DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Unidad 3: Planeando la ciberseguridad

Sistemas de gestión de la seguridad

Profesor
Juan Ignacio Iturbe A.

Frameworks de Seguridad

- En este punto ya sabemos que necesitamos cumplir (CIA).
- Conocemos que herramientas usar (controles administrativos, técnicos y físicos)
- Y las definiciones que hay que manejar (vulnerabilidades, amenazas, riesgo, control).
- Ahora se necesita construir un programa de seguridad para lo amplio de la organización.

Frameworks de Seguridad

- Primero, ¿Qué NO hacer?
  - Seguridad a través de la oscuridad (se asume que mis enemigos no son tan listos como uno). Ej:
    - Un vendedor que diga que sus productos son mejores que uno *opensource*, ya que los de él son compilados y no se puede ver el código fuente.
    - Un algoritmo criptográfico hecho en casa (Lo mejor es utilizar algoritmos ampliamente reconocidos)
    - Remapear puertos (fácilmente detectable con herramientas)

Frameworks de Seguridad

- Entonces, ¿Qué hacer?
  - Construir una fortaleza (También llamado "Programa de seguridad") de muchas piezas:
    - Mecanismos de protección lógicos, administrativos, físicos, procedimientos, procesos de negocio y personas.
    - Todos de gran importancia para el marco de trabajo.
    - Si una falla, todo el marco de trabajo se ve comprometido.
    - Este se construye en capas, cada capa da soporte a la siguiente.
    - Se necesitan los planos de la estructura de la fortaleza, por suerte existen estándares en la industria.

Estándares, mejores prácticas y frameworks

- Desarrollo de un programa de seguridad
  - Serie ISO/IEC 27000 estándares internacionales de cómo desarrollar y mantener un ISMS.
- Desarrollo de un arquitectura corporativa (no necesariamente orientado a la seguridad).
  - Zachman framework
  - TOGAF (The Open Group)
  - DoDAF (U.S. Department of Defense)
  - MODAF (British Ministry of Defense)

Estándares, mejores prácticas y frameworks

- Desarrollo de una arquitectura de seguridad corporativa
  - SABSA model
- Desarrollo de Controles de Seguridad
  - CobiT
  - SP 800-53 (NIST)
- Gobierno corporativo
  - COSO
- Gestión de procesos
  - ITIL, Six Sigma, CMMI

Serie ISO/IEC 27000

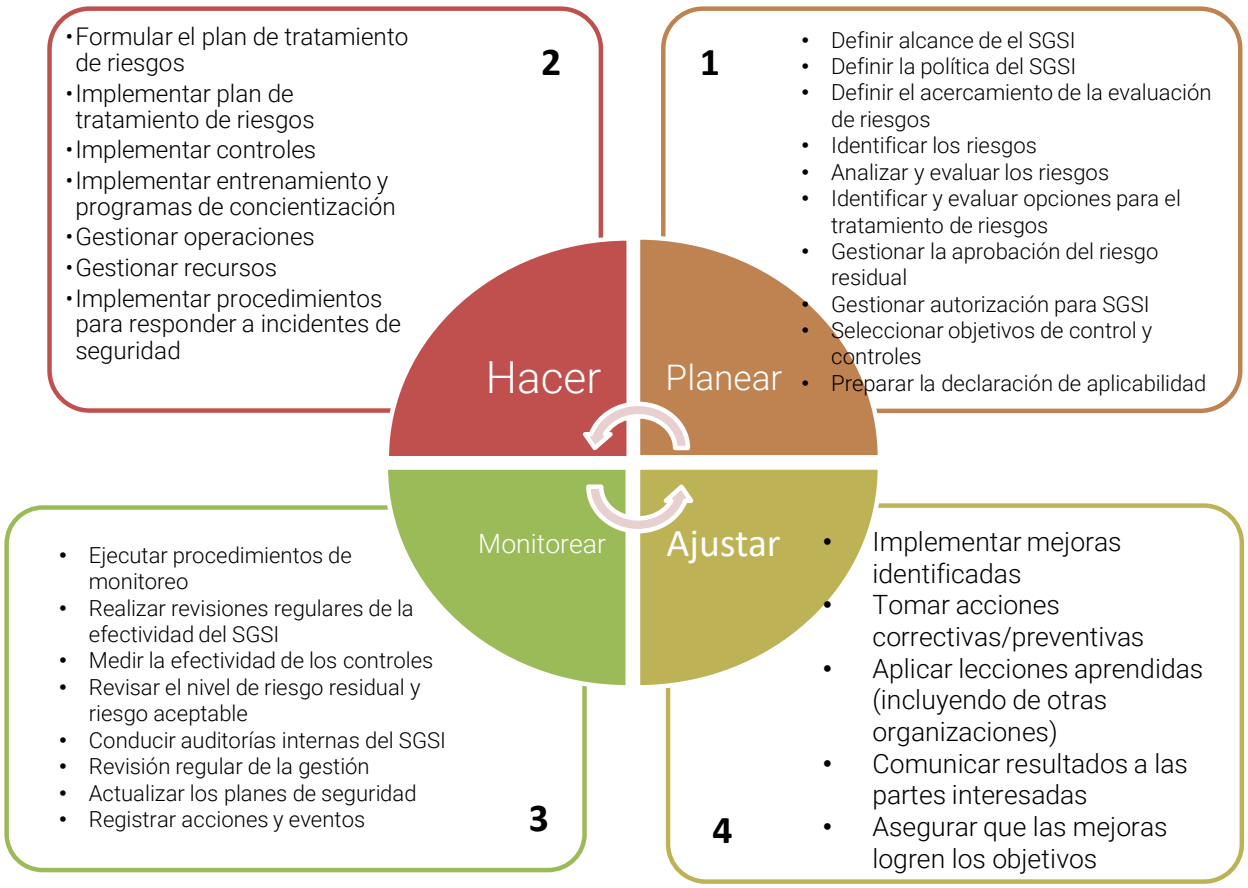
- Nace desde el estándar británico BS7799
- Este estándar delinea de qué trata un ISMS o SGSI (aka programa de seguridad). Y como debe ser este mantenido.
- El objetivo de este es :
  - proveer una guía de cómo diseñar, implementar y mantener políticas, procesos y tecnologías para manejar riesgos y activos con información sensible.
- Se tiene el manejo de los controles de seguridad centralmente (no adhoc).

Serie ISO/IEC 27000

- El BS7799 fue actualizado y derivo en el BS7799v1, BS7799v2, ISO 17799, BS7799-3:2005,etc.
- Finalmente se llego a la serie ISO/IEC 27000 que trata de modularizar y separar los componentes necesarios para el desarrollo de un ISMS.
- ISO sigue el ciclo Plan – DO – Check - Act

Serie ISO/IEC 27000

- Se busca:
  - Políticas de seguridad de la información (IS) para la organización
  - Creación de una infraestructura de IS
  - Clasificación de activos y controles
  - Seguridad del personal
  - Seguridad física y ambiental.
  - Manejo de las comunicaciones y operaciones
  - Control de acceso
  - Desarrollo y mantenimiento de sistemas
  - Manejo de la continuidad de negocio
  - Cumplimiento legales


Hacer
Planear
Monitorear
Ajustar
1
Definir alcance de el SGSI
Definir la política del SGSI
Definir el acercamiento de la evaluación de riesgos
Identificar los riesgos
Analizar y evaluar los riesgos
Identificar y evaluar opciones para el tratamiento de riesgos
Gestionar la aprobación del riesgo residual
Gestionar autorización para SGSI
Seleccionar objetivos de control y controles
Preparar la declaración de aplicabilidad
2
Formular el plan de tratamiento de riesgos
Implementar plan de tratamiento de riesgos
Implementar controles
Implementar entrenamiento y programas de concientización
Gestionar operaciones
Gestionar recursos
Implementar procedimientos para responder a incidentes de seguridad
3
Ejecutar procedimientos de monitoreo
Realizar revisiones regulares de la efectividad del SGSI
Medir la efectividad de los controles
Revisar el nivel de riesgo residual y riesgo aceptable
Conducir auditorías internas del SGSI
Revisión regular de la gestión
Actualizar los planes de seguridad
Registrar acciones y eventos
4
Implementar mejoras identificadas
Tomar acciones correctivas/preventivas
Aplicar lecciones aprendidas (incluyendo de otras organizaciones)
Comunicar resultados a las partes interesadas
Asegurar que las mejoras logren los objetivos

Serie ISO/IEC 27000

- ISO/IEC:
  - 27000 Revisión y vocabulario.
  - 27001 Requerimientos de un ISMS
  - 27002 Código de práctica para el manejo de la IS
  - 27003 Guía para la implementación ISMS
  - 27004 Guía para la IS del manejo de la medidas y métricas
  - 27005 Guía para el manejo de riesgo del IS
  - …
  - 27034 Guía para la Seguridad de aplicaciones
  - 27035 Guía para la seguridad del manejo de incidentes
  - 27036 Guía para el manejo del outsourcing
  - 27037 Guía para la identificación, recolección, adquisición y preservación de evidencia digital.

A tener en cuenta

- Cuando se tiene un requerimiento habilitador de negocio sobre la arquitectura de seguridad de la empresa, hay que recordar que el objetivo de las empresas es generar dinero. Estas no existen solamente para ser seguras.
- La seguridad no se debe interponer sobre el negocio, pero debe ser implementada de la mano con el negocio.
- La seguridad debe ayudar a realizar a la organización proveyendo mecanismos para hacer las nuevas cosas de forma segura.

A tener en cuenta

- Por ejemplo una compañía puede querer habilitar que su servicio de atención al cliente y soporte trabajen desde la casa.
  - Esto trae un montón de ahorro por ejemplo en arriendo de oficinas, servicios y gastos generales.
- La compañía debe moverse a este nuevo modelo con la utilización de VPN, firewalls, filtrado de contenidos, etc.
- Entonces, la seguridad habilita a la compañía a moverse a un diferente modelo de trabajo proveyendo los mecanismos de protección necesarios.

Desarrollo de controles de seguridad

- Hasta ahora se tiene la serie 27000, la cual describe los componentes necesarios de un programa de seguridad de la organización.
- También se tiene la arquitectura de seguridad corporativa, lo cual ayuda a integrar los requisitos descritos en la estructura empresarial existente.
- Ahora nos centraremos en los objetivos de control que se podrán en marcha para lograr los objetivos planteados en el programa de seguridad y la arquitectura corporativa.

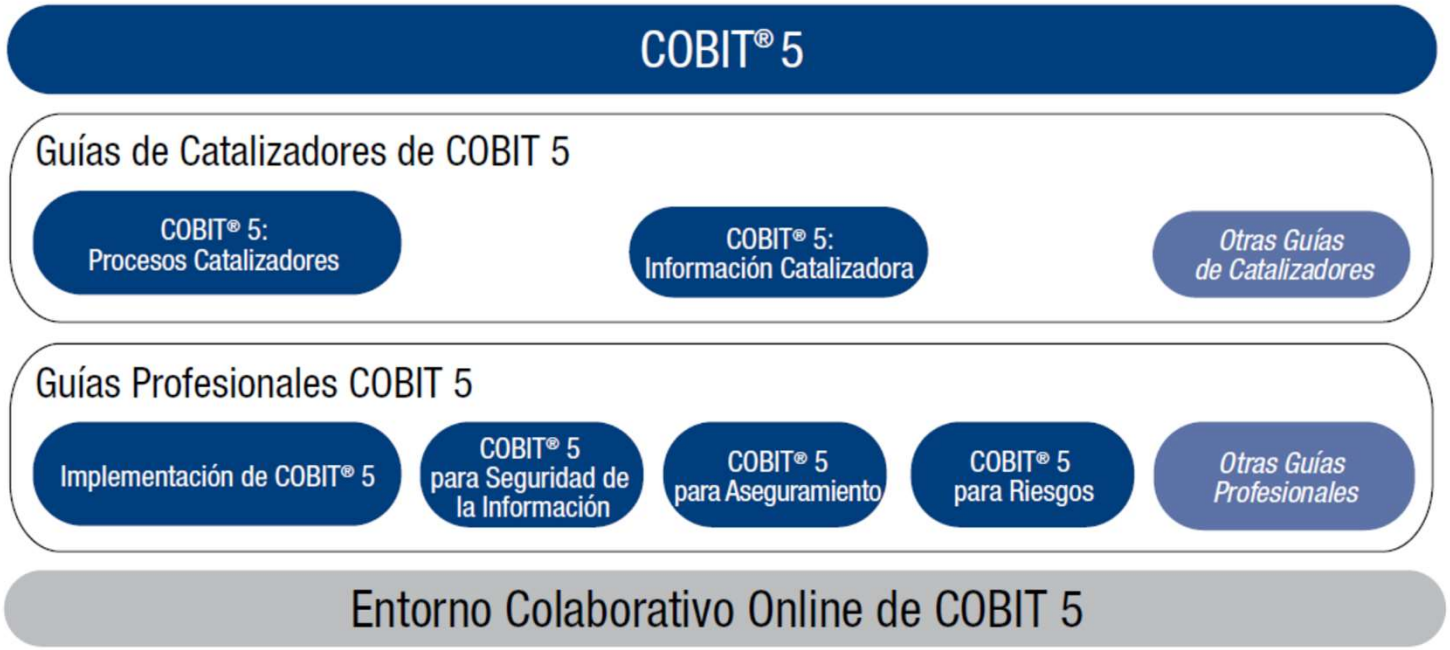
Lectura 1

- Leer:
  - ISO/IEC 27000:2016
- Responder prueba con alternativa que se encuentra en USACH Virtual (20 minutos).
- Tienen una semana.

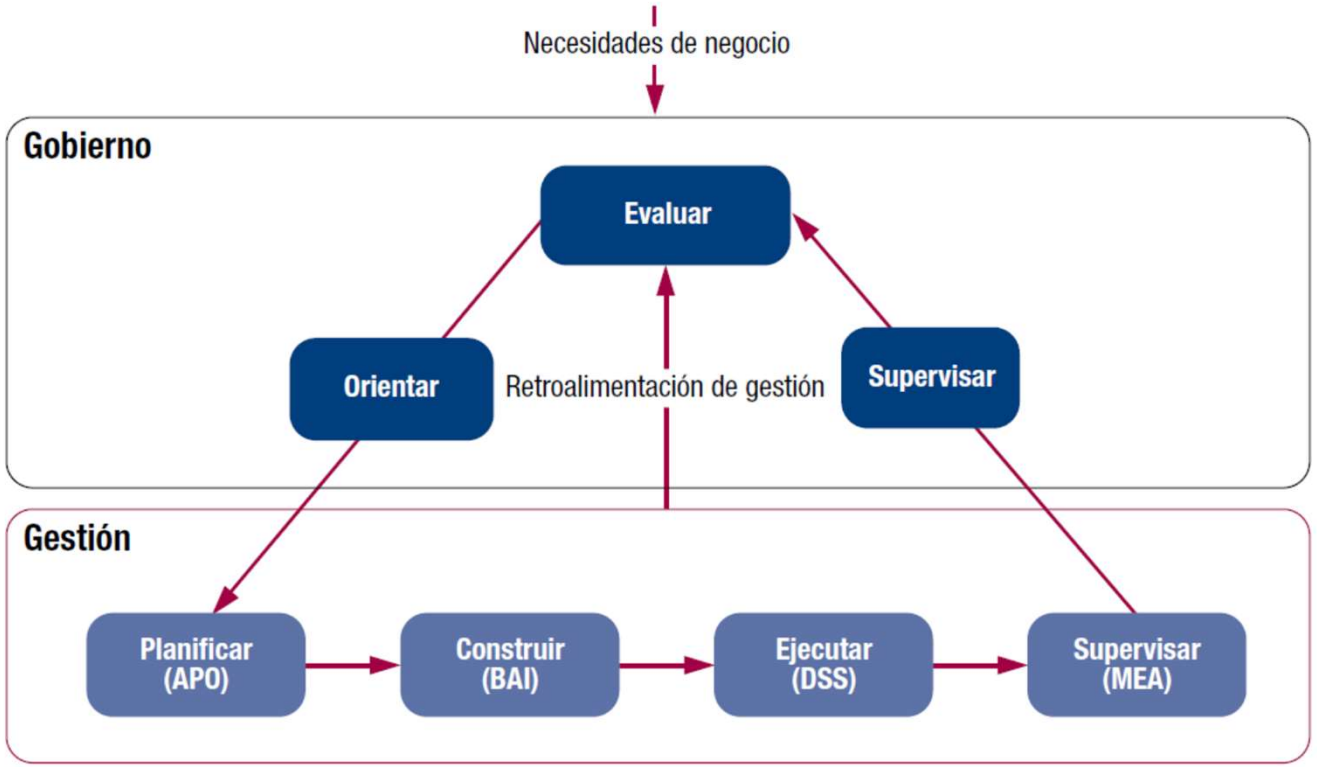
CobiT

- Desarrollado por ISACA
- Es un marco de gobierno de las tecnologías de información que entrega una serie de herramientas para que la alta dirección pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos de negocio.
- Define los objetivos para los controles que se deben utilizar para la gobernanza y gestión adecuadamente TI y garantizar que TI soporte lo que el negocio requiera.
- Enfatiza el cumplimiento regulatorio, ayuda a las organizaciones a incrementar us valor a través de las tecnologías, y permite su alineamiento con los objetivos del negocio.

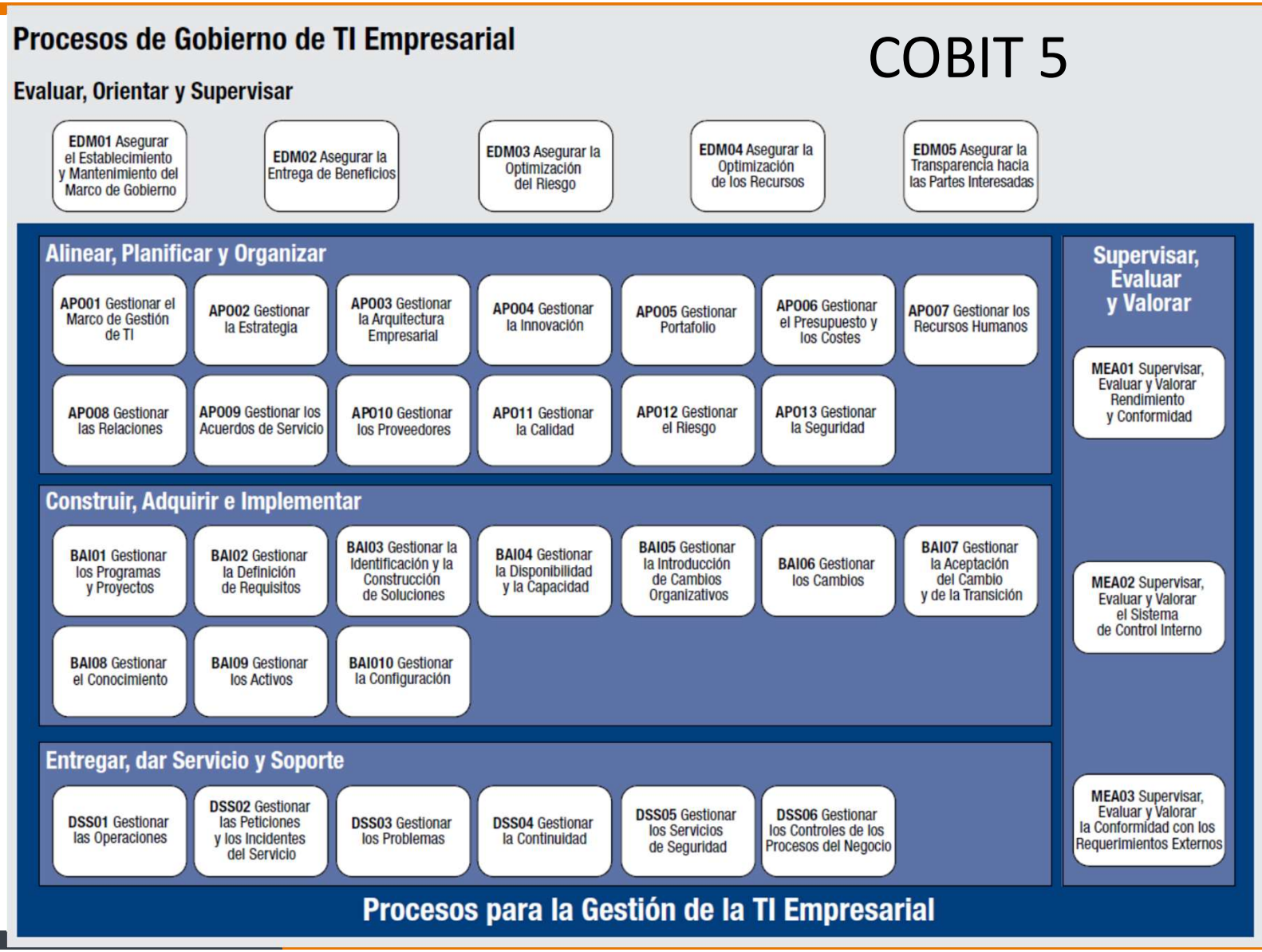
Libros de CobiT 5



Áreas claves de Gobierno y Gestión de COBIT 5



COBIT 5


Procesos de Gobierno de TI Empresarial
Evaluar, Orientar y Supervisar
EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno
EDM02 Asegurar la Entrega de Beneficios
EDM03 Asegurar la Optimización del Riesgo
EDM04 Asegurar la Optimización de los Recursos
EDM05 Asegurar la Transparencia hacia las Partes Interesadas
Alinear, Planificar y Organizar
APO01 Gestionar el Marco de Gestión de TI
APO02 Gestionar la Estrategia
APO03 Gestionar la Arquitectura Empresarial
APO04 Gestionar la Innovación
APO05 Gestionar 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
Construir, Adquirir e Implementar
BAI01 Gestionar los Programas y Proyectos
BAI02 Gestionar la Definición de Requisitos
BAI03 Gestionar la Identificación y la Construcción de Soluciones
BAI04 Gestionar la Disponibilidad y la Capacidad
BAI05 Gestionar la Introducción de Cambios Organizativos
BAI06 Gestionar los Cambios
BAI07 Gestionar la Aceptación del Cambio y de la Transición
BAI08 Gestionar el Conocimiento
BAI09 Gestionar los Activos
BAI010 Gestionar la Configuración
Entregar, dar Servicio y Soporte
DSS01 Gestionar las Operaciones
DSS02 Gestionar las Peticiones y los Incidentes del Servicio
DSS03 Gestionar los Problemas
DSS04 Gestionar la Continuidad
DSS05 Gestionar los Servicios de Seguridad
DSS06 Gestionar los Controles de los Procesos del Negocio
Supervisar, Evaluar y Valorar
MEA01 Supervisar, Evaluar y Valorar Rendimiento y Conformidad
MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno
MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos
Procesos para la Gestión de la TI Empresarial

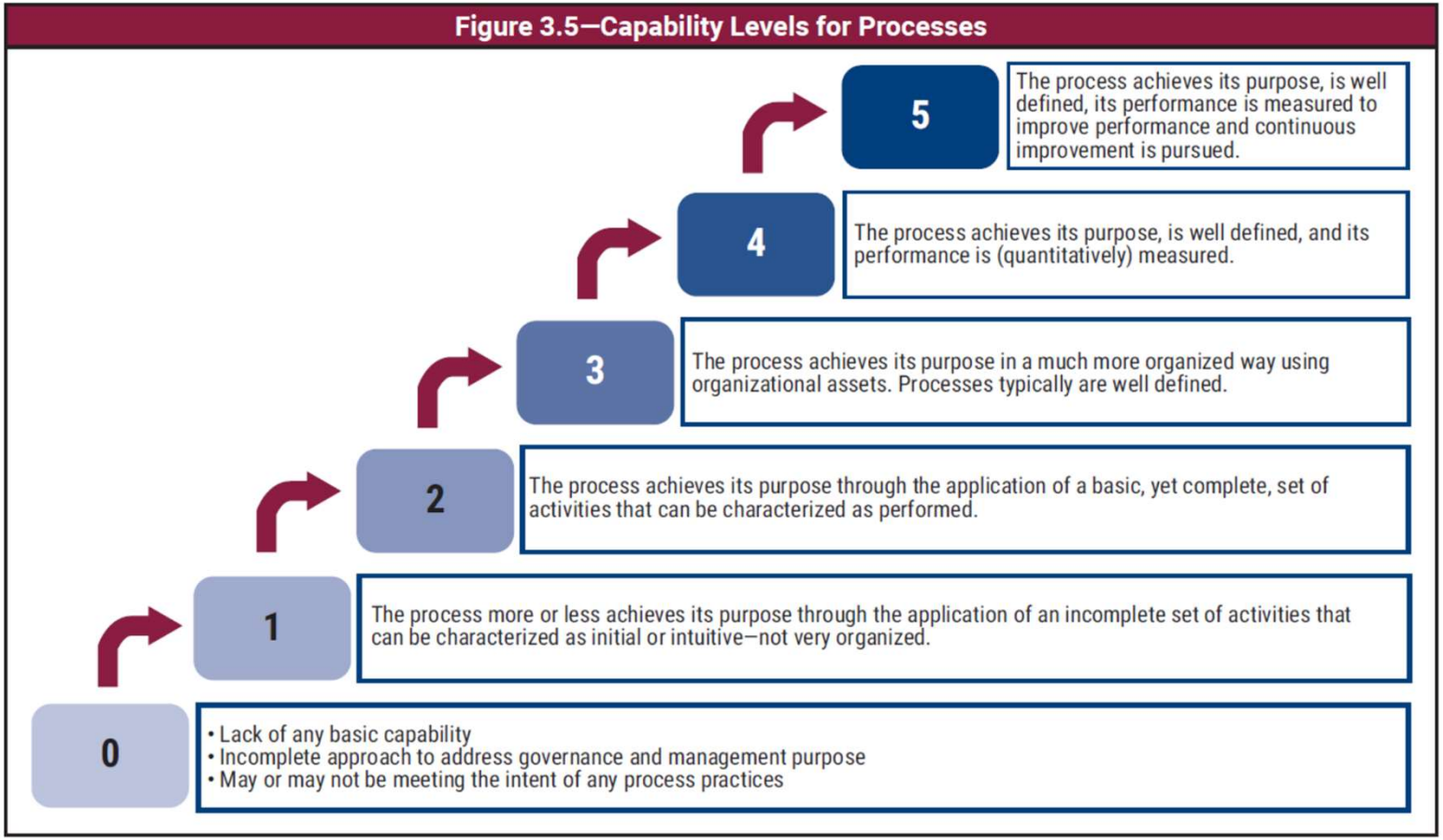


Figure 3.5—Capability Levels for Processes
5
The process achieves its purpose, is well defined, its performance is measured to improve performance and continuous improvement is pursued.
4
The process achieves its purpose, is well defined, and its performance is (quantitatively) measured.
3
The process achieves its purpose in a much more organized way using organizational assets. Processes typically are well defined.
2
The process achieves its purpose through the application of a basic, yet complete, set of activities that can be characterized as performed.
1
The process more or less achieves its purpose through the application of an incomplete set of activities that can be characterized as initial or intuitive—not very organized.
0
• Lack of any basic capability
• Incomplete approach to address governance and management purpose
• May or may not be meeting the intent of any process practices

Atención

- Una empresa puede organizar sus procesos como crea conveniente, siempre y cuando las metas de gobierno y gestión queden cubiertas.
- Empresas más pequeñas pueden tener pocos procesos;
- Empresas más grandes y complejas pueden tener numerosos procesos, pero todos con el ánimo de cubrir las mismas metas.

BAI03 Gestionar la Identificación y Construcción de Soluciones	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción del Proceso Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.	
Declaración del Propósito del Proceso Establecer soluciones puntuales y rentables capaces de soportar la estrategia de negocio y objetivos operacionales.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. El diseño de la solución, incluyendo los componentes relevantes, debe cumplir con las necesidades de la empresa, alineándose con estándares y tratando todos los riesgos identificados.	• Número de rediseños realizados debido a discordancias con los requerimientos • Tiempo para aprobar que el entregable de diseño ha cumplido los requerimientos
2. La solución conforme al diseño, es acorde a las normas organizativas y cuenta con controles, seguridad y 'auditabilidad' apropiadas.	• Número de excepciones al diseño observadas durante la fase de revisión
3. La solución es de una calidad aceptable y ha sido probada convenientemente.	• Número de errores encontrados durante las pruebas • Tiempo y esfuerzo para completar las pruebas
4. Los cambios aprobados de los requerimientos están correctamente incorporadas a la solución.	• Número de cambios aprobados y registrados que generan nuevos errores
5. Las actividades de mantenimiento cumplen satisfactoriamente con las necesidades tecnológicas y de negocio.	• Número de solicitudes de mantenimiento no atendidas

Matriz RACI BAI03

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
BAI03.01 Diseñar soluciones de alto nivel.						R		I	R							C	C	I	C	A	C		C	C	C	C
BAI03.02 Diseñar los componentes detallados de la solución						R		I	R							C	C	I	C	A	C		C	C	C	C
BAI03.03 Desarrollar los componentes de la solución						R		I	R							C	C	I	C	A	C		C	C	C	C
BAI03.04 Obtener los componentes de la solución					I	R		I	I							C	C	A	I	R	R	R	C	C	C	C
BAI03.05 Construir soluciones.						R		I	R							C	C	I	C	A	C		C	C	C	C
BAI03.06 Realizar controles de calidad.					I	R		A	R							C	C	I	C	R	C		C	C	C	C
BAI03.07 Preparar pruebas de la solución						R		A	I							C	C	I		R	R		R	R	R	R
BAI03.08 Ejecutar pruebas de la solución						R		A	I							I	I	I		R	R		I	I	I	I
BAI03.09 Gestionar cambios a los requerimientos.					I	R		A	R							I	I	C	R	R	C		C	C	C	C
BAI03.10 Mantener soluciones.						R			R							C	C	I	C	A	C		C	C	C	C
BAI03.11 Definir los servicios TI y mantener el catálogo de servicios.					I	I			I							I	I	R	I	C	C	C	A	I	I	

BAI03 Prácticas, Entradas/Salidas y Actividades del Proceso

Prácticas de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	Hacia
BAI03.01 Diseñar soluciones de alto nivel. Desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas. Asegurar el alineamiento con la estrategia TI y la arquitectura empresarial. Revalorar y actualizar los diseños cuando sucedan cuestiones significativas durante las fases de diseño detallado o de construcción o según la solución evolucione. Asegurar que las partes interesadas participen activamente en el diseño y en la aprobación de cada versión.	APO03.01	Principios de arquitectura	Aprobación de las especificaciones del diseño de alto nivel.	BAI04.03 BAI05.01
	APO03.02	Descripciones de los dominios de referencia y la definición de arquitectura		
	APO04.03	Análisis de investigación de las posibilidades de innovación		
	APO04.04	Evaluación de las ideas de innovación		
	BAI02.01	• Confirmar los criterios de aceptación por las partes interesadas • Repositorio de la definición de requerimientos		
	BAI02.02	Plan de alto nivel de adquisiciones/desarrollo		

Actividades

1. Establecer especificaciones de diseño a alto nivel que traduzcan la solución propuesta en procesos de negocio, servicios soportados, aplicaciones, infraestructura y repositorios de información capacidades de cumplir con los requerimientos de arquitectura de negocio y empresa.
2. Involucrar a usuarios experimentados y apropiadamente cualificados así como especialistas TI en el proceso de diseño para asegurar que el diseño proporciona una solución que usa las capacidades TI de manera optimiza para mejorar el proceso de negocio.
3. Crear un diseño acorde a los estándares de diseño de la organización, a un nivel de detalle que sea apropiado para la solución y el método de desarrollo y en consonancia con el negocio, empresa, estrategias TI, la arquitectura empresarial, el plan de seguridad, leyes aplicables, regulaciones y contratos.
4. Tras la aprobación de la garantía de calidad, remitir el diseño final a alto nivel del proyecto a las partes interesadas y al patrocinador/dueño del proceso de negocio para su aprobación basada en los criterios establecidos. Este diseño evolucionará durante todo el proyecto según mejore la comprensión.

Prácticas de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	Hacia
BAI03.02 Diseñar los componentes detallados de la solución. Desarrollar, documentar y elaborar diseños detallados progresivamente usando técnicas de desarrollo ágiles o por fases acordadas previamente considerando todos los componentes (procesos de negocio y automatización relacionada y controles manuales, aplicaciones soporte de TI, servicios de infraestructura y productos tecnológicos y proveedores/fabricantes). Asegurar que el diseño detallado incluye ANSs y OLAs internos y externos	APO03.01	Principios de arquitectura	Especificaciones de diseño detalladas y aprobadas	BAI04.03 BAI05.01
	APO03.02	• Modelo de arquitectura de la información • Descripciones de los dominios de referencia y definición de arquitectura	ANSs y OLAs	BAI04.02
	APO03.05	Guía de desarrollo de la solución		
	APO04.06	Evaluaciones de utilización de aproximaciones innovadoras		
	BAI02.01	• Confirmar los criterios de aceptación por parte de las partes interesadas • Repositorio de definición de los requerimientos		
	BAI02.02	Informe de estudio de viabilidad		
	BAI02.03	• Acciones de mitigación de riesgos • Registro de riesgos de requerimientos		
	BAI02.04	Aprobación del patrocinador de los requerimientos y soluciones propuestas		

BAI03.02 Actividades

1. Diseñar progresivamente las actividades del proceso de negocio y los flujos de trabajo necesarios para llevar a cabo conjuntamente con el nuevo sistema de aplicación para alcanzar los objetivos de la empresa, incluyendo el diseño de las actividades de control manuales.
2. Diseñar las etapas de procesamiento de la aplicación, incluyendo especificaciones de tipos de transiciones y reglas de negocio, controles automatizados, definiciones de datos/objetos de negocio, casos de uso, interfaces externos, limitaciones de diseño y otros requerimientos (por ejemplo, licencias, legales, estándares e internacionalización/localización).

BAI03 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*

3. Clasificar las entradas y salidas de datos acorde a los estándares de arquitectura empresarial. Especificar el diseño de los datos de origen, documentar las entradas de datos (independientemente de la fuente) y validaciones para las transacciones así como los métodos de validación. Diseñar las salidas identificadas, incluyendo el origen de los datos.
4. Diseñar el interfaz del sistema/solución, incluyendo cualquier intercambio automatizado de datos.
5. Diseñar el almacenamiento de los datos, localización y capacidad de recuperación.
6. Diseñar la redundancia, recuperación y copia de seguridad apropiadas.
7. Diseñar el interfaz entre el usuario y la aplicación del sistema para que sea fácil de usar y sea auto explicativo.
8. Considerar el impacto de las necesidades de la solución en el rendimiento de la infraestructura, considerando el número de activos informáticos, intensidad de ancho de banda y tiempo en que la información se considera sensible.
9. Evaluar proactivamente las debilidades del diseño (por ejemplo, inconsistencias, falta de claridad, fallos potenciales) a través de todo el ciclo de vida, identificando mejoras cuando se requieran.
10. Proporcionar métodos para auditar las transacciones e identificar la causa raíz de los problemas en el procesamiento.

Práctica de Gestión	Entradas		Salidas	
BAI03.03 Desarrollar los componentes de la solución. Desarrollar los componentes de la solución progresivamente conforme el diseño detallado siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación. Asegurar que se consideran todos los requerimientos de control en los procesos de negocio, soportando las aplicaciones TI y servicios de infraestructura, productos tecnológicos y servicios y proveedores/suministradores.	**De**	**Descripción**	**Descripción**	**Hacia**
	BAI02.02	Informe de estudio de viabilidad	Documentar los componentes de la solución	BAI04.03 BAI05.05 BAI08.03 BAI08.04
	BAI02.04	Aprobaciones de los patrocinadores de los requerimientos y soluciones propuestas		

Activities

1. Desarrollar procesos de negocio, servicios de soporte, aplicaciones e infraestructura y repositorios de información basados en las especificaciones acordadas y requerimientos técnicos, funcionales y de negocio.
2. Cuando proveedores terceros estén involucrados en el desarrollo de la solución, asegurar que el mantenimiento, soporte, estándares y licenciamiento están contempladas en las obligaciones contractuales.
3. Registrar las peticiones de cambio y revisar el diseño, rendimiento y calidad, asegurando una participación activa de las partes interesadas afectadas.
4. Documentar todos los componentes de la solución acorde a los estándares definidos y mantener el control de la versión sobre los mismos y la documentación asociada.
5. Evaluar el impacto de la personalización de la solución y la configuración en el rendimiento y eficiencia de las soluciones adquiridas y en su interoperabilidad con las aplicaciones, sistemas operativos y otra infraestructura existentes. Adaptar los procesos de negocio como se requiera para aprovechar las capacidades de la aplicación.
6. Asegurar que las responsabilidades por usar una alta seguridad o acceso restringido a los componentes de la infraestructura están claramente definidas y son comprendidas por todos aquellos que desarrollan e integran los componentes de la infraestructura. Su uso debería ser supervisado y evaluado.

Práctica de Gestión	Entradas		Salidas	
BAI03.04 Obtener los componentes de la solución. Obtener los componentes de la solución sobre la base del plan de adquisiciones y conforme a los requerimientos y diseños detallados, principios de arquitectura y estándares y en los procedimientos generales contractuales y de adquisiciones de la empresa, requerimientos de calidad (QA) y aprobación de estándares. Asegurar que todos los requerimientos legales y contractuales son identificados y cumplidos por el proveedor.	**De**	**Descripción**	**Descripción**	**Hacia**
	BAI02.04	Aprobación del patrocinador de los requerimientos y soluciones propuestas	Plan de adquisiciones aprobado	APO10.03
			Actualizaciones del inventario de activos	BAI09.01

Actividades

1. Crear y mantener un plan de adquisiciones de los componentes de la solución, considerando una flexibilidad futura para añadir capacidad, costes de transición, riesgos y actualizaciones a lo largo de la vida del proyecto.
2. Revisar y aprobar todos los planes de adquisiciones, considerando riesgos, costes, beneficios y conformidad técnica con los estándares de arquitectura empresarial.
3. Evaluar y documentar en qué grado las soluciones adquiridas requieren adaptación a los procesos de negocio para aprovechar los beneficios de la solución adquirida.
4. Realizar seguimiento de las aprobaciones requeridas en puntos de decisión clave durante los procesos de contratación.
5. Registrar los recibos de todas las adquisiciones realizadas de software e infraestructura en el inventario de activos.

BAI03 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*

Práctica de Gestión	Entradas		Salidas	
BAI03.05 Construir soluciones. Instalar y configurar las soluciones e integrarlas con las actividades de los procesos de negocio. Implementar controles, medidas de seguridad y 'auditabilidad' durante la configuración y durante la integración del hardware e infraestructura del software para proteger los recursos y asegurar la disponibilidad e integridad de los datos. Actualizar el catálogo de servicios para reflejar la nueva situación.	**De**	**Descripción**	**Descripción**	**Hacia**
			Componentes de la solución integrados y configurados	BAI06.01

Actividades

1. Integrar y configurar los componentes de la solución TI y de negocio así como los repositorios de información en línea con las especificaciones detalladas y los requerimientos de calidad. Considerar el rol de los usuarios, interesados de negocio y el dueño del proceso en la configuración de los procesos de negocio.
2. Completar y actualizar cuando sea necesario el proceso de negocio y los manuales de operaciones para registrar cualquier personalización o condiciones especiales únicas en la implementación.
3. Considerar toda la información relevante en los controles de los requerimientos en la integración y configuración de los componentes de la solución, incluyendo cuando sea necesario, controles en la implementación de negocio, controles automatizados en la aplicación para que el procesamiento sea fiable, completo, a tiempo, autorizado y auditable.
4. Implementar pistas de auditoría durante la configuración e integración del hardware e infraestructura del software para proteger los recursos y asegurar la disponibilidad e integridad.
5. Considerar cuando el efecto de las personalizaciones y las configuraciones acumuladas (incluyendo cambios menores que no estaban sujetos a unas especificaciones de diseño formal) requieran una revalidación a alto nivel de la solución y funcionalidad asociada.
6. Asegurar la interoperabilidad de los componentes de la solución con las pruebas de soporte preferiblemente automatizadas.
7. Configurar que el software de aplicación adquirido cumple con los requerimientos de proceso de negocio.
8. Definir el catálogo de servicios para los grupos de objetivos internos y externos basados en los requerimientos de negocio.

Práctica de Gestión	Entradas		Salidas	
BAI03.06 Realizar controles de calidad. Desarrollar y ejecutar un plan de calidad (QA) alineado con el SGC para obtener la calidad especificada en la definición de los requerimientos y de acuerdo a las políticas y procedimientos de calidad de la empresa.	**De**	**Descripción**	**Descripción**	**Hacia**
	APO11.01	Resultados de las revisiones de efectividad del SGC	Plan de aseguramiento de la calidad (QA)	APO11.04
	BAI01.09	Plan de gestión de calidad	Resultados de la revisión de calidad, excepciones y correcciones	APO11.04

Actividades

1. Definir un plan de calidad (QA) y prácticas incluyendo, por ejemplo, especificación de criterios de calidad, procesos de validación y verificación, definición de cómo se revisará la calidad, calificaciones necesarias para la evaluaciones de calidad y roles y responsabilidades para la consecución de la calidad.
2. Supervisar frecuentemente la solución de calidad, basada en los requerimientos del proyecto, políticas de empresa, adhesión a metodologías de desarrollo, procedimientos de gestión de calidad y criterios de aceptación.
3. Utilizar apropiadamente inspección de código, pruebas conducidas sobre el desarrollo, pruebas automatizadas, integración continua, revisiones y pruebas sobre aplicaciones. Informar de los resultados del proceso de supervisión y prueba al equipo de desarrollo de software de aplicación y a la dirección TI.
4. Supervisar todas las excepciones de calidad y tratar todas las acciones correctivas. Mantener un registro con todas las revisiones, resultados, excepciones y correcciones. Repetir las evaluaciones de calidad cuando sea necesario, basándose en la cantidad de reelaboración (*rework*) y acciones correctivas.

Práctica de Gestión	Entradas		Salidas	
BAI03.07 Preparar pruebas de la solución. Establecer un plan de pruebas y entornos necesarios para probar los componentes individualmente y de la solución integrada incluyendo los procesos de negocio y servicios, aplicaciones e infraestructura que los soportan.	**Desde**	**Descripción**	**Descripción**	**Hacia**
			Plan de pruebas	BAI07.03
			Procedimientos de pruebas	BAI07.03

Actividades

1. Crear un plan de pruebas integradas y prácticas acordes al entorno de la empresa y planes estratégicos de tecnología que catalizarán la realización de pruebas apropiadas en entornos de simulación para ayudar a verificar que la solución estará operativa satisfactoriamente en el entorno real y entregar los resultados esperados y que los controles son adecuados.
2. Crear un entorno de pruebas que soporte el alcance completo de la solución y refleje, lo más fielmente posible, las condiciones del mundo real, incluyendo los procesos y procedimientos de negocio, rango de usuarios, tipos de transacciones y condiciones de desarrollo.
3. Crear procedimientos de prueba alineados con el plan y las prácticas y que permitan la evaluación de la operativa de la solución en condiciones reales. Asegurar que los procedimientos de prueba evalúan la adecuación de los controles, basado en estándares de toda la empresa que definan roles, responsabilidades y criterios de prueba y sean aprobado por las partes interesadas del proyecto y por el patrocinador/dueño del proceso de negocio.

BAI03 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	Hacia
BAI03.08 Ejecutar pruebas de la solución. Ejecutar pruebas continuamente durante el desarrollo, incluyendo pruebas de control, en concordancia con el plan de pruebas y con las prácticas de desarrollo en el entono apropiado. Hacer partícipes a los dueños de los procesos de negocio y usuarios finales en el equipo de pruebas. Identificar, registrar y priorizar los errores e incidentes identificados durante las pruebas.	APO04.05	Análisis de las iniciativas rechazadas	Registros de resultados de pruebas y pistas de auditoría	BAI07.03
			Comunicaciones del resultado de las pruebas	BAI07.03

Actividades

1. Realizar las pruebas de las soluciones y sus componentes en concordancia con el plan de pruebas. Incluir probadores independientes del equipo de la solución, con representación de los dueños de los procesos y usuarios finales del negocio. Asegurar que las pruebas son realizadas solo en los entornos de desarrollo y pruebas.
2. Utilizar instrucciones de pruebas claramente definidas, tal y como se indica en el plan de pruebas y considerar un equilibrio adecuado entre pruebas automatizadas y pruebas con interactividad del usuario.
3. Realizar todas las pruebas conforme el plan y prácticas de pruebas incluyendo la integración de los procesos de negocio y los componentes de la solución TI y los requerimientos no funcionales (por ejemplo, seguridad, interoperabilidad, usabilidad).
4. Identificar, registrar y clasificar (por ejemplo, fallos menores, significativos, críticos) los errores durante las pruebas. Repetir las pruebas hasta que todos los errores significativos hayan sido resueltos. Asegurarse que existen y se mantienen pistas de auditoría de los resultados de las pruebas.
5. Registrar los resultados de las pruebas y comunicar los resultados a las partes interesadas conforme al plan de pruebas.

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	Hacia
BAI03.09 Gestionar cambios a los requerimientos. Hacer seguimiento del estado de los requerimientos individuales (incluyendo todos los requerimientos rechazados) a través de todo el ciclo de vida del proyecto y gestionar la aprobación de los cambios a los requerimientos.	APO04.05	Resultados y recomendaciones de las iniciativas de pruebas de concepto	Registro de todas las peticiones de cambio aprobadas y aplicadas	BAI06.03
	BAI02.01	Registro de peticiones de cambio de los requerimientos		

Actividades

1. Evaluar el impacto de todas las peticiones de cambio de la solución en el desarrollo de la solución, el caso de negocio original y en el presupuesto, y categorizar y priorizar las peticiones convenientemente.
2. Hacer seguimiento de los requerimientos, facilitando a las partes interesadas la supervisión, revisión y aprobación de los cambios. Asegurar que los resultados de los procesos de cambio están completamente entendidos y están de acuerdo todos las partes interesadas y el patrocinador/ propietario del proceso de negocio.
3. Aplicar las peticiones de cambio, manteniendo la integridad de la integración y configuración de los componentes de la solución. Evaluar el impacto de cualquier actualización mayor de la solución y clasificarla conforme a criterios objetivos acordados (tales como los requerimientos de empresa) basados en los resultados del análisis de riesgos que lo acompaña (tales como el impacto en los sistemas existentes y procesos o seguridad), justificación del coste/beneficio y otros requerimientos.

Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	Hacia
BAI03.10 Mantener soluciones. Desarrollar y ejecutar un plan para el mantenimiento de la solución y componentes de la infraestructura. Incluir revisiones periódicas respecto a las necesidades de negocio y requerimientos operacionales.			Plan de mantenimiento	APO08.05
			Componentes de la solución actualizados y documentación relacionada	BAI05.05

Actividades

1. Desarrollar y ejecutar un plan para el mantenimiento de los componentes de la solución que incluya revisiones periódicas respecto a las necesidades de negocio y requerimientos operacionales tales como la gestión de parches, estrategias de actualización, riesgos, análisis de vulnerabilidades y requerimientos de seguridad.
2. Evaluar la significatividad de las actividades de mantenimiento propuestas sobre el diseño de la solución, funcionalidad y/o procesos de negocio actuales. Considerar el riesgo, impacto en los usuarios y disponibilidad de recursos. Asegurar que los propietarios de los procesos de negocio comprenden el efecto de los cambios designados como mantenimiento.
3. En el caso de cambios mayores a las soluciones existentes que resulten en un cambio significativo en el diseño actual y/o funcionalidad y/o procesos de negocio, seguir el proceso de desarrollo usado para nuevos sistemas. Para actualizaciones de mantenimiento usar los procesos de gestión de cambios.
4. Asegurar que el patrón y volumen de las actividades son analizadas periódicamente para buscar tendencias anormales indicando una merma en la calidad o problemas de rendimiento, coste/beneficio de las actualizaciones mayores o remplazo en lugar de mantenimiento.
5. Para actualizaciones de mantenimiento, utilizar el proceso de gestión de cambio para controlar todas las peticiones de mantenimiento.

BAI03 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gestión	**Entradas**		**Salidas**	
	Desde	**Descripción**	**Descripción**	**Hacia**
BAI03.11 Definir los servicios TI y mantener el catálogo de servicios Definir y acordar nuevos servicios TI o cambios y opciones de nivel de servicio. Documentar nuevas definiciones o cambios en los servicios y opciones de nivel de servicio que serán actualizadas en el catálogo de servicios.	EDM04.01	Directrices para la asignación de recursos y capacidades	Definiciones de servicio	APO05.01 DSS01.03
	APO02.04	• Valorar beneficios para el entorno objetivo • Cambios requeridos para ajustar la capacidad objetivo	Catálogo de servicios actualizado	APO05.05
	APO06.02	Asignaciones de presupuesto		
	APO06.03	• Comunicación del presupuesto • Plan y presupuesto TI		
	APO08.05	Definición de mejoras potenciales de proyectos		
	BAI10.02	Configuración de la línea de referencia		
	BAI10.03	Aprobación de cambios a la línea de referencia		
	BAI10.04	Informes del estado de la configuración		

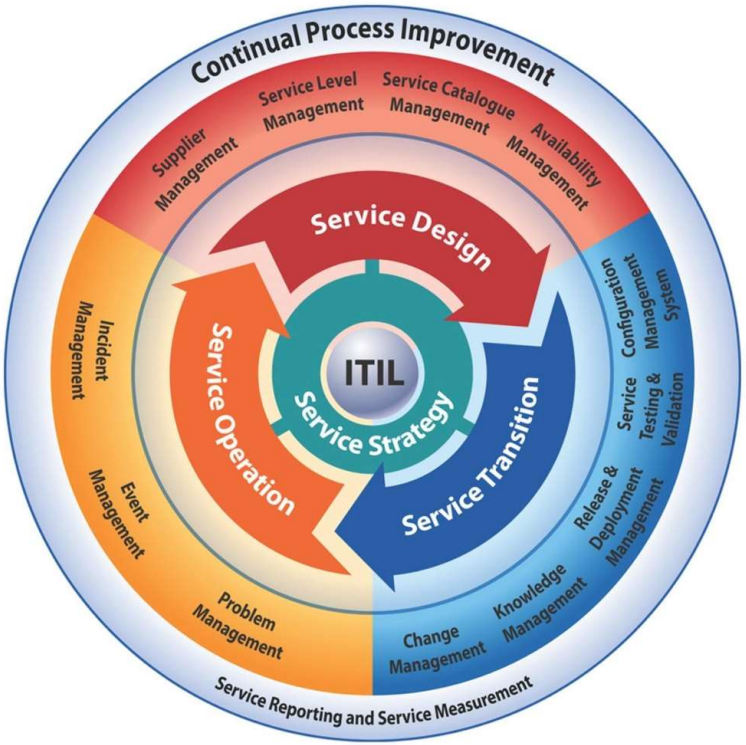
Actividades
1. Proponer definiciones de los nuevos o modificados servicios TI que aseguren que los servicios cumplen con el propósito. Documentar las definiciones de servicio propuestas en la lista del catálogo de los servicios a desarrollar.
2. Proponer cambios o nuevas opciones de niveles de servicios (franjas horarias del servicio, satisfacción del usuario, disponibilidad, rendimiento, capacidad, seguridad, continuidad, cumplimiento regulatorio, usabilidad) para asegurar que los servicios TI son adecuados para su uso. Documentar las opciones de niveles de servicio propuestas en el catálogo de servicios.
3. Intermediar con el gestor de relaciones de negocio y el gestor del portafolio para acordar las definiciones y opciones de niveles de servicio.
4. Si los cambios a los servicios provienen de una autoridad de aprobación adecuada, construir los cambios o los nuevos servicios TI o las opciones de los niveles de servicio. De otro modo, pasar los cambios de servicio a la gestión de la cartera de servicios para su oportuna revisión.

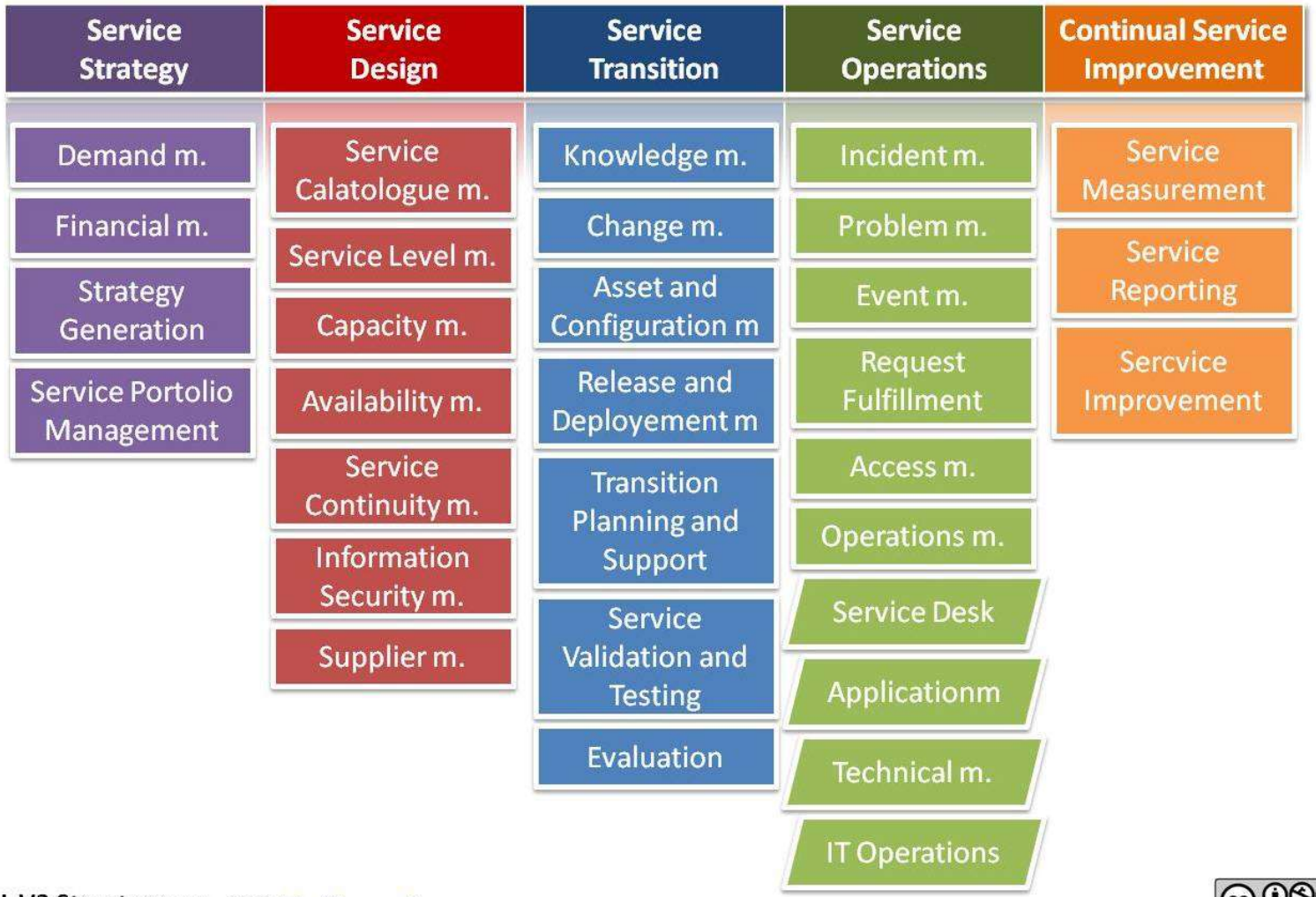
BAI03 Guías Relacionadas	
Estándar Relacionado	**Referencia Detallada**
Ninguno	

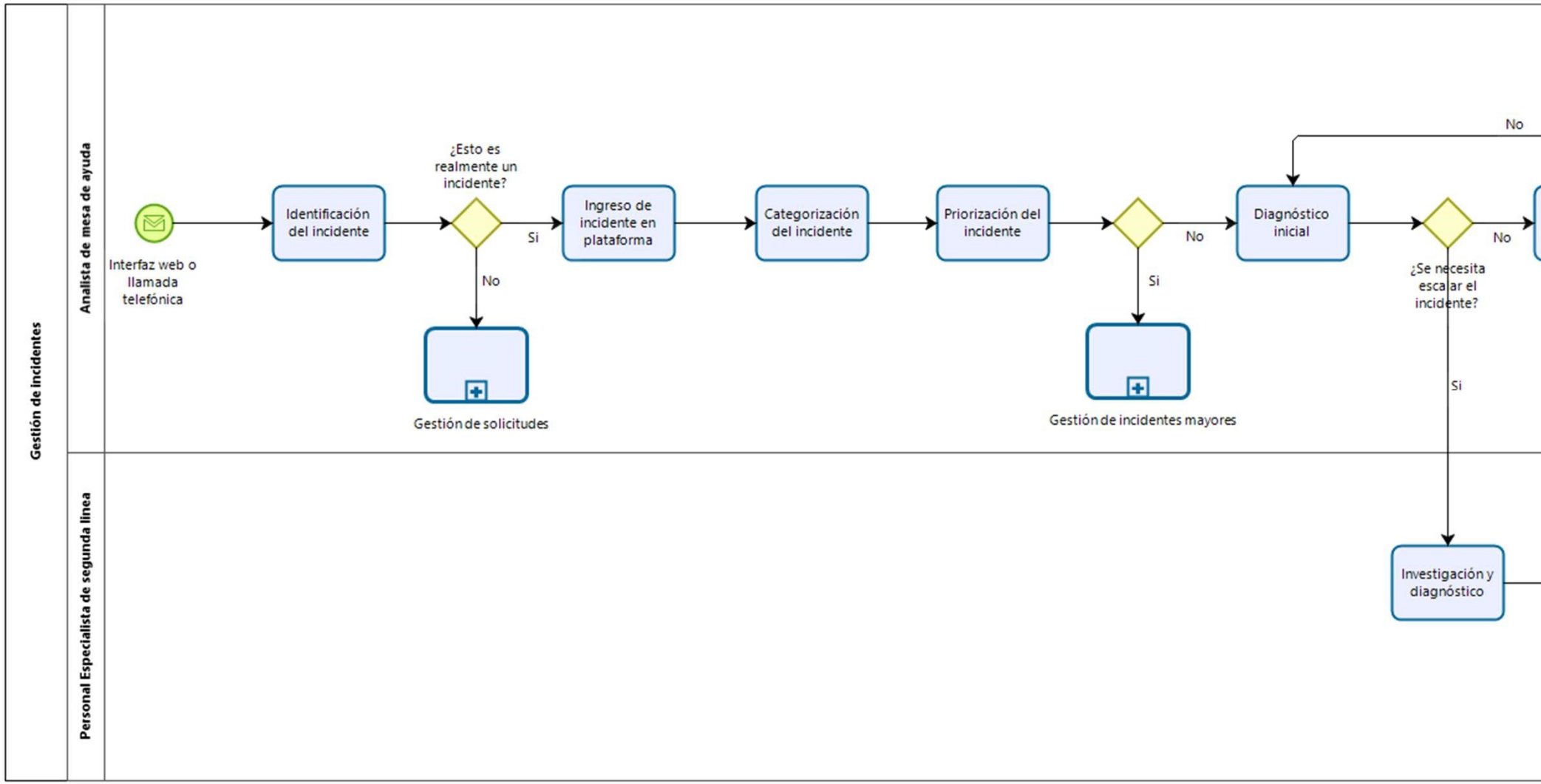
ITIL

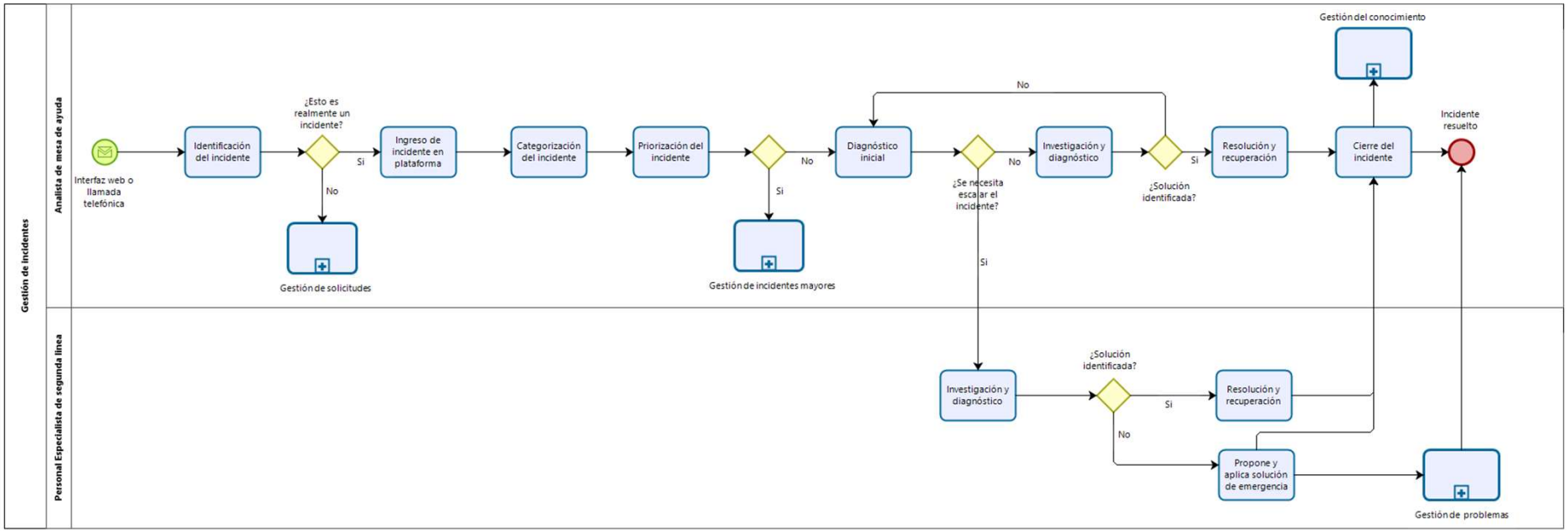
- El *Information Technology Infraestructure Library* (ITIL)
- Estándar de facto de las mejores prácticas para el manejo de los servicios de TI.
- Creado por la dependencia entre las necesidades del negocio y las TI.
- Es un conjunto de libros que proveen los objetivos a largo plazo y las actividades necesarias para conseguir estos objetivos.
- Es orientado a brindar, internamente en una empresa, un SLA adecuado.

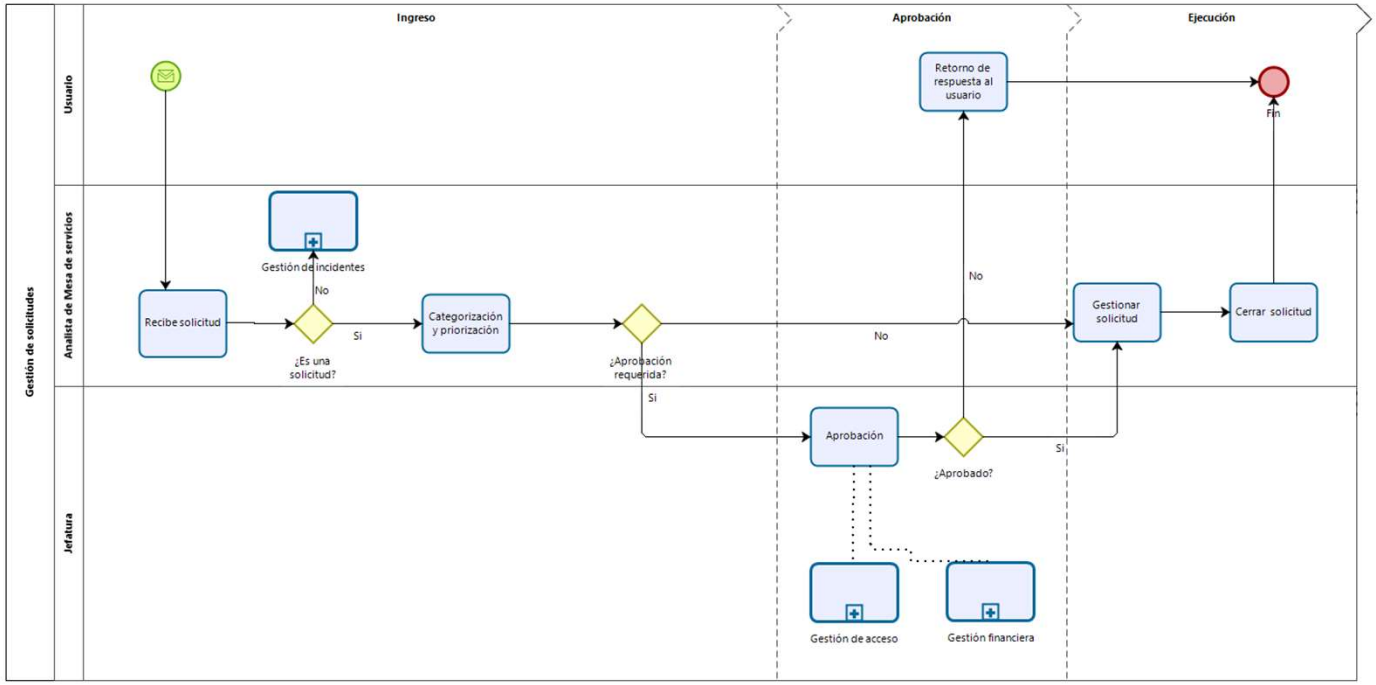
ITIL


Continual Process Improvement
Service Level Management
Service Catalogue Management
Availability Management
Supplier Management
Service Design
Service Strategy
Service Transition
Service Operation
ITIL
Configuration Management System
Service Testing & Validation
Release & Deployment Management
Knowledge Management
Change Management
Problem Management
Event Management
Incident Management
Service Reporting and Service Measurement


Service Strategy
Demand m.
Financial m.
Strategy Generation
Service Portolio Management
Service Design
Service Calatologue m.
Service Level m.
Capacity m.
Availability m.
Service Continuity m.
Information Security m.
Supplier m.
Service Transition
Knowledge m.
Change m.
Asset and Configuration m
Release and Deployement m
Transition Planning and Support
Service Validation and Testing
Evaluation
Service Operations
Incident m.
Problem m.
Event m.
Request Fulfillment
Access m.
Operations m.
Service Desk
Applicationm
Technical m.
IT Operations
Continual Service Improvement
Service Measurement
Service Reporting
Sercvice Improvement


Gestión de incidentes
Analista de mesa de ayuda
Personal Especialista de segunda línea
Interfaz web o llamada telefónica
Identificación del incidente
¿Esto es realmente un incidente?
Si
No
Gestión de solicitudes
Ingreso de incidente en plataforma
Categorización del incidente
Priorización del incidente
Si
No
Gestión de incidentes mayores
Diagnóstico inicial
No
¿Se necesita escalar el incidente?
Si
No
Investigación y diagnóstico


Gestión de incidentes
Analista de mesa de ayuda
Personal Especialista de segunda línea
Interfaz web o llamada telefónica
Identificación del incidente
¿Esto es realmente un incidente?
Si
No
Gestión de solicitudes
Ingreso de incidente en plataforma
Categorización del incidente
Priorización del incidente
Si
No
Gestión de incidentes mayores
Diagnóstico inicial
¿Se necesita escalar el incidente?
No
Si
Investigación y diagnóstico
¿Solución identificada?
No
Si
Resolución y recuperación
Gestión del conocimiento
Cierre del incidente
Incidente resuelto
Investigación y diagnóstico
¿Solución identificada?
Si
No
Resolución y recuperación
Propone y aplica solución de emergencia
Gestión de problemas


Gestión de solicitudes
Usuario
Analista de Mesa de servicios
Jefatura
Ingreso
Aprobación
Ejecución
Retorno de respuesta al usuario
Fin
Gestión de incidentes
No
Recibe solicitud
¿Es una solicitud?
Si
Categorización y priorización
¿Aprobación requerida?
No
Gestionar solicitud
Cerrar solicitud
Si
Aprobación
¿Aprobado?
Si
Gestión de acceso
Gestión financiera
Powered by
bizagi
Modeler

CMMi

- Capability Maturity Model Integration (CMMI)
- Proviene del mundo de la ingeniería en seguridad.
- Constantemente debemos ir mejorando nuestros programas de seguridad. ¿Pero como mejorar? (este concepto es vago).
- Debemos definir niveles de madurez del programa de seguridad.

CMMi

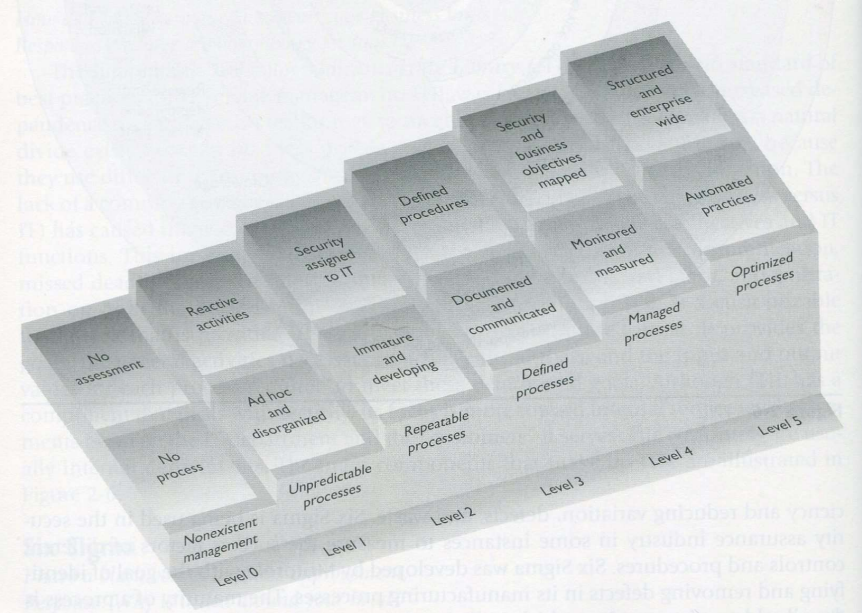


Figure 2-7 Capability Maturity Model for a security program

Importante

- Todo programa de seguridad debe seguir un acercamiento Top-Down.
  - Este asegura que la administración de la empresa está preocupada por proteger sus activos.
  - Se suministran los recursos necesarios para su construcción.
  - Se asegura el seguimiento de las políticas generadas.
- Un acercamiento Bottom-up
  - es menos efectivo.
  - No abarca todos los riesgos
  - Y finalmente falla estrepitosamente

Importante

- Ninguna organización va a colocar todos los estándares vistos anteriormente en práctica.
- Pero estas son buenos *toolbox* de donde sacar las herramientas adecuadas para nuestra organización.
- A medida que el programa de seguridad madura, se van utilizando.
- Toda organización es distinta, pero todas están compuestas de gente, procesos, datos y tecnologías y cada una de ellos debe ser protegidos.

Recursos bibliográficos

- Alineando CobiT 4.1, ITILv3 e ISO 27002 en beneficio del negocio [Link]
- Cobit 5 en español. [Link]
- Introducción a COBIT 5 [Link]
- Cobit 4.1