CONTROLES GENERALES DE TI

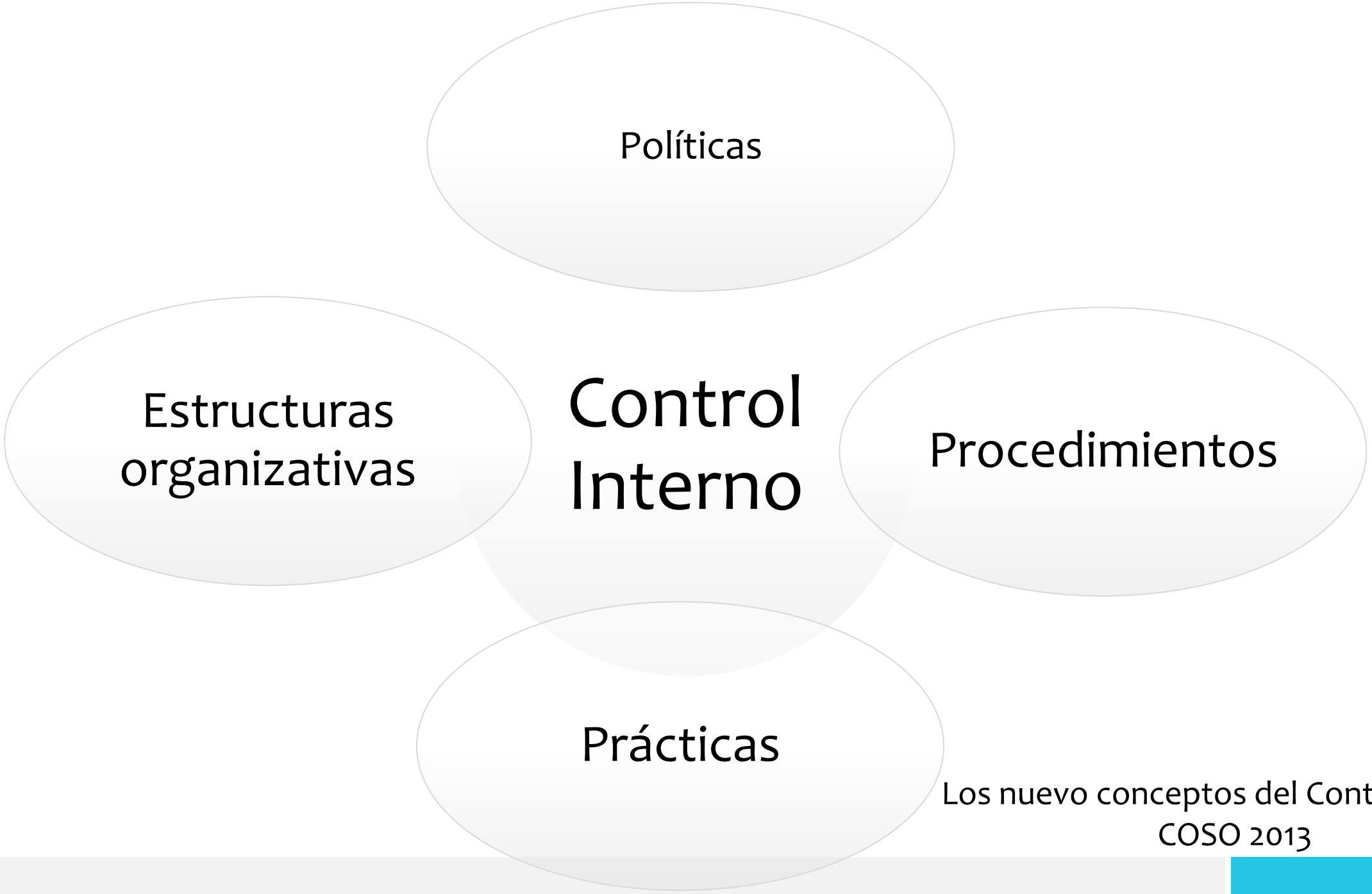
Josué F. Chete

CISA, CLRM, SFPC

Control Interno

Es un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos.

Los nuevo conceptos del Control Interno
COSO 2013



Los nuevo conceptos del Control Interno COSO 2013

Controles Generales de TI - Definición

Los controles generales, incluyen políticas y prácticas (tareas y actividades) que son establecidos por la gerencia para proveer una certeza razonable de que se alcanzarán objetivos específicos. Son aplicables a todas las áreas de la organización, incluyendo infraestructura y servicios de soporte de TI.

Manual de Preparación CISA

Auditoría de Sistemas de Información ¿Qué es?

Revisión y evaluación de los controles y **sistemas** de informática, así como la utilización, eficiencia y seguridad (CID), en el procesamiento de la información de una organización.


1
AVAILABILITY
INFORMATION SECURITY
2
INTEGRITY
3
CONFIDENTIALITY

Proceso de Auditoria de Sistemas de Información

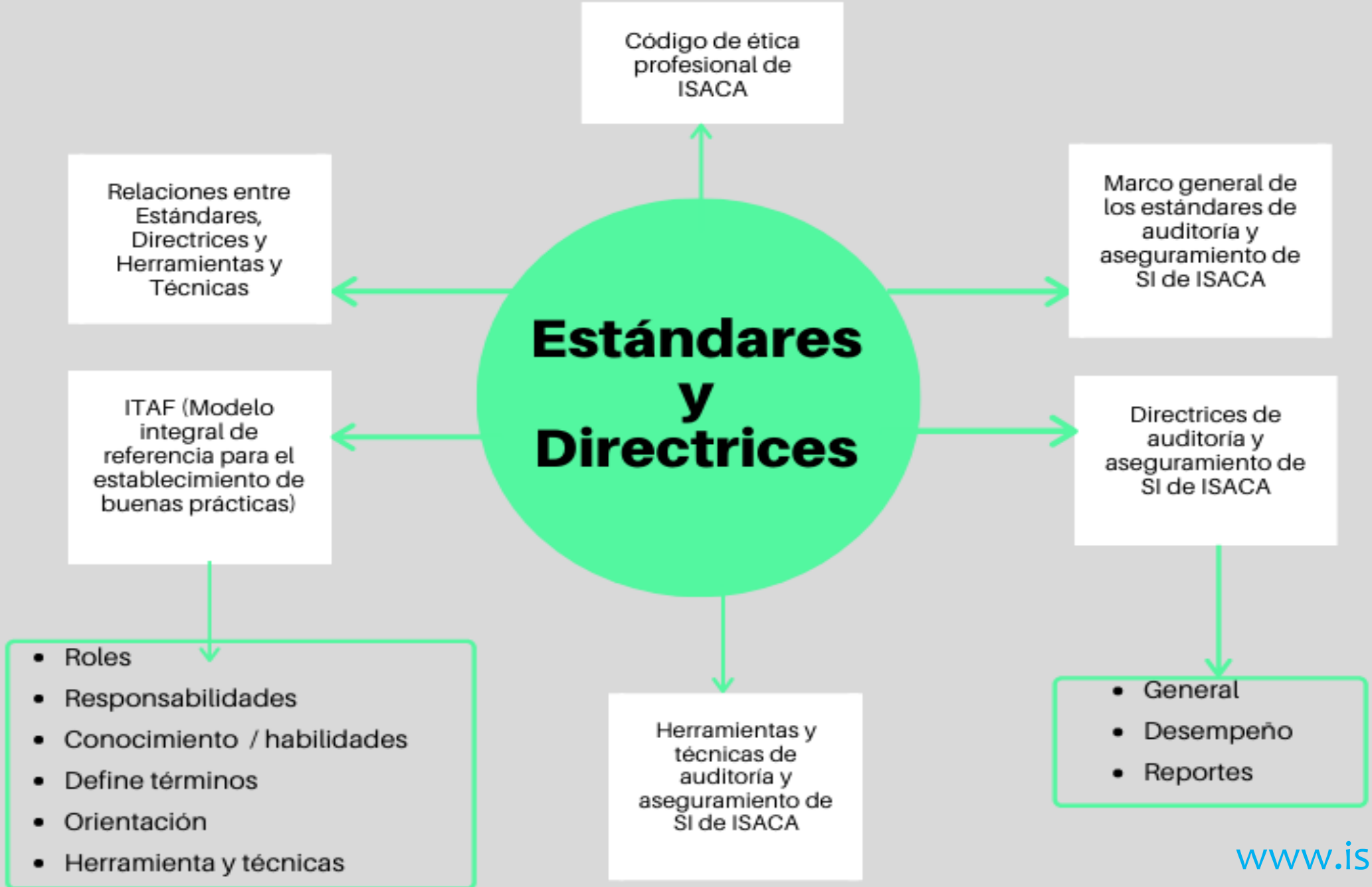
Gobierno de TI

Operación y Servicio

Adquisición y Desarrollo

Proteción de Activos

Estándares y Directrices



www.isaca.org

EL PROCESO DE LA AUDITORÍA - GLOBAL

Conocer el negocio

- Objetivos estratégicos (Misión, Visión, Valores)
- Normas y regulaciones
- Sector donde se desarrolla
- Procesos / Productos
- Ambiente interno
- Roles y funciones
- Clientes
- Partes Interesadas

Evaluación de riesgos

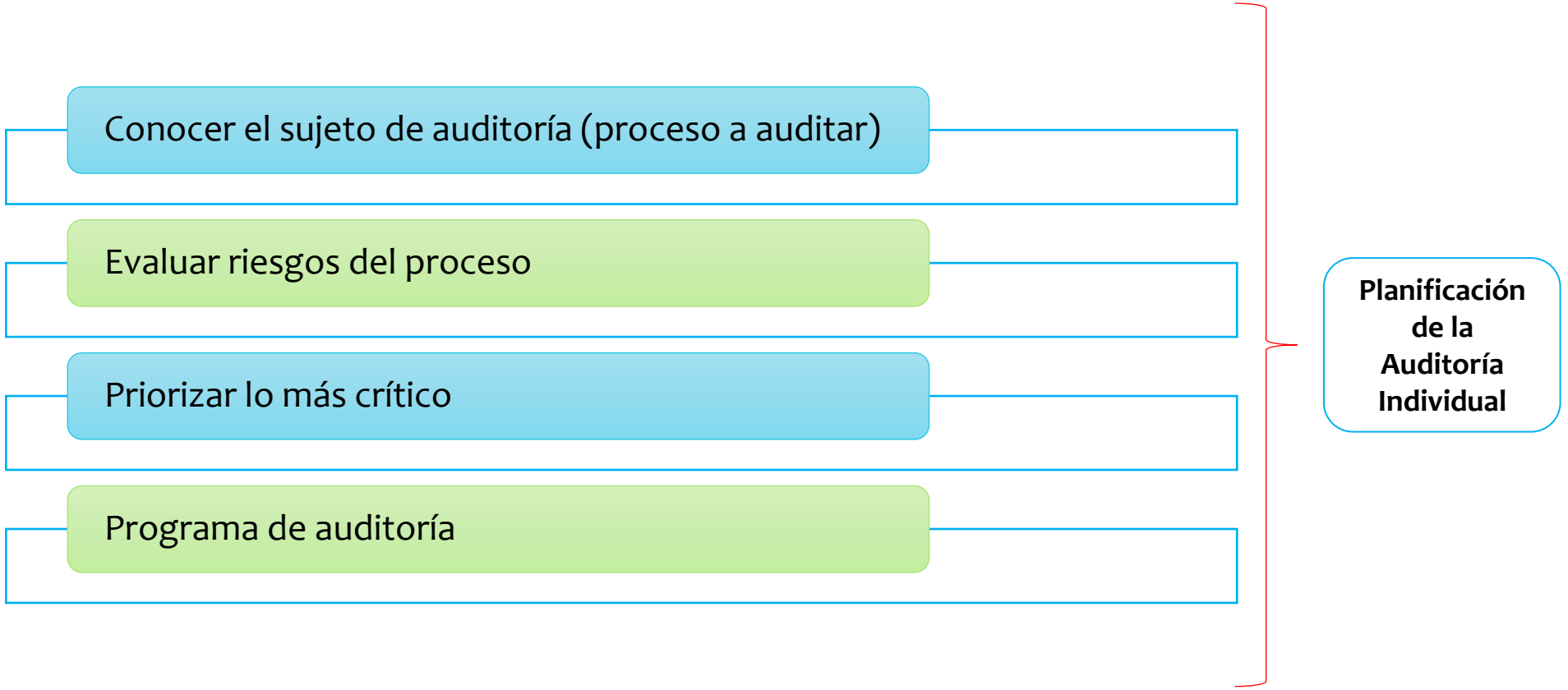
- Identificación
- Medición
- Matriz de riesgos
- Control interno

Priorizar por criticidad (Objetivos, Procesos, áreas)

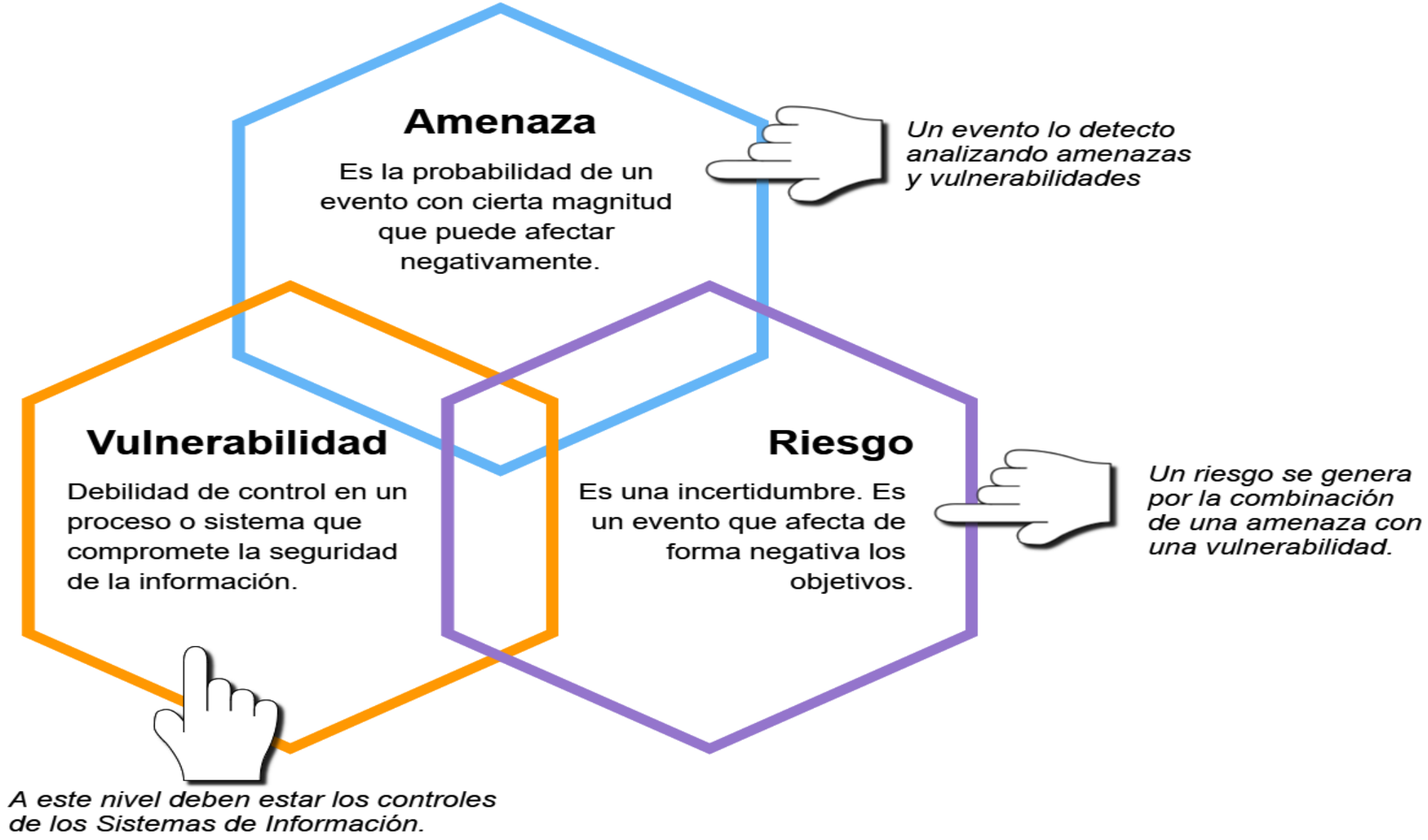
Plan de auditoría basado en riesgos

Planificación de la Auditoría

EL PROCESO DE LA AUDITORÍA - ESPECÍFICO



ANÁLISIS DE RIESGOS



Proceso de Auditoria de Sistemas de Información

EVALUANDO LA *GESTIÓN* DE TI

Gobierno y Gestión

- Plan Estratégico de TI
- Políticas de TI
- Estructura organizacional existente
- Documentación de procesos
- Infraestructura tecnológica
- Segregación de funciones
- Proyectos críticos en desarrollo
- Cambios importantes (Organizacional, Infraestructura, software)

Controles Generales de Tecnología

- Adquisición, desarrollo y cambios
- Operación, mantenimiento y soporte
- Protección de activos

Procesos del CISA

Esto es lo mínimo que debe de conocer el Auditor.

EVALUANDO LA *GESTIÓN* DE TI

Adquisición, Desarrollo y Cambios

- Realización de beneficios (Business Case)
- Estructura de la gestión de proyectos
- Prácticas de gestión de proyectos
- Desarrollo de aplicaciones de negocio (Enfoque tradicional / Ágil)
- Sistemas de aplicaciones de negocio (IED, Banca, Finanzas, ATM)
- Desarrollo de la infraestructura / prácticas de adquisición
- Prácticas de mantenimiento de sistemas de información
- Prácticas de mejoramiento de procesos -BPM

Controles Generales de Tecnología

- Gobierno y gestión de TI
- Operación, mantenimiento y soporte
- Protección de activos

Procesos del CISA

Esto es lo mínimo que debe de conocer el Auditor.

EVALUANDO LA *GESTIÓN* DE TI

Operación, Mantenimiento y Soporte

- Operaciones de los sistemas de información
- Hardware de los sistemas de información
- Arquitectura y software de sistemas de información
- Infraestructura de las redes de SI
- Sistemas de gestión de bases de datos (DBMS)
- Gestión de servicios de TI – centro de soporte (Help Desk)
- Gestión de respaldos, control de cambios y programas de utilidad
- Recuperación en caso de desastres (DRP)

Controles Generales de Tecnología

- Gobierno y gestión de TI
- Adquisición, desarrollo y cambios
- Protección de activos

Procesos del CISA

Esto es lo mínimo que debe de conocer el Auditor.

EVALUANDO LA *GESTIÓN* DE TI

Protección de Activos

- Gestión de la seguridad de la información
- Accesos Lógicos
- Seguridad de la infraestructura de red
- Seguridad cliente - servidor
- Encriptación
- Software malintencionado (Malware)
- Exposiciones y controles ambientales y de acceso físico
- Computo Móvil

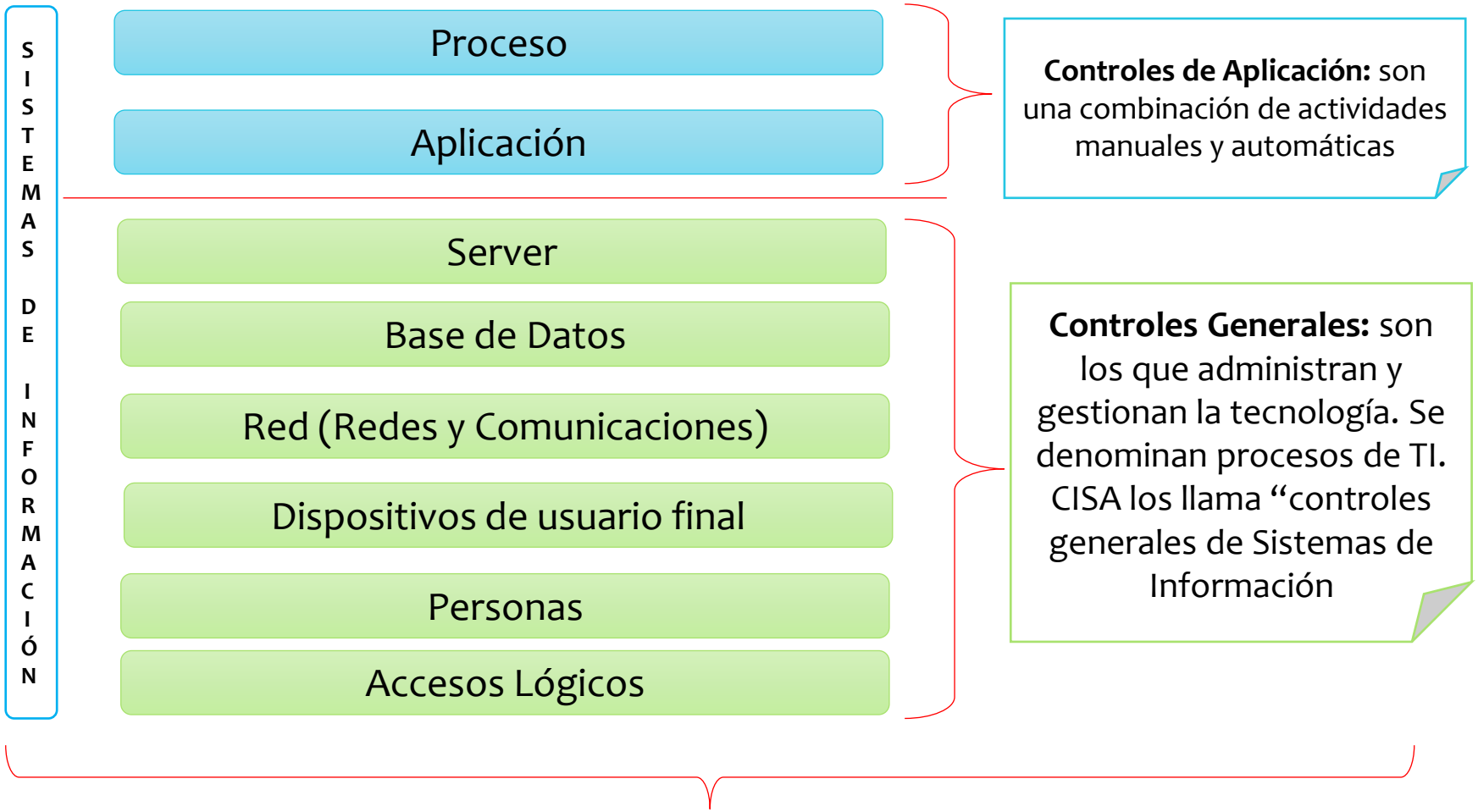
Controles Generales de Tecnología

- Gobierno y gestión de TI
- Adquisición, desarrollo y cambios
- Operación, mantenimiento y soporte

Procesos del CISA

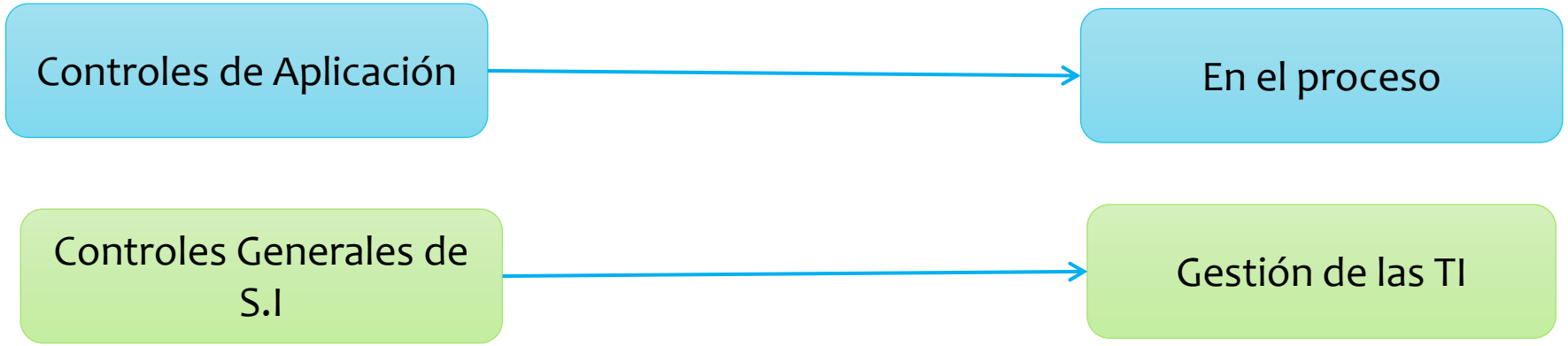
Esto es lo mínimo que debe de conocer el Auditor.

CONTROLES EN SISTEMAS DE INFORMACIÓN



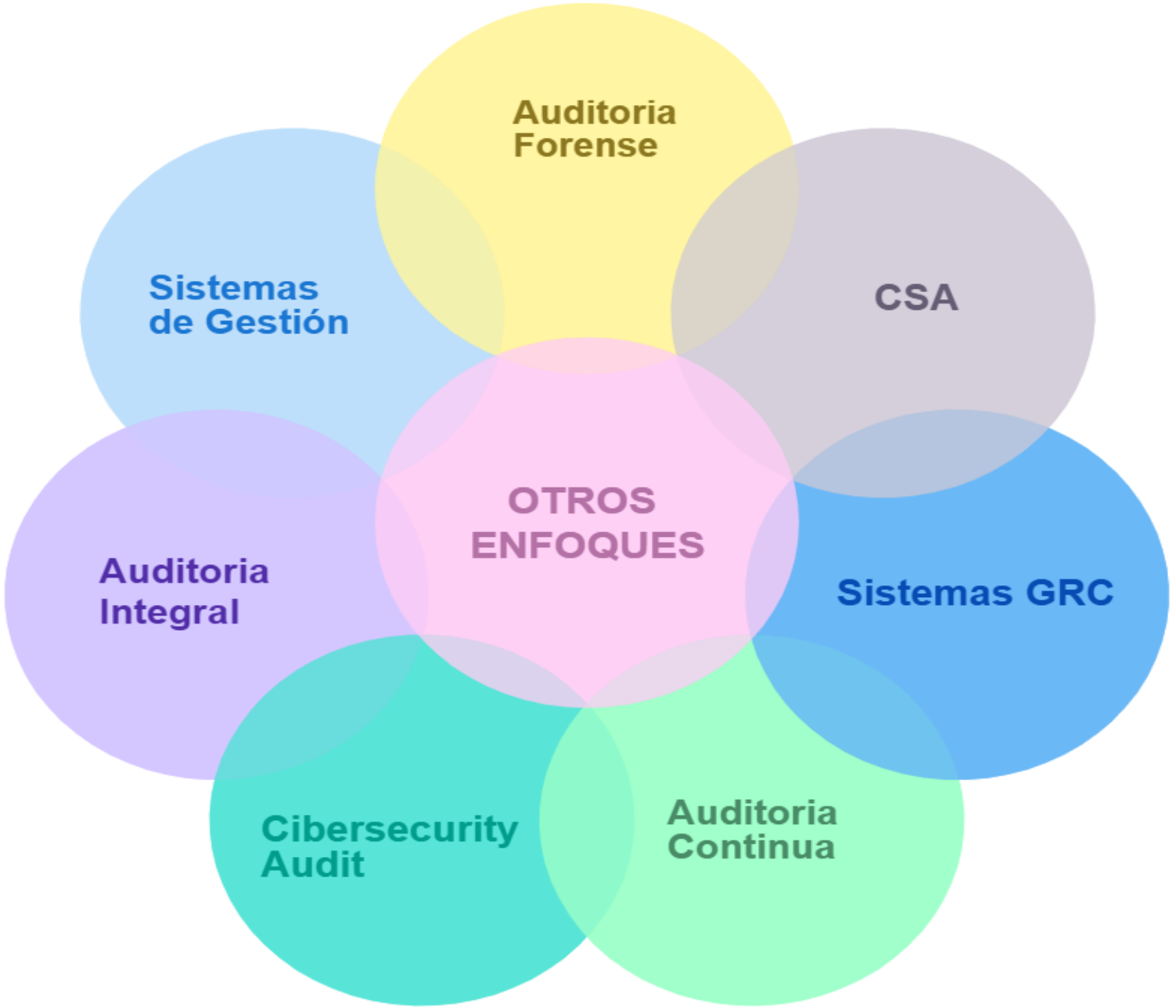
El proceso de auditoría debe ser integral, debe de observarse, no solo una parte. Todo debe ser integrado en base a los procesos, no por componentes, sino por sistemas de información con sus componentes

CONTROLES EN SISTEMAS DE INFORMACIÓN



Técnicas de cómo probar controles:

- ☑ Observación
- ☑ Seguimiento en tiempo real
- ☑ Entrevistas
- ☑ Flujogramas
- ☑ Pruebas sustantivas
- ☑ Comprobaciones


Auditoria Forense
Sistemas de Gestión
CSA
OTROS ENFOQUES
Auditoria Integral
Sistemas GRC
Cibersecurity Audit
Auditoria Continua

Gracias

Josué F. Chete

Auditor de Sistemas de Información

jchete.gt@outlook.com

+502 56992941

LinkedIn: Josué F. Chete

Facebook: Josué F. Chete