GOBERNANZA DE TI

ELSA ESTEVEZ
UNIVERSIDAD NACIONAL DEL SUR
DEPARTAMENTO DE CIENCIAS E INGENIERIA DE LA COMPUTACION

OBJETIVO Y AGENDA

OBJETIVO

Introducir el concepto de Gobernanza de TI, explicar el enfoque de “Control Objectives for Information and Related Technologies (COBIT)” para la gobernanza de TI y cómo la gobernanza de TI se puede aplicar, por ejemplo, en gobierno

AGENDA

1	CONCEPTO	¿Qué es la Gobernanza de TI?
2	ENFOQUE	¿Cuál es el enfoque de COBIT a la Gobernanza de TI? ○ Marco ○ Elementos
3	APLICACIONES	¿Qué experiencias existen de aplicar COBIT en el sector público?
4	RESUMEN	¿Qué se cubrió en esta sesión?

CONCEPTO

La Gobernanza de TI es un subconjunto de Gobierno Corporativo de las organizaciones que se centra en los sistemas de TI, su desempeño y los riesgos asociados.

GOBERNANZA DE TI

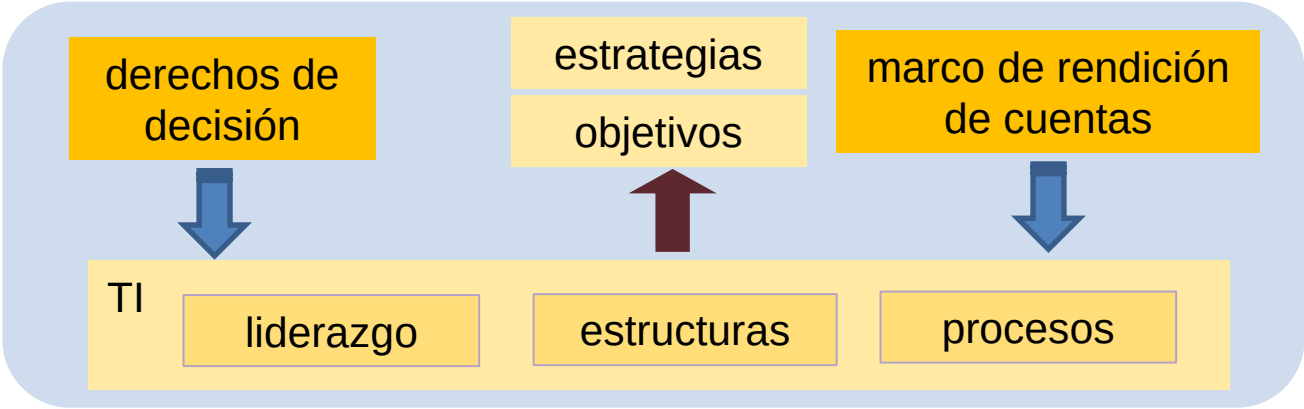
- trata con la relación entre el enfoque empresarial y la gestión de TI
- destaca la importancia de las cuestiones de TI
- promueve que las decisions estratégicas de TI deben ser tomadas por una junta directiva corporativa

METAS

- asegurar que las inversiones en TI generen valor
- mitigar riesgos asociados con TI

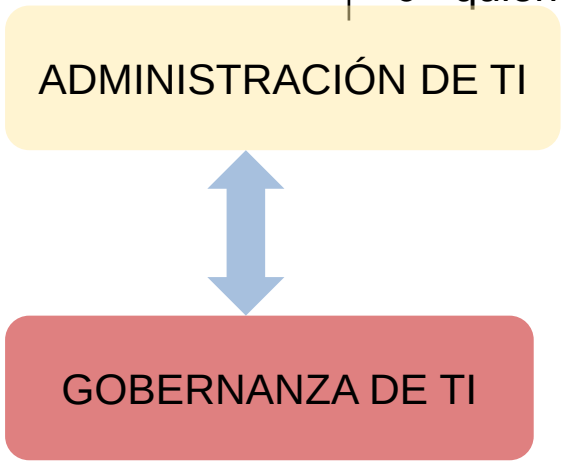
DEFINICIONES

INSTITUTO DE GOBERNANZA DE TI	son estructuras y procesos de liderazgo y organizativos que aseguran que las TI de la organización sostienen y extienden las estrategias y los objetivos de la organización
WEILL, ROSS	se trata de especificar los derechos de decision y el marco de rendición de cuentas para fomenter el comportamiento deseable en el uso de TI
ESTANDAR AUSTRALIANO PARA EL GOBIERNO CORPORATIVO DE TI	es el sistema por el cual se dirige y controla el uso actual y futuro de las TIC. Implica evaluar y dirigir los planes para el uso de las TIC para apoyar a la organización y monitorear este uso para alcanzar los planes. Incluye la estrategia y las políticas para el uso de las TIC dentro de una organización



DOS CONCEPTOS DIFERENTES

ADMINISTRACIÓN DE TI	se trata de tomar e implementar decisiones de TI
GOBERNANZA DE TI	se trata de quién toma las decisiones de TI ○ quién tiene autoridad para tomar las decisiones importantes ○ quién tiene información para tomar las decisiones importantes ○ quién es responsible por implementar las decisions importantes

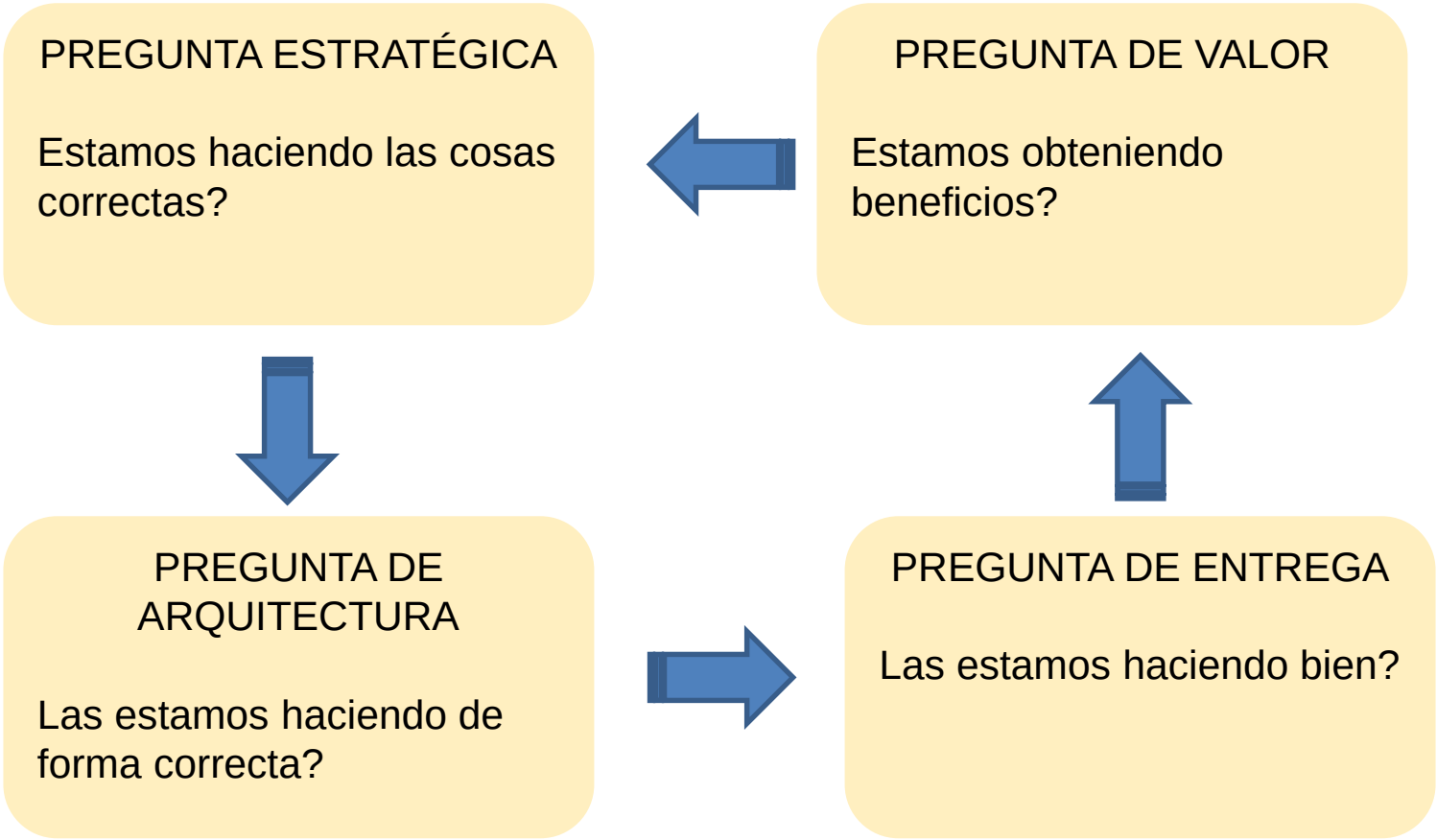


ÁREAS DE ENFOQUE

CINCO ÁREAS DE ENFOQUE – todas impulsadas por el valor de las partes interesadas

RESULTADOS	1) entrega de valor 2) manejo de riesgos
CONDUCTORES	3) alineamiento estratégico 4) manejo de recursos 5) mediciones de desempeño

PREGUNTAS CLAVE



PREGUNTA ESTRATÉGICA

La inversión en TI …

1	está alineada con la visión?
2	es consistente con los principios de negocio?
3	está contribuyendo a los objetivos estratégicos?
4	está proporcionando un valor óptimo, a un costo accesible y un nivel de riesgo aceptable?

EJEMPLO – SERVICIO DE INSPECCIÓN Y SEGURIDAD ALIMENTARIA (FSIS), DEPARTAMENTO DE AGRICULTURA DE LOS ESTADOS UNIDOS (US DOA)

VISION DE LA AGENCIA	Una agencia confiable de regulación de la salud pública comprometido a prevenir enfermedades transmitidas por alimentos. http://www.fsis.usda.gov/PDF/Strategic_Plan_2011-2016.pdf
INVERSIÓN EN TI	SISTEMA DE INFRAESTRUCTURA DE COMUNICACIÓN DE DATOS DE SALUD PÚBLICA (PHDCIS) mejora la capacidad de los empleados, las plantas, el comercio, los laboratorios, la frontera y las oficinas centrales y de campo de recibir información para analizar, trabajar en equipo y responder a emergencias en tiempo real y tomar medidas preventivas para reducer las enfermedades transmitidas por alimentos. http://www.itdashboard.gov/investment&buscid=230

PREGUNTA DE ARQUITECTURA

La inversión en TI…

1	está alineada con la arquitectura de la agencia?
2	es consistente con los principios arquitectónicos de la agencia?
3	está contribuyendo a la población de nuestra arquitectura?
4	está en línea con otras iniciativas?

EJEMPLO– FSIS, US DOA, PHDCIS

ARQUITECTURA DE LA AGENCIA	Para cumplir con su misión, FSIS require un robusto sistema de infraestructura de TI que sea capaz de soportar todas las actividades de campo y todos los demás sistemas de TI de FSIS http://www.itdashboard.gov/investment&buscid=230
INVERSIÓN EN TI	○ automatiza y reemplaza muchos de los sistemas FSIS existentes, tales como PBIS, RIS y AIIS. ○ Integra estos sistemas separados y dispares en un sistema completo de análisis de datos fácil de usar e impulsado por datos. http://www.fsis.usda.gov/PPT/PHIS_Stakeholder_Briefing.ppt

PREGUNTA DE ENTREGA

Tenemos …

1	procesos efectivos y disciplinados de administración, entrega y gestión de cambios?
2	recursos técnicos y gubernamentales competentes y disponibles para entregar: ○ las prestaciones requeridas? ○ Los cambios organizacionales necesarios para aprovechar las prestaciones?

EJEMPLO – FSIS, US DOA, PHDCIS

PRESTACIONES REQUERIDAS	se desarrolló y brindó capacitación a través de 10 sesiones en 3 ubicaciones geográficas, proporcionando un total de 100 clases. El programa de capacitación enseñó a más de 4000 empleados de campo sobre la consolidación, reemplazo y expansión de los sistemas heredados de FSIS de PHIS, incluyendo el Sistema de Inspección Basado en el Rendimiento (PBIS), el Sistema Automatizado de Información de Importaciones (AIIS), el Sistema de Seguimiento de Portadores Positivos de E. coli O157:H7 (STEPS), y otros sistemas. En sesiones adicionales se proporcionan reseñas para el personal de la industria y de las oficinas centrales. (META 7 – Brindar a los empleados capacitación, recursos y herramientas para lograr el éxito en la protección de la salud pública) http://www.fsis.usda.gov/PDF/FY2013_Budget_Explanatory_Notes.pdf

PREGUNTA DE VALOR

Tenemos …

1	una comprensión clara y compartida de los beneficios esperados?
2	una clara responsabilidad para la obtención de los beneficios?
3	métricas relevantes para la medición de los beneficios?
4	un proceso efectivo de realización de beneficios?

EJEMPLO – FSIS, US DOA

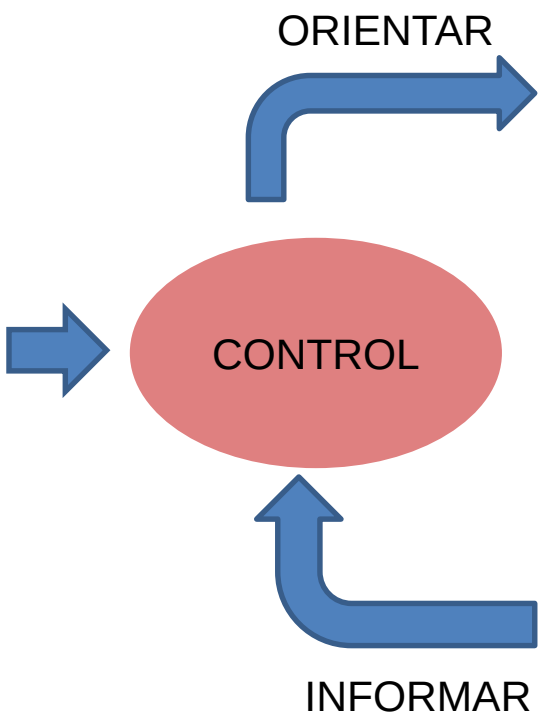
BENEFICIO	SATISFACCIÓN DEL CLIENTE MÉTRICA: Encuestas de satisfacción del cliente para interfaces de servicios de escritorio, 4 puntos o mejor en una escala del 1-5. MUESTRA: 114 clientes BASE: 85; MÁS RECIENTE: 91, INFORMES: mensualmente Métricas de rendimiento - https://explore.data.gov/download/ambf-v8fe/CSV

CICLO DE VIDA

GOBERNANZA DE TI

OBJETIVOS

- La TI está alineada con las metas de la organizació
- Los recursos de TI son usados responsablemente
- Los riesgos relacionados con TI son gestionados adecuadamente



ACTIVIDADES DE TI

PLAN	Planear y Organizar
DO	Adquirir e Implementar
USE	Entregar y Mantener
CHECK	Monitorear y Evaluar

GESTIONAR RIESGOS	OBTENER BENEFICIOS

ÁREAS RELACIONADAS

La Gobernanza de TI es apoyada por :

1	Gestión de los activos de TI
2	Gestión del portfolio de TI
3	Gestión de infraestructura de TI y arquitectura empresarial
4	Estándares de TI
5	Gestión de programas
6	Gestión de proyectos
7	Gestión de servicios de TI
8	Gestión de la seguridad de TI
…	otros

ENFOQUES

1	OBJETIVOS DE CONTROL PARA INFOMACIÓN Y TECNOLOGÍA RELACIONADA (COBIT) Enfoque para estandarizar buenas practices de TI y control. Provee herramientas para accede y medir el desempeño de los procesos de gobernanza y administración de TI de una organización. Desarrollado y mantenido por el Instituto de Governanza de TI - *http://www.itgi.org/*
2	BIBLIOTECA DE INFRAESTRUCTURA DE TI (ITIL) Marco detallado con información sobre cómo lograr una gobernanza de TI exitosa. Desarrollado y mantenido por la Oficina de Comercio Gubernamental del Reino Unido - *http://www.ogc.gov.uk*
3	ISO 27001 Conjunto de buenas prácticas a seguir para las organizaciones cuando se implementa y mantiene un programa de seguridad.
4	MODELO DE MADUREZ DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ISM3) Proceso basado en el modelo de madurez de gestión de la seguridad de la información - *http://www.ism3.com*
5	AS8015-2005 Estándar Australiano para el Gobierno Corporativo de las Tecnologías de Información y Comunicación

OBJETIVO Y AGENDA

OBJETIVO

Introducir el concepto de Gobernanza de TI, explicar el enfoque de “Control Objectives for Information and Related Technologies (COBIT)” para la gobernanza de TI y cómo la gobernanza de TI se puede aplicar, por ejemplo, en gobierno

AGENDA

1	CONCEPTO	¿Qué es la Gobernanza de TI?
2	ENFOQUE	¿Cuál es el enfoque de COBIT a la Gobernanza de TI? ○ Marco
		○ Elementos
3	APLICACIONES	¿Qué experiencias existen de aplicar COBIT en el sector público?
4	RESUMEN	¿Qué se cubrió en esta sesión?

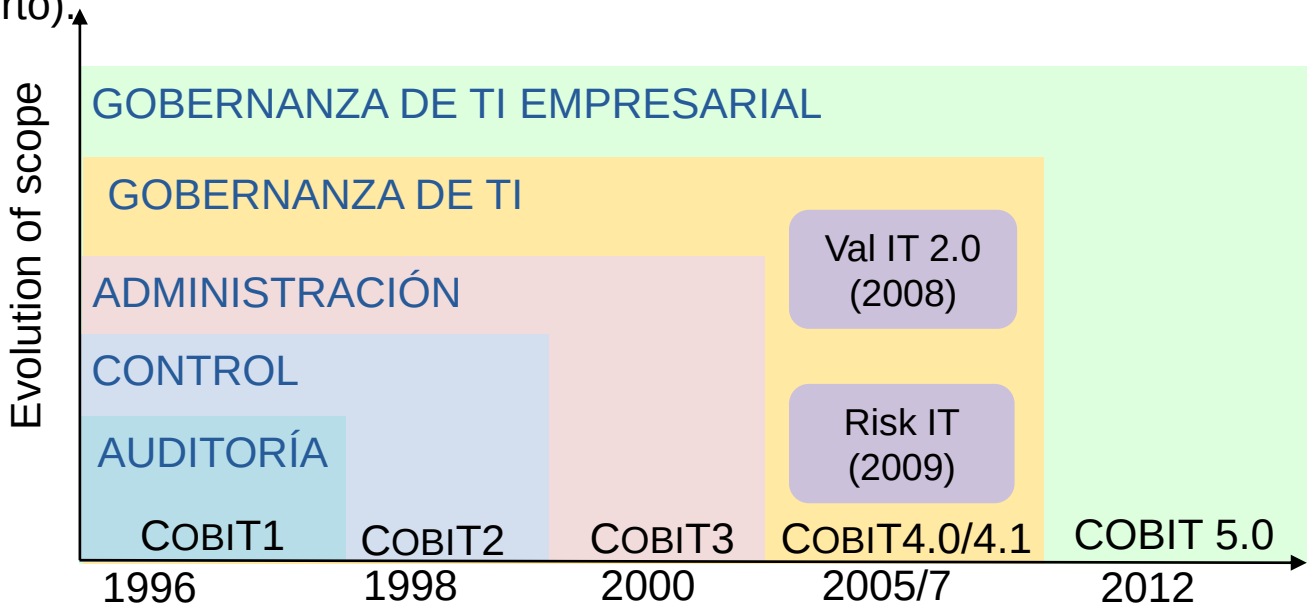
COBIT

OBJETIVOS DE CONTROL PARA INFORMACIÓN Y TECNOLOGÍA RELACIONADA (COBIT) es un conjunto de recursos que contienen toda la información que las organizaciones necesitan para adopter un marco de gobernanza y control de TI.

Fue creado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, www.isaca.org) y el Instituto de Gobernanza de TI en 1992.

COBIT 5 consolida COBIT 4.1, Val IT y Risk IT en un marco y se ha actualizado para alinearse con las mejores prácticas actuales, por ejemplo ITIL V3 2011, TOGAF (El Marco de Arquitectura de Grupo Abierto).

1996	Primera edición
1998	Segunda edición
2000	Tercera edición
2003	Edición online
2005	Cuarta edición
2007	Versión 4.1
2012	Versión 5.0



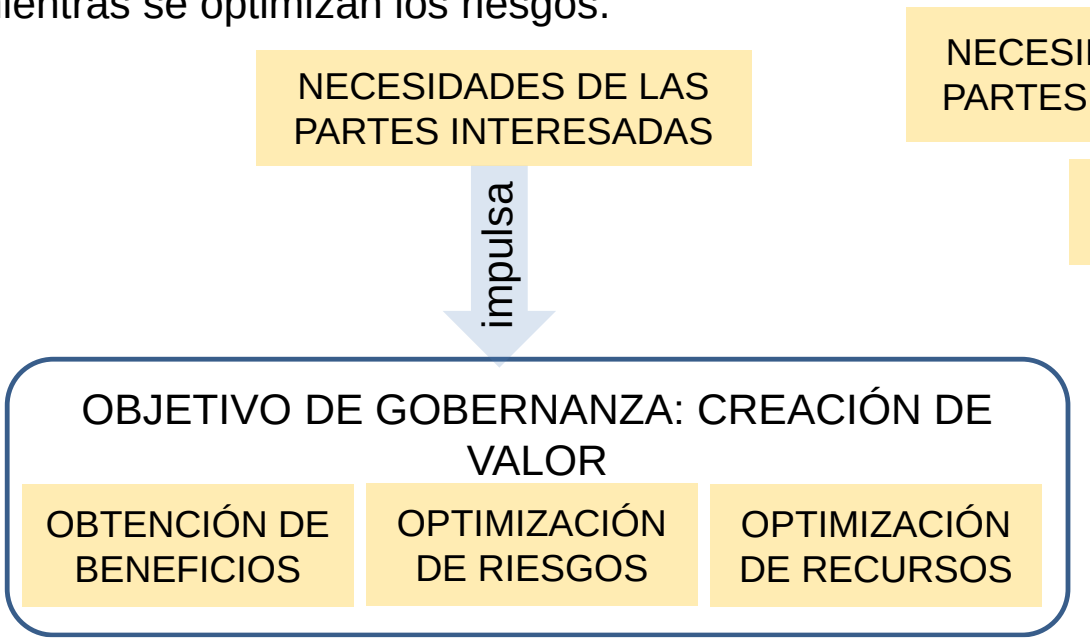
PRINCIPIOS

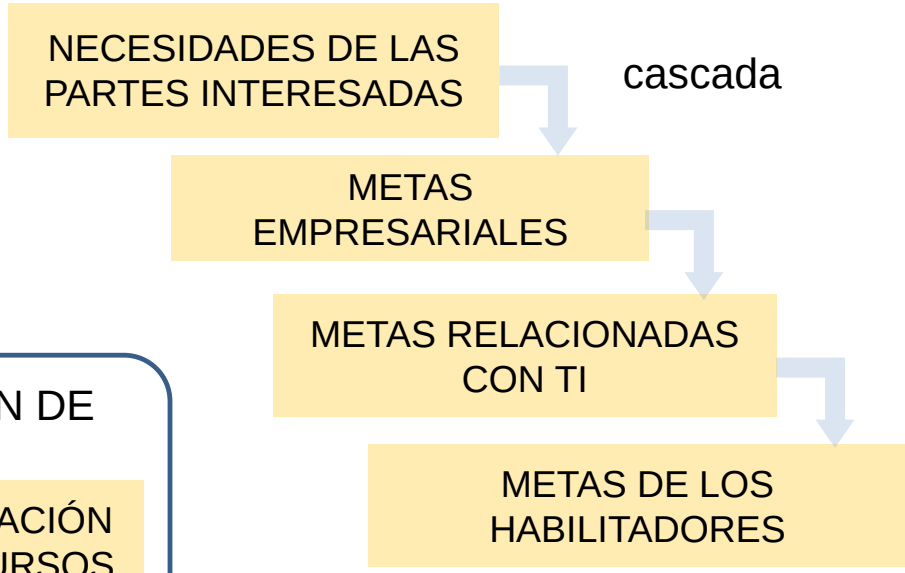
1) Satisfacer las necesidades de las partes interesadas	Garantizar que las empresas aporten valor a sus partes interesadas mediante la obtención de beneficios, la optimización del uso de los recursos y la gestión de riesgos.
2) Cubrir la empresa de extremo a extremo	Tener en cuenta todos los sistemas de gobernanza y administración relacionados con TI para que sean integrales y de extremo a extremo – incluyendo tanto sistemas internos como externos.
3) Aplicar un marco integrado	Alinearse con otros estándares y buenas prácticas relacionadas con TI, sirviendo de marco general para la gobernanza y administración de TI empresarial.
4) Habilitar un enfoque holístico	Tener en cuenta los elementos que interactúan, especificar un conjunto de habilitadores para definer un sistema integral de gobernanza y administración de TI empresarial.
5) Separar las funciones principales	Establecer una distinción clara entre las funciones de gobernanza y administración.

P1 – SATISFACER LAS NECESIDADES DE LAS PARTES INTERESADAS – CASCADA DE METAS

Todas las empresas deben aportar valor a sus partes interesadas. Por lo tanto, la creación de valor es un objetivo de gobernanza de toda organización.

El valor puede ser creado mediante la obtención de beneficios a un costo óptimo de recursos mientras se optimizan los riesgos.





Las necesidades de las partes interesadas necesitan ser transformadas en una estrategia empresarial. La cascada de metas es un mecanismo para transformar las necesidades de las partes intersadas en metas empresariales, metas relacionadas con TI y metas de los habilitadores.

METAS - EJEMPLO

Las metas empresariales y las relacionadas con TI se estructuran según de las dimensiones del Cuadro de Mando Integral (CMI) y del CMI TI.

Dim.	Metas Empresariales	Metas Relacionadas con TI
Financiera (F)	1. Valor de las partes interesadas de las inversions empresariales	1. Alineación de TI y estrategia empresarial
	5. Transparencia financiera	4. Gestión de riesgos de negocio relacionados con TI
Cliente (C)	6. Cultura de servicio orientada al cliente	7. Entrega de servicio de TI en línea con los requerimientos del negocio
	7. Continuidad y disponibilidad del servicio empresarial	8. Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna (I)	12. Optimización de los costos de los procesos de negocio	9. Agilidad de TI
	14. Productividad operativa y de personal	10. Seguridad de la información, infraestructura de procesamiento y aplicaciones
Aprendizaje y crecimiento (LG)	16. Personas calificadas y motivadas	16. Personal empresarial y de TI competente y motivado
	17. Cultura de innovación de productos y negocios	17. Conocimiento, experiencia e iniciativas para la innovación empresarial

CASCADA DE METAS - EJEMPLO

Meta Estratégica	Mejorar la satisfacción del cliente
Metas Empresariales	6. Cultura de servicio orientada al cliente (C)
	7. Continuidad y disponibilidad del servicio empresarial (C)
	8. Respuestas ágiles a un ambiente empresarial cambiante (C)
Metas Relacionadas con TI	1. Alineación de TI y estrategia empresarial (F)
	4. Gestión de riesgos de negocio relacionados con TI (F)
	7. Entrega de servicio de TI en línea con los requerimientos del negocio (C)
	9. Agilidad de TI (I)
	10. Seguridad de la información, infraestructura de procesamiento y aplicaciones (I)
	14. Disponibilidad de información confiable y útil para la toma de decisiones (I)
	17. Conocimiento, experiencia e iniciativas para la innovación empresarial (LG)

La organización decide priorizar las primeras cuatro metas relacionadas con TI. Las metas relacionadas con TI impulsan las metas de los habilitadores, las cuales incluyen las metas de proceso.

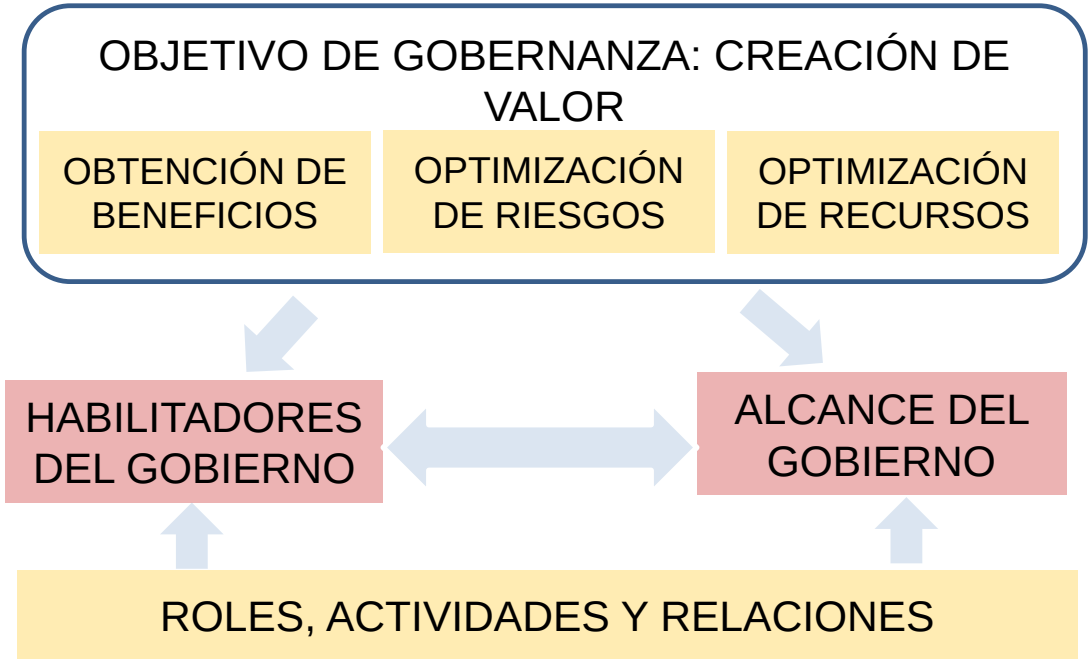
CASCADA DE METAS Y PROCESOS DE TI - EJEMPLO

Figure 23—Mapping COBIT 5 IT-related Goals to Processes *(cont.)*

			IT-related Goal															
			Alignment of IT and business strategy	IT compliance and support for business compliance with external laws and regulations	Commitment of executive management for making IT-related decisions	Managed IT-related business risk	Realised benefits from IT-enabled investments and services portfolio	Transparency of IT costs, benefits and risk	Delivery of IT services in line with business requirements	Adequate use of applications, information and technology solutions	IT agility	Security of information, processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of business processes by integrating applications and technology into business processes	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	Availability of reliable and useful information for decision making	IT compliance with internal policies	Competent and motivated business and IT personnel	Knowledge, expertise and initiatives for business innovation
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
	COBIT 5 Process		Financial						Customer		Internal							Learning and Growth	
nd Implement	BAI01	Manage Programmes and Projects	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Manage Requirements Definition	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Manage Solutions Identification and Build	S			S	S		P	S			S	S	S	S			S
	BAI04	Manage Availability and Capacity				S	S		P	S	S		P		S	P			S

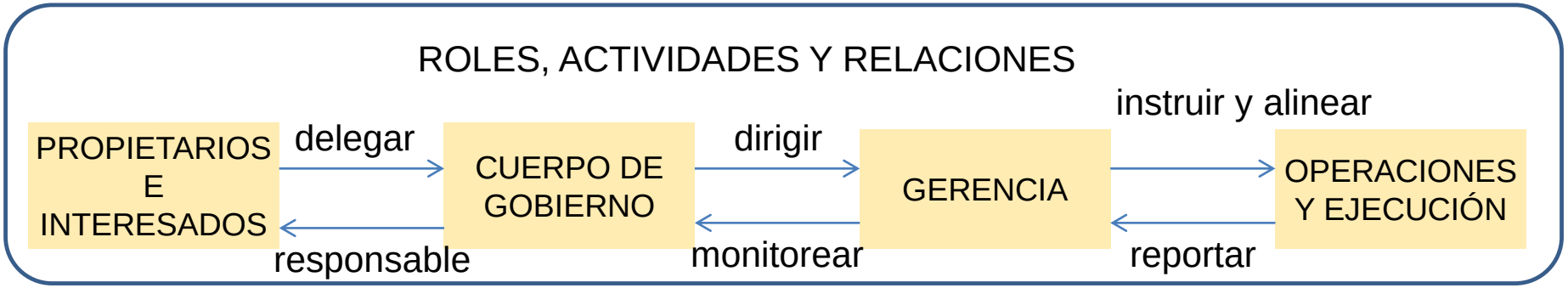
[Cortesía: COBIT 5 – An ISACA Framework www.isaca.org]

P2 – ENFOQUE DE GOBERNANZA DE EXTREMO A EXTREMO



HABILITADORES – recursos organizacionales para gobernanza, como marcos, principios, estructuras, etc., y recursos empresariales, como servicios, capacidades, personas, información.

ALCANCE: la empresa o cualquier punto de vista de la empresa - entidad, active – a los que se puede aplicar la gobernanza

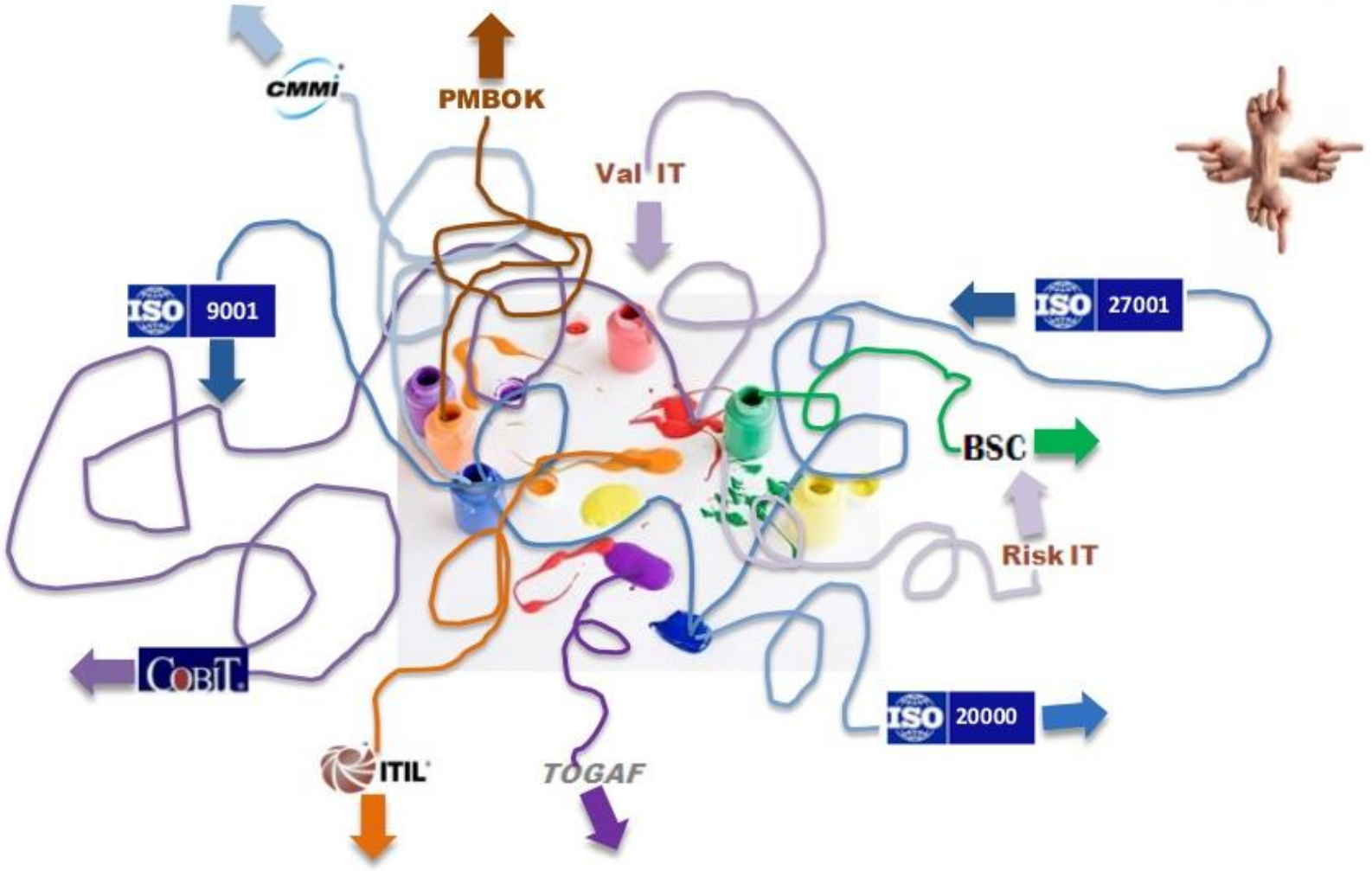


P3 – APLICAR UN MARCO INTEGRADO

COBIT 5:

- Se alinea con los estándares y marcos más recientes y pertinentes
- Es completo en la cobertura de la empresa
- Proporciona una base para integrar efectivamente otros marcos, estándares y prácticas utilizadas
- Integra todo el conocimiento hasta ahora disperso en diferentes marcos de ISACA
- Proporciona una arquitectura simple para la estrucuración de los materiales de orientación y la producción de un conjunto de productos compatibles

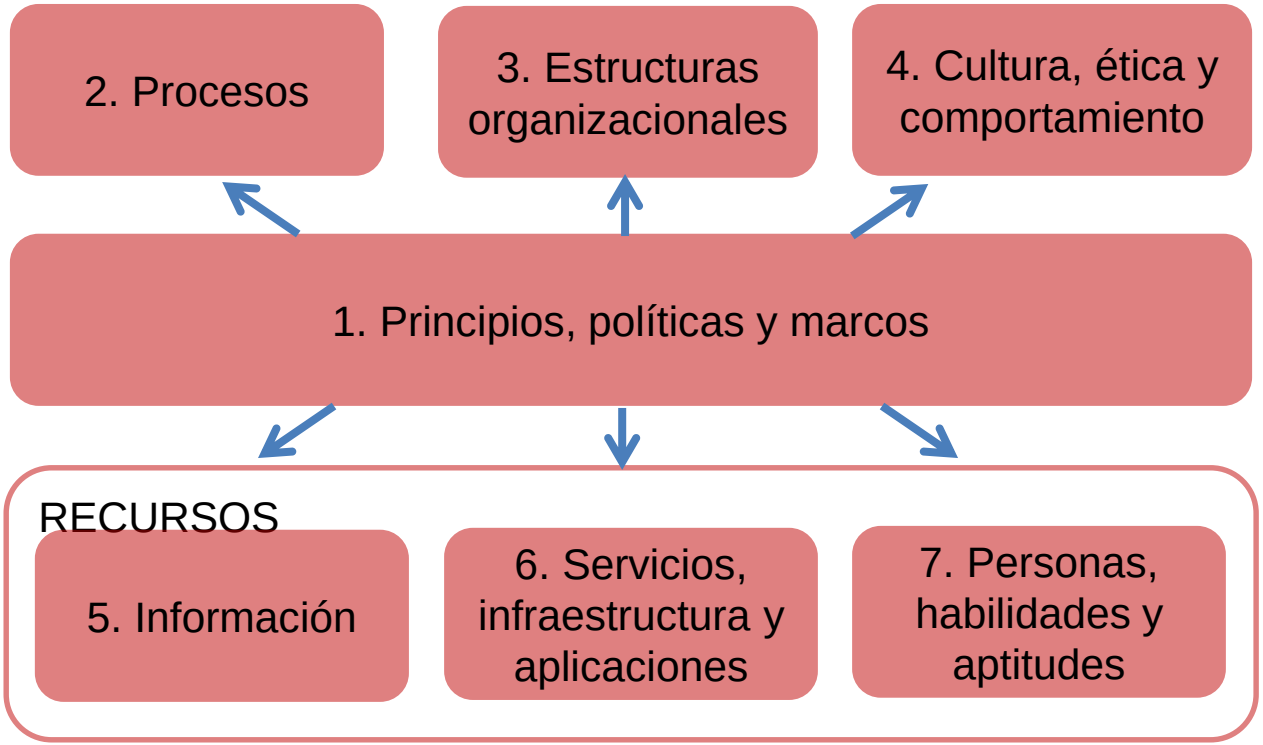
LA MARAÑA DE LAS MEJORES PRÁCTICAS



P4 – HABILITAR UN ENFOQUE HOLÍSTICO

Los habilitadores son factores que, de manera individual y colectiva, influyen en si algo funcionará, en este caso, la gobernanza y administración de TI de la empresa.

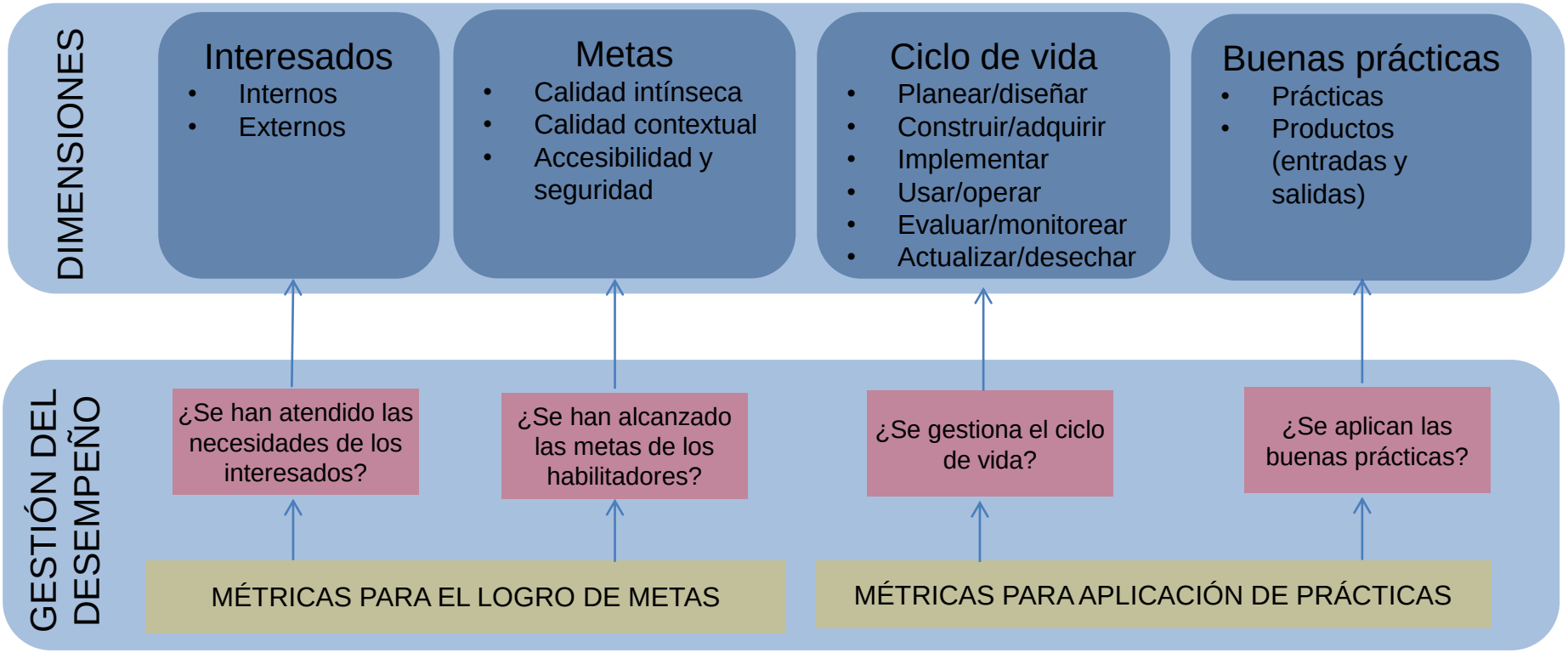
COBIT define siete categorías de habilitadores



DIMENSIONES DE LOS HABILITADORES DE COBIT 5

Todos los habilitadores tienen un conjunto de dimensiones comunes:

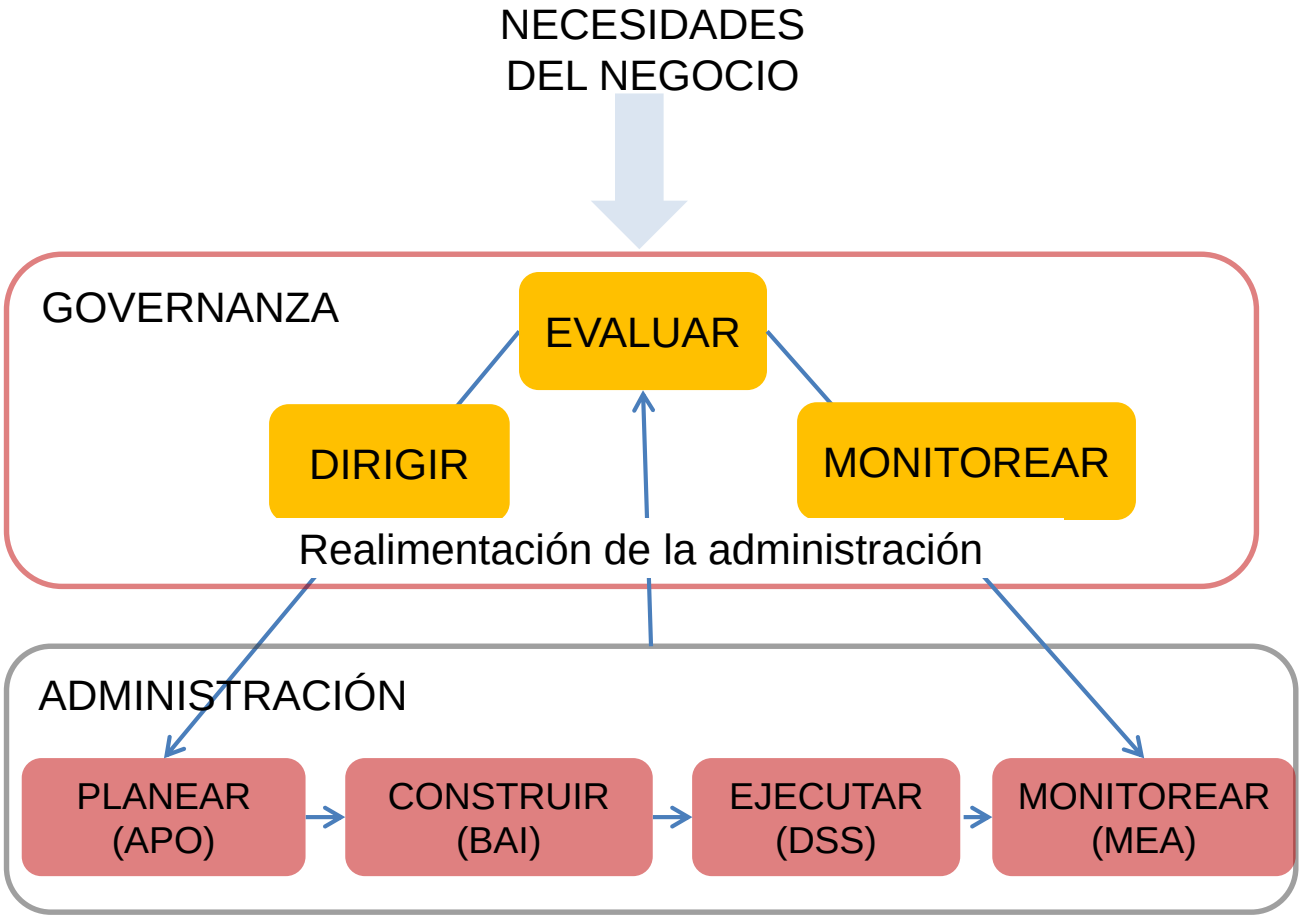
- Es una forma sencilla y estructurada para tratar los habilitadores
- Le permite a una entidad gestionar sus complejas interacciones
- Facilita el éxito de los resultados de los habilitadores



P5 – SEPARAR LAS FUNCIONES PRINCIPALES

GOBERNANZA	asegura: ○ que las necesidades, condiciones y opciones de las partes interesadas son evaluadas para determinar objetivos empresariales a alcanzar equilibrados y acordados ○ establecer la dirección a través de la priorización y la toma de decisiones ○ supervisando el desempeño y cumplimiento contra la dirección y objetivos acordados
ADMINISTRACIÓN	planifica, construye, ejecuta y monitorea las actividades en consonancia con la dirección establecida por el cuerpo de gobierno para alcanzar los objetivos empresariales

MODELO DE REFERENCIA DEL PROCESO



COBIT 5.0 divide los procesos en 2 dominios:

1) GOVERNANZA – incluye 5 procesos, dentro de cada uno de ellos se definen prácticas de Evaluar, Dirigir y Monitorear.

2) ADMINISTRACIÓN – incluye 32 procesos clasificados en 4 dominios – APO, BAI, DSS y MEA.

CARACTERÍSTICAS PRINCIPALES

- incorpora los principales estándares internacionales
- está centrado en los negocios, orientado a procesos, controlado y medido
- opera a un nivel más alto que los estándares de tecnología pura para la administración de sistemas de información
- puede ser adaptado por organizaciones mundiales comerciales, gubernamentales y profesionales

AUDIENCIA

GERENTES	les ayuda a equilibrar el riesgo y control de la inversion en un ambiente de TI a menudo impredecible
USUARIOS	les garantiza seguridad y control de los servicios de TI internos o proporcionados por terceros
AUDITORES	les ayuda a definir el nivel de seguridad sobre el objeto particular a auditar los asesora sobre la gestión de los controles internos

OBJETIVO Y AGENDA

OBJETIVO

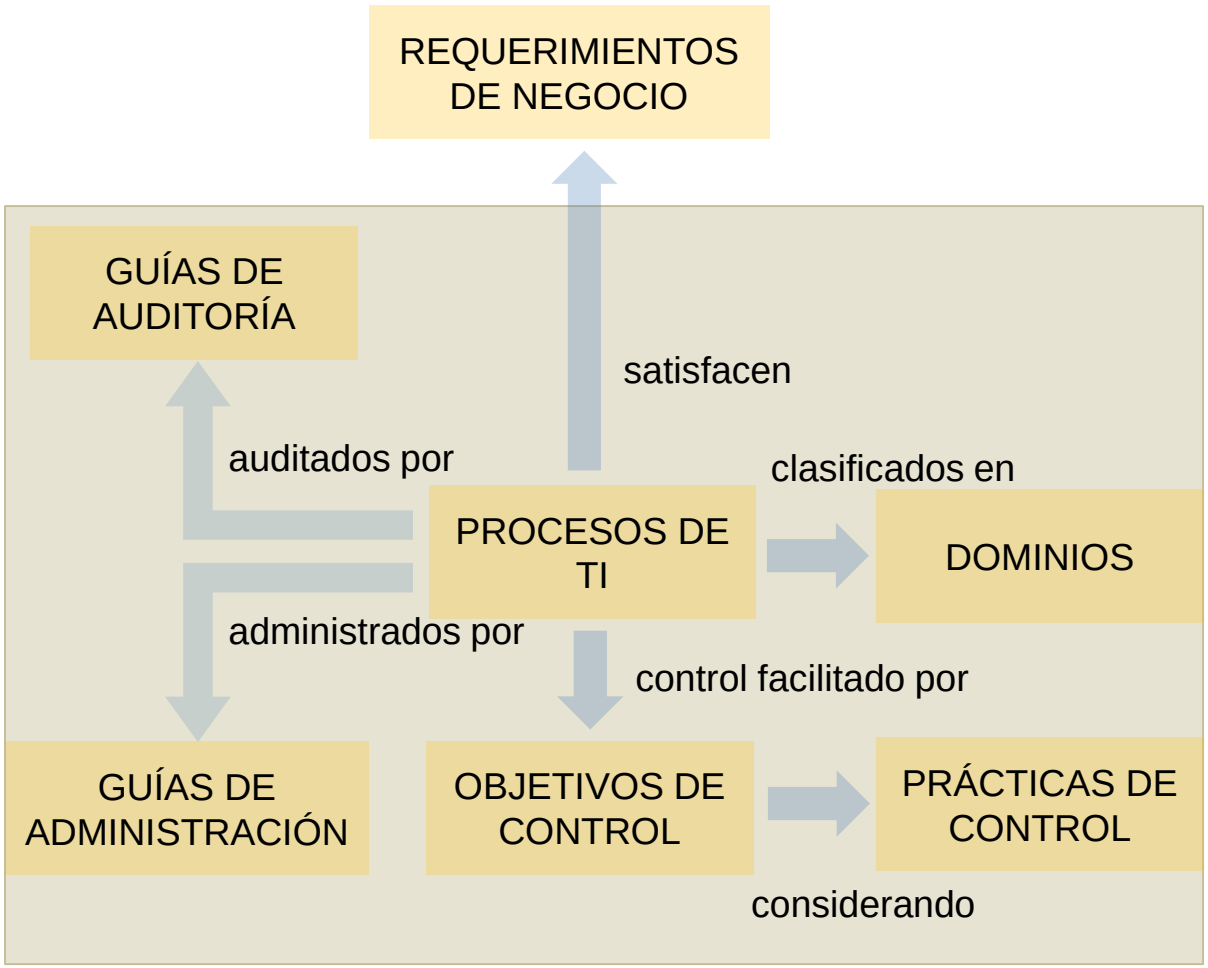
Introducir el concepto de Gobernanza de TI, explicar el enfoque de “Control Objectives for Information and Related Technologies (COBIT)” para la gobernanza de TI y cómo la gobernanza de TI se puede aplicar, por ejemplo, en gobierno

AGENDA

1	CONCEPTO	¿Qué es la Gobernanza de TI?
2	ENFOQUE	¿Cuál es el enfoque de COBIT a la Gobernanza de TI?
		○ Marco
		○ Elementos
3	APLICACIONES	¿Qué experiencias existen de aplicar COBIT en el sector público?
4	RESUMEN	¿Qué se cubrió en esta sesión?

ELEMENTOS

1. Procesos de TI y Dominios (5)
2. Objetivos de Control (4.1)
3. Prácticas de Control (4.1)
4. Guías de Auditoría (4.1)
5. Guías de Administración (4.1)



PROCESOS DE GOBERNANZA

Contiene cinco procesos de gobernanza. Para cada proceso se definen prácticas de evaluar, dirigir y monitorear (EDM).

EDM se interesa en:

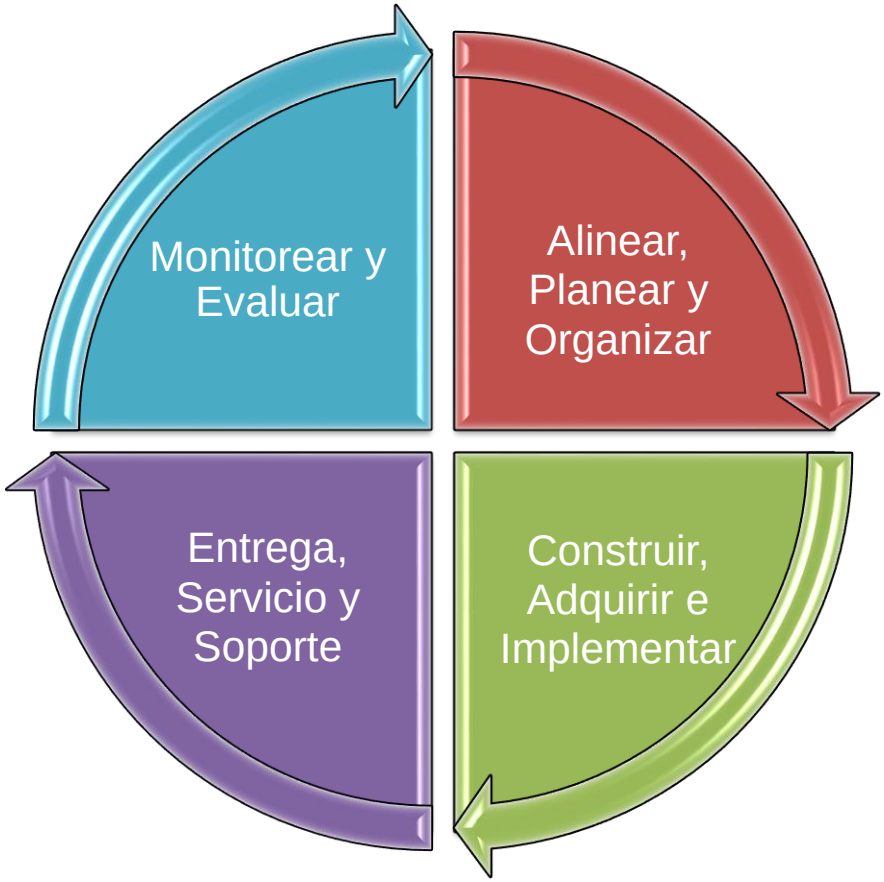
- establecer un marco de gobernanza
- crear valor para las partes interesadas
- asegura que los objetivos de la empresa sean alcanzados EVALUANDO las necesidades, condiciones y opciones de las partes interesadas, ´estableciendo DIRECCIÓN mediante la priorización y la toma de decisions, y MONITOREANDO el desempeño, el cumplimiento y el progreso contra la dirección y los objetivos acordados (EDM).

EDM – PROCESOS DE TI	
EDM1	Asegurar el marco de gobernanza, el establecimiento y el mantenimiento
EDM2	Asegurar la entrega de beneficios
EDM3	Asegurar la optimización de riesgos
EDM4	Asegurar la optimización de recursos
EDM5	Asegurar la transparencia de las partes interesadas

PROCESOS DE ADMINISTRACIÓN

COBIT clasifica la Administración de TI en 4 dominios:

Alinear, Planear y Organizar (APO)	proporciona direcciones a la entrega de soluciones y servicios
Construir, Adquirir e Implementar (BAI)	provee soluciones a DSS para la entrega de servicios
Entrega, Servicio y Soporte (DSS)	recibe soluciones y las hace utilizables para los usuarios finales
Monitorear y Evaluar (MEA)	monitorea todos los procesos para asegurar que se siga la dirección provista



ALINEAR, PLANEAR Y ORGANIZAR

Alinear, Planear y Organizar (APO) abarca estrategias y tácticas y se interesa en la forma que TI puede contribuir a alcanzar los objetivos de negocio.

APO se interesa en:

- la comprensión de la vision a planificar, comunicar y gestionar
- una organización e infraestructura adecuadas para su puesta en marcha

APO – PROCESOS DE TI	
APO01	Gestionar el marco de administración de TI
APO02	Gestionar estrategias
APO03	Gestionar la arquitectura empresarial
APO04	Gestionar la innovación
APO05	Gestionar el portfolio
APO06	Gestionar presupuesto y costos
APO07	Gestionar los recursos humanos
APO08	Gestionar las relaciones
APO09	Gestionar los acuerdos de servicio
APO10	Gestionar proveedores
APO11	Gestionar la calidad
APO12	Gestionar los riesgos
APO13	Gestionar la seguridad

CONSTRUIR, ADQUIRIR E IMPLEMENTAR

Construir, Adquirir e Implementar (BAI) abarca soluciones de TI que necesitan ser identificadas, desarrolladas o adquiridas, implementadas e integradas en el proceso de negocio

BAI se enfoca en:

- los cambios en las soluciones de TI existentes
- el mantenimiento de sistemas existentes
- asegurar que las soluciones continúan cumpliendo con las metas empresariales

BAI – PROCESOS DE TI	
BAI01	Gestionar programas y proyectos
BAI02	Gestionar la definición de requerimientos
BAI03	Gestionar la identificación y construcción de soluciones
BAI04	Gestionar la disponibilidad y capacidad
BAI05	Gestionar la habilitación del cambio organizacional
BAI06	Gestionar cambios
BAI07	Gestionar el cambio de aceptación y transición
BAI08	Gestionar el conocimiento
BAI09	Gestionar activos
BAI10	Gestionar la configuración

ENTREGA, SERVICIO Y SOPORTE

Entrega, Servicio y Soporte (DSS) trata sobre la entrega efectiva de los servicios requeridos, incluyendo operaciones, seguridad y capacitaciones de continuidad.

DSS se enfoca en:

- la gestión de seguridad y continuidad del servicio
- el soporte de servicios para usuarios
- la administración de datos
- instalaciones operacionales

DSS – PROCESOS DE TI	
DSS01	Gestionar operaciones
DSS02	Gestionar peticiones e incidents de servicio
DSS03	Gestionar problemas
DSS04	Gestionar continuidad
DSS05	Gestionar servicios de seguridad
DSS06	Gestionar procesos de control del negocio

MONITOREAR Y EVALUAR

Monitorear y Evaluar (MEA) trata de la evaluación regular de los procesos de TI para controlar su calidad y el cumplimiento de los requisitos de control.

MEA se enfoca en:

- la gestión de desempeño
- el cumplimiento normativo
- el control interno

MEA – PROCESOS DE TI	
MEA01	Monitorear y evaluar el desempeño y conformidad
MEA02	Monitorear y evaluar el sistema de controles internos
MEA03	Monitorear y evaluar el cumplimiento de los requisitos externos

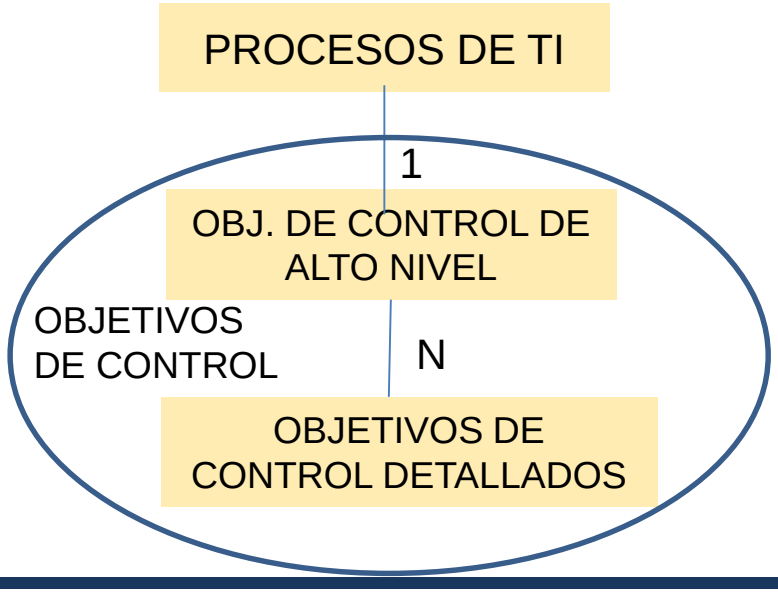
OBJETIVO DE CONTROL DE TI

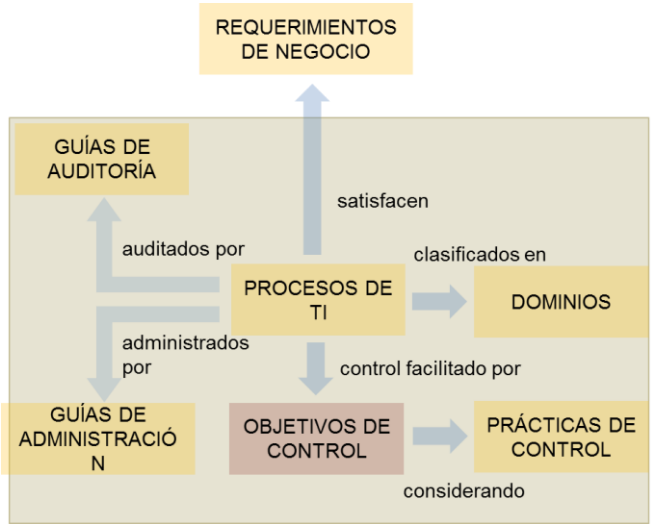
Declaración del resultado o proposito a alcanzar mediante la implementación de procesos de control en una actividad particular de TI,

COBIT proporciona un conjunto de 34 objetivos de control de alto nivel, uno para cada uno de los procesos de TI.

Cada objetivo de control de alto nivel se subdivide en una lista de objetivos de control detallados.

COBIT contiene 318 objetivos de control detallados para los 34 procesos de TI.





OBJETIVOS DE CONTROL DE ALTO NIVEL - EJEMPLO

OBJETIVOS DE CONTROL DE TI: DS2 – GESTIONAR SERVICIOS DE TERCEROS

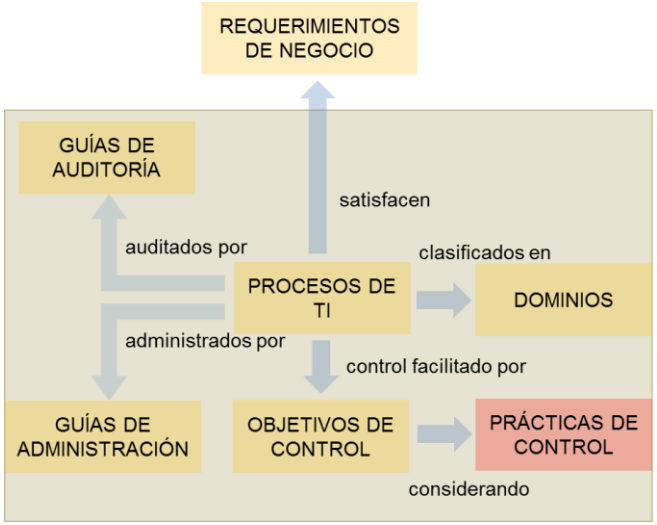
satisface los requisitos de negocio	para asegurar que los roles y las responsabilidades de terceros estén claramente definidos, adheridos y continúen satisfaciendo los requerimientos
está habilitado por	medidas de control destinadas a la revision y el monitoreo de los acuerdos y procedimientos existentes para su eficacia y cumplimiento de las políticas de la organización
tiene en consideración	○ acuerdos de servicio de terceros ○ gestión de contratos ○ acuerdos de no divulgación ○ requisitos legales y regulatorios ○ monitoreo de la entrega de servicios y reportes ○ evaluación de riesgos empresariales y de TI ○ recompensas y penalizaciones de desempeño ○ responsabilidad organizacional interna y externa ○ análisis de costos y variaciones de servicio

OBJETIVOS DE CONTROL DETALLADOS – EJEMPLO

OBJETIVOS DE CONTROL DE TI: DS2 – GESTIONAR SERVICIOS DE TERCEROS		
OBJETIVOS DE CONTROL DETALLADOS	DS2.1	INTERFACES DEL PROVEEDOR La dirección debe asegurarse que están debidamente identificados todos los servicios de terceros y las interfaces técnicas y organizacionales con los proveedores
	DS2.2	RELACIONES CON EL DUEÑO
	DS2.3	CONTRATOS DE TERCEROS
	DS2.4	CALIFICACIONES DE TERCEROS
	DS2.5	CONTRATOS DE EXTERNALIZACIÓN
	DS2.6	CONTINUIDAD DE SERVICIOS
	DS2.7	RELACIONES DE SEGURIDAD
	DS2.8	MONITOREO

PRÁCTICAS DE CONTROL

Las prácticas de control de TI proporcionan el más detallado POR QUÉ y CÓMO que necesitan los administradores, los proveedores de servicios, los usuarios finales y los profesionales de control para implementar controles específicos basados en un análisis de los riesgos operacionales y de TI.



ESTRUCTURA DE CONTROL EFECTIVA

QUÉ?

Procesos de TI
Requisitos de negocio
Objetivos de control detallados

CÓMO, POR QUÉ?

Prácticas de control de TI

PRÁCTICAS DE CONTROL - EJEMPLO

DS2.1 INTERFACES DEL PROVEEDOR

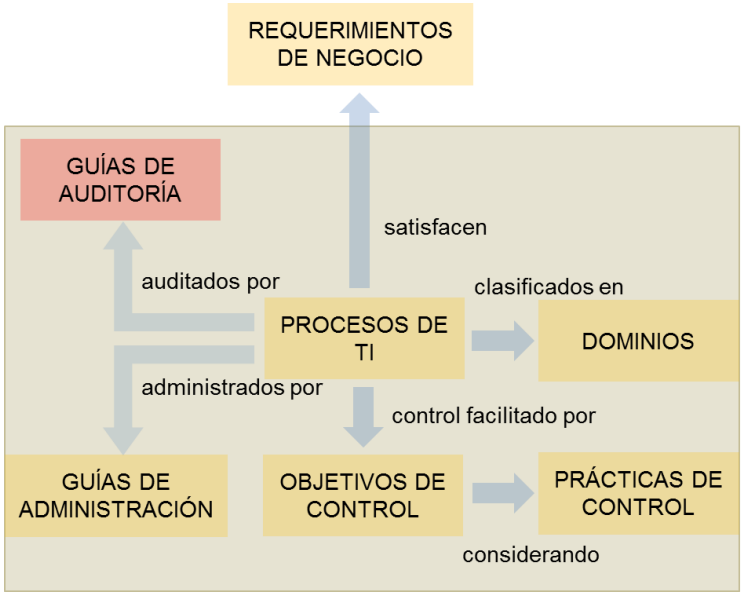
POR QUÉ HACERLO?	La identificación y definición de interfaces técnicas y organizativas proporcionadas por proveedores en línea con las prácticas de control: ○ Promoverá relaciones que apoyen los objetivos organizacionales generales (tanto de negocio como de TI) ○ Facilitará una comunicación efectiva (incluyendo la resolución de problemas) entre las organizaciones para ayudar a mantener una entrega de servicios efectiva …
PRÁCTICAS DE CONTROL	○ Se desarrollan políticas y procedimientos para mantener un registro de proveedores clave para la función de TI. El registro detalla el nombre, el proveedor y la naturaleza, el alcance y el propósito de la relación. Los procedimientos se vinculan, y deben integrarse, con los procedimientos de administración de la obtención y configuración. ○ El registro de proveedores de TI se revisa periódicamente para asegurarse de que permanence actualizado. …

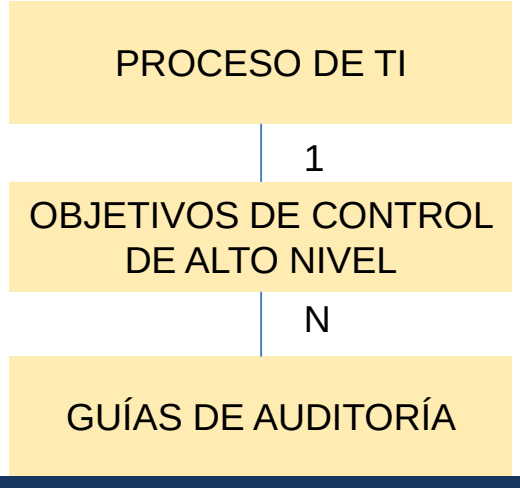
GUÍAS DE AUDITORÍA

Las guías de auditoria describen y sugieren las actividades de evaluación que se corresponderán a cada uno de los 34 objetivos de TI de alto nivel

Proporcionan direcciones sobre:

- a quién entrevistar y qué preguntas hacer
- cómo evaluar el cumplimiento de los controles y las evaluaciones
- cómo comprobar el riesgo de que no se cumplan los controles identificados





GUíAS DE AUDITORÍA - EJEMPLO

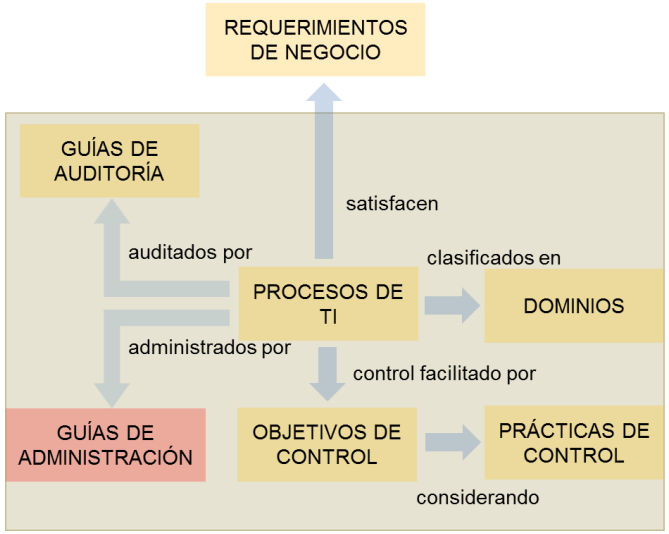
DS2 – GESTIONAR SERVICIOS DE TERCEROS

ENTREVISTANDO	○ Dirección de información ○ Dirección de TI ○ Administración de contratos y servicios de TI ○ Administración de operaciones de TI ○ Oficina de seguridad
OBTENIENDO	○ Políticas y procedimientos de la organización relacionados con los servicios adquiridos y, en particular, las relaciones con proveedores ○ Políticas y procedimientos de TI relacionadas con las relaciones con terceros, procedimientos de selección, contratos de las relaciones, seguridad física y lógica, mantenimiento de calidad de los proveedores, planes de contingencia y externalización ○ Lista de todas las relaciones con terceros y contratos reales…
EVALUANDO EL CONTROL POR...	Existen políticas y procedimientos de TI relacionados con relaciones con terceros y son consistentes con las políticas generales de la organización …

GUÍAS DE ADMINISTRACIÓN

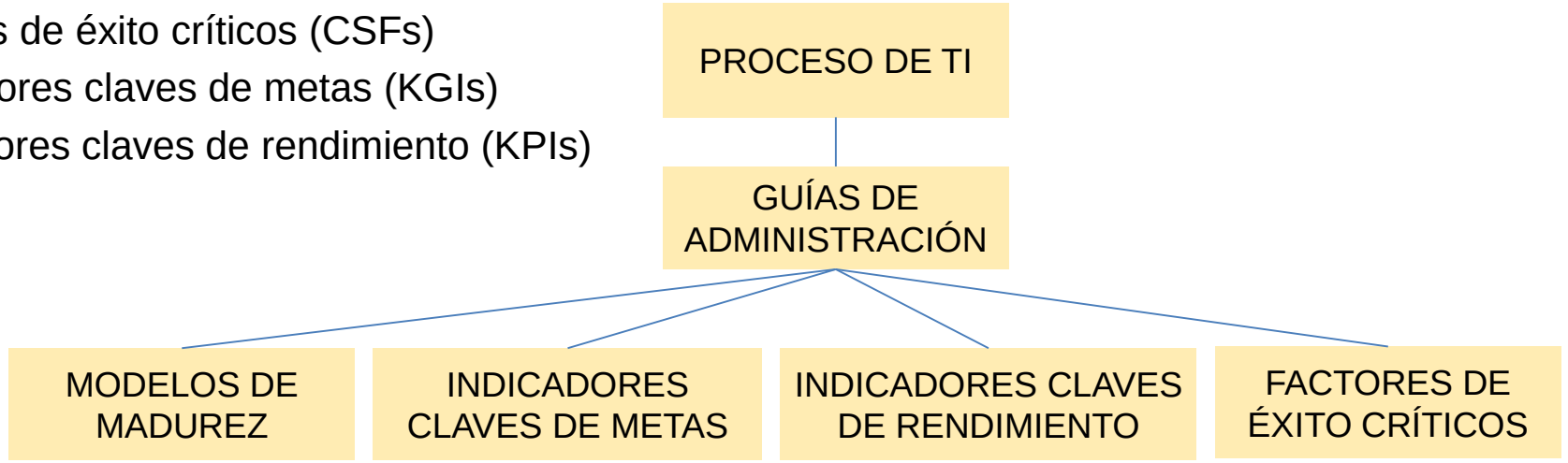
Las guías de administración proporcionan direcciones para:

- tener bajo control la información de la empresa y los procesos relacionados
- alcanzar los objetivos de la organización
- monitorear y mejorar el desempeño de cada proceso de TI
- comparar logros organizacionales



Para cada proceso de TI, las guías de administración incluyen:

- modelos de madurez(MMs),
- factores de éxito críticos (CSFs)
- Indicadores claves de metas (KGIs)
- indicadores claves de rendimiento (KPIs)



GUíAS DE ADMINISTRACIÓN – EJEMPLO MODELO DE MADUREZ (4.1)

DS2 – GESTIONAR SERVICIOS DE TERCEROS

0 – Inexistente	No se definen responsabilidades ni rendición de cuentas.
1 – Inicial	La administración es consciente de la necesidad de tener políticas y procedimientos documentados para la obtención de servicios de terceros y la firma de contratos, pero la medición del servicio es informal y reactiva.
2 – Repetible	El proceso de supervición de proveedores de servicios de terceros y la entrega de servicios es informal.
3 – Definido	Se tienen procedimientos bien documentados para la obtención de servicios de terceros, con procesos claros que aseguran una negociación con los proveedores e investigación adecuada.
4 – Administrado	Se establecen las responsabilidades de la gestión de contratos y proveedores para definir el alcance del trabajo, los servicios que se proveen, los entregables, etc**.**
5 – Optimizado	El contrato firmado conjuntamente se revisa periódicamente después de empezar el trabajo. Se asigna responsabilidad por la aseguración de la calidad de la prestación del servicio y del soporte.

GUíAS DE ADMINISTRACIóN – EJEMPLO FACTORES DE ÉXITO E INDICADORES

DS2 – GESTIONAR SERVICIOS DE TERCEROS

FACTORES DE ÉXITO CRÍTICOS	○ Existen requisites de servicio y medidas de rendimiento claramente definidos ○ La organización mantiene la responsabilidad y el control y gestiona proactivamente los servicios externos …
INDICADORES CLAVES DE METAS	○ Porcentaje de proveedores de servicios con objetivos formalmente acordados ○ Porcentaje de proveedores de servicios formalmente calificados ….
INDICADORES CLAVES DE RENDIMIENTO	○ Número y frecuencia de reuniones de revisión ○ Número de asuntos pendientes ○ Plazo para resolver problemas …

OBJETIVO Y AGENDA

OBJETIVO

Introducir el concepto de Gobernanza de TI, explicar el enfoque de “Control Objectives for Information and Related Technologies (COBIT)” para la gobernanza de TI y cómo la gobernanza de TI se puede aplicar, por ejemplo, en gobierno

AGENDA

1	CONCEPTO	¿Qué es la Gobernanza de TI?
2	ENFOQUE	¿Cuál es el enfoque de COBIT a la Gobernanza de TI? ○ Marco ○ Elementos
3	APLICACIONES	¿Qué experiencias existen de aplicar COBIT en el sector público?
4	RESUMEN	¿Qué se cubrió en esta sesión?

ALGUNAS EXPERIENCIAS

ORGANIZACIÓN	MOTIVACIÓN
Gobierno de Dubai, UEA	Provee objetivos de control y mejora la gobernanza de TI
Oficina de Servicios Civiles de Bahréin, Bahréin	El marco de trabajo más detallado y globalmente respetado para implementar la gobernanza de TI
Organización Gubernamental Australiana, Canberra, Australia	Un marco de trabajo muy detallado para la implementación de controles, auditoria y estrategias de testeo
Consejo de Pensión de Ontario, Canadá	Conducir una auto-evaluacion de las funciones de TI como parte del proceso de mejora continua
Corte de Auditores de Mendoza, Argentina	Mejorar la gobernanza de y la administración de fondos públicos dedicados a sistemas de información.

Fuentes: [http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Studies.aspx], An Analytical Study of IT Security Governance and its Adoption on Australian Organizations, Tanveer Zia

OFICINA DE SERVICIOS CIVILES DE BAHRÉIN

APLICACIÓN	COBIT se ha utilizado para fortalecer la infraestructura de TI de la Oficina de Servicios Civiles de Bahréin (CSB) y convertirse en la línea de base para todos los procesos de TI Los controles internos existentes se analizaron utilizando el marco COBIT Las áreas que recibieron la mayor atención relacionada con el control fueron el desarrollo de software, la administración de nómina y la administración de la base de datos.
RESULTADOS	Se preparó una matriz de modelo de madurez para mostrar los puntos fuertes y débiles en el entorno actual de CSB. Se aplicaron controles COBIT para eliminar los puntos débiles y este procedimiento se realizó con éxito Al implementar controles COBIT, se implementan los sistemas de control de acceso adecuados y se reducen los riesgos generales.

KINGDOM OF BAHRAIN
Civil Service Bureau

BENEFICIOS - GENERALES

- permite a los administradores públicos cerrar la brecha entre los requisitos de control, los problemas técnicos y los riesgos comerciales
- permite un desarrollo claro de políticas y buenas prácticas para el control de TI en todas las organizaciones gubernamentales
- enfatiza el cumplimiento regulatorio
- ayuda a las organizaciones del sector público a aumentar el valor obtenido de TI
- permite la alineación y simplifica la implementación de la gobernanza de TI en el sector público
- ayuda a los gobiernos a proporcionar servicios mejores y más personalizados a los ciudadanos y las empresas
- optimiza las inversiones en TI, garantiza una prestación de servicios efectiva y proporciona medidas

BENEFICIOS - ESPECÍFICOS

INSTITUCIÓN	BENEFICIO
Departamento Estadounidense de Asuntos de Veteranos, EEUU	○ cerrar las brechas entre los requisitos de control, los problemas técnicos y el riesgo comercial ○ permitir un desarrollo claro de políticas y mejores prácticas ○ enfatizar el cumplimiento regulatorio
Parlamento Europeo, Europa	El Parlamento Europeo identificó los proyectos adecuados para implementar y tiene una forma de hacer un seguimiento de los beneficios generados por estos proyectos.
Consejo de Pensión de Ontario, Canadá	○ brindar mejores y más servicios personalizados ○ establecer un marco integral para la gobernanza de TI que ayude a cerrar las brechas, optimizar las inversiones de TI, garantizar la prestación efectiva de servicios y proporcionar medidas

OBJETIVO Y AGENDA

OBJETIVO

Introducir el concepto de Gobernanza de TI, explicar el enfoque de “Control Objectives for Information and Related Technologies (COBIT)” para la gobernanza de TI y cómo la gobernanza de TI se puede aplicar, por ejemplo, en gobierno

AGENDA

1	CONCEPTO	¿Qué es la Gobernanza de TI?
2	ENFOQUE	¿Cuál es el enfoque de COBIT a la Gobernanza de TI? ○ Marco ○ Elementos
3	APLICACIONES	¿Qué experiencias existen de aplicar COBIT en el sector público?
4	RESUMEN	¿Qué se cubrió en esta sesión?

RESUMEN – 1

GOBERNANZA DE TI	parte del Gobierno Corporativo, consiste en especificar los derechos de decisión y el marco de rendición de cuentas para formentar el comportamiento deseable en el uso de TI	
ADMINISTRACIÓN DE TI	consiste en la toma e implementación de decisiones de TI	
GOBERNANZA	acerca de quién toma las decisiones de TI	
FOCO	RESULTADOS	CONDUCTORES
	1) entrega de valor 2) manejo de riesgos	3) alineamiento estratégico 4) manejo de recursos 5) mediciones de desempeño
ENFOQUES	○ COBIT ○ BIBLIOTECA DE INFRAESTRUCTURA DE TI (ITIL) ○ AS8015-2005	○ ISO 27001 ○ MODELO DE MADUREZ DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ISM3)

RESUMEN – 2

COBIT 5	es un conjunto de recursos que contienen todas las organizaciones de información que necesitan para adoptar una gobernanza de TI y un marco de control	
ELEMENTOS	Procesos de TI se dividen en 5 dominios (COBIT 5):	
	GOBERNANZA	ADMINISTRACIÓN
	1) Evaluar, Dirigir y Monitorear	2) Alinear, Planear y Organizar 3) Construir, Adquirir e Implementar 4) Entrega, Servicio y Soporte 5) Monitorear y Evaluar
	Objetivos de Control (COBIT 4.1)	
	Prácticas de Control (COBIT 4.1)	
	Guías de Auditoría (COBIT 4.1)	
	Guías de Administración (COBIT 4.1)	
APLICACIÓN EN EL SECTOR PÚBLICO	Argentina, Australia, Bahrain, Canada, UAE	

Elsa Estevez
ece@cs.uns.edu.ar