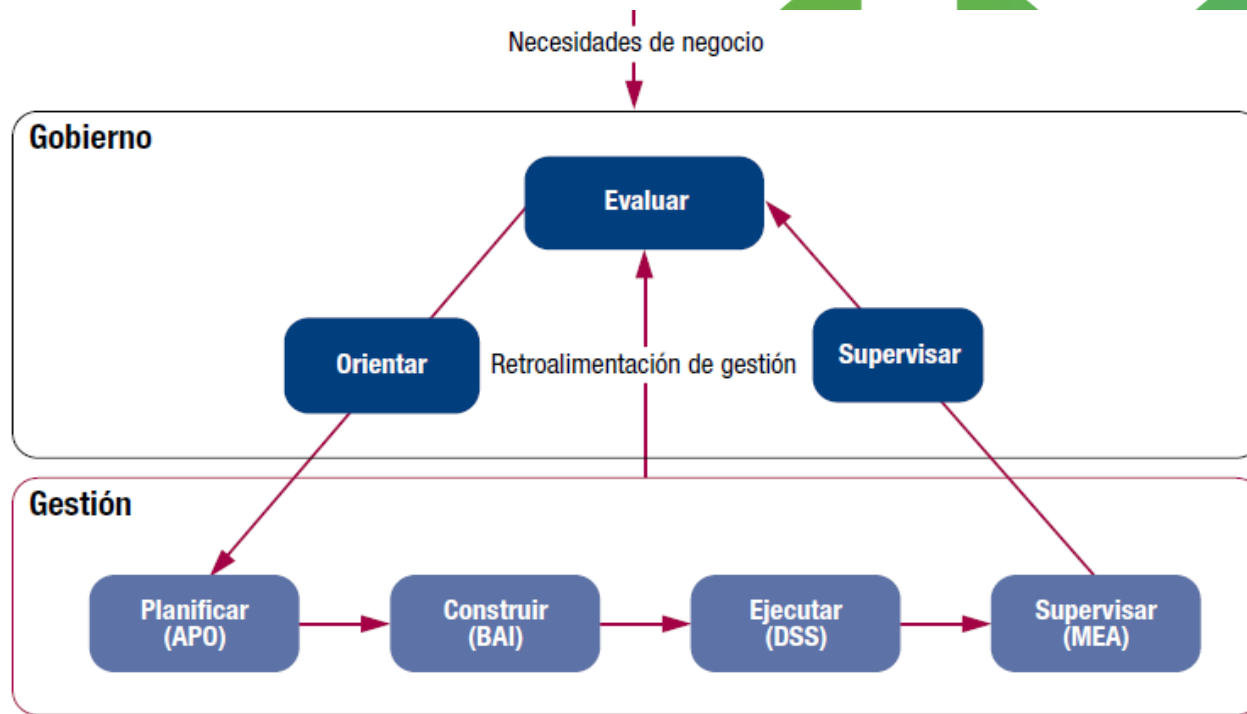
# GEIT

El Gobierno Empresarial de I & T es:

- Una parte integral del gobierno corporativo y consiste en la dirección, la estructura y los procesos organizacionales que aseguran que la Tecnología de la Información corporativa *soporta la consecución de la estrategia de la organización y sus objetivos.*
- La responsabilidad del Gobierno Empresarial de I & T es de los ejecutivos y el directorio de la organización.



# Separar Gobierno de Gestión



## Sistema de Gobierno Integro (End to End)

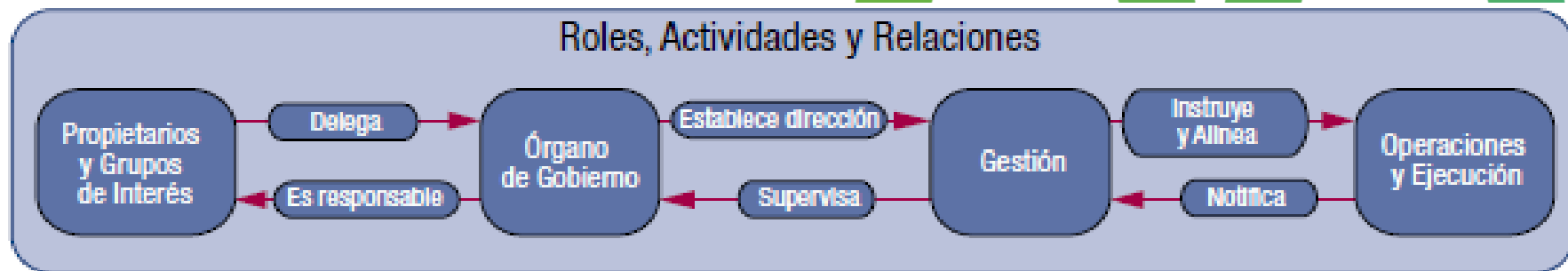
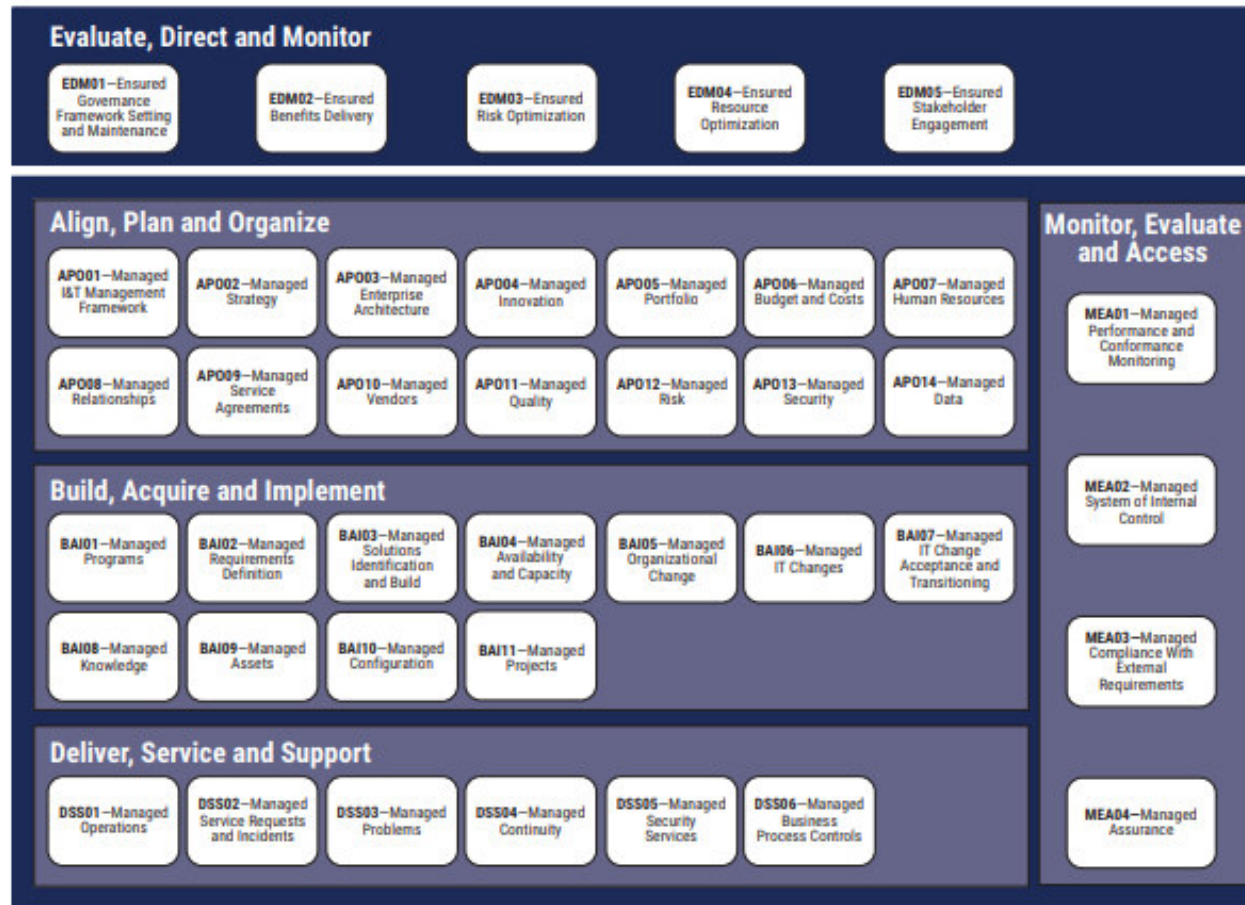


Figure 1.2—COBIT Core Model



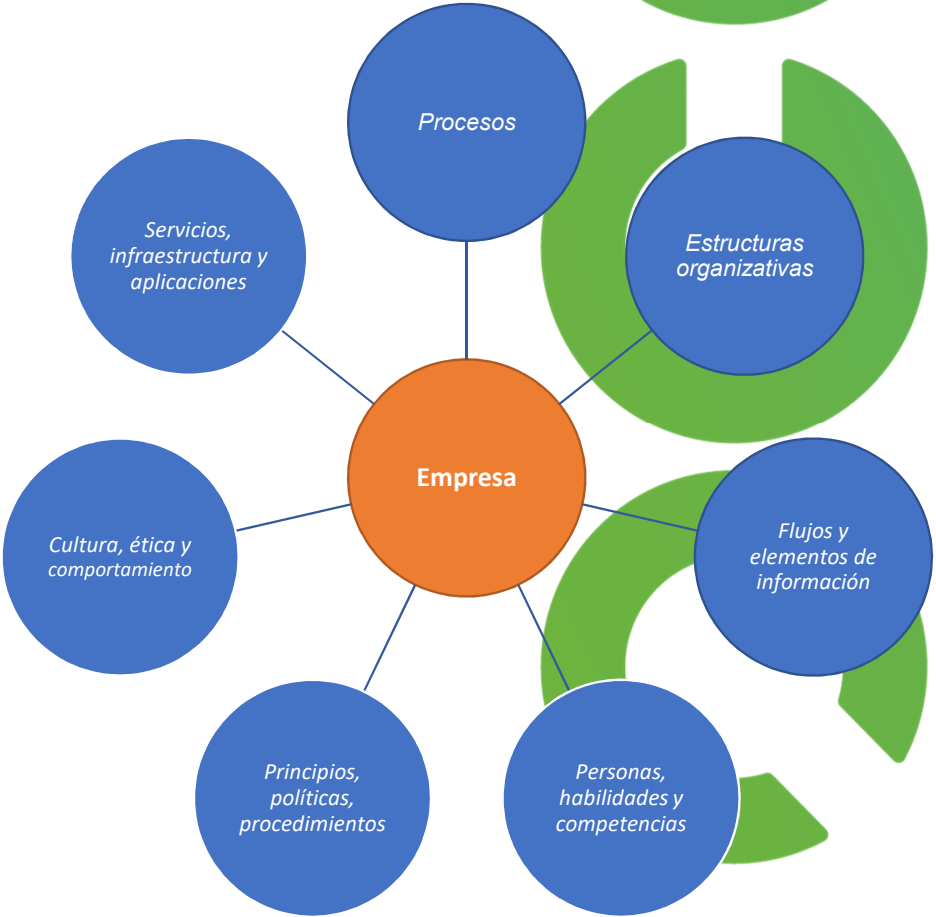
Source: ISACA, COBIT 2019 Framework: Introduction and Methodology, USA, 2018, figure 4.2

# GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

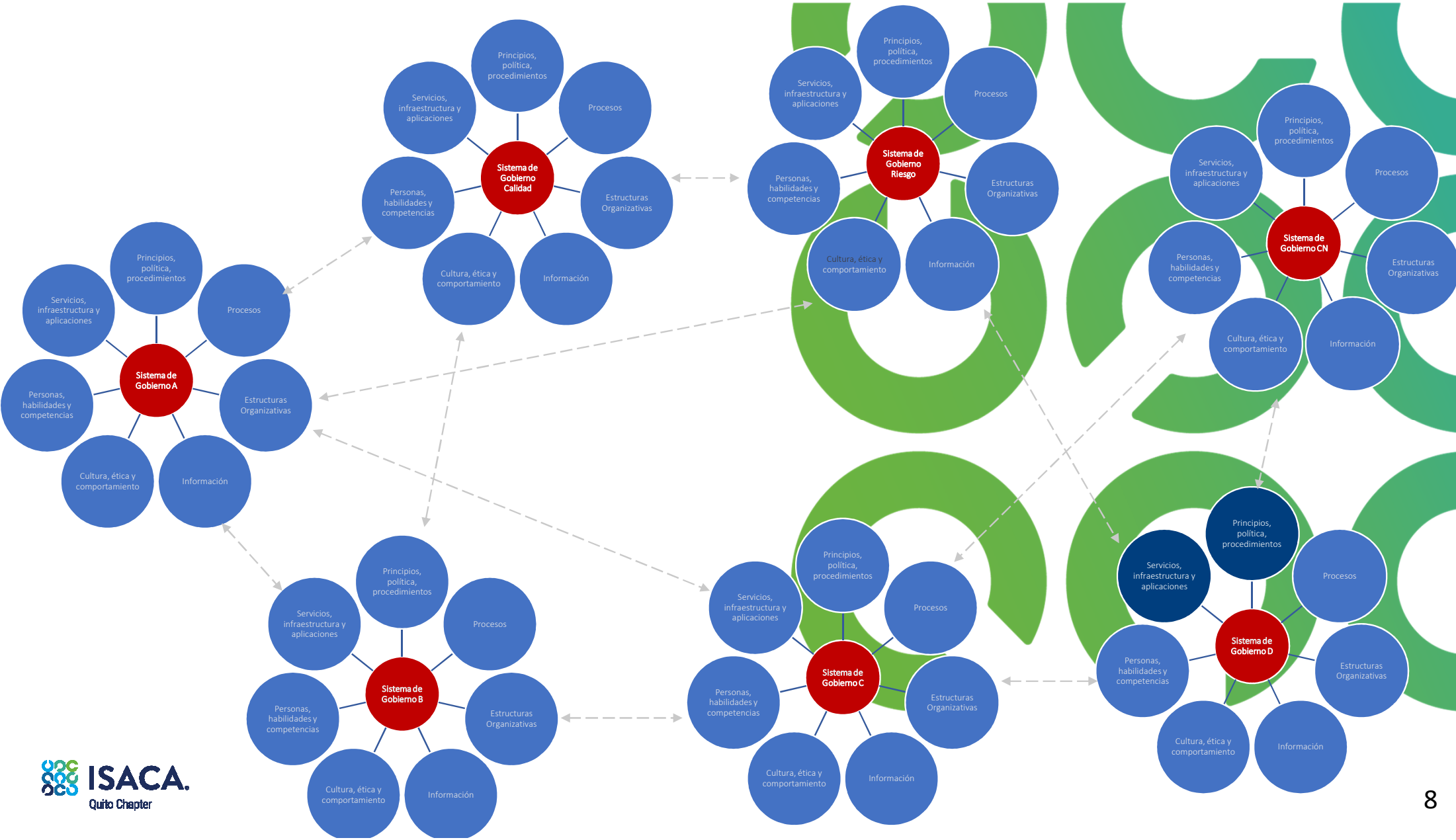
---

Sistemas de Gobierno y  
Gestión

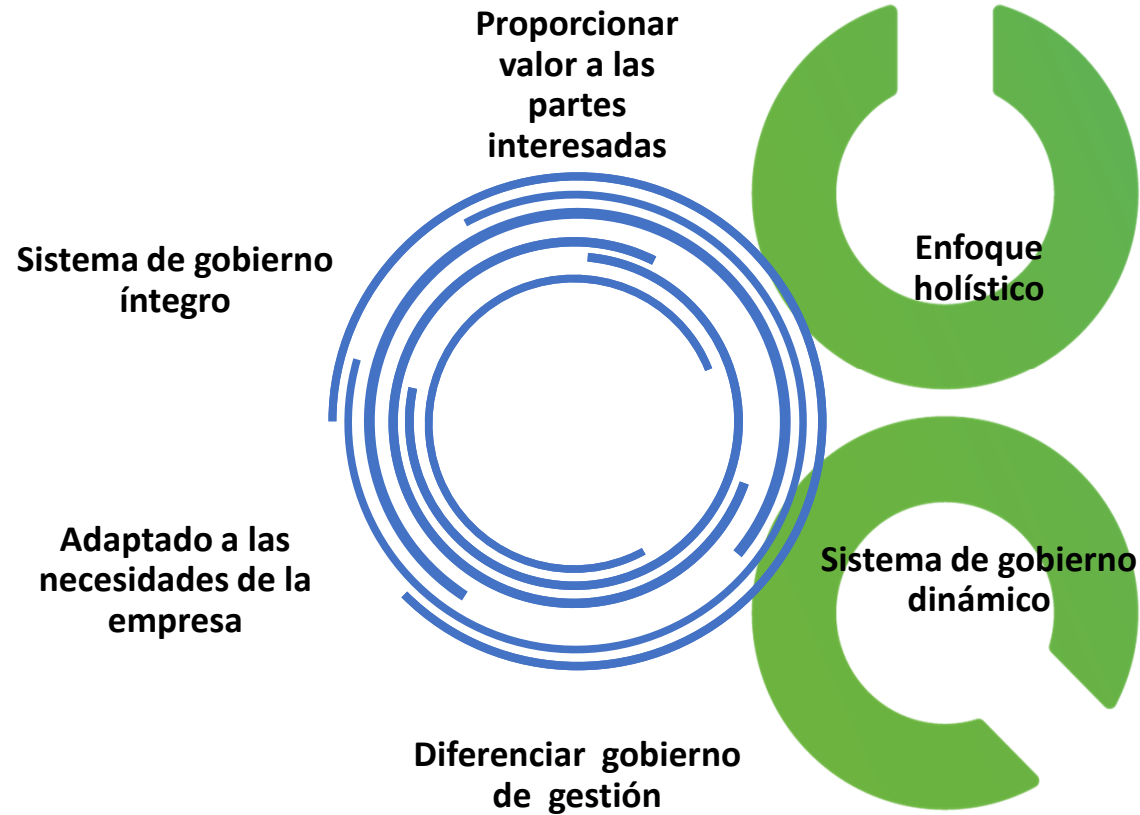
# Componentes de un sistema de gobierno







# Principios del sistema de gobierno



OBJETIVO DE GOBIERNO.

**El contexto del gobierno empresarial de la información y la tecnología incluye:**



*Un buen gobierno conduce al alineamiento, lo que conduce a su vez a la creación de valor.*

## Crear valor a las partes Interesadas

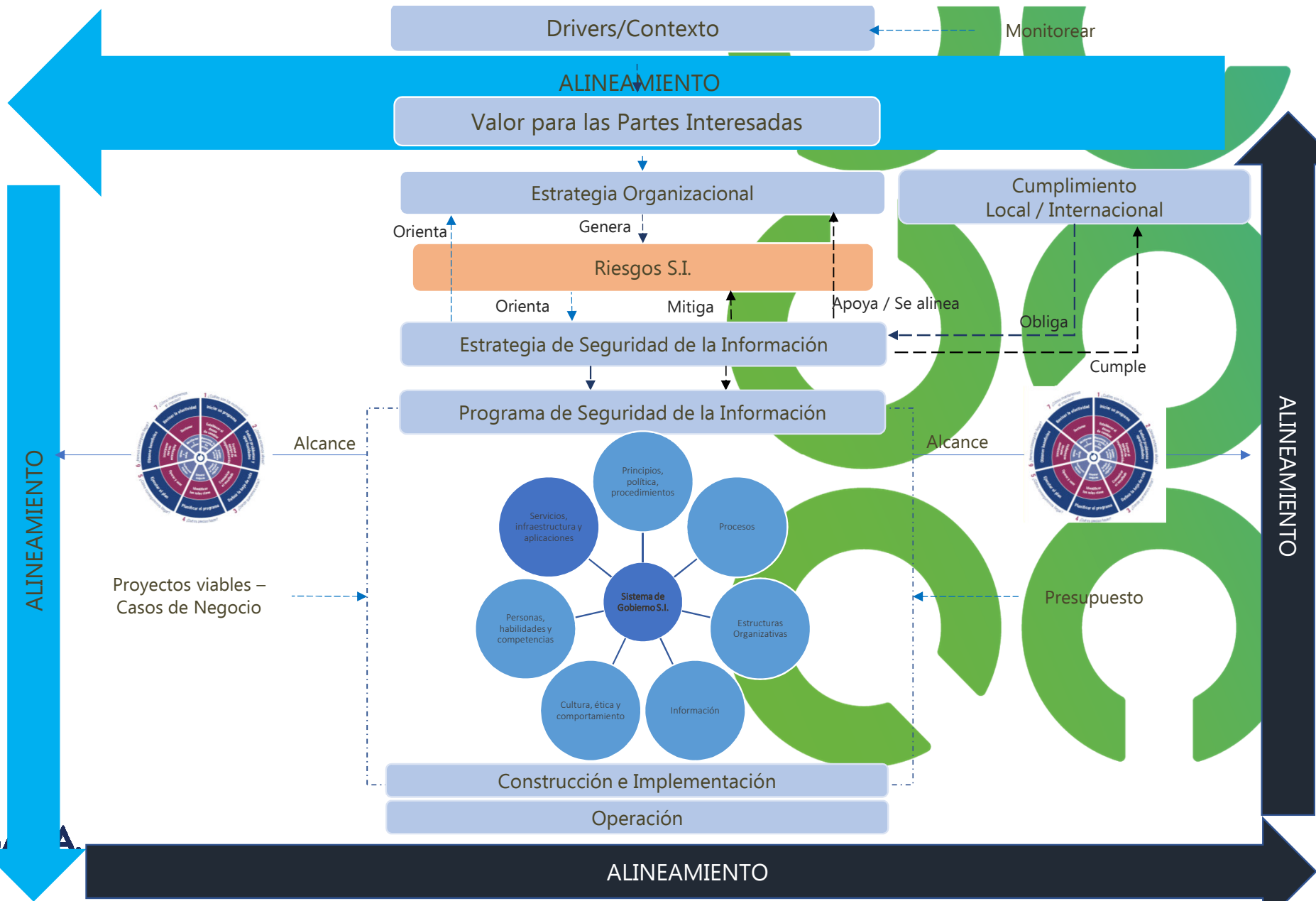
- Las empresas existen **para crear valor** para las partes interesadas.



- **Creación de Valor:** conseguir los beneficios a un costo óptimo de los recursos mientras se optimiza el riesgo.

# GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

—  
SGSI



- Seguridad de la Información

- This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization.
- The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.





- Seguridad de la Información

- The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.
- It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.



- Security Organization Goals And Objectives



- Security Organization Goals And Objectives

- **Confidentiality** is the protection of information from unauthorized access or disclosure. Different types of information require different levels of confidentiality, and the need for confidentiality can change over time. Personal, financial and medical information require a higher degree of confidentiality than publicly available information. Similarly, some enterprises need to protect information on competitive products (e.g., business strategies, marketing information, Intellectual property).



- Security Organization Goals And Objectives

- **Integrity** is the protection of information from unauthorized modification. The concept of integrity also applies to electronic messaging, files, software and configurations.



- Security Organization Goals And Objectives

- **Availability** ensures the timely and reliable access to and use of information and systems. Availability includes safeguards to make sure data are not accidentally or maliciously deleted. This is particularly important with mission critical systems because any interruptions in availability can result in significant loss of productivity and revenue. Similarly, the loss of data can impact management's ability to make effective decisions and responses. Availability can be protected by the use of redundancy, backups, and implementation of business continuity management and planning.



## • Cybersecurity Definition

- Cybersecurity is concerned with protecting digital network hardware, software and the information that is processed, stored within isolated systems and transported by internetworked information environments. Cybersecurity should be considered as a component of information security. State-sponsored network attacks and advanced persistent threats (APTs) belong almost exclusively to cybersecurity.
- The terms cybersecurity and information security are often used interchangeably, but cybersecurity is a part of information security. ISACA defines cybersecurity as the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.

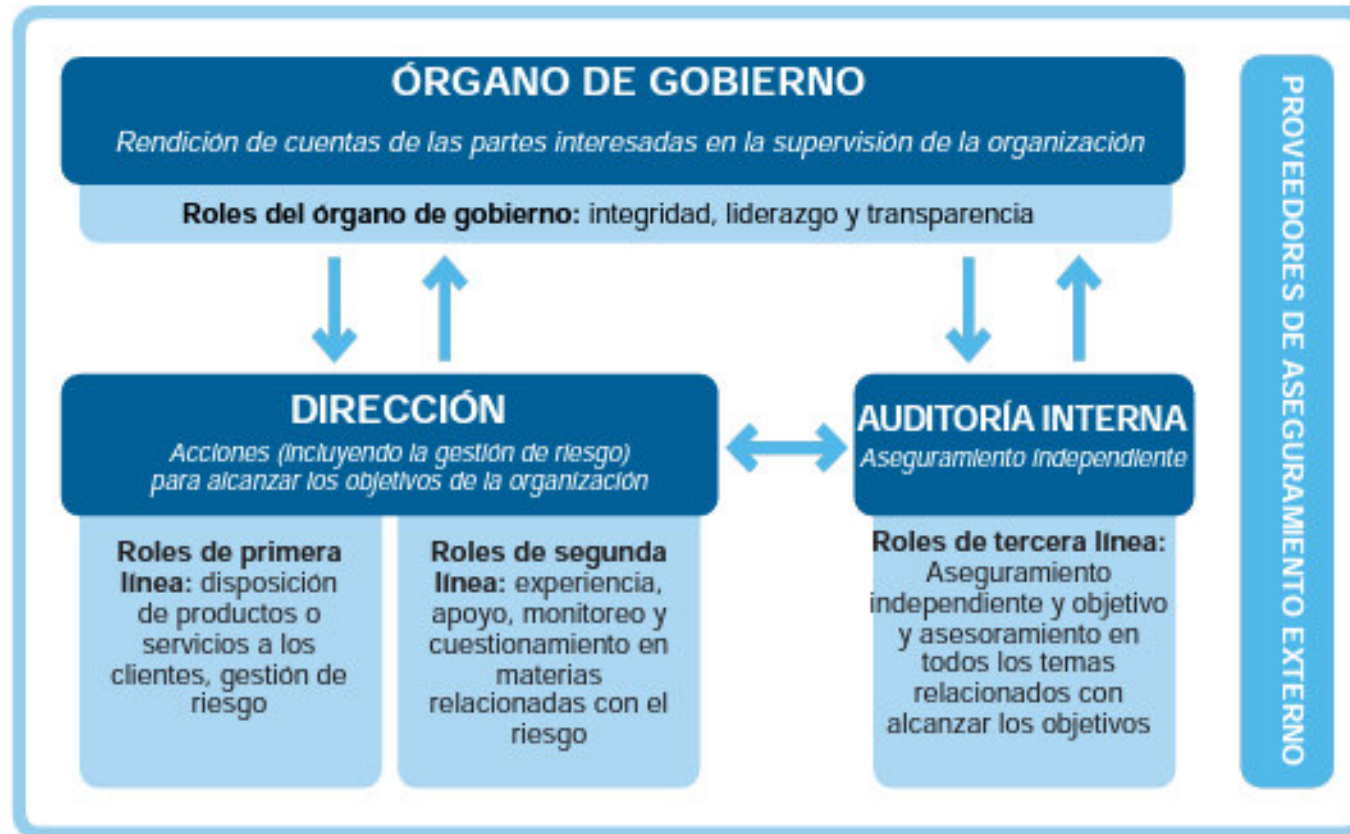
## • Cybersecurity Definition

- The International Organization for Standardization (ISO), in its ISO(IEC 27032 cybersecurity standard, defines:
- **Cybersecurity or cyberspace security** as the "preservation of confidentiality, integrity and availability of information in the Cyberspace"
- **Cyberspace** as "the complex environment resulting from the information of people, software and services on the Internet by means of technology devices and networks connected to it: which does not exist in any physical form"





## El modelo de las tres líneas del IIA



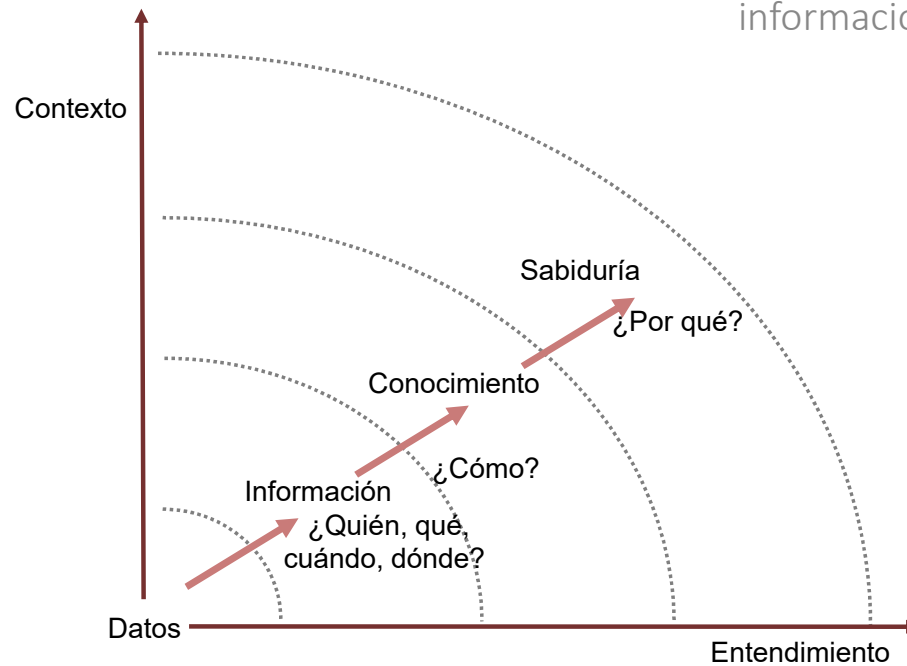
**CLAVE:**

- ↑ Rendición de cuentas, informes
- ↓ Delegar, dirección, recursos, supervisar
- ↔ Alineamiento, comunicación, coordinación, colaboración

# VISIÓN GENERAL

## Información

### • El Modelo DIKW



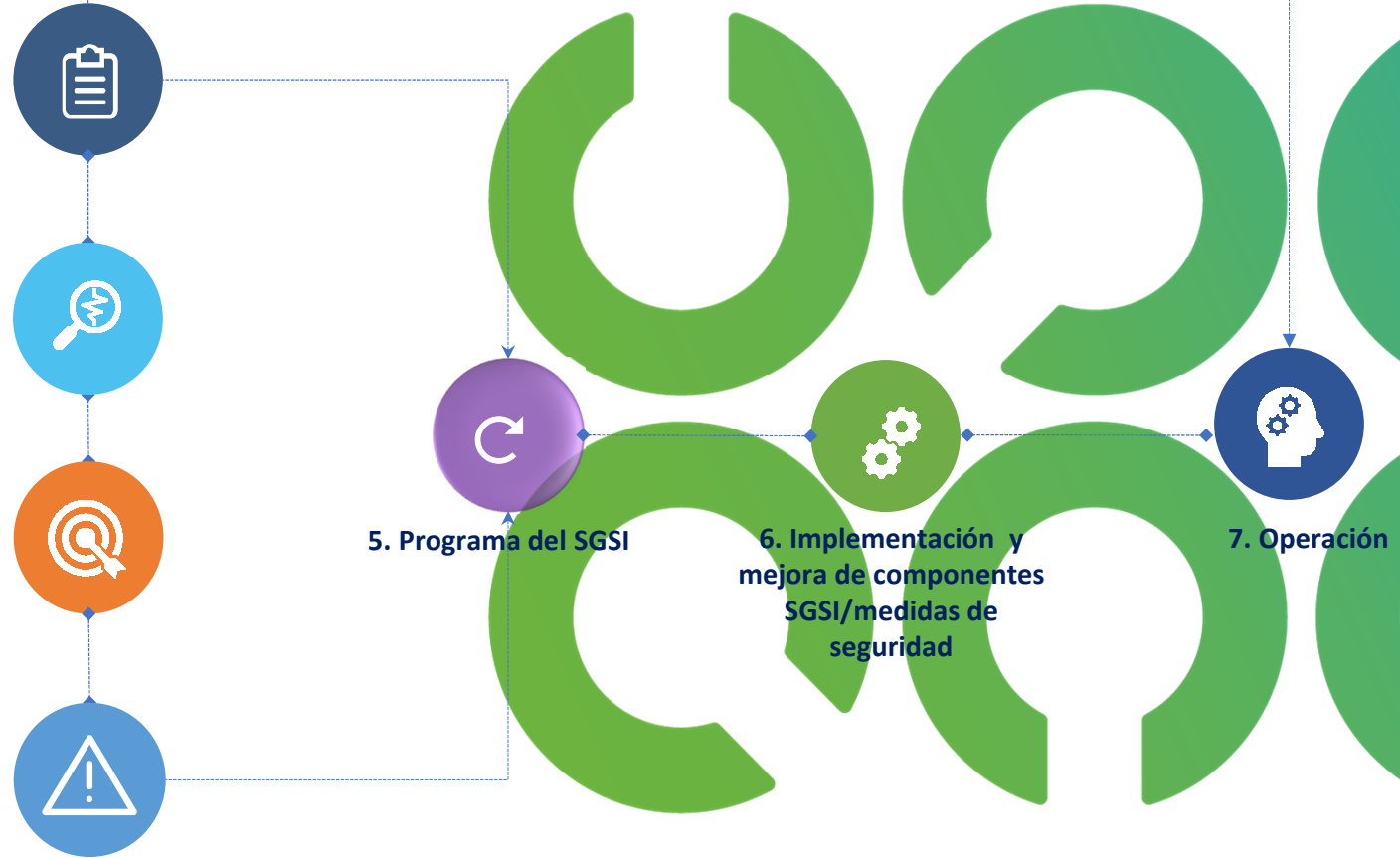
- **Confidencialidad:** es la garantía de acceso a la información de los usuarios que se encuentran autorizados.
- **Integridad:** es la preservación de la información completa y exacta.
- **Disponibilidad:** es la garantía de que el usuario accede a la información que necesita en ese preciso momento.

# SGSI

CONTEXTO

ESTRATEGIA

1. Diagnóstico/Evaluación SGSI
2. Clasificación de Información
3. Inventarios de activos de Información
4. Análisis de amenazas y vulnerabilidades de activos de información críticos





ISACA®

Quito Chapter

[presidencia@isaca.org.ec](mailto:presidencia@isaca.org.ec)

[jclopez@exacta.com.ec](mailto:jclopez@exacta.com.ec)