Cumplimiento de la normativa de la SEPS respecto de la Seguridad de la Información, un enfoque práctico. Enfoque en el artículo 10.

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

presidencia@isaca.org.ec
jclopez@exacta.com.ec

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.

Objetivo

Proponer un enfoque de implementación práctico del artículo 10 de la Norma de Control de Seguridad de la Información

Temario

1. *Repaso de lo que es un SGSI*
2. *Conceptos básicos de gestión de información y datos*
   - Dominios de Datos
   - Tipos de Información
3. *Activos de Información*
   - Como identificar ACTIVOS
   - Como Valorar activos

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
- 20 años de vida
- Entrenamientos en COBIT, CISA, CISM, CRISC. CSX

ISACA
Quito Chapter

PLANIFICACIÓN DE CAPACITACIONES

CISM Certified Information Security Manager An ISACA® Certification

10 de marzo/2023
(10, 11, 17, 18, 24, 25, 31
de marzo y 1 de abril)

CISA Certified Information Systems Auditor An ISACA® Certification

14 de abril/2023
(14, 15, 21, 22 de abril, 5,
6, 12, 13, 19, 20 de mayo)

CDPSE Certified Data Privacy Solutions Engineer An ISACA® Certification

5 de mayo /2023
(5, 6, 12, 13, 19, 20 de
mayo, 2, 3 de junio)

CSX™ CYBERSECURITY NEXUS

29 de mayo/2023
(29, 30, 31 de mayo,
1, 2 de junio)

CRISC Certified in Risk and Information Systems Control An ISACA® Certification

2 de junio/2023
(2, 3, 9, 10, 16, 17, 23,
24 de junio)

ISACA Quito Chapter

ISACA®
Quito Chapter

La Norma

Artículo 10.- Sistema de Gestión de Seguridad de la Información (SGSI).- Las entidades, empresas y la CONAFIPS que conforman este régimen, deberán implementar y mantener un SGSI, orientado a garantizar la adecuada gestión de seguridad de la información, con base en la serie de estándares ISO/IEC 27000, y acorde a la normativa legal vigente.

Para establecer el alcance del SGSI, además de lo previsto en el artículo anterior y la serie de estándares ISO/IEC 27000, deberán considerar:

1) Definición de tipos de información con criterios de integridad, confidencialidad y disponibilidad; y,
2) Identificación y clasificación de activos de información, que contendrá:
   a) Personas;
   b) Procesos agregadores de valor y/o catalogados como sensibles o críticos;
   c) Unidades intervinientes en los procesos;
   d) Infraestructura tecnológica;
   e) Ubicaciones físicas y puntos de atención, oficina matriz, sucursales, agencias, puntos móviles, corresponsales solidarios; y,
   f) Relaciones con personas naturales y/o jurídicas que pudieren acceder a información crítica o sensible.

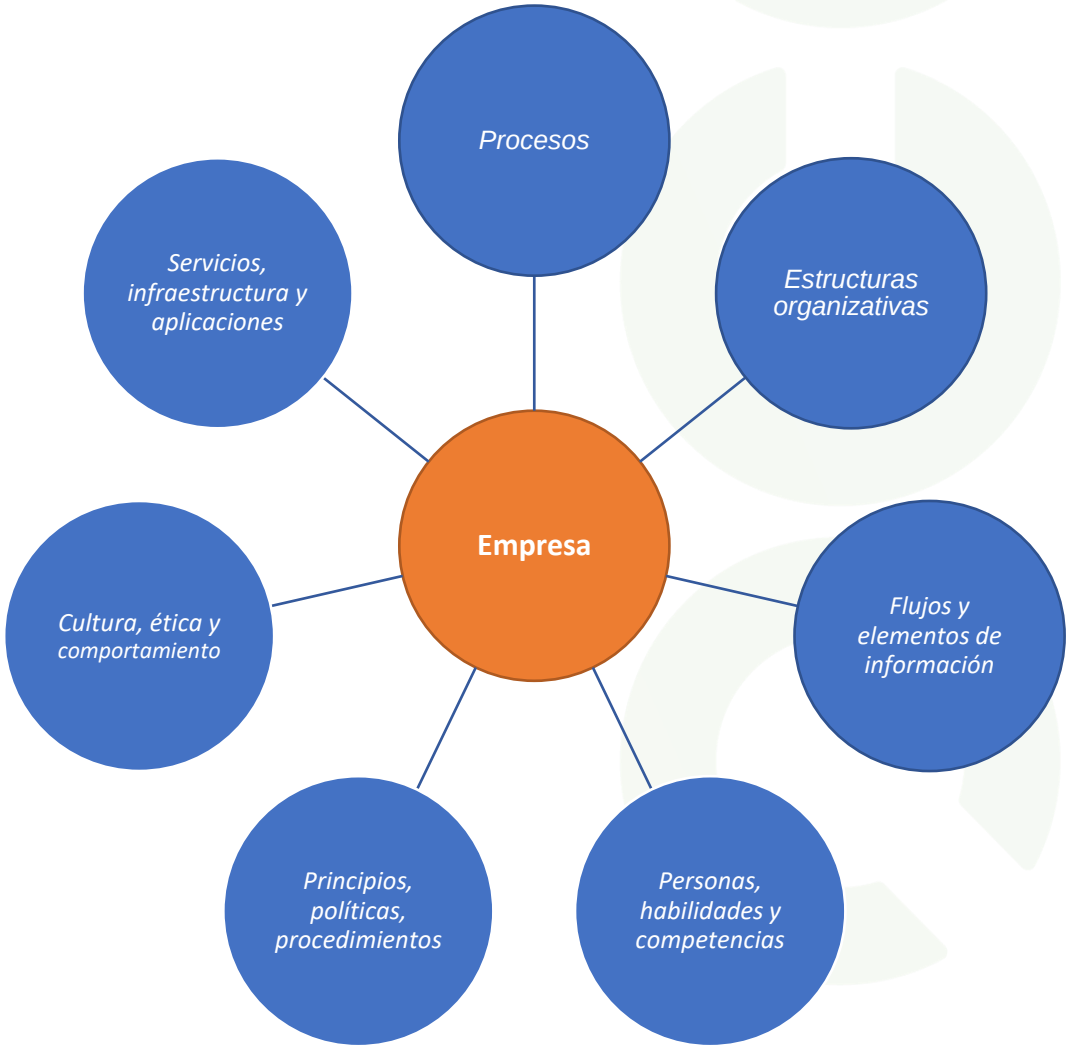
4.3 Determinar el alcance del sistema de gestión de seguridad de la información

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance.

Cuando se determina este alcance, la organización debe considerar:
a) las cuestiones externas e internas a las que se hace referencia en 4.1;
b) los requisitos mencionados en 4.2; y
c) las interfaces y las dependencias entre las actividades realizadas por la organización, y las que son realizadas por otras organizaciones.
El alcance debe estar disponible como información documentada.

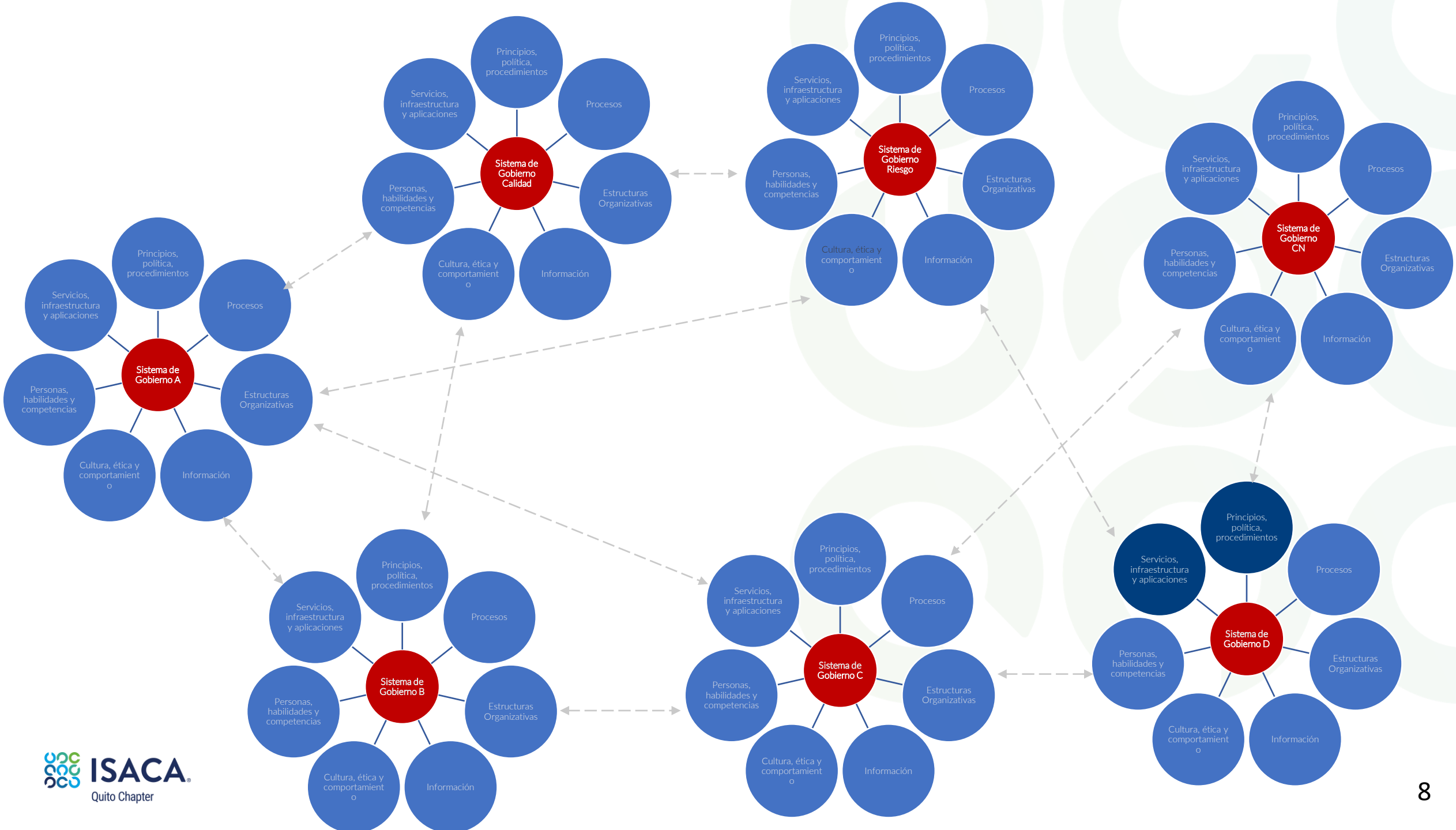
- Que es un Sistema?

Componentes de un sistema de gobierno



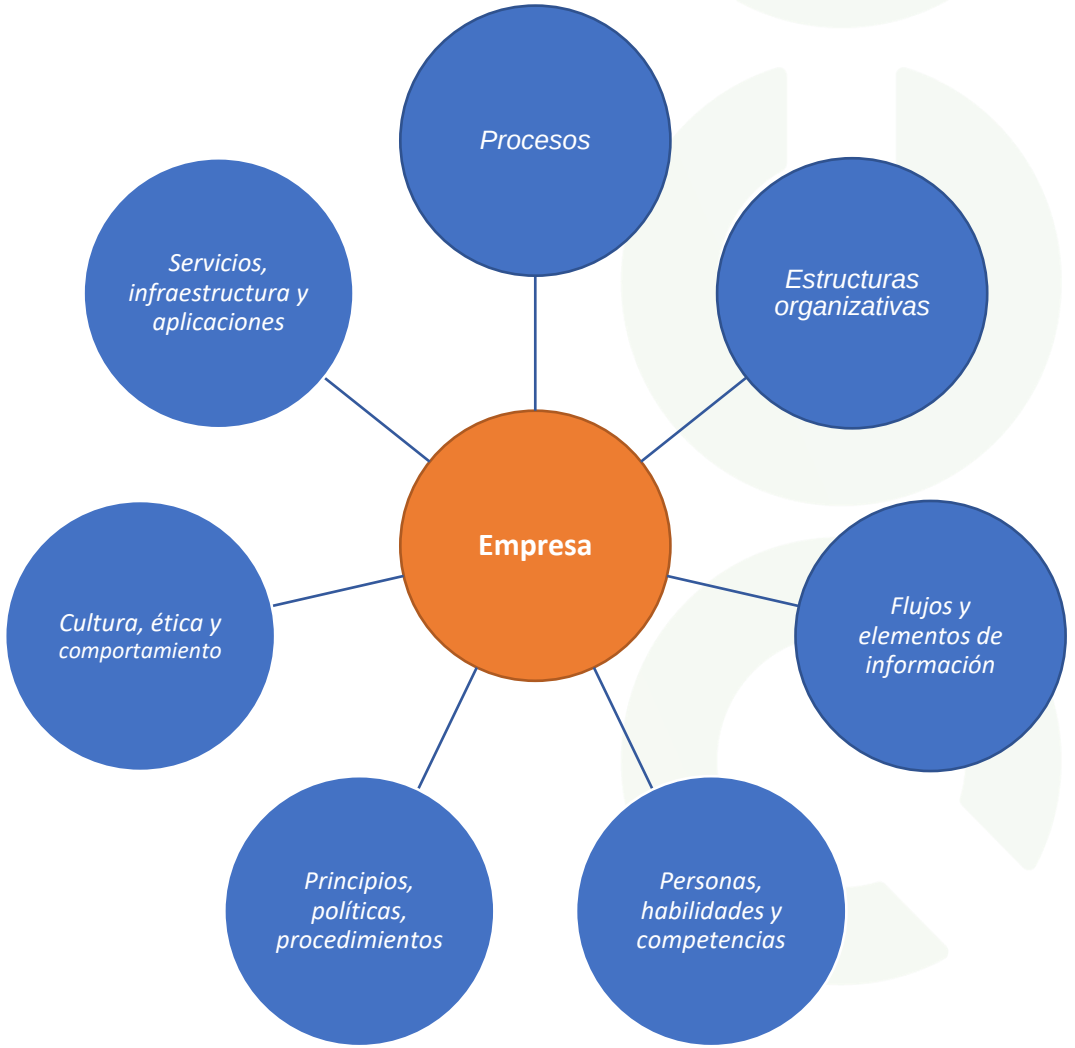
ISACA Quito Chapter

11 *Referencia: Marco de referencia COBIT 2019: Conceptos básicos: Sistemas de gobierno y componentes, Capítulo 4*



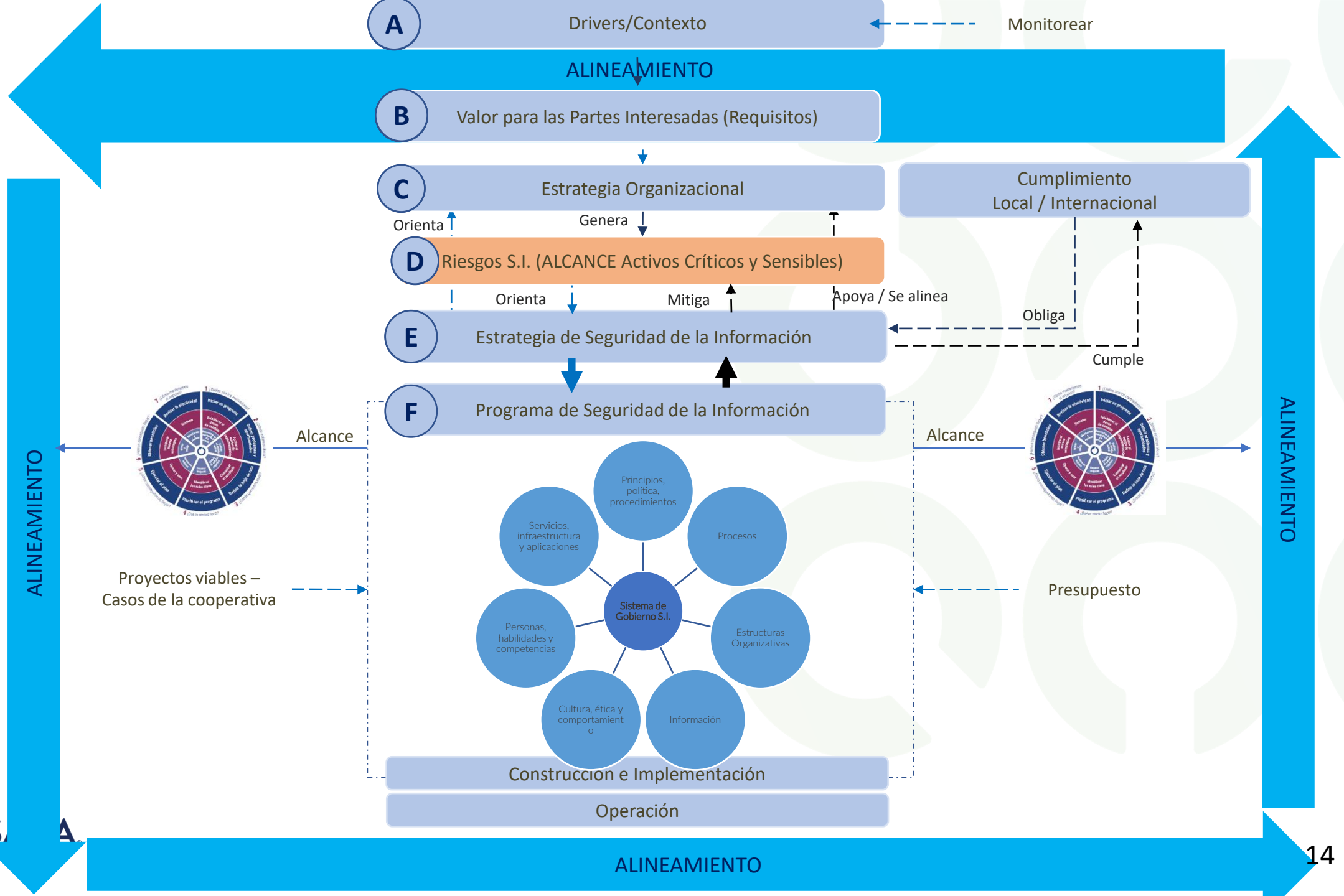
ISACA Quito Chapter

Componentes de un sistema de gobierno



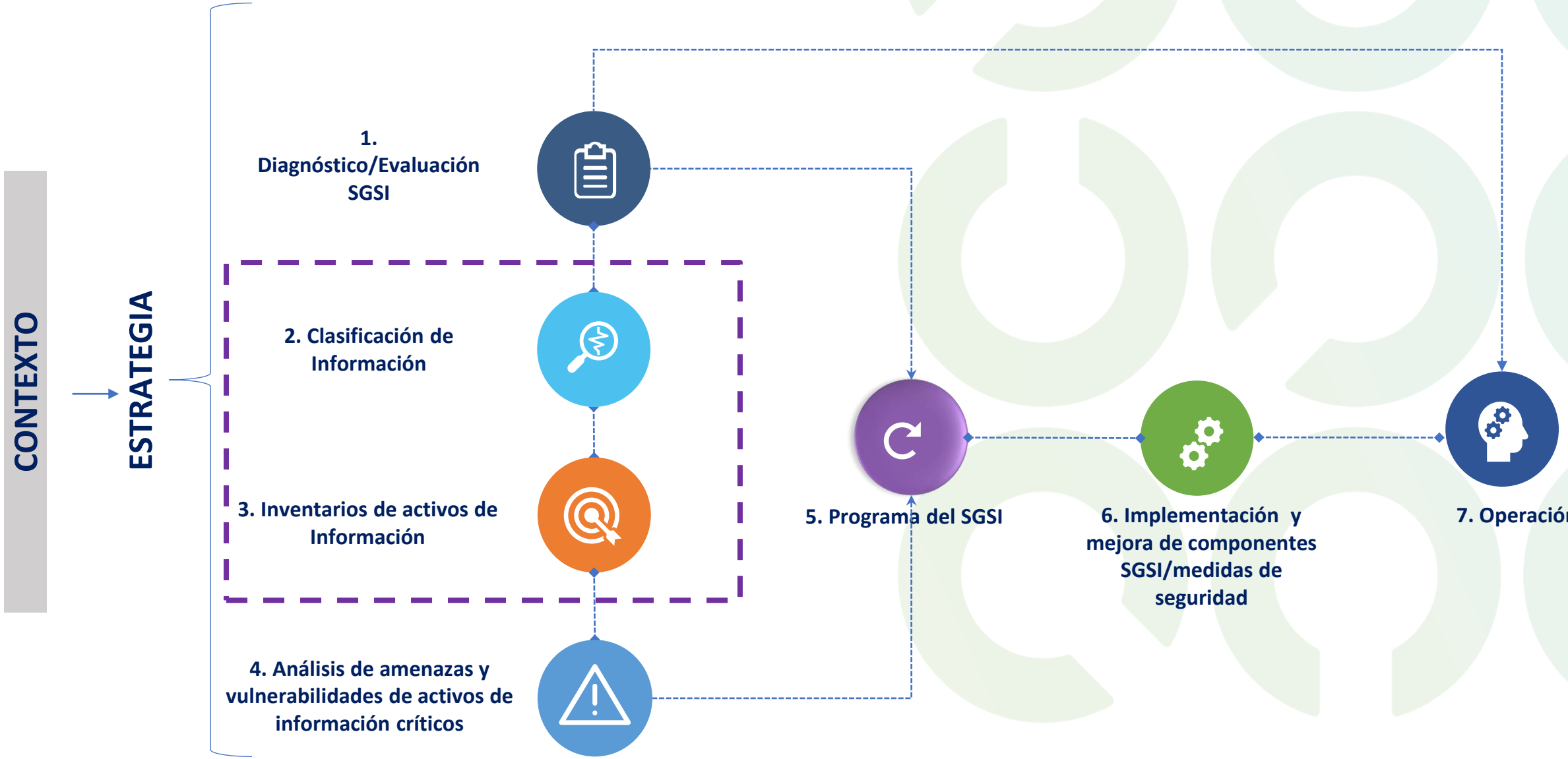
ISACA Quito Chapter

Referencia: Marco de referencia COBIT 2019: Conceptos básicos: Sistemas de gobierno y componentes, Capítulo 4


A
Drivers/Contexto
Monitorear
ALINEAMIENTO
B
Valor para las Partes Interesadas (Requisitos)
C
Estrategia Organizacional
Cumplimiento
Local / Internacional
Orienta
Genera
D
Riesgos S.I. (ALCANCE Activos Críticos y Sensibles)
Orienta
Mitiga
Apoya / Se alinea
Obliga
E
Estrategia de Seguridad de la Información
Cumple
F
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 la cooperativa
Presupuesto
Construcción e Implementación
Operación
ALINEAMIENTO
ALINEAMIENTO
ALINEAMIENTO

14

SGSI

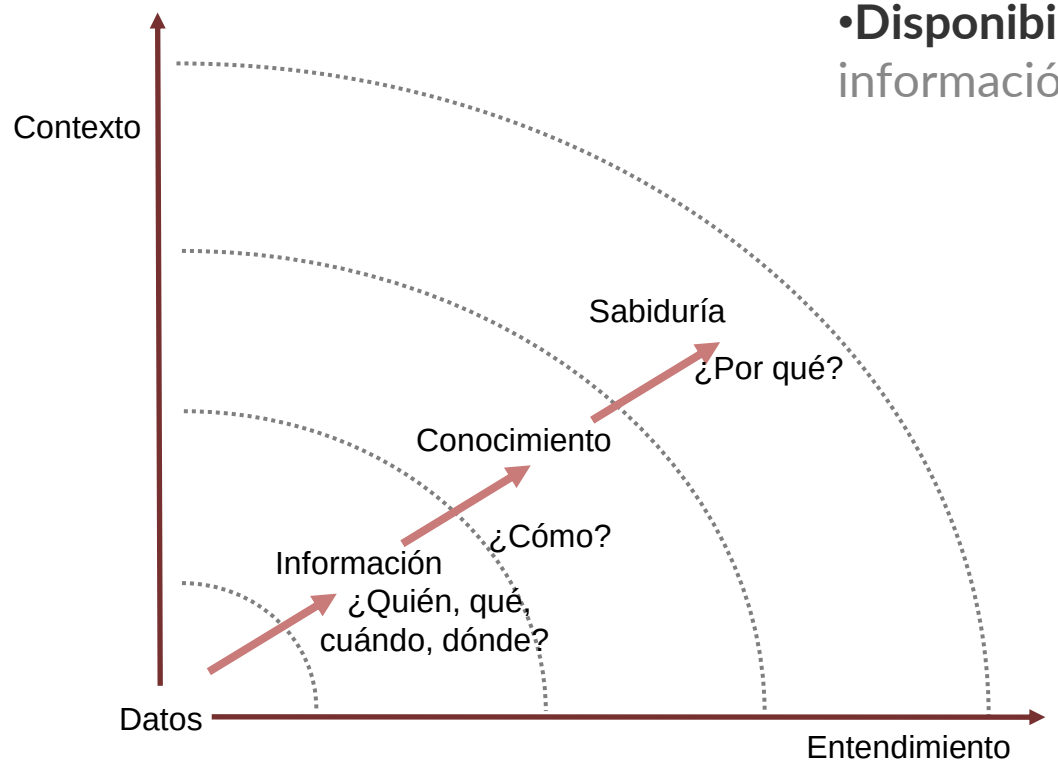

CONTEXTO
ESTRATEGIA
1. Diagnóstico/Evaluación SGSI
2. Clasificación de Información
3. Inventarios de activos de Información
4. Análisis de amenazas y vulnerabilidades de activos de información críticos
5. Programa del SGSI
6. Implementación y mejora de componentes SGSI/medidas de seguridad
7. Operación

- Security Organization Goals And Objectives

Referencia: Cybersecurity Audit Certificate: Study Guide

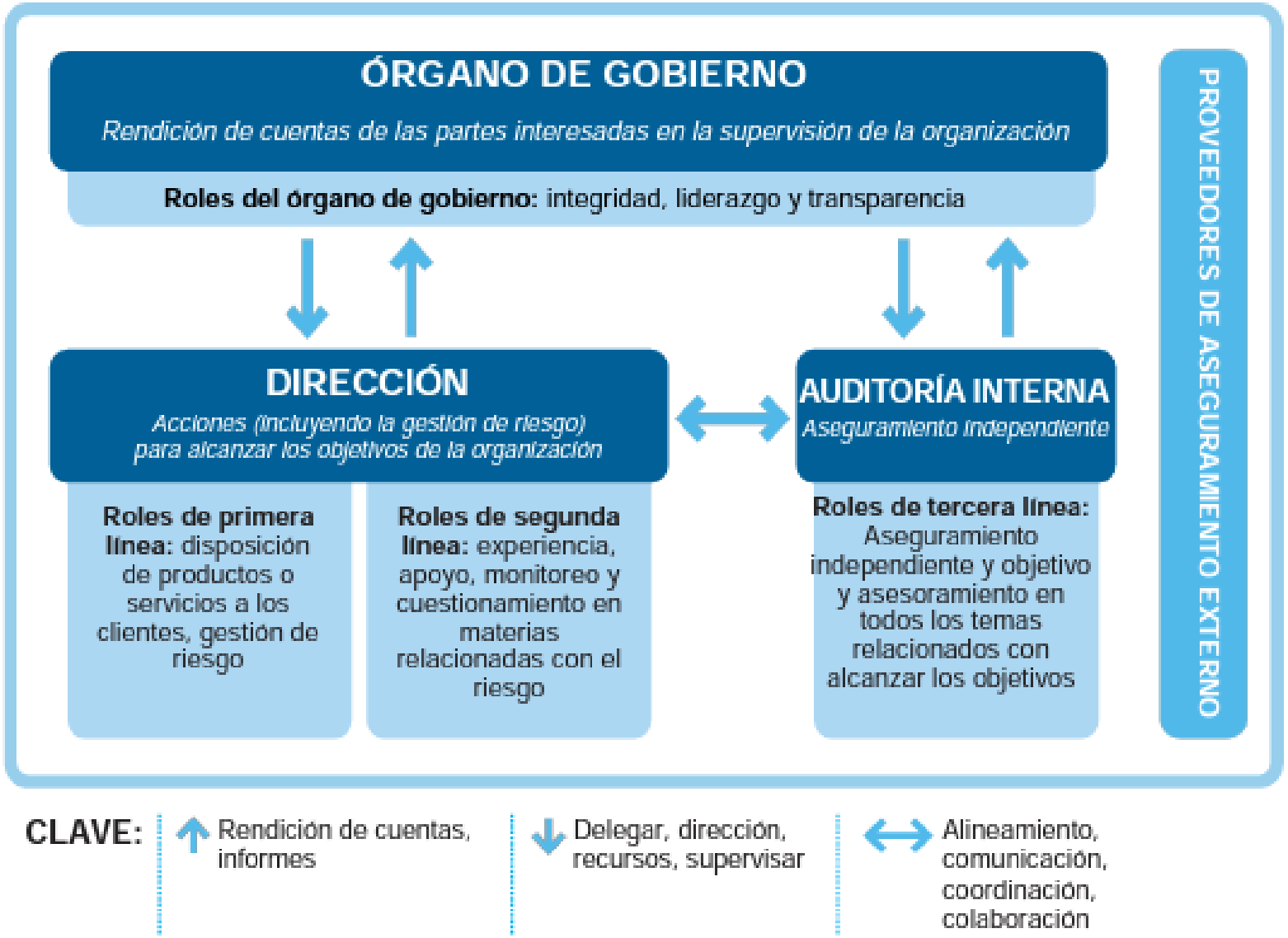
VISIÓN GENERAL
Información

- El Modelo DIKW



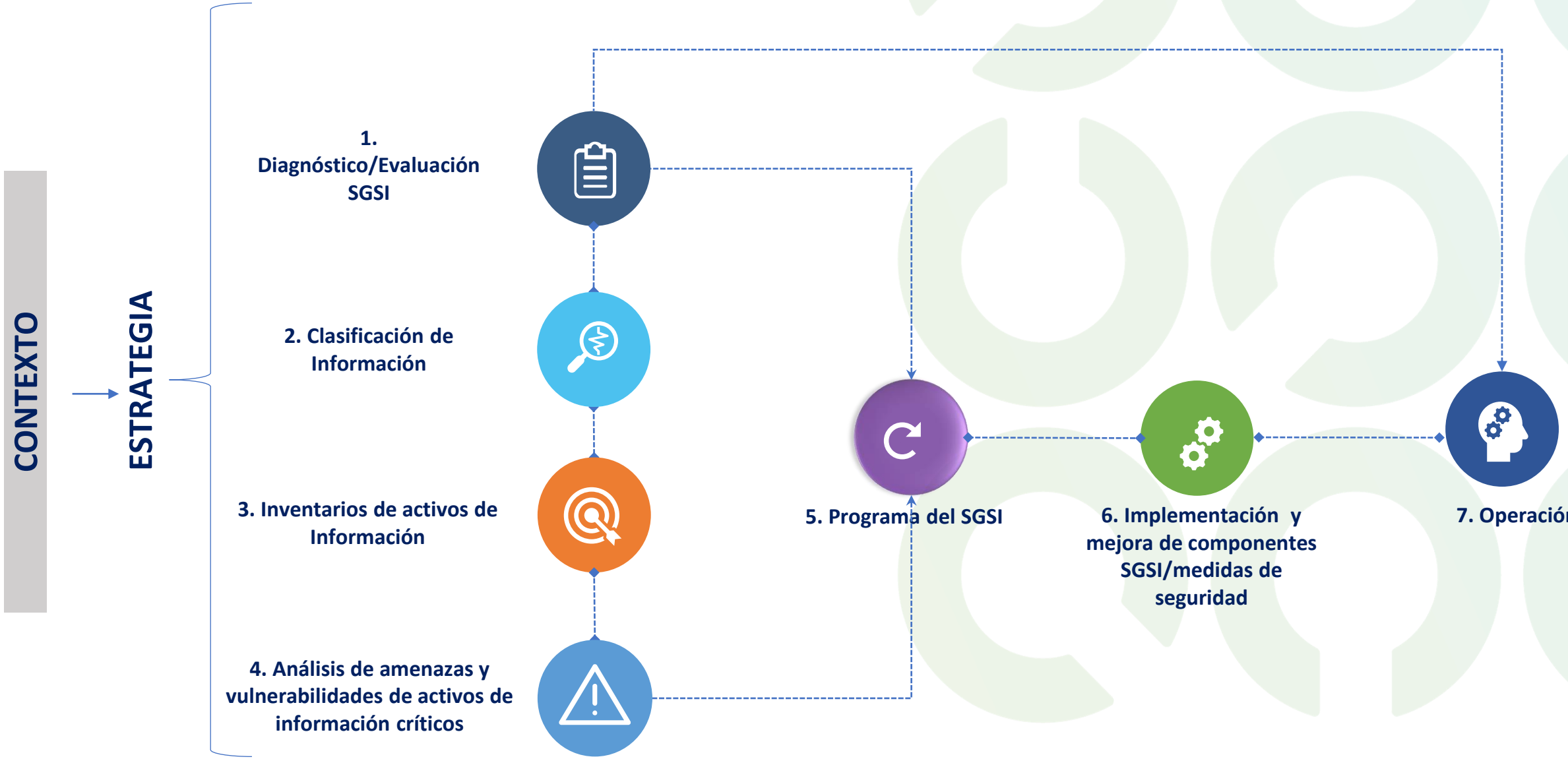
- **Confidencialidad:** es la garantía de acceso a la información de los usuarios que se encuentran autorizados.
- **Integridad:** es la preservación de la información completa y exacta.
- **Disponibilidad:** es la garantía de que el usuario accede a la información que necesita en ese preciso momento.

El modelo de las tres líneas del IIA



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

PLANIFICACIÓN DE CAPACITACIONES

CISM Certified Information Security Manager An ISACA® Certification

10 de marzo/2023
(10, 11, 17, 18, 24, 25, 31
de marzo y 1 de abril)

CISA Certified Information Systems Auditor An ISACA® Certification

14 de abril/2023
(14, 15, 21, 22 de abril, 5,
6, 12, 13, 19, 20 de mayo)

CDPSE Certified Data Privacy Solutions Engineer An ISACA® Certification

5 de mayo /2023
(5, 6, 12, 13, 19, 20 de
mayo, 2, 3 de junio)

CSX™ CYBERSECURITY NEXUS

29 de mayo/2023
(29, 30, 31 de mayo,
1, 2 de junio)

CRISC Certified in Risk and Information Systems Control An ISACA® Certification

2 de junio/2023
(2, 3, 9, 10, 16, 17, 23,
24 de junio)

ISACA Quito Chapter

ISACA®

Quito Chapter

presidencia@isaca.org.ec
jclopez@exacta.com.ec