

Escuela Politécnica Nacional

Facultad de Ingeniería de Sistemas

Gestión de Tecnologías de la Información y Comunicación

Capítulo No. 4: Marcos de Referencia para Gestión de TICs

Clase Tema 4.1 Introduccion a modelos y marcos de referencia para gestión de TICs



Diego Tamayo

1 Modelos de Gestión de TICs

Propósito general

Los modelos y marcos para la gestión de Tecnologías de la Información y Comunicación (TICs) proporcionan lineamientos estructurados para organizar, controlar y mejorar procesos tecnológicos dentro de una organización.

Los beneficios principales que aportan estos modelos y marcos incluyen:

- Estandarización de prácticas
- Optimización de recursos tecnológicos
- Alineación entre tecnología y negocio

Modelos vs. Marcos de Referencia

Diferencia esencial

Un **modelo** describe conceptos y relaciones (visión teórica), mientras que un **marco de referencia (framework)** establece procesos, actividades y guías prácticas para su implementación operativa.

- **Modelo:** representación conceptual o explicativa
- **Marco:** conjunto estructurado de prácticas, procesos y roles

Analogía

Un modelo es un mapa conceptual; un marco es un manual operativo con instrucciones detalladas.

Concepto general

Un **marco de referencia** establece principios, estructuras y buenas prácticas, mientras que un **marco de gestión** define procesos operativos, roles y actividades para ejecutar dichas prácticas dentro de las TICs.

- Un **marco de referencia** sirve como guía conceptual y normativa.
- Un **marco de gestión** convierte esa guía en procedimientos concretos.
- Ambos funcionan de manera complementaria para asegurar gobernanza y operación eficiente de las TICs.

Ejemplo

COBIT actúa como **marco de referencia**, definiendo principios y dominios; ITIL funciona como **marco de gestión**, proporcionando procesos específicos para operación y entrega de servicios.

Ejemplo Concreto: COBIT vs. ITIL en la Gestión de TICs

Contexto práctico

Para diferenciar claramente un **marco de referencia** (COBIT) de un **marco de gestión** (ITIL), se presenta un ejemplo aplicado al manejo de incidentes en TICs.

COBIT como marco de referencia

COBIT establece el objetivo de control **DSS02: Gestionar Servicios e Incidentes**, definiendo *qué se debe lograr*: minimizar el impacto de los incidentes, definir responsabilidades, asegurar métricas y mantener la continuidad del negocio. No indica procedimientos detallados.

ITIL como marco de gestión

ITIL define **cómo ejecutar** la gestión de incidentes: pasos específicos (registro, categorización, priorización, diagnóstico, escalamiento y cierre), roles operativos (Service Desk, analistas N1/N2), y flujos de trabajo detallados.

Modelo de Madurez de Seguridad (En general)

Evalúa el grado de desarrollo de la gestión de seguridad en una organización, describiendo niveles que van desde un estado **reactivo** hasta uno **optimizado**. Permite medir la evolución y situar a la organización en un nivel, aunque no detalla actividades específicas para mejorar.

Marco de gestión: Norma ISO/IEC 27001

Proporciona un conjunto estructurado de procesos, políticas, controles y roles para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Define **cómo aplicar** la gestión de seguridad de forma sistemática y verificable.

Marcos con presencia en Gobernanza

- **COBIT** (Control Objectives for Information and Related Technologies): gobernanza y gestión de TI
- **ISO/IEC 38500** (Gobierno Corporativo de TI): directrices para la alta dirección
- **ITIL** (Information Technology Infrastructure Library): introduce elementos de gobernanza en su versión moderna
- **TOGAF** (The Open Group Architecture Framework): incluye gobierno de arquitectura

Importante

La gobernanza pertenece principalmente a marcos como COBIT e ISO/IEC 38500; otros marcos solo la integran parcialmente.

Enfoque general

Las normas técnicas ISO/IEC/IEEE orientadas a procesos de TICs funcionan como **marcos de gestión**, ya que definen prácticas, actividades, roles y controles para operar y mejorar áreas específicas.

- ISO/IEC 27001: Gestión de Seguridad de la Información
- ISO/IEC 20000: Gestión de Servicios TI
- ISO/IEC 29119: Gestión del Proceso de Pruebas
- ISO 22301: Gestión de Continuidad del Negocio

Propósito del estándar

ISO/IEC/IEEE 12207 establece un marco de procesos para gestionar integralmente el ciclo de vida del software, cubriendo adquisición, desarrollo, operación, mantenimiento y retiro.

- Procesos de adquisición y suministro
- Procesos de desarrollo y mantenimiento
- Procesos de soporte: verificación, validación, documentación, aseguramiento de la calidad
- Procesos organizacionales: gestión de proyectos, gestión de riesgos y mejora continua

Clasificación

ISO/IEC/IEEE 12207 es un **marco de gestión del ciclo de vida del software**, orientado a procesos operativos y de soporte. No es un marco de gobernanza.

Modelo y Marco asociados a CMMI

Naturaleza dual

CMMI (Capability Maturity Model Integration) funciona simultáneamente como **modelo de madurez** y como **marco de procesos** (caso atípico), combinando una escala conceptual con prácticas detalladas de mejora.

- **Modelo:** define una *escala sintética de madurez* (niveles 1 a 5) que describe el estado general de capacidad de la organización, sin detallar actividades.
- **Marco:** proporciona las prácticas y áreas de proceso que permiten avanzar sistemáticamente entre los niveles 1 a 5, indicando *cómo* lograr el progreso definido en el modelo.

Resultado

El modelo indica en qué nivel se encuentra la organización, y el marco establece las prácticas que permiten evolucionar hacia niveles superiores.

Distinción clave

Los **modelos** son representaciones conceptuales y los **marcos** son guías prácticas aplicables a la gestión de TICs.

- **Modelos:** escalas conceptuales o de madurez (ej.: niveles de CMMI).
- **Marcos de gestión:** procesos y controles operativos (ISO/IEC 27001, ISO/IEC 20000, ISO/IEC/IEEE 12207, ITIL).
- **Marcos de gobernanza:** principios y responsabilidades estratégicas (COBIT, ISO/IEC 38500).

Cierre

La gestión de TICs requiere modelos conceptuales para analizar capacidad y marcos para dirigir, controlar y operar la función tecnológica.

Modelos de Gestión de TICs

Modelo: CMMI (Capability Maturity Model Integration)

Propósito

CMMI proporciona una escala estructurada para evaluar y mejorar la madurez de procesos organizacionales relacionados con el desarrollo, operación y mantenimiento de productos y servicios de TICs.

- Orientado a medir capacidad y madurez de procesos
- Niveles de madurez del 1 al 5
- Base para planificar mejoras sistemáticas

Aplicación típica

Se utiliza para diagnosticar procesos, establecer prioridades de mejora y orientar iniciativas de calidad en proyectos de software y servicios de TICs.

Modelo: COBIT PAM (Process Assessment Model)

Propósito

COBIT PAM proporciona un modelo para evaluar la capacidad de los procesos de gobernanza y gestión de TICs mediante niveles estructurados y criterios de desempeño definidos.

- Evalúa procesos usando un enfoque basado en atributos de capacidad
- Niveles de capacidad del 0 al 5
- Permite medir el grado de logro y consistencia de los procesos

Aplicación típica

Se emplea para auditorías, diagnósticos de madurez y evaluaciones de desempeño de procesos en marcos como COBIT 2019, permitiendo priorizar mejoras en la gobernanza y gestión de TICs.

Propósito

El modelo de madurez de ITIL permite evaluar la capacidad y consistencia de los procesos de gestión de servicios de TICs, alineándolos con las mejores prácticas del ciclo de vida del servicio.

- Basado en niveles que van de inicial a optimizado
- Evalúa calidad, estandarización y mejora continua de procesos ITIL
- Usado para medir desempeño en gestión de incidentes, cambios, problemas y otros procesos

Aplicación típica

Se utiliza para identificar brechas en la gestión de servicios, priorizar mejoras y demostrar la madurez operativa frente a auditorías o iniciativas de certificación.

Propósito

SSE-CMM (Systems Security Engineering Capability Maturity Model) proporciona un modelo para evaluar la madurez de los procesos de ingeniería de seguridad, garantizando que las prácticas de protección de sistemas de TICs sean consistentes, repetibles y medibles.

- Evalúa prácticas de seguridad durante todo el ciclo de vida de sistemas
- Niveles de madurez del 1 al 5
- Enfoque en capacidades organizacionales, no en controles específicos

Aplicación típica

Se utiliza para diagnosticar el grado de madurez en prácticas de seguridad, apoyar auditorías técnicas y orientar planes de mejora en organizaciones que desarrollan o integran sistemas críticos.

Marco: ISO/IEC 27001 (Seguridad de la Información)

Propósito

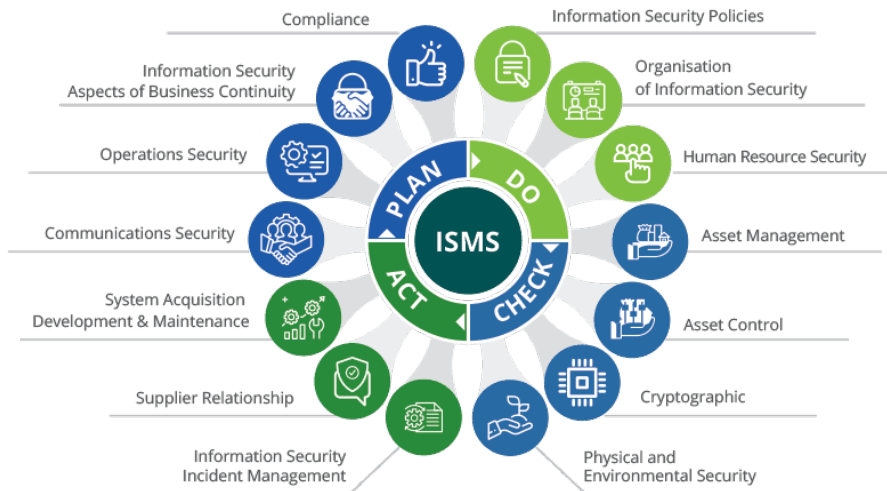
ISO/IEC 27001 establece un sistema de gestión para proteger la confidencialidad, integridad y disponibilidad de la información mediante controles, procesos y políticas aplicables a las TICs.

- Define requisitos para implementar, mantener y mejorar un SGSI
- Basado en enfoque de riesgo y mejora continua (ciclo PDCA)
- Contempla 93 controles en ISO/IEC 27002 como guía de implementación

Aplicación típica

Se utiliza para certificar organizaciones, estructurar auditorías de seguridad, gestionar riesgos y formalizar prácticas de protección de activos de información en ambientes de TICs.

Dominios de ISO/IEC 27001



¿Qué son los controles?

Los controles de seguridad en ISO/IEC 27001 son medidas técnicas, organizativas, físicas o legales que protegen la información de una organización. Su propósito es mitigar riesgos, reducir vulnerabilidades y asegurar la confidencialidad, integridad y disponibilidad de los datos.

En términos prácticos, los controles permiten:

- Reducir vulnerabilidades y reforzar la protección frente a amenazas.
- Implementar prácticas, políticas y herramientas de seguridad efectivas.
- Prevenir accesos no autorizados, fallos de sistemas y errores humanos.



Implementación de ISO/IEC 27001



Marco: ISO/IEC 20000-1 (Gestión de Servicios TICs)

Propósito

ISO/IEC 20000-1 define los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Servicios (SGS) que garantice la calidad y consistencia en la entrega de servicios de TICs.

- Basado en procesos alineados con buenas prácticas como ITIL
- Incluye planificación, entrega, soporte y mejora de servicios
- Enfatiza acuerdos de niveles de servicio y control operacional

Aplicación típica

Se utiliza para estructurar operaciones de servicios TICs, demostrar cumplimiento ante clientes, mejorar la calidad de atención y soportar procesos de certificación de gestión de servicios.

Marco: ISO/IEC/IEEE 12207 (Ciclo de vida del software)

Propósito

ISO/IEC/IEEE 12207 define un marco para gestionar el ciclo de vida del software mediante procesos estructurados que abarcan desde la adquisición hasta el retiro del producto.

- Incluye procesos de desarrollo, operación y mantenimiento
- Procesos de soporte como verificación, validación y documentación
- Procesos organizacionales como gestión de proyectos, calidad y riesgos

Aplicación típica

Se utiliza para estandarizar actividades del ciclo de vida del software, soportar auditorías técnicas y mejorar la calidad y trazabilidad en proyectos de TICs.

Propósito

ITIL proporciona un marco de mejores prácticas para gestionar servicios de TICs a lo largo de su ciclo de vida, asegurando calidad, eficiencia y alineación con las necesidades del negocio.

- Estructurado en prácticas como incidentes, problemas, cambios y niveles de servicio
- Enfoque en valor, experiencia del usuario y mejora continua
- Permite estandarizar operaciones y roles en la gestión de servicios

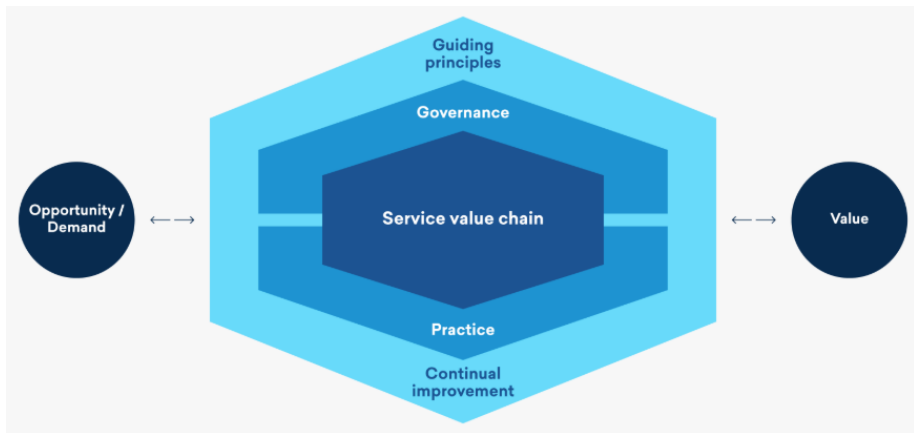
Aplicación típica

Se utiliza para organizar procesos operativos, mejorar tiempos de atención, estructurar centros de soporte y alinear servicios TICs con objetivos estratégicos.

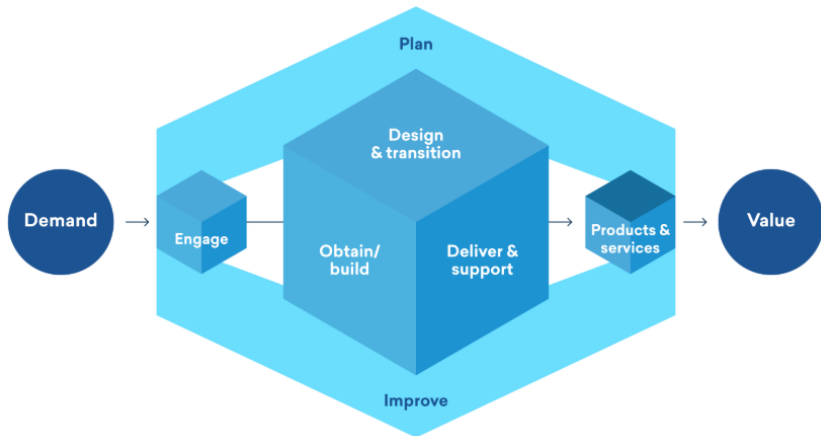
ITIL v4 - Principios Rectores (Guiding Principles)



Sistema de Valor del Servicio en ITIL v4



Cadena de Valor del Servicio en ITIL v4



Marco: NIST SP 800-53 (Seguridad y Privacidad)

Propósito

NIST SP 800-53 proporciona un catálogo estructurado de controles de seguridad y privacidad para proteger sistemas de información, con énfasis en entornos gubernamentales y organizaciones que gestionan activos críticos de TICs.

- Incluye familias de controles como acceso, auditoría, respuesta a incidentes y continuidad
- Basado en gestión de riesgos y categorización del sistema
- Útil para diseñar arquitecturas seguras y cumplir requisitos regulatorios

Aplicación típica

Se utiliza para implementar controles de seguridad en sistemas de TICs, realizar evaluaciones técnicas, definir arquitecturas de seguridad y cumplir marcos regulatorios basados en riesgo.

Propósito

PMBOK, desarrollado por el Project Management Institute (PMI), establece un marco de buenas prácticas para gestionar proyectos de forma estructurada, aplicable también a iniciativas y proyectos de TICs.

- Incluye áreas de conocimiento como alcance, tiempo, costo, riesgos y calidad
- Define procesos de inicio, planificación, ejecución, control y cierre
- Fomenta estandarización y previsibilidad en la gestión de proyectos

Aplicación típica

Se utiliza para estructurar proyectos de TICs, mejorar la planificación, controlar riesgos y asegurar entregables alineados con objetivos de negocio y expectativas del cliente.

Principios de PMBOK Séptima edición

12 Principles PMBOK Guide 7th Edition

Stewardship

Team

Stakeholders

Value

System thinking,
Holistic approach

Leadership

Tailoring

Quality

Complexity

Risk

Adaptability and
resilience

Change Management

8 Project Performance Domains



Grupos de procesos en PMBOK Séptima edición



Marco: PRINCE2 (Projects IN Controlled Environments)

Propósito

PRINCE2 establece un marco estructurado para la gestión de proyectos basado en principios, temas y procesos, orientado al control, la trazabilidad y la gobernabilidad de proyectos de TICs.

- Basado en siete principios, siete temas y siete procesos
- Enfoque en casos de negocio, roles claros y control por etapas
- Aporta disciplina, documentación y repetibilidad en proyectos complejos

Aplicación típica

Se utiliza para gestionar proyectos de TICs con alta necesidad de control, formalidad y visibilidad, asegurando decisiones basadas en el caso de negocio y un gobierno claro del proyecto.

[1] Omnex Inc.

Iso/iec 27001:2022 cybersecurity – consulting, implementation & coaching (aerospace).

<https://www.omnex.com/aerospace/consulting-implementation-coaching-aerospace-iso-27001>
2025.

Consultado el 19 de noviembre de 2025.

[2] hiChex.

Controles iso 27001: Te contamos qué y cuáles son.

<https://www.hichex.com/controles-iso-27001-te-contamos-que-y-cuales-son/>,
2025.

Consultado el 19 de noviembre de 2025.

[3] UCS ISO.

Iso/iec 27001:2022 information security management systems.

<https://ucsiso.com/>

iso-iec-27001-information-security-management-systems-2025.

Consultado el 19 de noviembre de 2025.

[4] Freshworks.

Itil v4: Guía completa y novedades.

<https://www.freshworks.com/es/freshservice/itil/itil-v4/>, 2025.

Consultado el 19 de noviembre de 2025.

[5] AXELOS / ITIL Foundation.

Itil 4 guiding principles.

<https://www.itsmtools.com/Articles/2025/01/17/ITIL-4-Guiding-Principles.aspx>

<https://www.itsmtools.com/Articles/2025/01/17/ITIL-4-Guiding-Principles.aspx>,
2025.

Consultado el 19 de noviembre de 2025.

[6] Yassine Tounsi.

Everything you need to know about the pmbok guide 7th edition.

<https://yassinetounsi.com/everything-you-need-to-know-about-the-pmbok-guide-7th-edition/>

[everything-you-need-to-know-about-the-pmbok-guide-7th-edition/](https://yassinetounsi.com/everything-you-need-to-know-about-the-pmbok-guide-7th-edition/)
2025.

Consultado el 19 de noviembre de 2025.

[7] Kai Sulkowski.

Project management with pmi and pmbok guide – a proven standard in transition.

<https://www.projektron.de/en/blog/details/pmi-pmbok-4017/>, 2025.

Consultado el 19 de noviembre de 2025.