UPeU ESCUELA DE INGENIERÍA DE SISTEMAS

2018-2

HACEMOS LA DIFERENCIA

Sé Íntegro
Sé Misionero
Sé Innovador

Contexto del Gobierno de TI

Unidad 1. Introducción al Gobierno Empresarial de Tecnologías de Información – GETI

GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN

Mtro. José Bustamante

Campus Tarapoto

Agenda

- Introducción
- Marcos de trabajo
- ISO/IEC 38500:2008 - Gobernanza corporativa de la Tecnología de la Información (TI)
- COBIT 2019
- Diferencias entre gobierno y gestión de TI
- Actividades

ISO/IEC 38500:2008 - Gobernanza corporativa de la Tecnología de la Información (TI)

ISO/IEC 38500:2015

Corporate Governance of Information Technology

La norma ISO/IEC 38500 establece que el gobierno de las TI “es el **sistema** a través del cual se **dirige** y **controla** la **utilización de las TI actuales y futuras**. Supone la **evaluación y dirección de los planes** de utilización de las **TI** que dan soporte a la organización y la monitorización de dicho uso **para alcanzar los objetivos establecidos en los planes**. Incluye las estrategias y políticas de uso de las TI dentro de la organización”

Objeto
ISO/IEC 38500:2015

- Esta norma **proporciona principios orientadores** para los administradores de las organizaciones (incluyendo propietarios, miembros del consejo directivo, directivos, socios, altos ejecutivos o similares) sobre el uso eficaz, eficiente y aceptable de la Tecnología de Información (TI) en sus organizaciones.
- Esta norma se aplica a la **gobernanza de los procesos** (y decisiones) **de gestión relativos a los servicios de información y comunicación utilizados por una organización**. Estos procesos podrían ser controlados tanto por especialistas en TI de la organización como por proveedores de servicios externos o unidades de negocio dentro de la organización.

Fuente: ISO/IEC 38500:2015 Gobernanza corporativa de la Tecnología de la Información (TI)

Objeto
ISO/IEC 38500:2015

También **proporciona orientación** a los que **asesoran**, **informan**, o **ayudan** a los administradores, entre los que se incluyen:

- Altos directivos / gerentes
- Miembros de los grupos de monitorizan los recursos dentro de la organización
- Especialistas externos, técnicos o de negocios, como pueden ser jurídicos o contables; asociaciones comerciales minoristas u organizamos profesionales
- Proveedores de servicios internos y externos (incluidos consultores)
- Auditores de TI

Fuente: ISO/IEC 38500:2015 Gobernanza corporativa de la Tecnología de la Información (TI)

Campo de aplicación
ISO/IEC 38500:2015

- Esta Norma Técnica Peruana es aplicable a todas las organizaciones, incluyendo compañías públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro. Esta Norma Técnica Peruana es aplicable a organizaciones de todo tamaño, desde la más pequeña a la más grande, independientemente del grado de uso de TI

Fuente: ISO/IEC 38500:2015 Gobernanza corporativa de la Tecnología de la Información (TI)

Propósitos
ISO/IEC 38500:2015

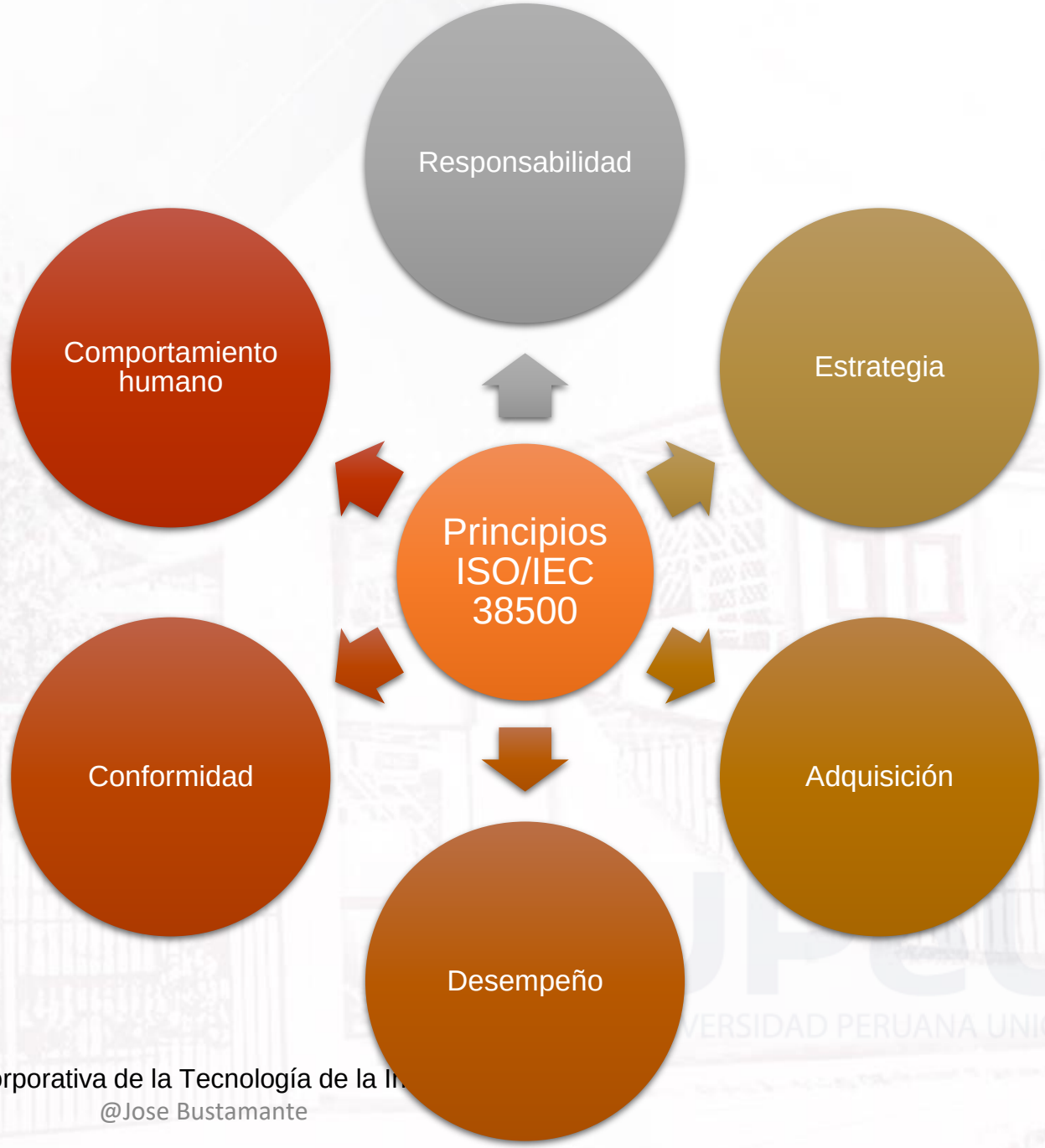
Promover el uso eficaz, eficiente y aceptable de la TI en todas las organizaciones por medio de:

1. Asegurar a las partes interesadas (incluidos clientes, accionistas y empleados) que si siguen la norma, pueden confiar en la gobernanza corporativa de la TI dentro de la organización.
2. Informar y orientar a los administradores sobre el gobierno del uso de la TI en su organización
3. Proporcionar una base de referencia para la evaluación objetiva de la gobernanza corporativa de la TI

Fuente: ISO/IEC 38500:2015 Gobernanza corporativa de la Tecnología de la Información (TI)

Principios
ISO/IEC 38500:2015

Los principios expresan comportamientos preferentes para guiar la toma de decisiones.



Fuente: ISO/IEC 38500:2015 Gobernanza corporativa de la Tecnología de la I

Principios
ISO/IEC 38500:2015

Responsabilidad	• Permite definir el actuar de los colaboradores y la toma de decisiones en pro del cumplimento de los resultados requeridos.
Estrategia	• Que determine la planeación necesaria para el cumplimento de los objetivos.
Adquisición	• Requerida de TI en base a un análisis y validación previa.
Desempeño	• Debe verse optimizado con la TI usada.
Conformidad	• En relación a los requerimientos debe estar plenamente cubierta con la TI implementada.
Comportamiento	• Humano como base fundamental no debe verse afectado en el uso de las TI.

Fuente: ISO/IEC 38500:2015 Gobernanza corporativa de la Tecnología de la Información (TI)

Modelo: Tareas principales

ISO/IEC 38500:2015

Los órganos de gobierno deben gobernar la TI a través de tres tareas principales:

EVALUAR

- el uso actual y futuro de TI

DIRIGIR

- la preparación e implementación de estrategias y políticas para asegurar que el uso de TI cumpla con los objetivos del negocio

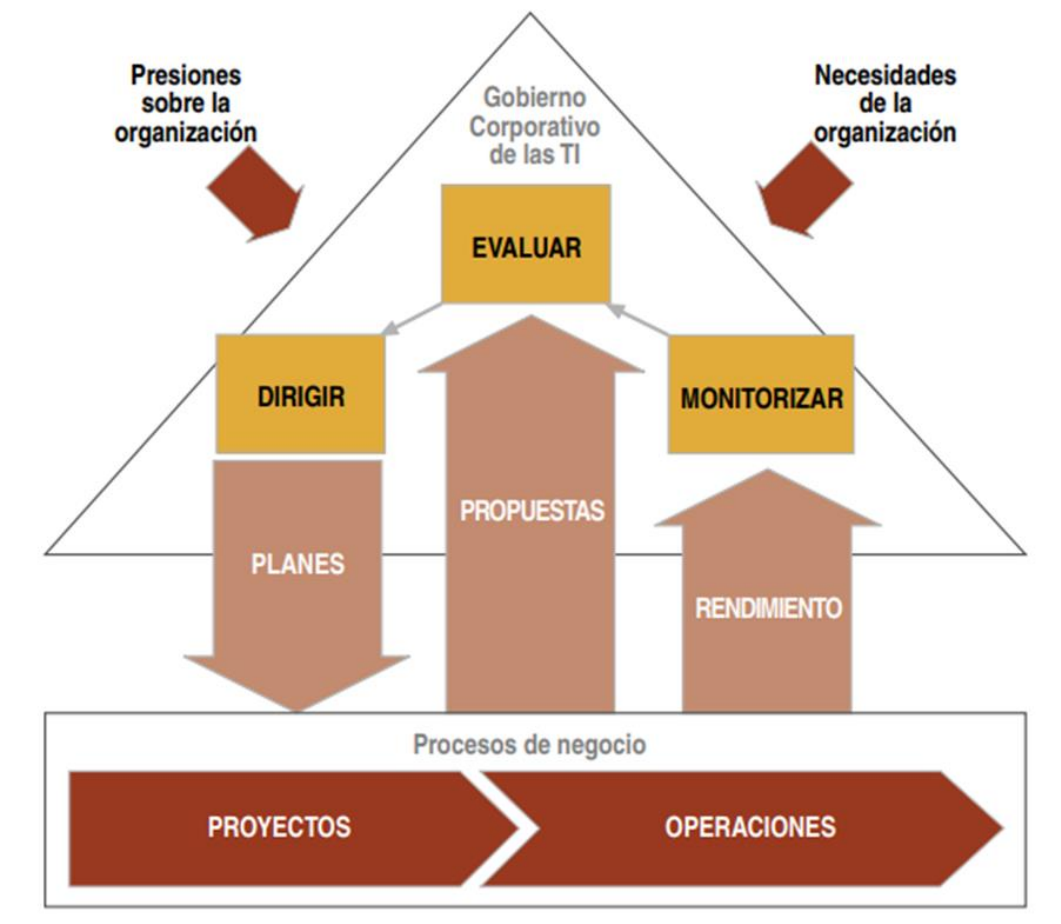
MONITORIZAR

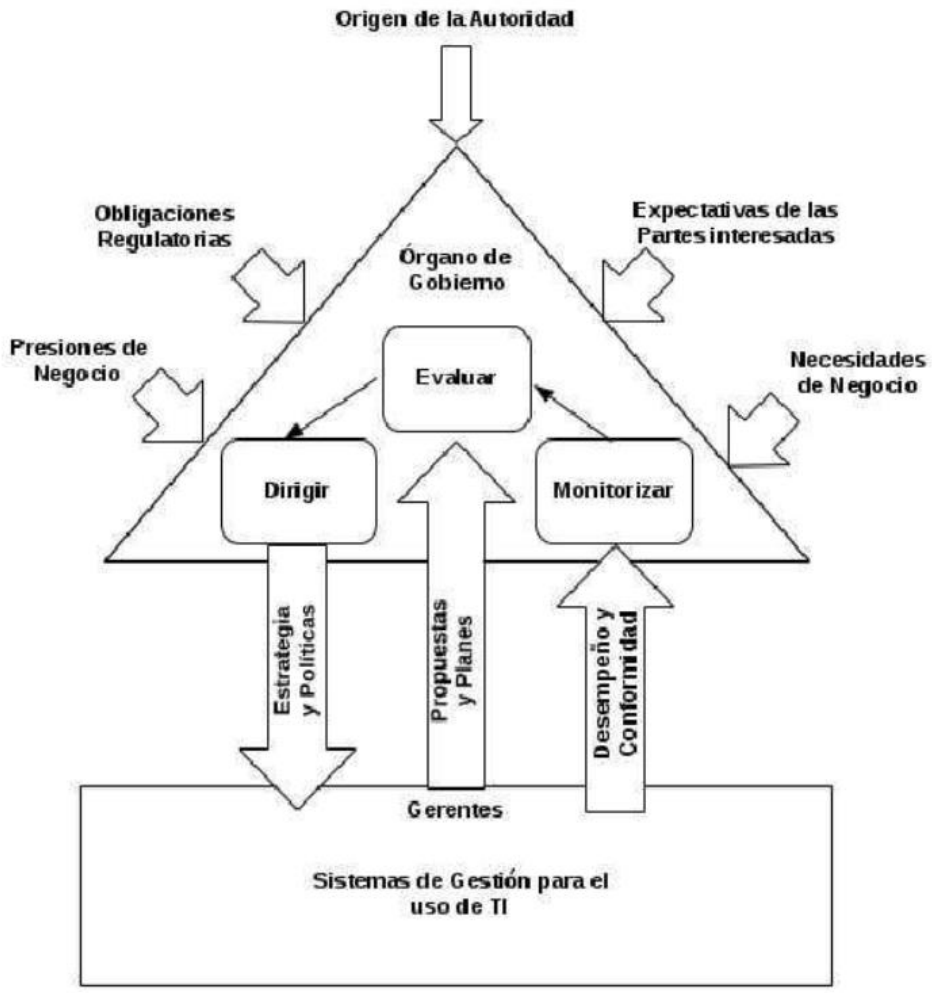
- la conformidad con las políticas y su desempeño en relacióncon las estrategias.

Fuente: ISO/IEC 38500:2008 Gobernanza corporativa de la Tecnología de la Información (TI)

Modelo de la Gobernanza Corporativa de TI

ISO/IEC 38500:2015



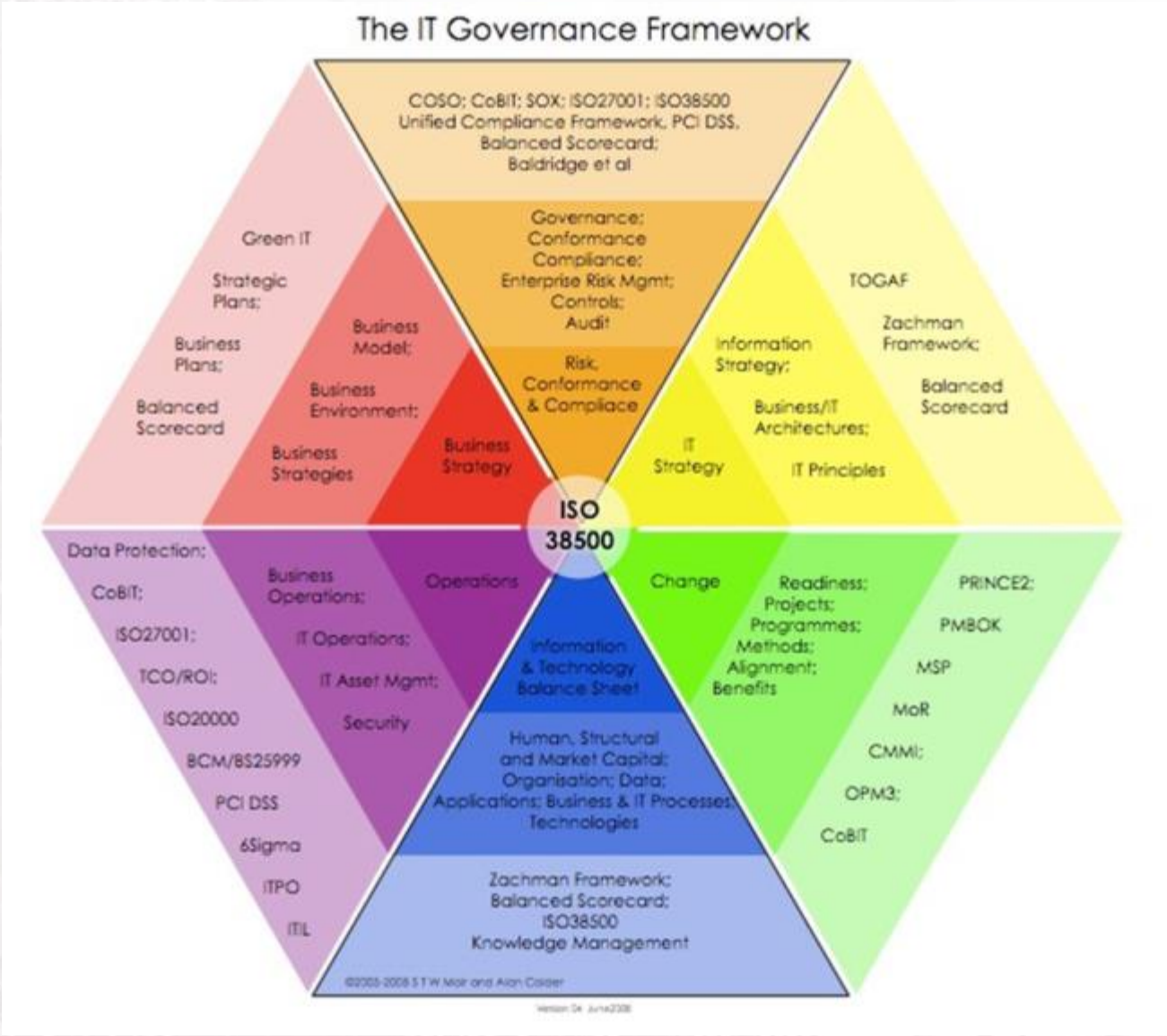


Resumen de las recomendaciones de buen gobierno de las TI de la norma ISO 38500

	EVALUAR	DIRIGIR	MONITORIZAR
RESPOSABILIDAD	• Los modelos y opciones para asignar responsabilidades • Las capacidades de aquellos que reciben la responsabilidad	• Que se lleven a cabo los planes diseñados • Que los directivos reciban la información que necesitan para tomar decisiones	• Ver si están establecidos los mecanismos de Gobierno de las TI • Comprobar si se comprenden las responsabilidades asignadas • Medir si rinden adecuadamente las responsabilidades asignadas
ESTRATÉGIA	• Los desarrollos de TI para comprobar que darán soporte al negocio en un futuro • Si las actividades de TI están alineadas con los objetivos de negocio • Si se gestionan los riesgos relacionados con el uso de las TI	• Que se diseñen políticas y planes que aprovechen el valor de las TI • Que se innove en TI	• Comprobar si se alcanzan los objetivos en el plazo y con los recursos planificados • Medir los resultados para comprobar que se han alcanzado los beneficios esperados
ADQUISICIÓN	• Diferentes opciones con ofertas de TI en relación al coste y al riesgo	• Que el procedimiento de compra sea el adecuado • Que se satisfagan las necesidades de la organización	• Comprobar que las inversiones proporcionan las capacidades esperadas • Ver hasta que grado se comparte los objetivos de la adquisición con el proveedor
DESEMPEÑO	• Las propuestas operativas de los gestores de TI para mantener la capacidad del negocio • El riesgo de las TI en relación a la continuidad de las operaciones de negocio • El riesgo para la integridad de la información • La eficacia de las decisiones de TI para el negocio • El rendimiento eficiente del sistema de gobierno de las TI	• Que se disponga de suficientes recursos TI • Que se proporcione a la dirección la información correcta y actualizada como soporte a las decisiones	• Ver en que medida las TI dan soporte al negocio • Comprobar que la asignación de recursos se prioriza en relación a los objetivos de negocio • Comprobar que se cumplen las políticas y normas establecidas
CUMPLIMIENTO	• En qué medida se cumple la legislación y las normas internas establecidas • El cumplimiento interno de los procedimientos propios del Gobierno de las TI establecido en la organización	• Que se establezcan mecanismos para comprobar el cumplimiento de leyes, normas y estándares • Que se establezcan políticas que apoyen el uso y la integración de las TI • Que el personal de TI tenga un comportamiento profesional y respete los procedimientos • Que se realice un uso ético de las TI	• Realizar auditorías y redactar informes del rendimiento y cumplimiento • Comprobar que las TI preservan la privacidad y el conocimiento estratégico.
COMPONENTE HUMANO	• Que el componente humano está identificado y se tiene en cuenta en todas las actividades de TI	• Que las actividades de TI sean consistentes con el componente humano • Que sean identificados y reportados por cualquiera los riesgos y oportunidades para que sean estimados por los directivos	• Si se percibe como importante el componente humano • Si se aplican las prácticas adecuadas para hacerlo consistente con el uso de las TI

Beneficios
ISO/IEC 38500:2015

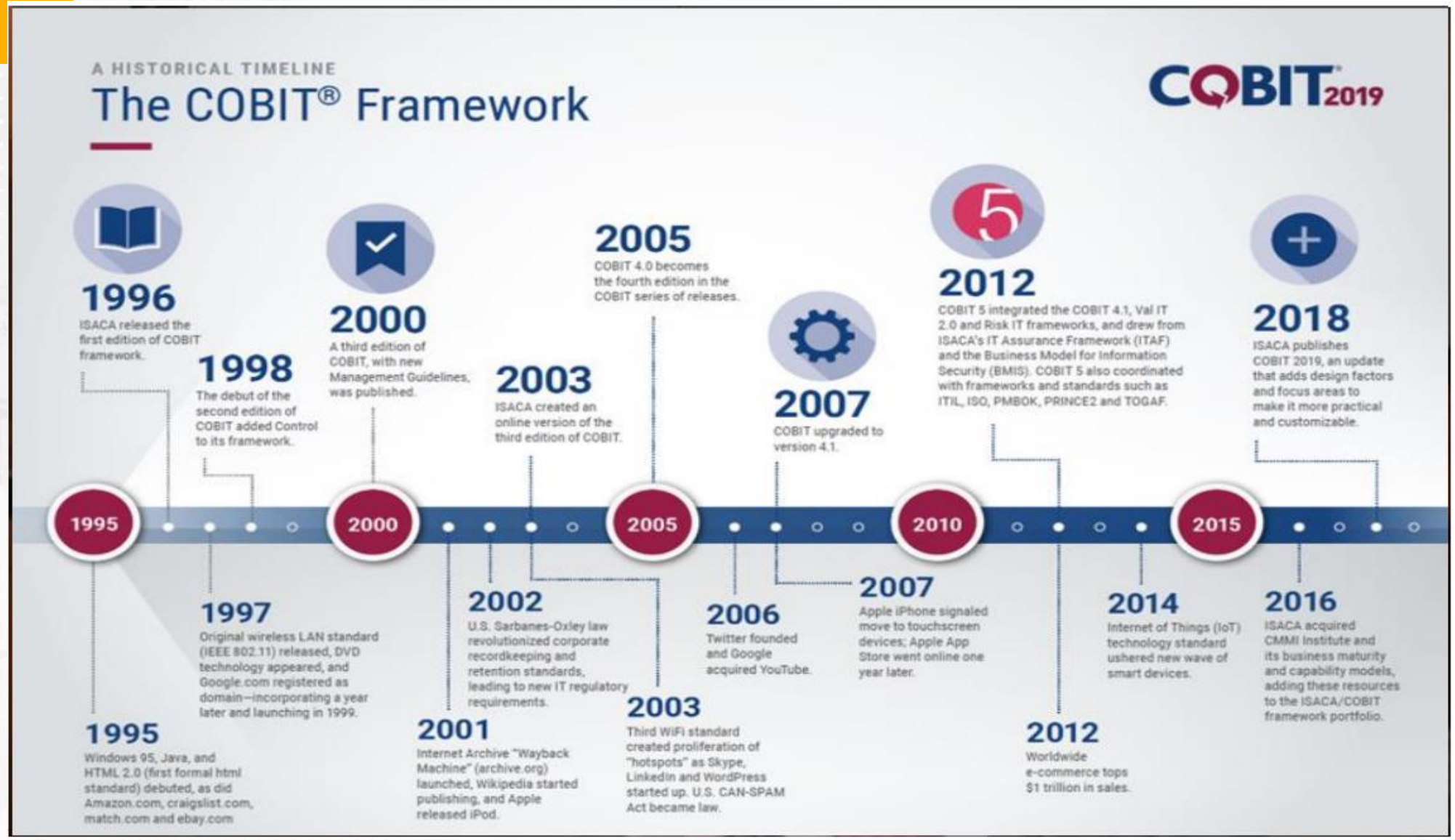
- Administre las inversiones de TI adecuadamente
- Mejorar el desempeño de la organización.
- Mejorar la gobernanza del proyecto.
- Mejorar la posición competitiva de la organización.
- Minimiza los riesgos de TI
- Asegurar mayores tasas de éxito del proyecto



https://www.itgovernance.eu/images/calder-moir-650px.png

COBIT 2019

Historia COBIT



COBIT 2019 como un Marco de Gobierno de I&T

- A lo largo de los años, se han desarrollado y promovido marcos de mejores prácticas para ayudar en el proceso de comprensión, diseño e implementación de EGIT
- COBIT® 2019 se basa e integra más de 25 años de desarrollo en este campo, no solo incorporando nuevos conocimientos de la ciencia, sino también operando estos conocimientos como prácticas.
- Desde su nacimiento en la comunidad de auditoría de TI, COBIT ha pasado a ser un marco de referencia de gestión y gobierno de I&T más amplio y exhaustivo.
- COBIT sigue estableciéndose como un marco generalmente aceptado para el gobierno de I&T.

¿Qué es COBIT?

- COBIT es un marco de referencia para el gobierno y la gestión de la información y la tecnología de la empresa,
- COBIT está dirigido a toda la empresa.
- COBIT hace una distinción clara entre gobierno y gestión.
- COBIT define los componentes para crear y sostener un sistema de gobierno.
- COBIT define los factores de diseño que la empresa debería considerar para crear un sistema de gobierno más adecuado.
- COBIT trata asuntos de gobierno mediante la agrupación de componentes de gobierno relevantes en objetivos de gobierno y gestión que pueden gestionarse según los niveles de capacidad requeridos.

Referencia: Marco de referencia COBIT 2019: Introducción y metodología Capítulo 1 Introducción

Esquema conceptual COBIT 2019

Nuevos conceptos: como las áreas de enfoque y los factores de diseño, permiten una orientación adicional para adaptar un sistema de gobierno a las necesidades de la empresa.

La alineación actualizada con los estándares globales, marcos y mejores prácticas mejora la relevancia de COBIT.

Un modelo de “fuente abierta” permitirá a la comunidad de gobierno global la capacidad de informar actualizaciones futuras al proporcionar comentarios.

Las nuevas guía y herramientas apoyan el desarrollo de un sistema de gobierno de mejor ajuste, lo que hace que COBIT 2019 sea más prescriptivo/preceptivo.

COBIT: Lo que es y lo que no es.

LO QUE ES

- ✓ Es un marco para el gobierno y la gestión de la información y tecnología.
- ✓ Esta dirigido a toda la empresa.
- ✓ Hace clara distinción entre el gobierno y gestión.
- ✓ Define los componentes para construir y sostener un sistema de gobierno.
- ✓ Define los factores de diseño que deberían considerarse por la empresa para construir un gobierno mejor ajustado.
- ✓ Aborda los problemas de gobierno agrupando los componentes de gobierno relevantes en los objetivos de gobierno y gestión que puedan ser gestionados a los niveles de capacidad requeridos.

LO QUE NO ES

- ❖ No es una completa descripción de todo el entorno de TI de una empresa.
- ❖ No es un marco para organizar procesos del negocio.
- ❖ No es un marco técnico de TI para gestionar la tecnología.
- ❖ No hace ni prescribe decisiones relacionadas a TI

Publico Objetivo

Referencia: Marco de referencia COBIT 2019: Introducción y metodología Capítulo 1 Introducción

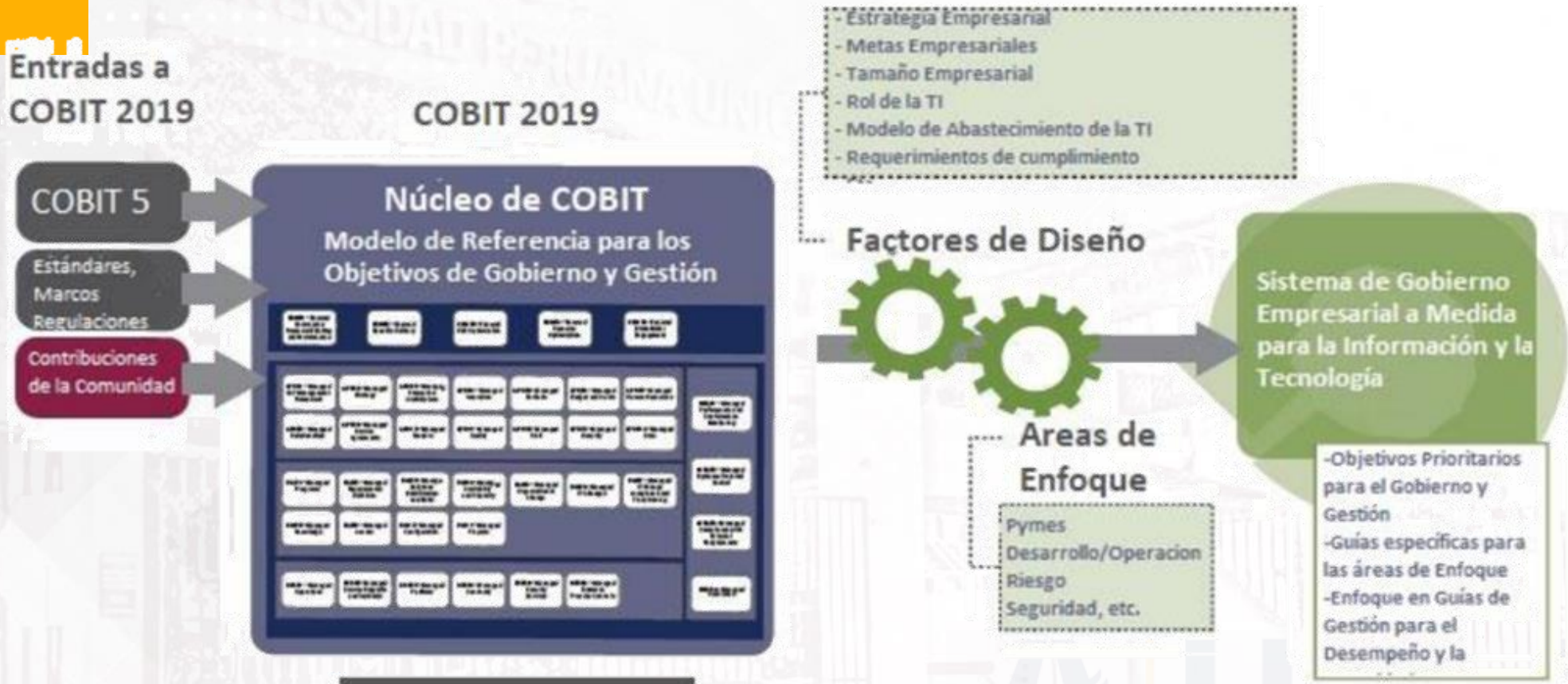
Público Objetivo

Referencia: Marco de referencia COBIT 2019: Introducción y metodología Capítulo 1 Introducción

COBIT 2019: Público Objetivo

- **Un cierto nivel de experiencia y un completo entendimiento** de la empresa son requeridos para beneficiarse del marco COBIT.
- Tal entendimiento y experiencia **permite al usuario adaptar el core de COBIT**, en una entallada y enfocada guía para la empresa, teniendo en cuenta el contexto de la empresa.
- La audiencia objetivo incluye a los **responsables durante todo el ciclo de vida** de las soluciones de gobierno, desde el diseño hasta la ejecución y garantía.

Formato y Arquitectura de productos de COBIT



Publicaciones Principales de Cobit 2019

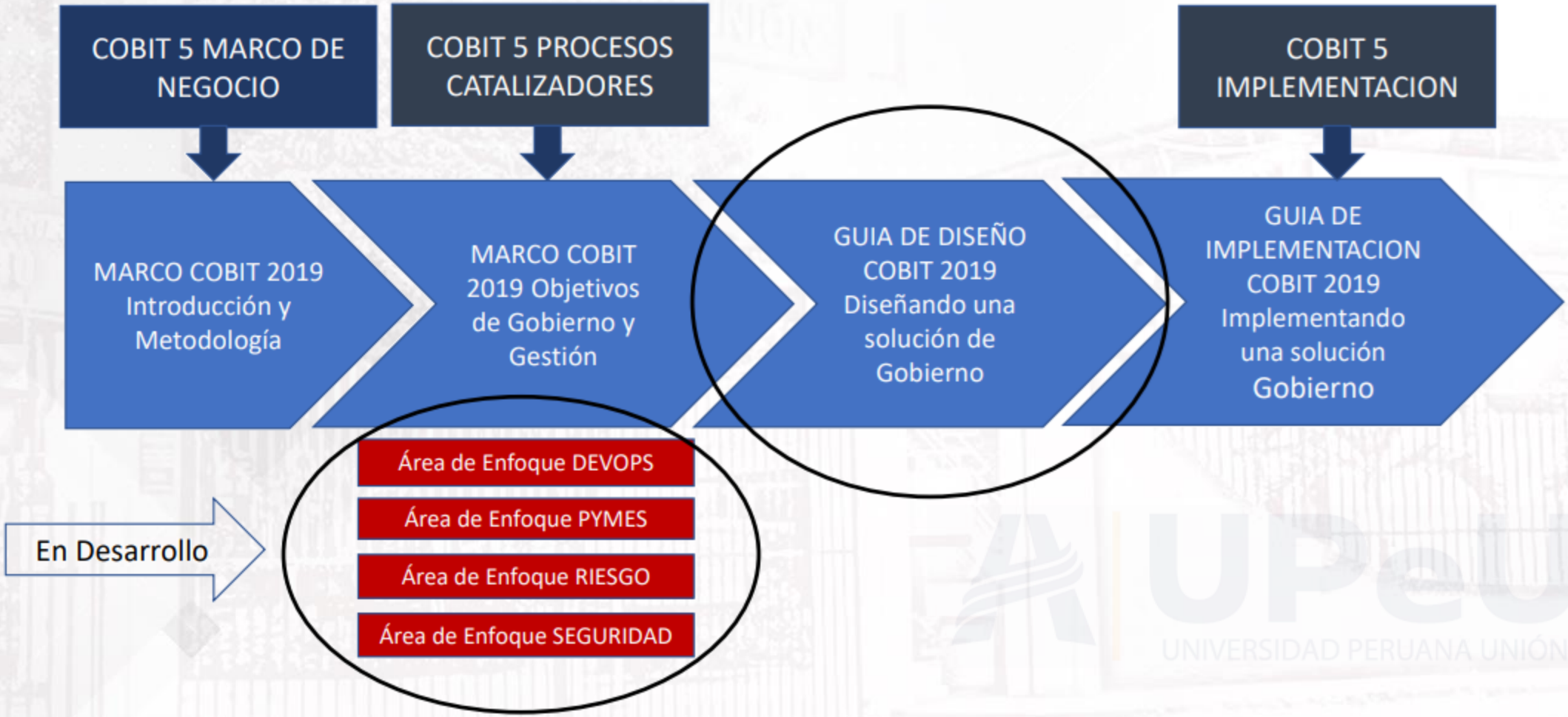
Marco COBIT 2019 Introducción Y Metodología		
Marco COBIT 2019 Objetivos de Gobierno y Gestión	Guía de Diseño COBIT 2019 Diseñando una Solución de Gobierno en Tecnología e Información	Guía de Implementación COBIT 2019 Implementando y Optimizando una solución de Gobierno en Tecnología e Información

Formato y Arquitectura de Productos de COBIT

- Marco de referencia COBIT® 2019: Introducción y metodología
- Marco de referencia COBIT® 2019: Objetivos de gobierno y gestión
- Guía de diseño COBIT® 2019: Diseño de una solución de Gobierno de Información y Tecnología
- Guía de implementación COBIT® 2019: Implementación y optimización de una solución de gobierno de Información y Tecnología

Referencia: Marco de referencia COBIT 2019: Introducción y metodología Capítulo 1 Introducción

Manuales COBIT 5 vs. COBIT 2019



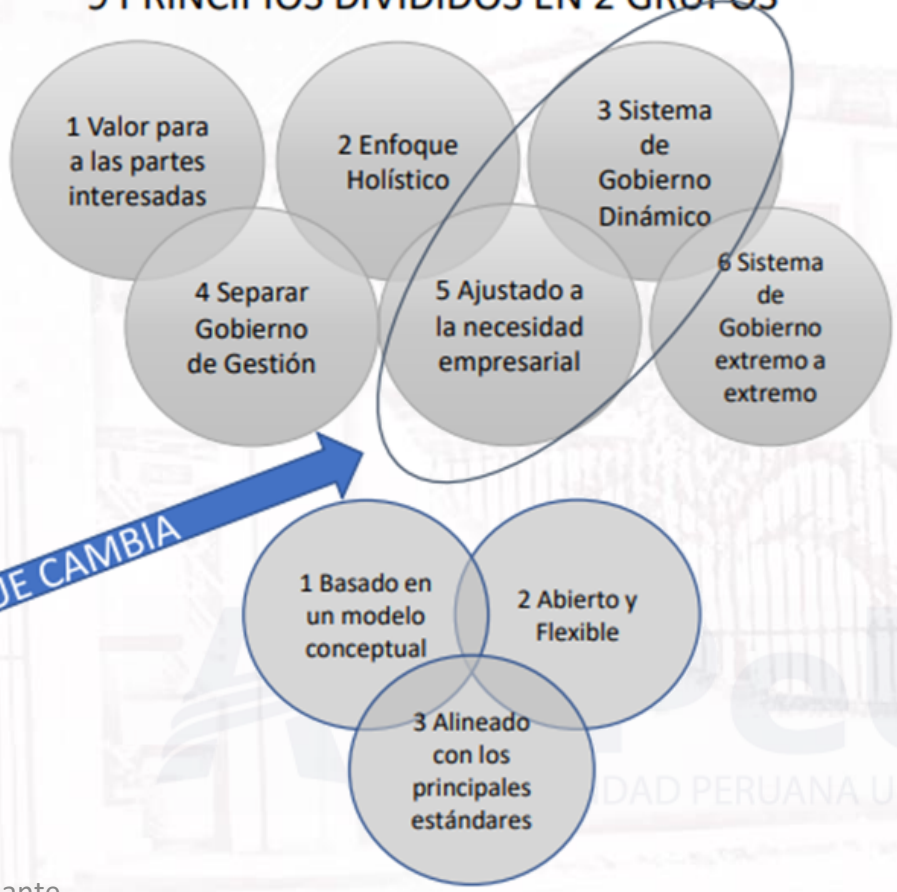
Principios COBIT5 vs. Principios COBIT 2019

COBIT 5
AN ISACA® FRAMEWORK

5 PRINCIPIOS

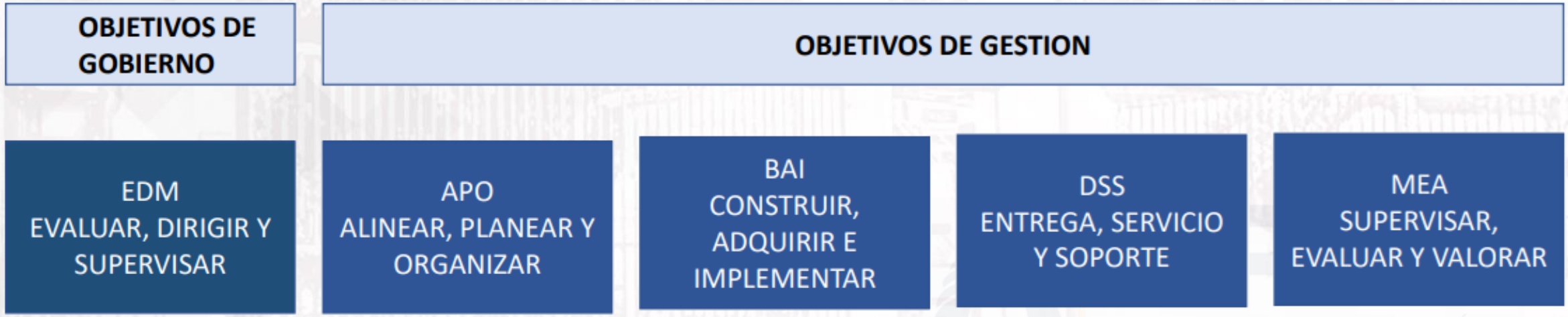
COBIT 2019

9 PRINCIPIOS DIVIDIDOS EN 2 GRUPOS



Dominios COBIT 2019

- De forma similar a COBIT 5 en COBIT2019 los objetivos de Gobierno y los objetivos de Gestión están agrupados en cinco Dominios. Los Dominios expresan el propósito de los objetivos que contienen



COBIT y Otros estándares

- Una de las reglas de oro que se aplicó a lo largo de todo el desarrollo de COBIT 2019 fue mantener la posición de COBIT como marco de referencia general (Esto significa que COBIT 2019 sigue alineado con una serie de estándares, marcos de referencia y/o regulaciones relevantes
  - COBIT no contradice ninguna directriz de los estándares relacionados
  - COBIT no copia los contenidos de dichas estándares relacionados
  - COBIT proporciona declaraciones o referencias equivalentes a la directrices vinculadas

COBIT y Otros estándares

- CIS® Center for Internet Security®, *The CIS Critical Security Controls for Effective Cyber Defense*, Versión 6.1, agosto 2016
- Cloud standards and good practices:
  - Amazon Web Services (AWS®)
  - *Security Considerations for Cloud Computing*, ISACA
  - *Controls and Assurance in the Cloud: Using COBIT® 5*, ISACA
- CMMI® Cybermaturity Platform, 2018
- CMMI® Data Management Maturity (DMM)℠ model, 2014
- CMMI® Development V2.0, CMMI Institute, USA, 2018
- Comité de Organizaciones Patrocinadoras (COSO) Enterprise Risk Management (ERM) Framework, junio 2017
- Comité europeo de normalización (CEN), *e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework*, EN 16234-1:2016
- HITRUST® Common Security Framework, version 9, September 2017
- Information Security Forum (ISF), *The Standard of Good Practice for Information Security 2016*
- Normativa de la Organización Internacional de Normalización / Comisión Electrotécnica Internacional (ISO/CEI)
  - ISO/CIE 20000-1:2011(E)
  - ISO/CIE 27001:2013/Cor.2:2015(E)
  - ISO/CIE 27002:2013/Cor.2:2015(E)
  - ISO/CIE 27004:2016(E)
  - ISO/CIE 27005:2011(E)
  - ISO/CIE 38500:2015(E)
  - ISO/CIE 38502:2017(E)
- PROSCI® 3-Phase Change Management Process
- Scaled Agile Framework for Lean Enterprises (SAFe®)
- Skills Framework for the Information Age (SFIA®) V6, 2015
- The Open Group IT4IT™ Reference Architecture, versión 2.0
- The Open Group Standard TOGAF® versión 9.2, 2018
- The TBM Taxonomy, The TBM Council
- Normativa del Instituto de Estándares y Tecnología de Estados Unidos (NIST):
  - *Framework for Improving Critical Infrastructure Cybersecurity* V1.1, abril 2018
  - Special Publication 800-37, Revisión 2 (Borrador), mayo 2018
  - Special Publication 800-53, Revisión 5 (Borrador), agosto 2017
- "Options for Transforming the IT Function Using Bimodal IT," *MIS Quarterly Executive* (documentación técnica)
- *A Guide to the Project Management Book of Knowledge: PMBOK® Guide, 6.ª Edición*, 2017

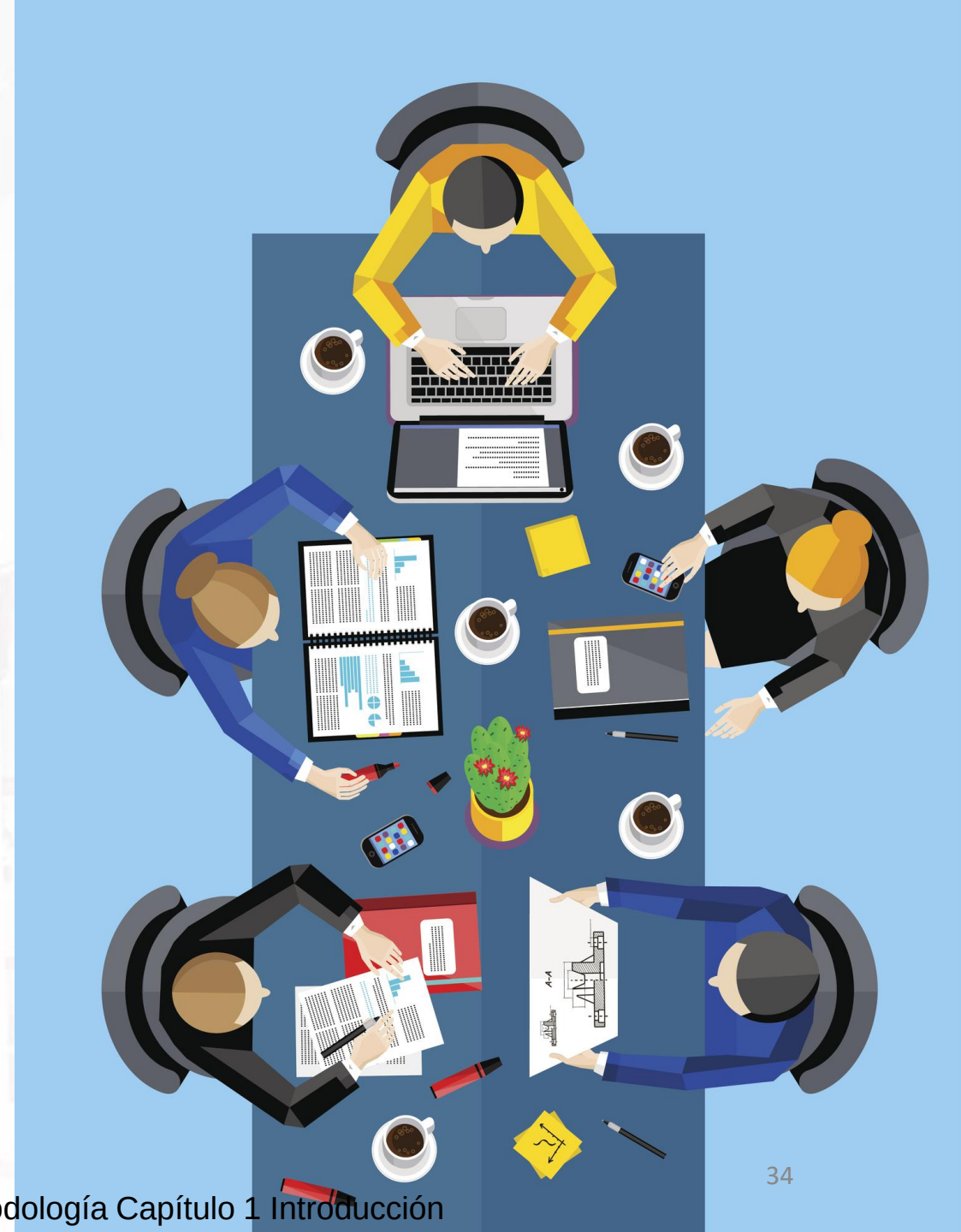
Comparativa ente Modelo de Gobierno de TI

	ISO/IEC 38500	COBIT
DEFINICIÓN	Define el ***qué*** hacer del buen gobierno.	Define el ***qué*** y ***cómo*** lo debe hacer.
ALCANCE	Tiene como alcance el ***qué*** del uso aceptable de las TI por parte de gobierno corporativo de TI.	Tiene como alcance la integralidad representada en el ***qué*** del uso aceptable de las TI por parte del gobierno corporativo y el gobierno de gestión de TI.
AMBITO	Se aplican a todas las organizaciones, pequeñas o grandes, públicas o privadas, con fines y sin fines de lucro.	Se aplican a todas las organizaciones, pequeñas o grandes, públicas o privadas, con fines y sin fines de lucro.
PRACTICAS	Evaluar, Dirigir y Monitorear	Evaluar, Orientar y Supervisar
BENEFICIOS	Genera beneficios prestando la debida atención al modelo y aplicando correctamente los Principios.	Genera beneficios en el soporte a las decisiones, valor en TI, alcance de excelencia operativa, control de riesgos, costes óptimos y, cumplimiento regulatorio y político.
PRINCIPIOS	6	9
METRICAS	No	Si
ENFOQUE	Actividades	Procesos

Gobierno vs Gestión

Gobierno vs Gestión

- El marco de referencia COBIT hace una distinción clara entre gobierno y gestión.
- Estas dos disciplinas abarcan distintos tipos de actividades, requieren distintas estructuras organizativas y sirven diferentes propósitos.
- ¿En que se diferencian?

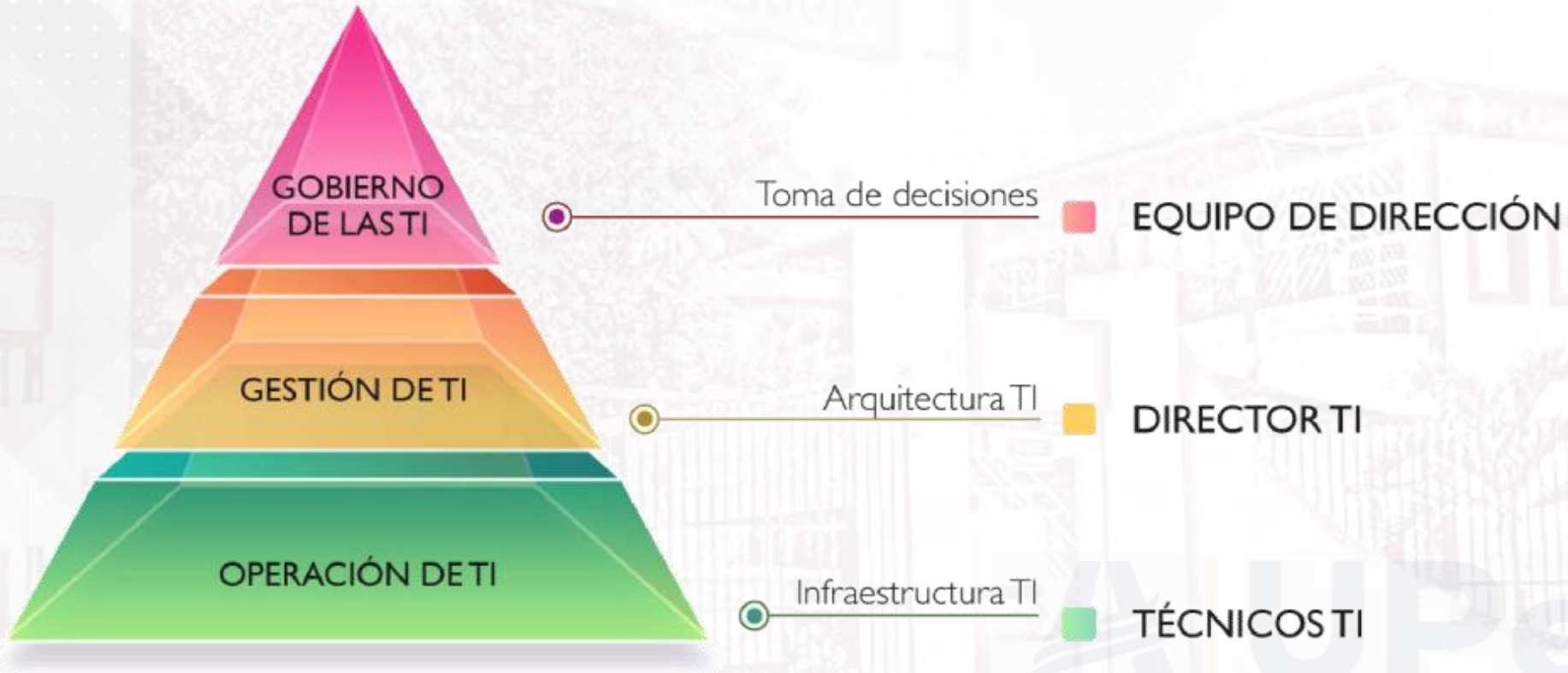


Referencia: Marco de referencia COBIT 2019: Introducción y metodología Capítulo 1 Introducción

Gobierno vs Gestión

- El **gobierno de las TI** es ver a nivel de bosque, mientras que la **gestión de las TI** es ver a nivel de árbol.
- **Administrar** es decidir el presente en función del pasado, mientras que **liderar** es decidir el presente en función del futuro.

Gobierno vs Gestión



https://tic.crue.org/gobierno-de-las-ti/

Gobierno vs Gestión

- El Gobierno **asegura** que:
  1. Las necesidades, condiciones y opciones de los interesados, son evaluados para determinar objetivos de la empresa balanceados y acordados.
  2. La dirección es establecida a través de la priorización y toma de decisiones.
  3. El rendimiento y cumplimiento es monitoreado contra la dirección y objetivos acordados.
- En la mayoría de empresas, todo **el gobierno es responsabilidad de la junta de directores**, bajo el liderazgo de su presidente
- Responsabilidades específicas de gobierno pueden ser delegadas a estructuras especiales de la organización en un apropiado nivel, en particular en empresas grandes o complejas.

Gobierno vs Gestión

- La **Gestión planifica**, **construye**, **ejecuta** y **monitorea** las actividades conforme a las directivas fijadas por el ente de Gobierno para lograr los objetivos de la Empresa.
- En la mayoría de las empresas, la gestión es responsabilidad de la gerencia ejecutiva, bajo el liderazgo del CEO.

Diferencia entre Gobierno y Gestión

La **gestión** se centraría en **administrar e implementar** las estrategias en el día a día, mientras que el **gobierno** se encargaría de **fijar** dichas estrategias junto con la política y la cultura de la organización.

El gobierno de TI se define como los procesos que aseguran el uso efectivo y eficiente de TI para permitir que una organización logre sus objetivos.

GARNER

https://www.gartner.com/en/information-technology/glossary/it-governance

Actividades

Desarrollar las actividades en Patmos

Referencias

- ISO 38500 (2013) Gobernanza corporativa de la Tecnología de la Información (TI)
- ISO 9001 Gestión de la Calidad
- ISO (2018) Organización Internacional de Normalización. Dirección electrónica: https://www.iso.org/home.html
- García. 2018. Gobierno de las tecnologías de la información. GRupo de investigación en InterAcción y eLearning (GRIAL). Universidad de Salamanca.
- Sachahuaman. N. 2020. Introducción al marco COBIT 2019. New Horizons. Computer Learning Centers.
- ISACA. 2018. MARCO DE REFERENCIA COBIT® 2019: INTRODUCCIÓN Y METODOLOGÍA.
- ISO/CEI 38500:2015. Tecnología de la información — Gobernanza de TI para la organización. Disponible en: https://www.iso.org/standard/62816.html