El Rol del Auditor Interno en los Sistemas de Gestión de Seguridad y Ciberseguridad

Juan Carlos López, PMP,
CISA, CGEIT, CRISC, CISM

presidencia@isaca.org.ec
jclopez@exacta.com.ec
+593 995061566

ISACA Quito Chapter

Juan Carlos López

Consultor con experiencia en definición, implementación y gestión de prácticas de gobierno, administración de riesgos, control interno planeación estratégica, auditoria 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.

ISACA

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.

ISACA
Quito Chapter

ISACA

Ecuador

- Más de 200 miembros
- 19 años de vida
- Entrenamientos en COBIT, CISA, CISM, CRISC. CSX

ISACA
Quito Chapter

Auditorías Informáticas

Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán realizar auditorías, revisiones generales y/o focalizadas internas y externas.

1.1 AUDITORÍA, SISTEMA, PROGRAMA

ISACA
Quito Chapter

Conceptos - Auditoría

1. Audits provide third-party assurance to various stakeholders that the subject matter is free from material misstatement.

2. A systematic process by which a competent, independent person objectively obtains and evaluates evidence regarding assertions[3] about an entity or event, processes, operations, or internal controls for the purpose of forming an opinion and providing a report on the degree to which the assertions conform to an identified set of standards.

ISACA Quito Chapter

Conceptos – Auditoría Interna

Internal **auditing** is an independent, objective *assurance and consulting* activity designed to add value and improve an organization's operations.

EL ROL DEL AUDITOR INTERNO

The role of internal audit is to provide independent assurance that an organisation's risk management, governance and internal control processes are operating effectively.

ISACA Quito Chapter

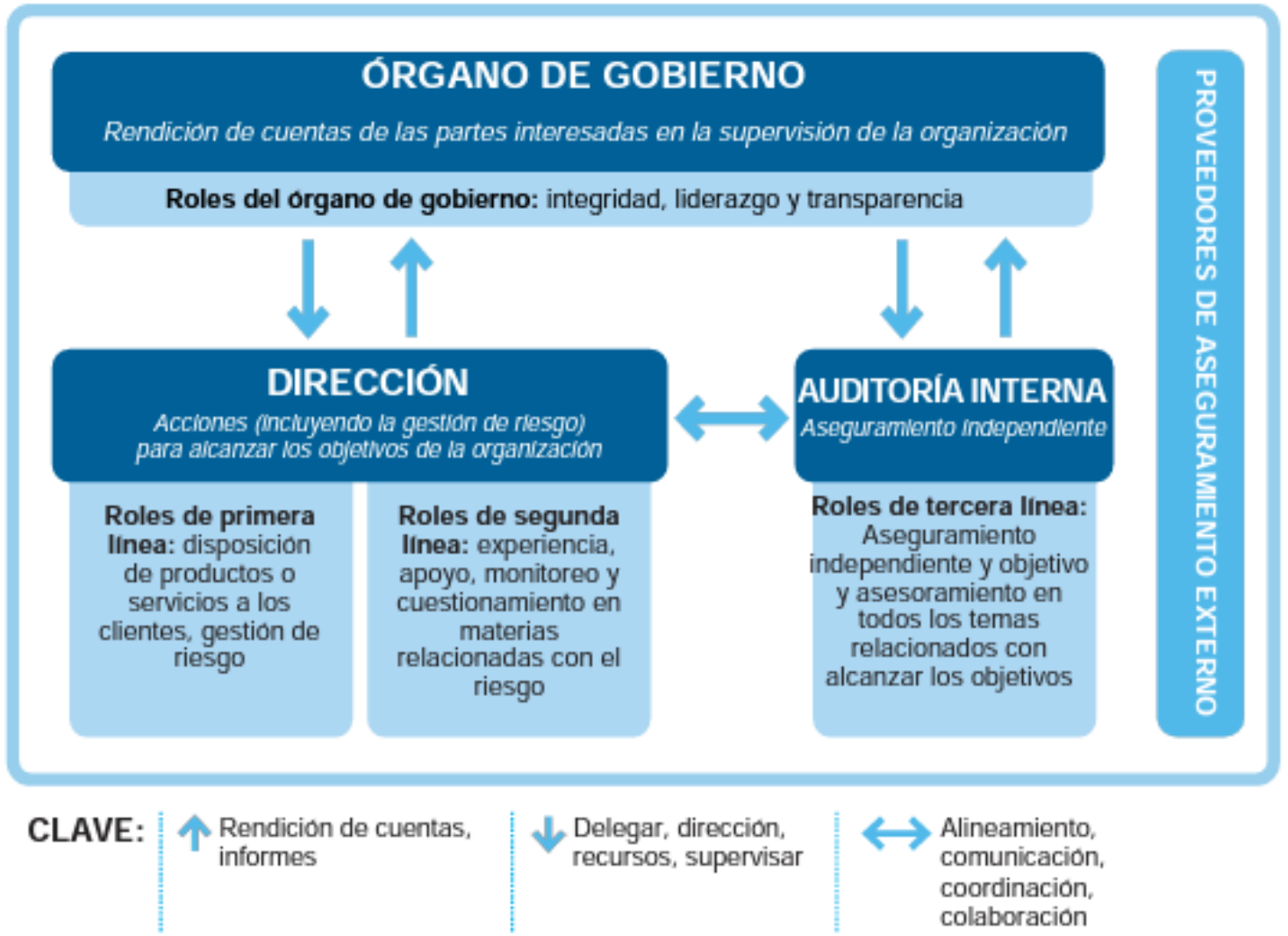
• Role of Audit

- The objectives of a cybersecurity audit are to:
- Provide management with an independent assessment of the effectiveness of cybersecurity processes, policies, procedures, governance and other controls.
- Identify security control concerns that could affect the confidentially, integrity or availability of the information assets due to weaknesses and vulnerabilities in the system of internal controls, including key security controls.
- Evaluate the effectiveness of response and recovery programs.
- Evaluate compliance with cybersecurity relevant laws and regulations.

ISACA Quito Chapter

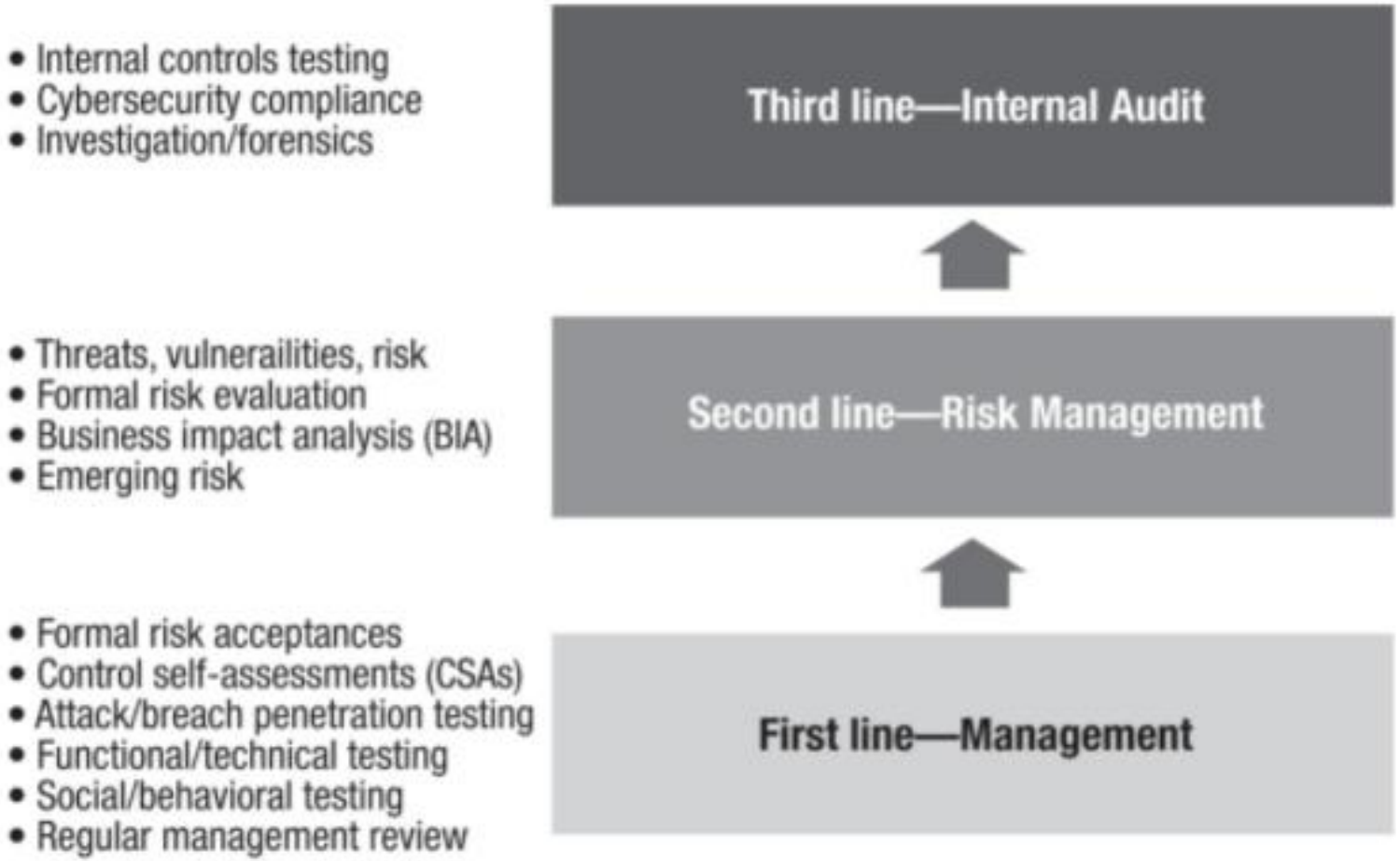
Referencia: Cybersecurity Audit Certificate: Study Guide

- Modelo de las Tres Líneas del IIA



Referencia: The IIA

- Lines of Defense and Typical Review Activity

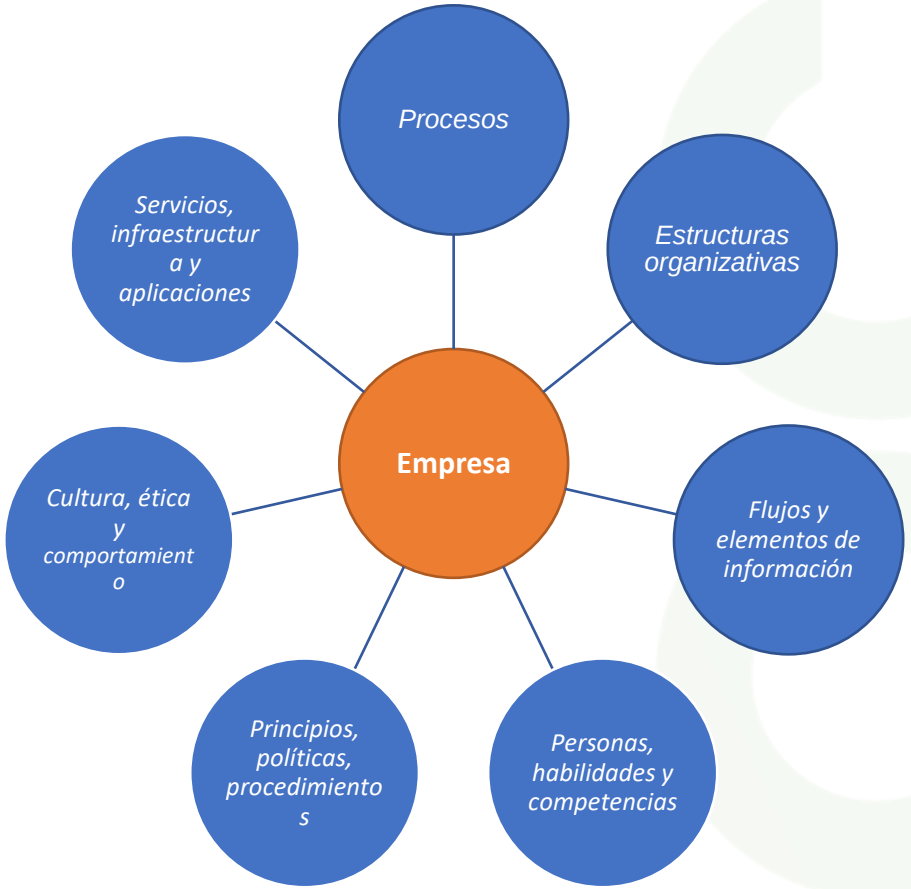


Referencia: Cybersecurity Audit Certificate: Study Guide

¿Que es un Sistema?

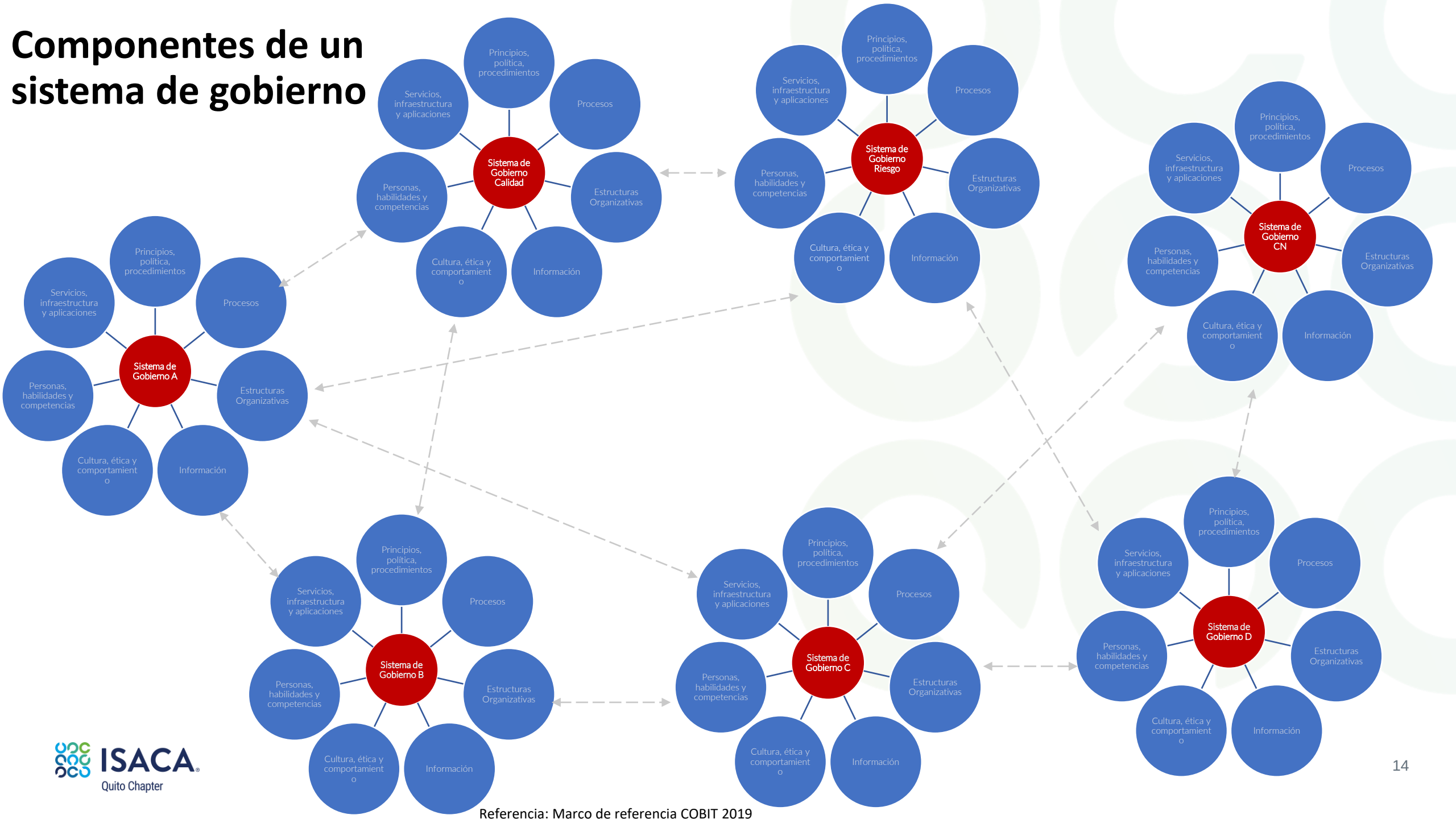
ISACA Quito Chapter

Componentes de un Sistema de Gobierno



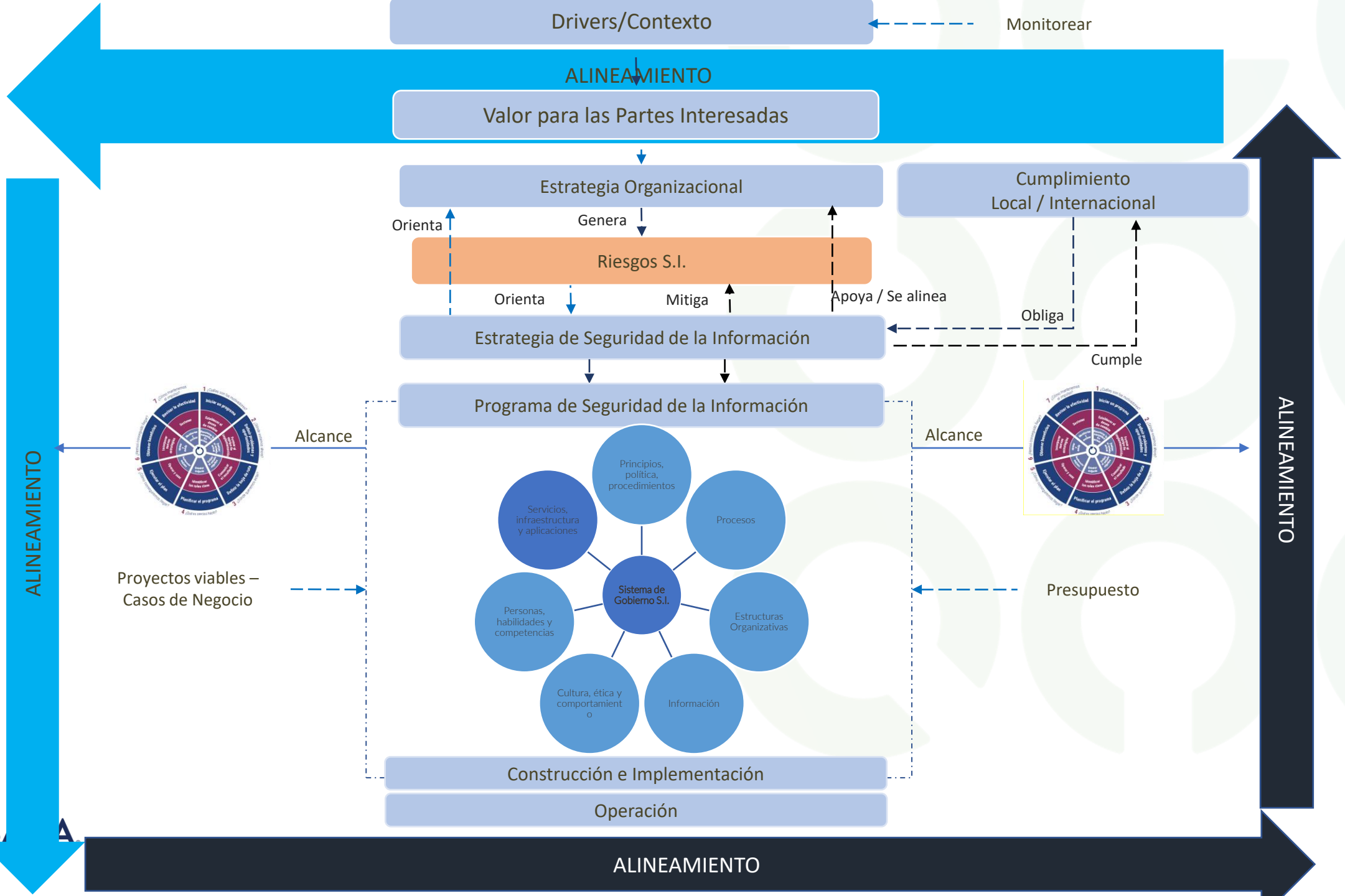
Referencia: Marco de referencia COBIT 2019

Componentes de un sistema de gobierno

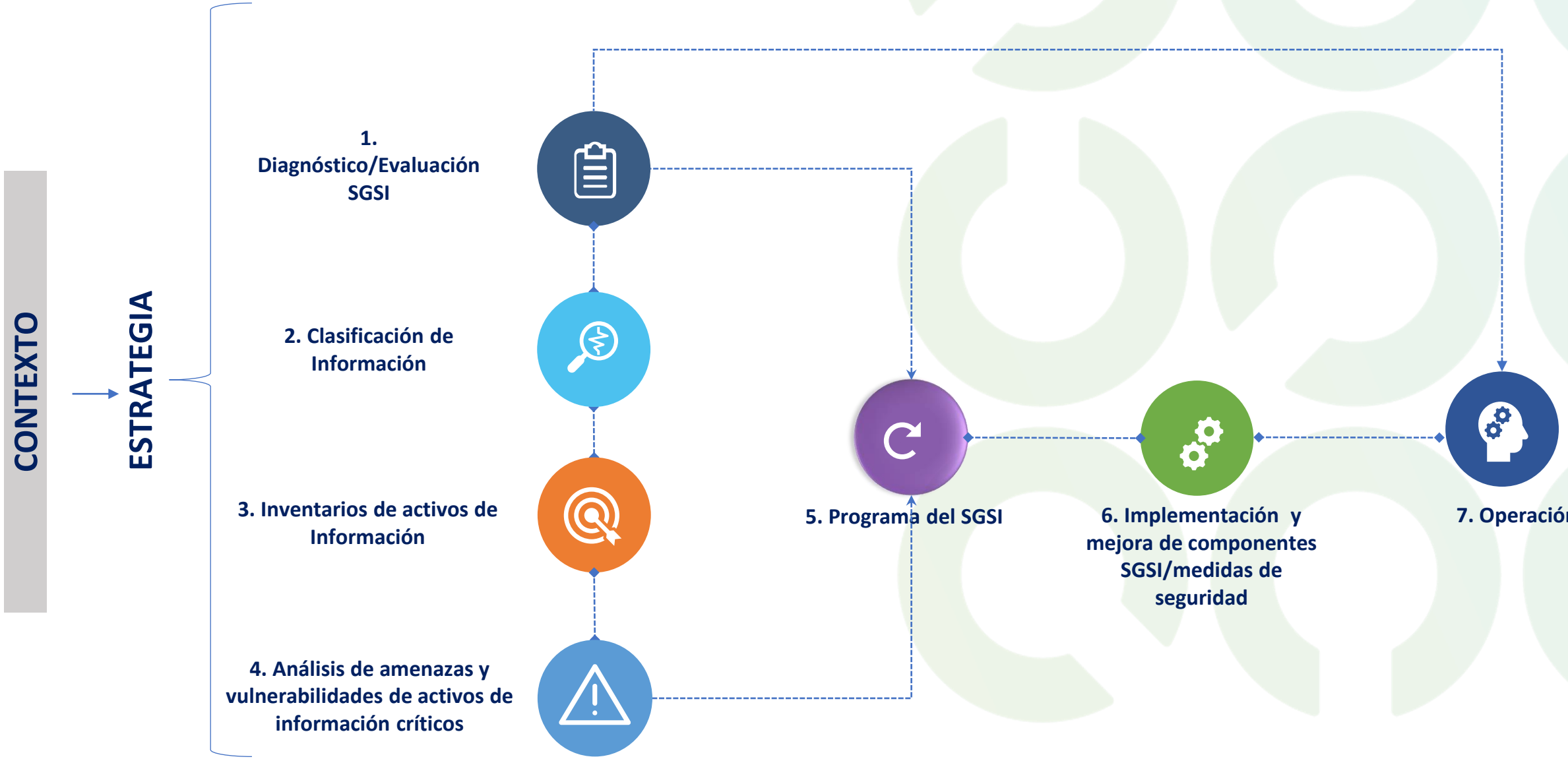


ISACA Quito Chapter

Referencia: Marco de referencia COBIT 2019

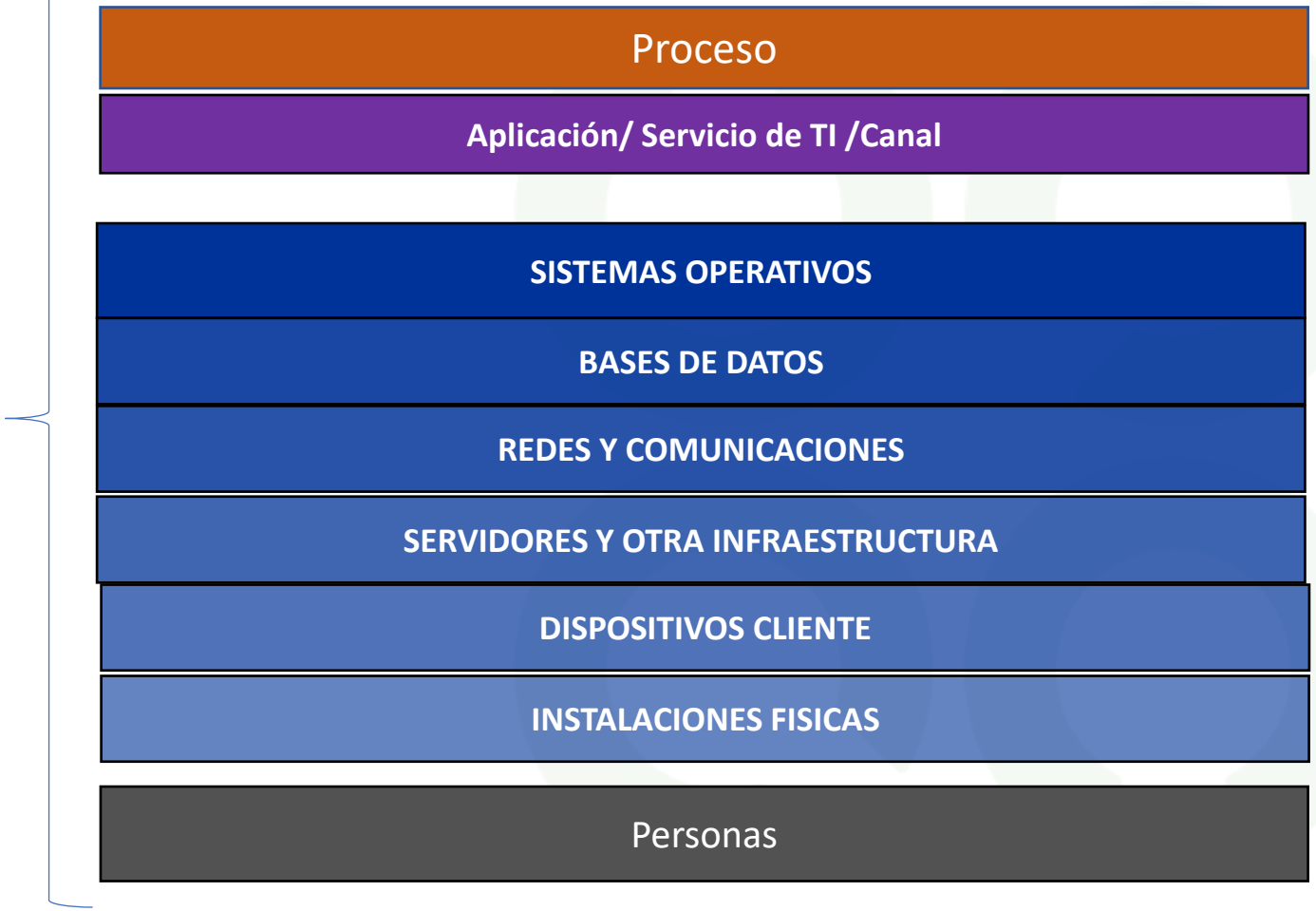

Drivers/Contexto
Monitorear
ALINEAMIENTO
Valor para las Partes Interesadas
Estrategia Organizacional
Cumplimiento
Local / Internacional
Orienta
Genera
Riesgos S.I.
Orienta
Mitiga
Apoya / Se alinea
Obliga
Estrategia de Seguridad de la Información
Cumple
Programa de Seguridad de la Información
Alcance
Alcance
Principios, política, procedimientos
Procesos
Servicios, infraestructura y aplicaciones
Sistema de Gobierno S.I.
Personas, habilidades y competencias
Estructuras Organizativas
Cultura, ética y comportamiento
Información
Proyectos viables – Casos de Negocio
Presupuesto
Construcción e Implementación
Operación
ALINEAMIENTO
ALINEAMIENTO
ALINEAMIENTO

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
5. Programa del SGSI
6. Implementación y mejora de componentes SGSI/medidas de seguridad
7. Operación

Gobierno y Gestión

- **Para Auditar debemos identificar el Sistema a Auditar – Alcance/Subject Matter**



Referencia: Marco de referencia COBIT 2019

1.3 SEGURIDAD Y CIBERSEGURIDAD

ISACA
Quito Chapter

• 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.

ISACA Quito Chapter

Referencia: ISO27001

- Security Organization Goals And Objectives

Referencia: Cybersecurity Audit Certificate: Study Guide

Auditoría en Detalle

ISACA
Quito Chapter

SGSI

CONTEXTO

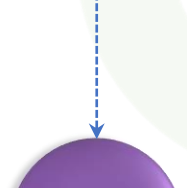
ESTRATEGIA

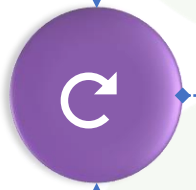
1. Diagnóstico/Evaluación SGSI

2. Clasificación de Información

3. Inventarios de activos de Información

4. Análisis de amenazas y vulnerabilidades de activos de información críticos





5. Programa del SGSI

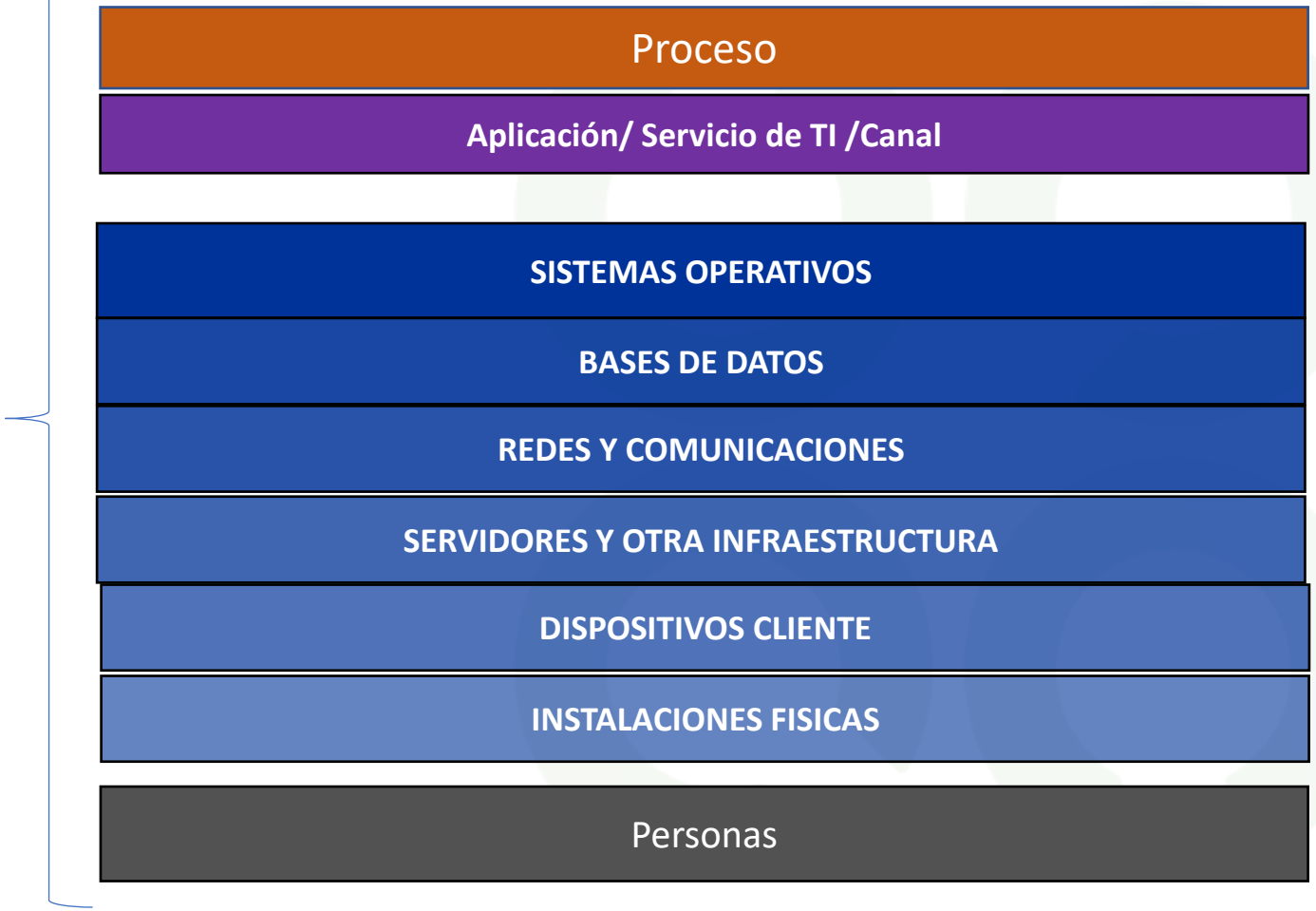
6. Implementación y mejora de componentes SGSI/medidas de seguridad

7. Operación

ISACA Quito Chapter

Gobierno y Gestión

- **Para Auditar debemos identificar el Sistema a Auditar – Alcance/Subject Matter**



Referencia: Marco de referencia COBIT 2019

Estructura de la Norma ISO 27001

- 0. Introducción
- 1. Alcance
- 2. Referencias normativas
- 3. Términos y definiciones

NO OBLIGATORIO

PLAN

4 Contexto de la Organización
- Entendimiento de la organización y su contexto
- Expectativas de las partes interesadas.
- Alcance del ISMS.

5 Liderazgo
- Liderazgo y compromiso de la Alta Dirección.
- Políticas.
- Organización de los roles, responsabilidades y autoridades.

6 Planeación
- Cómo abordar riesgos y oportunidades.

7 Soporte
- Recursos.
- Competencias.
- Conciencia.
- Comunicación.
- Información documentada.

DO

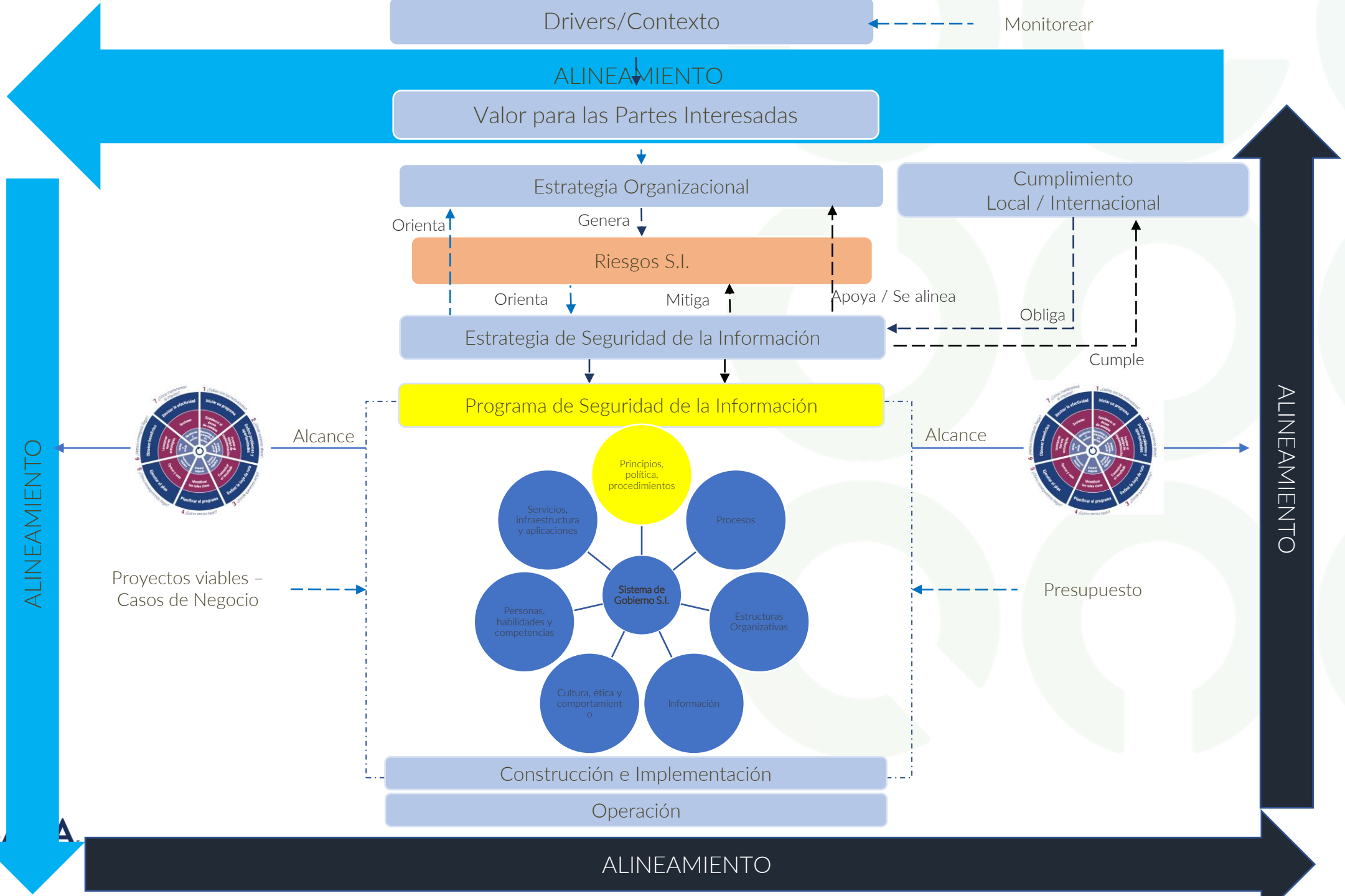
8 Operación
- Evaluación de riesgos de la seguridad de la información.
- Manejo de riesgos de la seguridad de la información.

CHECK

9 Evaluación del desempeño
- Evaluación de riesgos de la seguridad de la información.
- Manejo de riesgos de la seguridad de la información.

ACT

10 Mejora
- Monitoreo y auditorías internas.
- Revisión de la alta dirección.


Drivers/Contexto
Monitorear
ALINEAMIENTO
Valor para las Partes Interesadas
Estrategia Organizacional
Cumplimiento
Local / Internacional
Orienta
Genera
Riesgos S.I.
Orienta
Mitiga
Apoya / Se alinea
Obliga
Estrategia de Seguridad de la Información
Cumple
Programa de Seguridad de la Información
Alcance
Alcance
Principios, política, procedimientos
Servicios, infraestructura y aplicaciones
Procesos
Personas, habilidades y competencias
Sistema de Gobierno S.I.
Estructuras Organizativas
Cultura, ética y comportamiento
Información
Proyectos viables – Casos de Negocio
Presupuesto
Construcción e Implementación
Operación
ALINEAMIENTO
ALINEAMIENTO
ALINEAMIENTO