DIPLOMADO
CIBERSEGURIDAD
CAPACITACIÓN USACH - UNIVERSIDAD DE SANTIAGO DE CHILE

Verano 2024

Fundamentos de Controles

Fundamentos de COBIT

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

Qué es COBIT y Qué no es COBIT

- **COBIT ES:**
  - Un framework de gobernanza y gestión de la información y tecnología empresarial.
  - COBIT define las componentes para construir y soportar un sistema de gobierno
  - COBIT define los factores de diseño que debería ser considerados por las empresas para construir un sistema de gobierno
  - COBIT es flexible y permite su articulación con otras definiciones

- **COBIT NO ES:**
  - Una descripción detallada de el entorno de TI de una empresa
  - Un framework para organizar los procesos de negocio.
  - Un modelo técnico de TI para gestionar todas las tecnologías
  - COBIT no toma ni prescribe ninguna decisión relacionada con TI

COBIT: Objetivos de Control para la información y tecnologías relacionadas

Optimizando la gobernanza de la información y tecnologías

- TI: Utilizado para referirse al departamento organizacional con responsabilidad principal en la tecnología.
- I&T: Toda la información que la empresa genera, procesa y utiliza para lograr sus objetivos, así como la tecnología para respaldarla en toda la empresa.

Qué es COBIT y Qué no es COBIT

COBIT 2019 no es un control en sí mismo, sino un marco de referencia para la gestión y gobernanza de la tecnología de la información. Proporciona un conjunto comprensivo de prácticas, objetivos de control, herramientas de rendimiento y modelos de madurez que las organizaciones pueden utilizar para:

- Alinear las estrategias de TI con las estrategias de negocio.
- Asegurar que las inversiones en TI generen valor y su rendimiento sea medido.
- Gestionar los riesgos asociados a la TI.
- Asegurar que los servicios y soluciones de TI sean entregados eficientemente y de manera segura.

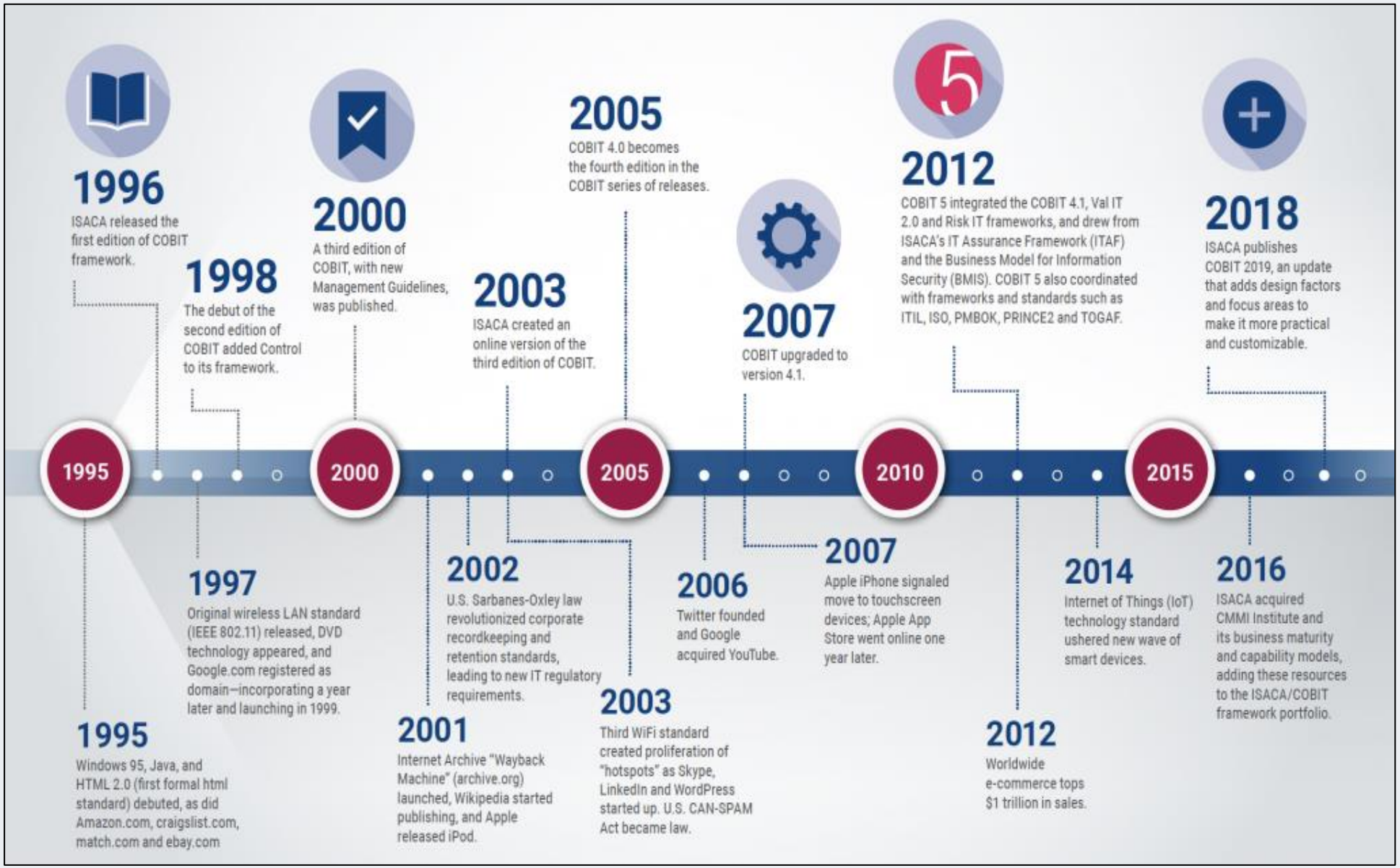
Los controles son componentes específicos dentro de un marco de referencia como COBIT que las organizaciones implementan para manejar riesgos, asegurar la fiabilidad de la información y cumplir con las políticas de TI. COBIT 2019 proporciona una estructura para ayudar a las organizaciones a desarrollar, implementar, monitorear y mejorar sus prácticas y controles de TI, pero en sí mismo no actúa como un control

DIPLOMADO CIBERSEGURIDAD

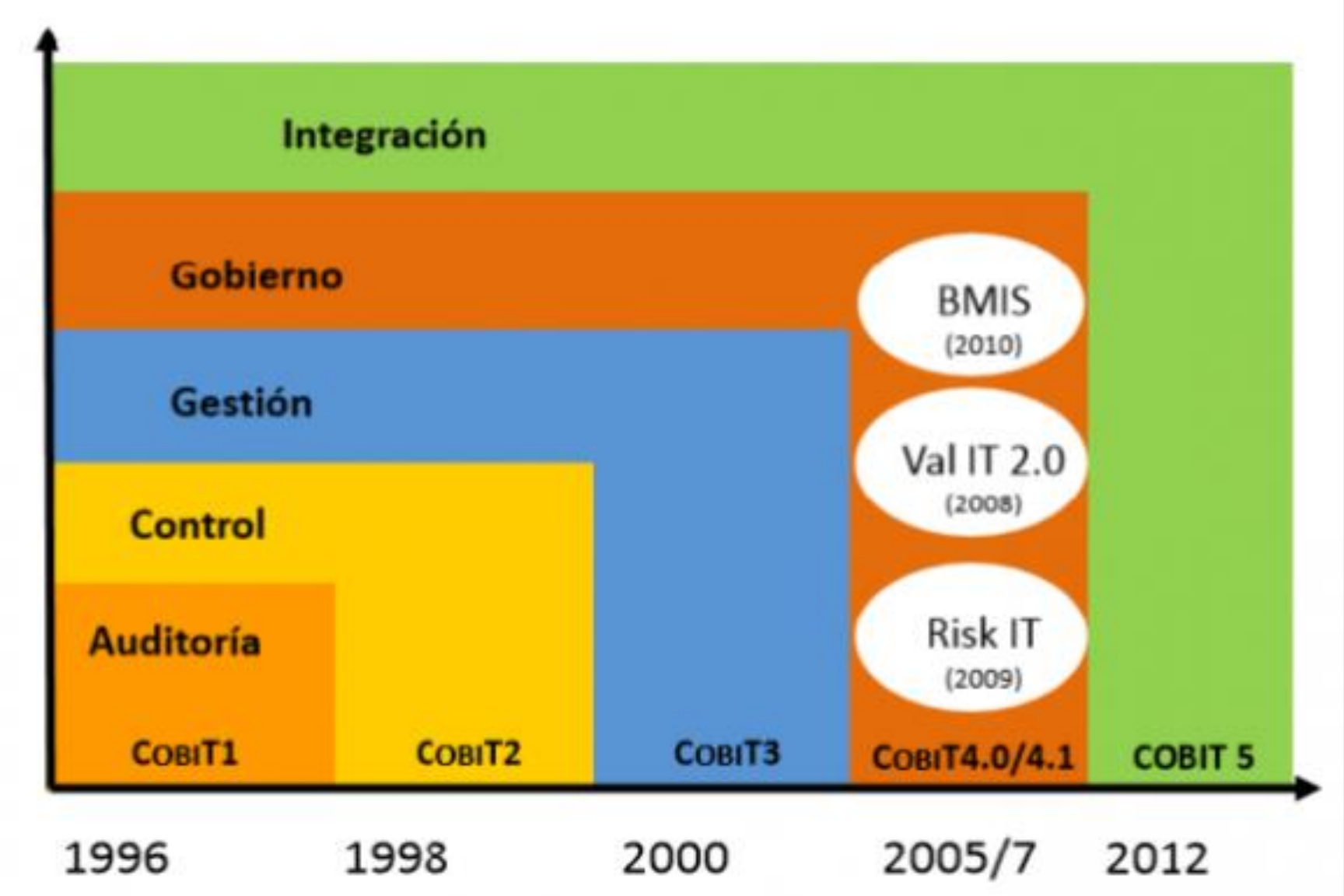
CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

ALIGNMENT

Línea Histórica de COBIT



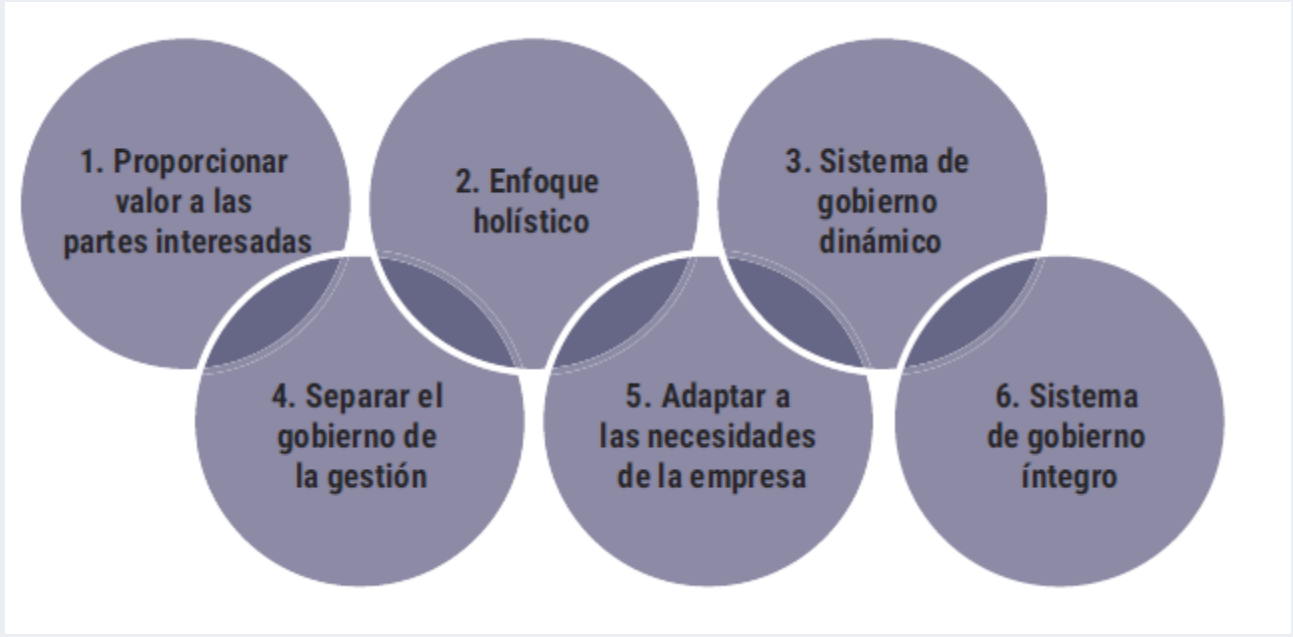
Evolución de COBIT de acuerdo a su foco



Principios del Sistema de Gobierno y Marco de Gobierno

COBIT 2019

PRINCIPIOS Sistema de Gobierno

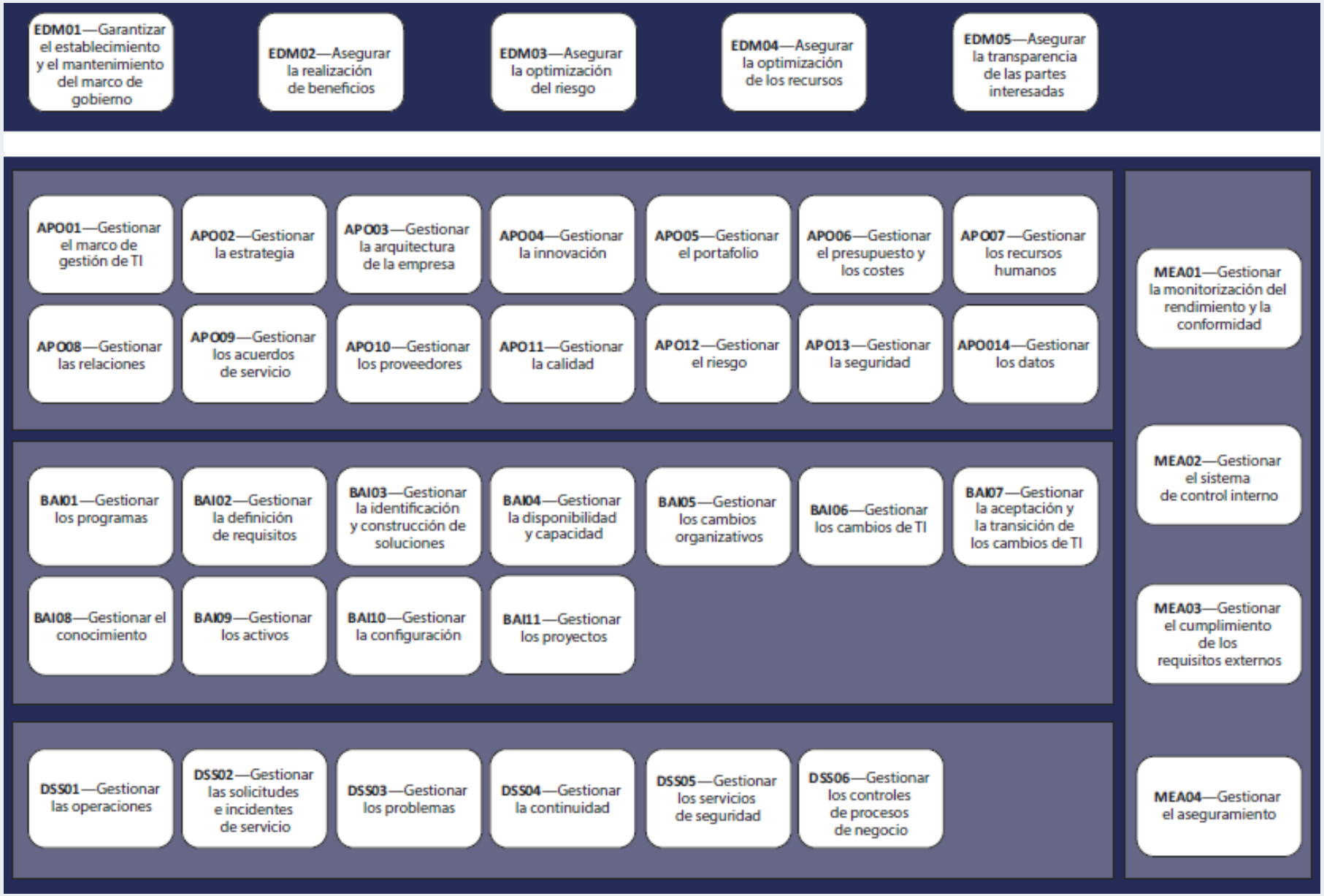


PRINCIPIOS Marco de Gobierno

Componentes del Sistema de Gobierno

- Con el objetivo de cumplir con los objetivos de gobierno y gestión, cada empresa debe establecer, personalizar y sostener un sistema de gobierno creado a partir de una serie de componentes.
- Estas componentes son factores que, de forma individual y colectiva, contribuyen al funcionamiento del sistema de gobierno de la empresa en cuanto a I&T.
- Los componentes interactúan entre sí, lo que da lugar a un sistema holístico de gobierno de I&T.

Objetivos de Gobierno y Gestión



Objetivos de Gobierno y Gestión – Visión General

EDM01—Garantizar el establecimiento y el mantenimiento del marco de gobierno

EDM02—Asegurar la realización de beneficios

EDM03—Asegurar la optimización del riesgo

EDM04—Asegurar la optimización de los recursos

EDM05—Asegurar la transparencia de las partes interesadas

APO01—Gestionar el marco de gestión de TI

APO02—Gestionar la estrategia

APO03—Gestionar la arquitectura de la empresa

APO04—Gestionar la innovación

APO05—Gestionar el portafolio

APO06—Gestionar el presupuesto y los costes

APO07—Gestionar los recursos humanos

APO08—Gestionar las relaciones

APO09—Gestionar los acuerdos de servicio

APO10—Gestionar los proveedores

APO11—Gestionar la calidad

APO12—Gestionar el riesgo

APO13—Gestionar la seguridad

APO014—Gestionar los datos

BAI01—Gestionar los programas

BAI02—Gestionar la definición de requisitos

BAI03—Gestionar la identificación y construcción de soluciones

BAI04—Gestionar la disponibilidad y capacidad

BAI05—Gestionar los cambios organizativos

BAI06—Gestionar los cambios de TI

BAI07—Gestionar la aceptación y la transición de los cambios de TI

BAI08—Gestionar el conocimiento

BAI09—Gestionar los activos

BAI10—Gestionar la configuración

BAI11—Gestionar los proyectos

DSS01—Gestionar las operaciones

DSS02—Gestionar las solicitudes e incidentes de servicio

DSS03—Gestionar los problemas

DSS04—Gestionar la continuidad

DSS05—Gestionar los servicios de seguridad

DSS06—Gestionar los controles de procesos de negocio

MEA01—Gestionar la monitorización del rendimiento y la conformidad

MEA02—Gestionar el sistema de control interno

MEA03—Gestionar el cumplimiento de los requisitos externos

MEA04—Gestionar el aseguramiento

Objetivos de Gobierno y Gestión – Estructura General

- Los 40 Objetivos de Gobierno y Gestión establecidos en el modelo están agrupados en torno a 5 dominios.

Objetivos de Gobierno	Objetivos de Gestión			
EDM Evaluar, Dirigir y Monitorizar	APO Alinear, Planificar y Organizar	BAI Construir, Adquirir e Implementar	DSS Entregar, Dar Servicio y Soporte	MEA Monitorizar, Evaluar y Valorar
5 Objetivos	14 Objetivos	11 Objetivos	6 Objetivos	4 Objetivos

Definición del Objetivo

Figura 3.1—Presentación de objetivos de gobierno y gestión	
Dominio: <NOMBRE> **Objetivo de gobierno/gestión:** <NOMBRE>	**Área prioritaria:** <NOMBRE>
Descripción	
<TEXTO> *Visión general de lo que hace el proceso y una visión a alto nivel de cómo el proceso lleva a cabo*	
Propósito	
<TEXTO> *Una completa descripción del propósito general del proceso*	

- Ejemplo APO13 – Gestionar el riesgo

Dominio: Alinear, Planificar y Organizar **Objetivo de gestión:** APO12—Gestionar el riesgo	**Área prioritaria:** Modelo Core de COBIT
Descripción	
Identificar, evaluar y reducir continuamente los riesgos relacionados con I&T dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa.	
Propósito	
Integrar la gestión del riesgo empresarial relacionado con la I&T con la gestión del riesgo empresarial global (ERM), y equilibrar los costes y beneficios de la gestión del riesgo empresarial relacionado con las I&T.	

DIPLOMADO
CIBERSEGURIDAD
CAPACITACIÓN USACH - UNIVERSIDAD DE SANTIAGO DE CHILE

Usando COBIT como Controles

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

ALIGNMENT

Ejemplo COBIT como Control

CIS Controls IS Audit/Assurance Program CSC 2: Inventory of Authorized and Unauthorized Software											
Process Sub-Area	*Ref. Risk*	*Control Objectives*	*Controls*	*Control Type*	*Control Classification*	*Control Frequency*	*Testing Step*	*Additional Ref. COBIT 5*	*Ref. Framework/ Standards*	*Ref. Workpaper*	*Pass/ Fail*	*Comments*
System		Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.	2.1 Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified. Advanced: File integrity is verified as part of a continuous monitoring program.	administrative	preventive		1. Assess governance arrangements over device-inventory management; in particular, confirm that a list of authorized software has been established by the organization. Assess whether it is in line with organizational risk profile and risk appetite. Assess whether it adequately covers servers as well as workstations/laptops and mobile devices. 2. Verify that the list contains software names and version information (potentially even required minimum patch levels). 3. Verify that the list contains 'signature' information that uniquely identifies the software as it is identified by the inventory scanning tool (i.e., its name and version as it appears when scanned, as well as file integrity information/cryptographic hashing etc., to identify unauthorized changes to software components). 4. Assess the security of the list (file integrity, access rights, change monitoring). 5. Assess the governance process over changes of the list. Who is authorized to request changes, who needs to approve, how is this documented, and how is the change actually performed on the list?	APO13 DSS05	NIST: Identify--AM (ID.AM-2 PR.DS-6) Critical Governance Item #1			

Controls	*Control Type*	*Control Classification*	*Control Frequency*	*Testing Step*	*Additional Ref. COBIT 5*
2.1 Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified. Advanced: File integrity is verified as part of a continuous monitoring program.	administrative	preventive		1. Assess governance arrangements over device-inventory management; in particular, confirm that a list of authorized software has been established by the organization. Assess whether it is in line with organizational risk profile and risk appetite. Assess whether it adequately covers servers as well as workstations/laptops and mobile devices. 2. Verify that the list contains software names and version information (potentially even required minimum patch levels). 3. Verify that the list contains 'signature' information that uniquely identifies the software as it is identified by the inventory scanning tool (i.e., its name and version as it appears when scanned, as well as file integrity information/cryptographic hashing etc., to identify unauthorized changes to software components). 4. Assess the security of the list (file integrity, access rights, change monitoring). 5. Assess the governance process over changes of the list. Who is authorized to request changes, who needs to approve, how is this documented, and how is the change actually performed on the list?	APO13 DSS05

Ejemplo COBIT como Control

Audit/Assurance Program Step	CobiT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. CONTINUITY FRAMEWORK AND POLICY									
2.1 IT continuity framework Audit/assurance objective: A framework for IT continuity to support enterprisewide business continuity management using a consistent process should be developed. The business continuity effort should be sponsored by the management of the business units or a business continuity task force. The framework should address the organizational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers, and the planning processes that create the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of critical resources, noting key dependencies; the monitoring and reporting of the availability of critical resources; alternative processing; and the principles of backup and recovery.									
2.1.1 Organization and governance **Control: The business has established a business continuity task force/ committee/organization to establish and maintain a business continuity process.**	DS4.1 DS4.2	X		X	X				
2.1.1.1 Determine if the enterprise has a BCP project plan or program, and indicate the date of acceptance and/or review.									
2.1.1.2 Determine if a budget for BCP and its components are included in the enterprise's budget.									
2.1.1.3 Determine if the BCP team member roles and responsibilities have been assigned at an appropriate level of authority to carry out responsibilities, and the team has appropriate executive sponsors.									
2.1.2 Participation **Control: The business continuity function includes representatives from affected business areas and IT, and the responsibility for the business continuity function is assigned to business operations and not IT.**	DS4.3			X	X	X			
2.1.2.1 Determine if the members of the BCP team are representatives from the affected organizations.									

Ejemplo del Práctica APO13.1. Recopilar Datos

Práctica de gestión	Métricas modelo
APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para habilitar una efectiva identificación, análisis y reporte de los riesgos relacionados con I&T.	a. Número de eventos de pérdida con características clave capturados en repositorios b. Porcentaje de auditorías, eventos y tendencias capturados en repositorios c. Porcentaje de sistemas críticos con problemas conocidos

Actividades	Nivel de capacidad
1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con el riesgo de I&T.	2
2. Registrar datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa.	
3. Adoptar o definir una taxonomía de riesgo para las definiciones consistentes de escenarios de riesgo y categorías de impacto y probabilidad.	3
4. Registrar datos de eventos de riesgo que han causado o podrían causar impacto en el negocio conforme a las categorías de impacto definidas en la taxonomía de riesgo. Capturar datos relevantes de cuestiones, incidentes, problemas e investigaciones.	
5. Estudiar y analizar los datos históricos de riesgo de I&T y de pérdidas experimentadas a partir de datos y tendencias externos disponibles, homólogos de la industria a través de logs de eventos de la industria, bases de datos, y acuerdos de la industria, para la publicación común de eventos.	4
6. Para clases de eventos similares, organizar los datos recopilados y resaltar los factores causantes. Determinar los factores causantes comunes en múltiples eventos.	
7. Determinar las condiciones específicas que existieron o estuvieron ausentes cuando tuvieron lugar los eventos de riesgo y la forma en que las condiciones afectaron a la frecuencia del evento y la magnitud de la pérdida.	
8. Realizar un análisis periódico de eventos y factores de riesgo para identificar riesgos nuevos o emergentes y para mejorar el entendimiento de los factores de riesgo internos y externos asociados.	

Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Data Management Maturity Model, 2014	Supporting Processes - Risk Management
COSO Enterprise Risk Management, junio de 2017	8. Performance—Principle 10
ISO/IEC 27005:2011(E)	8.2 Risk identification; 12. Information security risk monitoring and review
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018	3.1 Preparation (Task 7)

Ejemplo del Práctica APO13.1. Recopilar Datos

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
APO12.01 Collect data. Identify and collect relevant data to enable effective I&T-related risk identification, analysis and reporting.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Identify and collect relevant data to enable effective information security-related risk identification, analysis and reporting.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Risk Management
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 10
ISO/IEC 27005:2011(E)	8.2 Risk identification; 12. Information security risk monitoring and review
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 7)

Esta es un área prioritaria: Ciberseguridad

DIPLOMADO
CIBERSEGURIDAD
CAPACITACIÓN USACH - UNIVERSIDAD DE SANTIAGO DE CHILE

Un aliado en COBIT 2019: El modelo de Madurez

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

ALIGNMENT

Conceptos Claves

- **Modelo de Referencia de Procesos.** "Modelo que comprende definiciones de procesos en un dominio de aplicación descrito en términos de proceso propósito y resultados, junto con una arquitectura que describe las relaciones entre los procesos". (ISO 33.000:1)

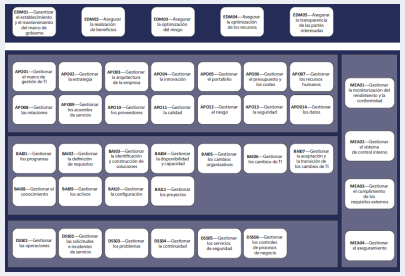
- **Modelo de Evaluación de Procesos.** "Un modelo adecuado para el propósito de evaluar la capacidad del proceso, basado en uno o más modelos de referencia de proceso." (ISO 15504:1)

- **Capacidad de Proceso.** "Una caracterización de la capacidad de un proceso para cumplir con los objetivos de negocio actuales o proyectadas." (ISO 15504:1).

- **Modelo de Madurez de Capacidades (CMM).** Es una colección organizada de recomendaciones para la mejora del rendimiento y del negocio. Las buenas prácticas del modelo se enfocan en qué es necesario hacer para mejorar el rendimiento, no en cómo hacerlo. (CMMI 2.0)

Características de la evaluación de madurez en COBIT 2019

Todo proceso está definido por un conjunto de prácticas, toda práctica está compuesta por un conjunto de actividades y toda actividad pose un nivel de madurez asociado.



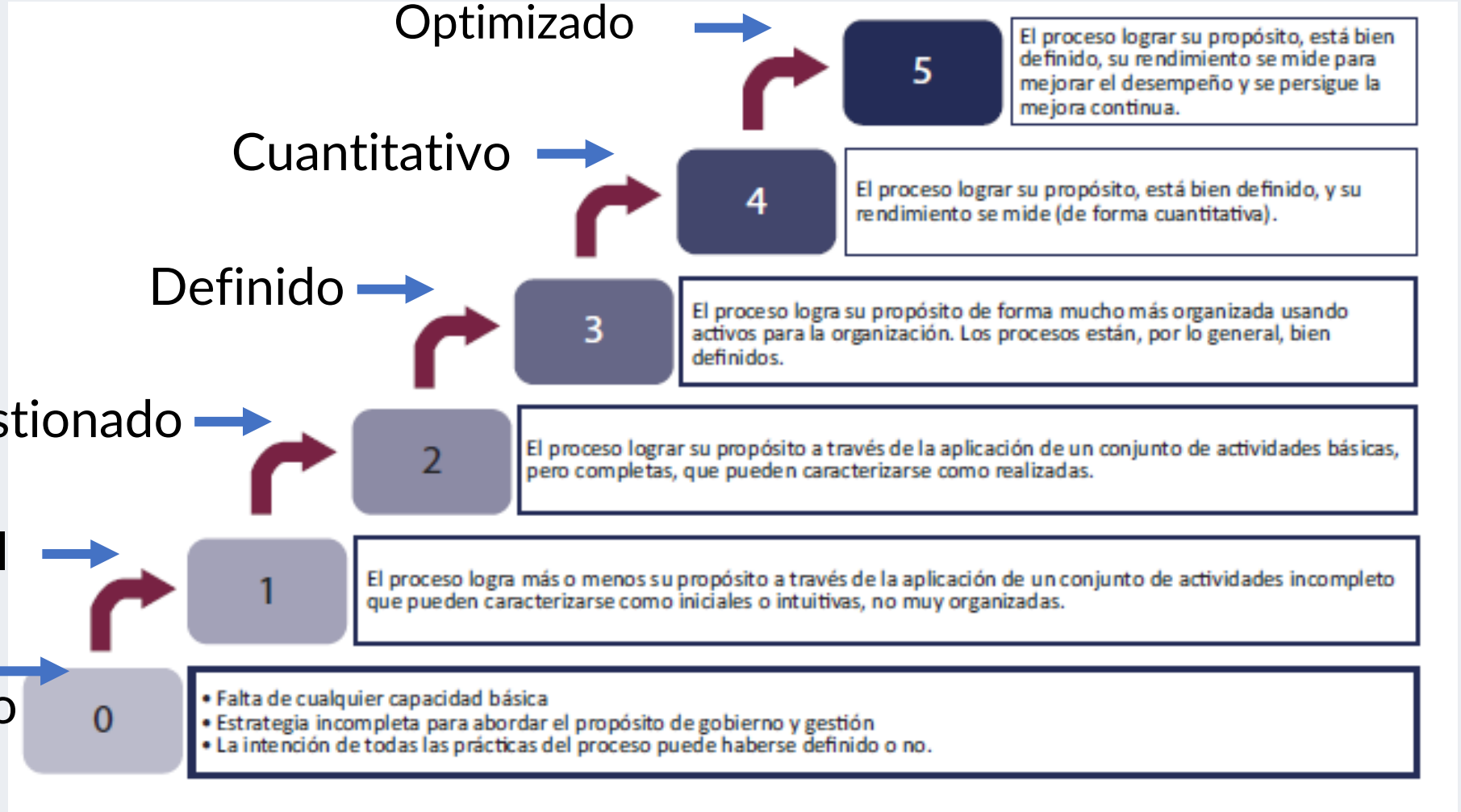
- Ejemplo de APO 12 Gestión de Riesgos
- Práctica APO12.03 Mantener el perfil de Riesgo

Práctica clave de gestión
APO12.01 Recopilar datos.
APO12.02 Analizar el riesgo.
APO12.03 Mantener un perfil de riesgo.
APO12.04 Articular el riesgo.
APO12.05 Definir un portafolio con acciones de gestión de riesgos.
APO12.06 Responder al riesgo.

APO12.03 Mantener un perfil de riesgo. Mantener un inventario de los riesgos conocidos y los atributos de riesgo, incluidos la frecuencia esperada, impacto potencial y respuestas. Documentar los recursos, capacidades y actividades de control actuales relacionados con elementos de riesgo.	a. Completitud de atributos y valores en el perfil de riesgo b. Porcentaje de procesos clave de negocio incluidos en el perfil de riesgo
Actividades	**Nivel de capacidad**
1. Hacer un inventario de los procesos de negocio y documentar su dependencia con los procesos de gestión de servicios de I&T y los recursos de infraestructura de TI. Identificar el personal de apoyo, aplicaciones, infraestructura, instalaciones, registros manuales críticos, contratistas, proveedores, y terceros.	2
2. Determinar y acordar qué servicios de I&T y recursos de infraestructura de TI son esenciales para sostener el funcionamiento de los procesos de negocio. Analizar las dependencias e identificar los eslabones débiles.	
3. Agregar los escenarios de riesgos actuales por categoría, línea de negocio y área funcional.	
4. Capturar regularmente toda la información del perfil de riesgo y consolidarla en un perfil de riesgo agregado.	3
5. Capturar información sobre el estado del plan de acción de riesgos para su inclusión en el perfil de riesgo de I&T de la empresa.	
6. Con base en todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan una identificación y monitorización rápida del riesgo actual y las tendencias de riesgo.	4
7. Capturar información sobre eventos de riesgo de I&T que se han materializado para su inclusión en el perfil de riesgo de TI de la empresa.	

Fuente: COBIT 2019

Niveles de capacidad para los procesos COBIT 2019



Fuente: COBIT 2019

Niveles de calificación de madurez en COBIT 2019

- Un nivel de capacidad puede alcanzarse en distinto grado, lo cual puede expresarse mediante una serie de calificaciones.

Calificación de madurez

- Completamente. El nivel de capacidad se alcanza para más del 85%.
- Largamente—El nivel de capacidad se alcanza entre el 50% y el 85%.
- Parcialmente—El nivel de capacidad se alcanza entre el 15% y el 50%.
- No—El nivel de capacidad se alcanza para menos del 15%.

- Cada nivel de capacidad puede ser alcanzado sólo cuando el nivel inferior se ha alcanzado por completo.