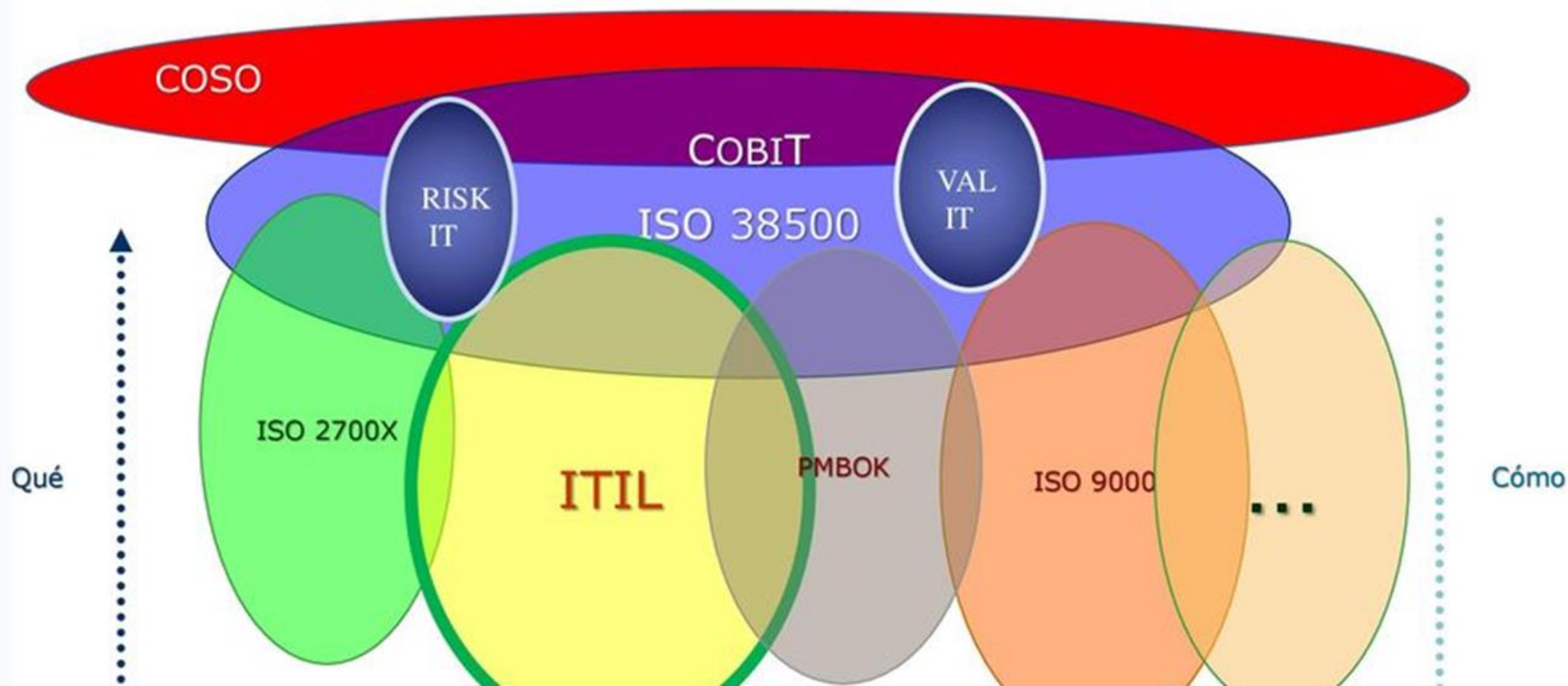




REPASO DE ESTANDARES

M.A., Inga. Evelyn Lobos

COBIT y las mejores Prácticas



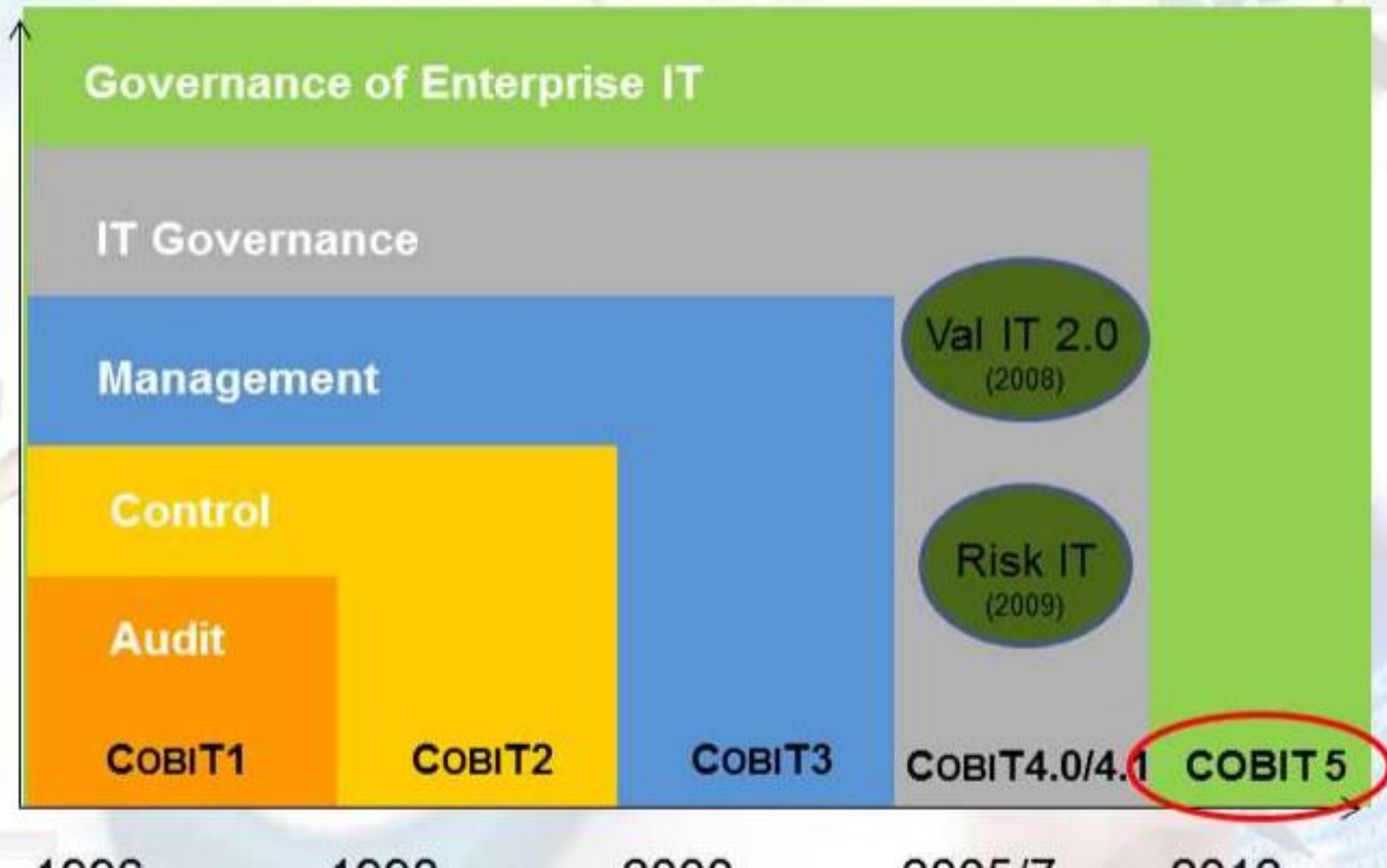
DEFINICIÓN DE COBIT



C Control
OB **OB**jectives
I for **I**nformation
T and Related **T**echnology

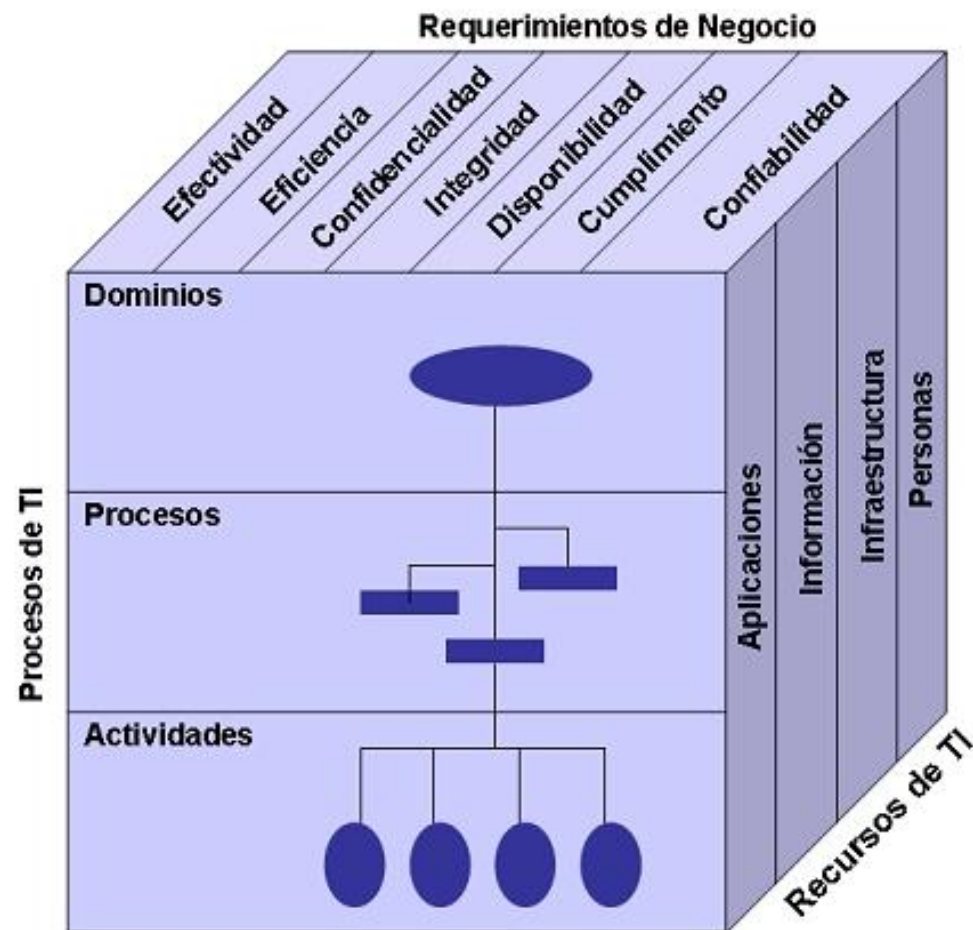
**OBJETIVOS DE CONTROL PARA LA
INFORMACION Y LA TECNOLOGIA**

Evolution of scope



COBIT 4.1

El Cubo de COBIT



COBIT 4.1. - Dominios

Planeación y Organización (PO)

Este dominio cubre las estrategias y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio.

Adquisición e Implementación (AI)

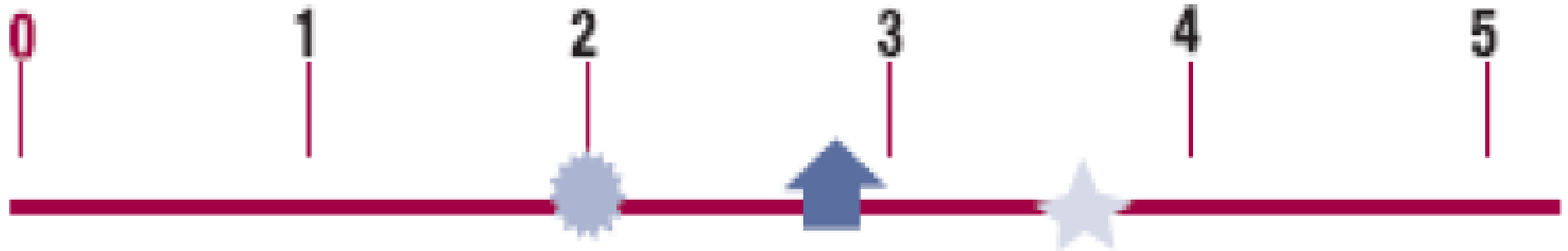
Las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Este dominio cubre los cambios y el mantenimiento a los sistemas existentes.

Entrega y Soporte (DS)


Este dominio hace referencia a la entrega o distribución de los servicios requeridos, que van desde las operaciones tradicionales hasta el entrenamiento, pasando por la seguridad en los sistemas y la continuidad de las operaciones.

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia


No existe Inicial Repetible Definido Administrado Optimizado



Símbolos utilizados

 **Estado actual de la empresa**

 **Promedio de la industria**

 **Objetivo de la empresa**

Calificativos utilizados

- 0- No se aplica la administración de procesos
- 1- Los procesos son ad-hoc y desorganizados
- 2- Los procesos siguen un patrón regular
- 3- Los procesos se documentan y se comunican
- 4- Los procesos se monitorean y miden
- 5- Se utilizan buenas practicas y están automatizadas

COBIT[®]



*Un Marco de Negocio
para el Gobierno y la Gestión
de las TI de la Empresa*

COBIT[®]
AN ISACA[®] FRAMEWORK

¿Qué es Cobit?

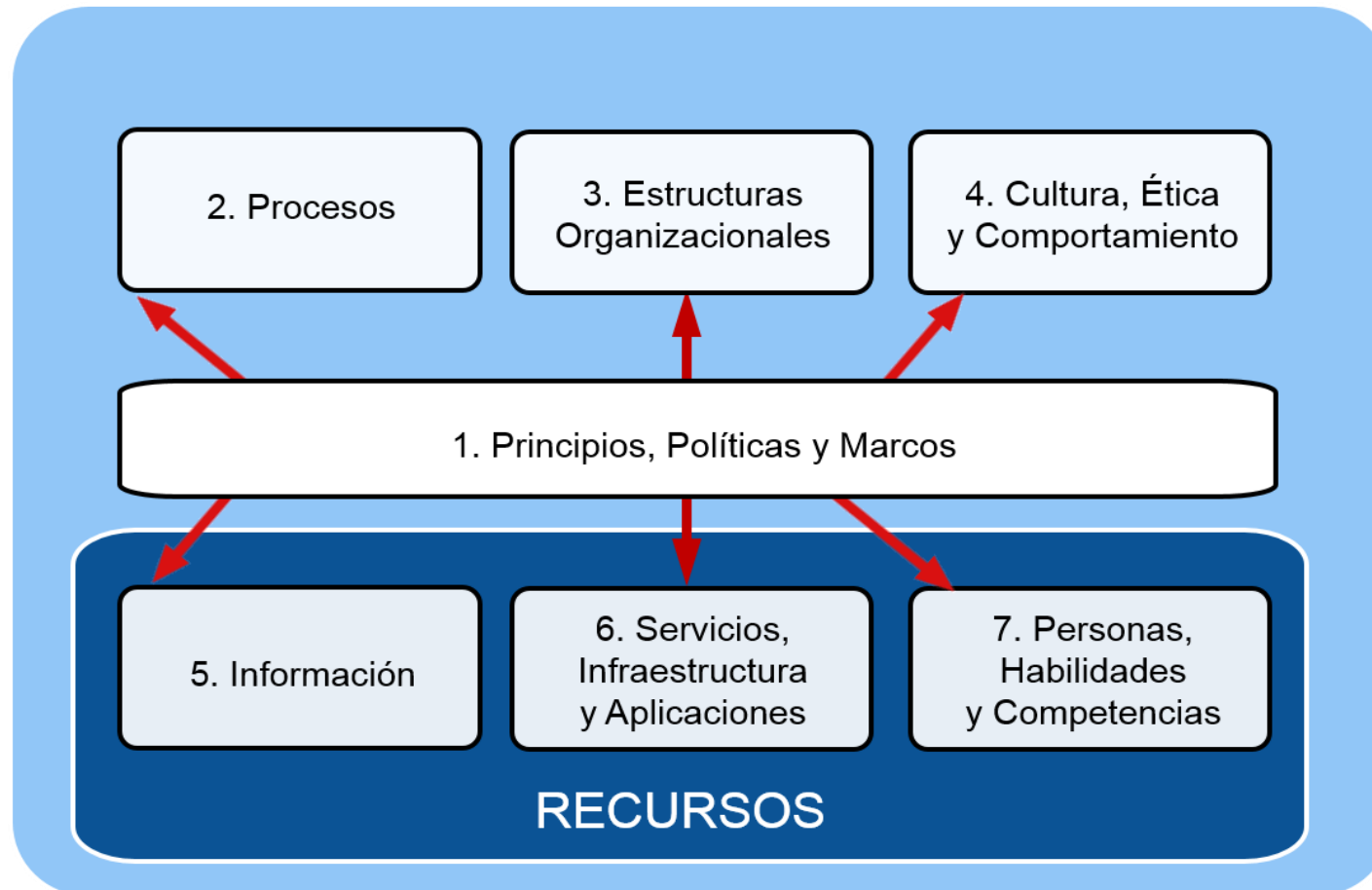
Es un marco de trabajo que permite comprender el gobierno y la gestión de las tecnologías de información (TI) de una organización, así como evaluar el estado en que se encuentran las TI en la empresa.



COBIT 5 proporciona la guía de ISACA para el gobierno y la gestión de las TI en la empresa, se basa en cinco principios claves para el gobierno y la gestión de las TI empresariales



Propone 7 categorías o 'clases' de elementos constituyentes o habilitadores (drivers) altamente interrelacionados, para construir el sistema específico de gobierno y gestión:



COBIT[®] 2019

A HISTORICAL TIMELINE

The COBIT® Framework

COBIT® 2019



1996

ISACA released the first edition of COBIT framework.



2000

A third edition of COBIT, with new Management Guidelines, was published.

2005

COBIT 4.0 becomes the fourth edition in the COBIT series of releases.



2012

COBIT 5 integrated the COBIT 4.1, Val IT 2.0 and Risk IT frameworks, and drew from ISACA's IT Assurance Framework (ITAF) and the Business Model for Information Security (BMIS). COBIT 5 also coordinated with frameworks and standards such as ITIL, ISO, PMBOK, PRINCE2 and TOGAF.



2018

ISACA publishes COBIT 2019, an update that adds design factors and focus areas to make it more practical and customizable.



1995

1995

Windows 95, Java, and HTML 2.0 (first formal html standard) debuted, as did Amazon.com, craigslist.com, match.com and ebay.com



2000

1997

Original wireless LAN standard (IEEE 802.11) released, DVD technology appeared, and Google.com registered as domain—incorporating a year later and launching in 1999.



2002

U.S. Sarbanes-Oxley law revolutionized corporate recordkeeping and retention standards, leading to new IT regulatory requirements.

2001

Internet Archive "Wayback Machine" (archive.org) launched, Wikipedia started publishing, and Apple released iPod.



2005

2003

Third WiFi standard created proliferation of "hotspots" as Skype, LinkedIn and WordPress started up. U.S. CAN-SPAM Act became law.



2007

COBIT upgraded to version 4.1.



2010

2007

Apple iPhone signaled move to touchscreen devices; Apple App Store went online one year later.



2015

2014

Internet of Things (IoT) technology standard ushered new wave of smart devices.

2012

Worldwide e-commerce tops \$1 trillion in sales.



2016

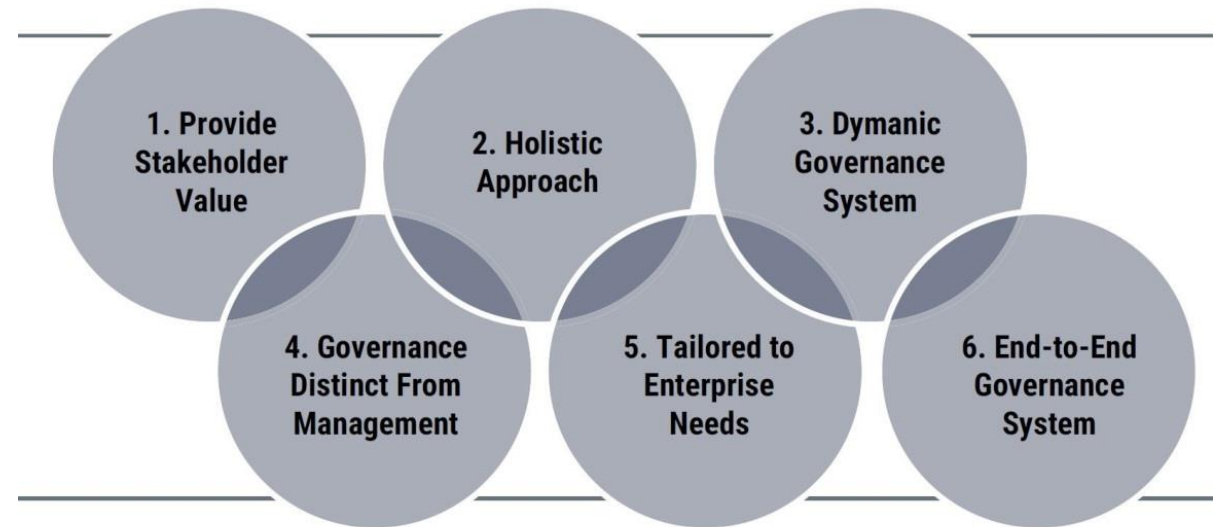
ISACA acquired CMMI Institute and its business maturity and capability models, adding these resources to the ISACA/COBIT framework portfolio.

Que ha cambiado en COBIT 2019

- Se aborda mejor la importancia del Gobierno de TI para la organización. La orientación basada en gobierno de COBIT ayuda a las organizaciones a lograr la realización de beneficios, la optimización de riesgos, la optimización de recursos y el alineamiento de TI con el negocio para la organización.
- Aborda las nuevas tendencias en tecnología. Por ejemplo, DevOps y Agile Development, Cloud, integración y gestión de servicios (SIAM) e Internet of Things (IoT).
- Está más actualizado, con los últimos estándares y métodos de trabajo. Con referencias y alineamiento a conceptos originados en otras fuentes. En este contexto, alineamiento significa: COBIT 2019 no contradice ninguna guía en los estándares relacionados, no copia el contenido de estos estándares relacionados y proporciona declaraciones equivalentes o referencias a la guía relacionada.
- Proporciona mayor flexibilidad. La Guía de Diseño de COBIT ayuda a que el contenido de COBIT se adapte a las necesidades particulares y al contexto de cada organización y de cada usuario.

Para el Sistema de Gobierno se considerarán 6 principios, ya no solo 5, como era para el COBIT5 ahora incluyen el personalizar el sistema para lo que la organización necesita:

1. Satisfacer las necesidades de los stakeholders
2. Habilitar un enfoque holístico
3. Sistema de gobierno dinámico
4. Distinguir entre gobierno y gestión
- 5. Adaptado a las necesidades de la empresa**
6. Cubrir la empresa de extremo a extremo



Áreas de Enfoque

Organizaciones de pymes

seguridad

DevOps

Regulaciones

ISO 27001

Los requisitos de la Norma **ISO 27001** norma nos aportan un **Sistema de Gestión de la Seguridad de la Información (SGSI)**, consistente en medidas orientadas a **proteger la información**, indistintamente del formato de la misma, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa.



DEFINICIÓN DE SEGURIDAD PARA ISO 270001

La seguridad de la información se define en el estándar ISO 27001 como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

ELEMENTOS O FASES PARA LA IMPLEMENTACIÓN DE UN SGSI



IMPLANTANDO LA NORMA ISO 27001

- Lo primero, es elegir una metodología de evaluación del riesgo apropiada para los requerimientos del negocio. Existen numerosas metodologías estandarizadas de evaluación de riesgos. Aquí explicaremos la metodología sugerida en la Norma.
- Las fases de esta metodología son los siguientes:



ISO/IEC 27002

Estándar para la seguridad de la información.



DOMINIOS DE ISO/IEC 27002

POLITICAS DE SEGURIDAD

- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

SEGURIDAD LIGADA A RECURSOS HUMANOS

- GESTIÓN DE ACTIVOS

DOMINIOS ISO 27002

CONTROL DE ACCESOS

- CIFRADO

CONTROLES CRIPTOGRAFICOS

- SEGURIDAD FISICA AMBIENTAL

DOMINIOS ISO 27002

SEGURIDAD OPERATIVA

- SEGURIDAD DE TELECOMUNICACIONES

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

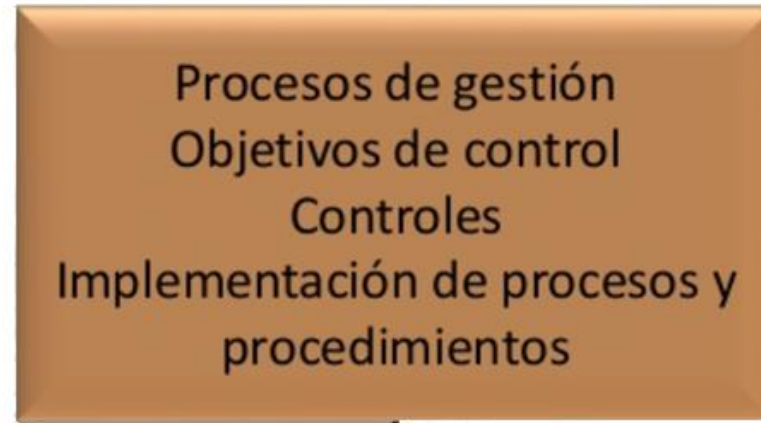
RELACIONES CON SUMINISTRADORES.

ISO/IEC 27004

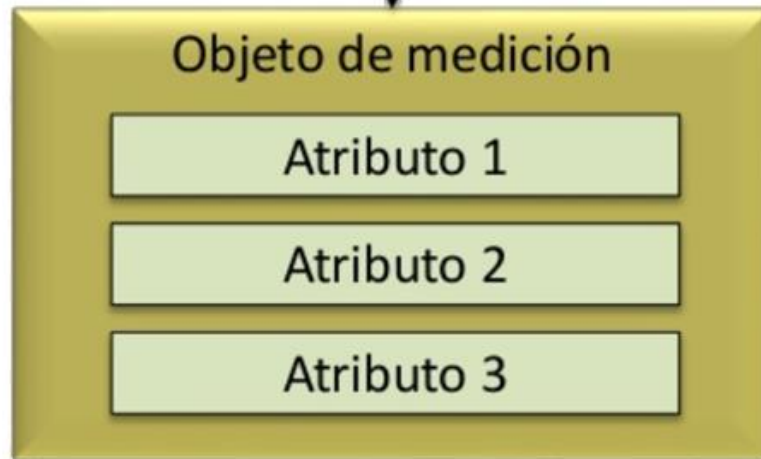
Medición de la Seguridad de la Información

Método para
monitorear,
medir,
analizar y
evaluar

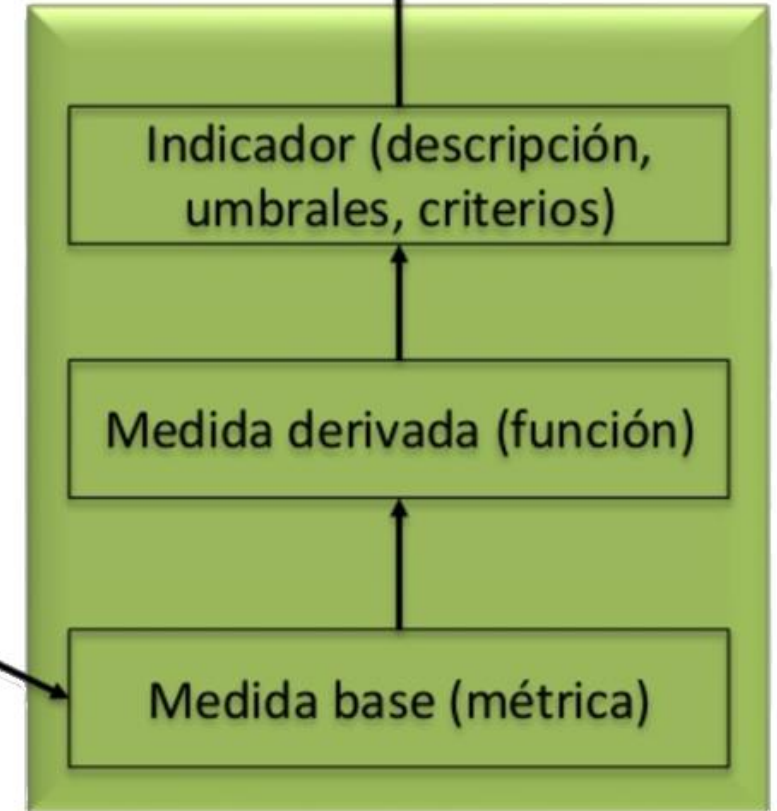
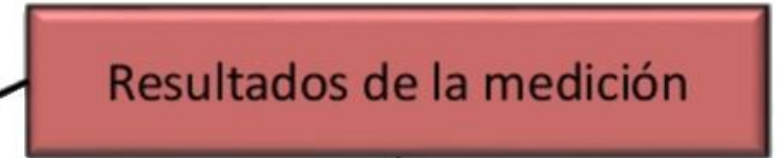
¿Que necesito medir?



¿Que voy a medir?



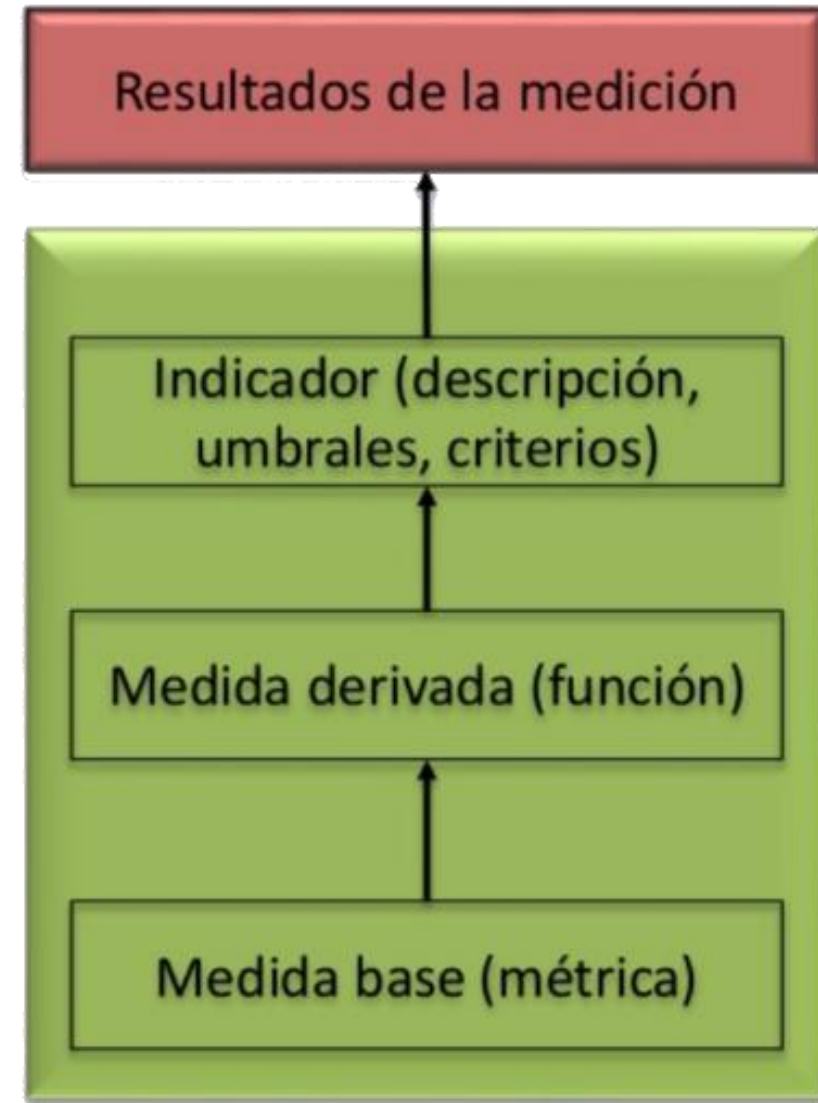
Validar el rendimiento y la eficacia



¿Cómo voy a medir?

Método para monitorear, medir, analizar y evaluar

- Métodos.:
- Factor Subjetivo
 - Factor Humano
- Factor Objetivo
 - Basado en reglas numéricas
 - Manual
 - Automático
 - Semiautomático



¿Qué debe incluir un programa de medición?

1. Políticas y objetivos del programa de medición de un sistema de gestión.
2. Criterios de análisis y evaluación de los resultados de la medición.
3. Alcance del programa de medición (a nivel de sistemas de gestión).
4. Estructura del cuadro de mando (objetos y atributos de medición, método).
5. Organización del programa de medición (asignación de responsabilidad y competencias).
6. Identificar los factores de éxito y los riesgos del programa de medición.
7. Establecer los procedimientos del programa (recolectar datos, elaboración de métricas e indicadores, generación de los informes).
8. Identificar los recursos necesarios.
9. Definir los objetivos específicos de los objetos y atributos seleccionados a medir.
10. Establecer la planeación de las mediciones y la forma de llevar a cabo las actividades.
11. Informes de los resultados de la medición.
12. Monitorear, revisar y mejorar el programa.

ISO 27005



Es el estándar internacional que se ocupa de en una empresa, apoyando particularmente la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información isitos del sistema de gestión de seguridad de la información definidos en ISO 27001.

DEFINICIONES IMPORTANTES

- Amenaza

Cualquier cosa (por ejemplo, un objeto, una sustancia, un ser humano) que es capaz de actuar contra un activo de una manera que pueda dañarlo. Una causa potencial de un incidente no deseado (ISO/IEC 13335)

- Vulnerabilidad

Una deficiencia en el diseño, la implementación, la operación o los controles internos en un proceso que podría explotarse para violar la seguridad del sistema.

- Control

Cualquier proceso que reduce directamente una amenaza o vulnerabilidad.

Gestión de riesgo

Es una actividad recurrente que se refiere al análisis, a la planificación, la ejecución, el control y el seguimiento de todas las medidas implantadas y la política de seguridad que ha sido impuesta.

FASES Y ESCALA DE VALORACIÓN DEL RIESGO

Fase del SGSI	Actividades en proceso de gestión del riesgo en SI
Planear	Establecer el contexto Valoración del riesgo Planificación de tratamiento del riesgo Aceptación del riesgo
Hacer	Implementación plan de tratamiento de riesgos
Verificar	Monitoreo y revisión continua Evaluación
Actuar	Mantener con la mejora continua el proceso de gestión del riesgo en seguridad de la información Comunicación

RIESGO		CRITERIOS PARA VALORAR EL RIESGO				
Activos	Amenazas	Impacto económico del riesgo	Tiempo de recuperación de la empresa	Probabilidad de ocurrencia del riesgo	Probabilidad de interrumpir actividades de la empresa	Total