

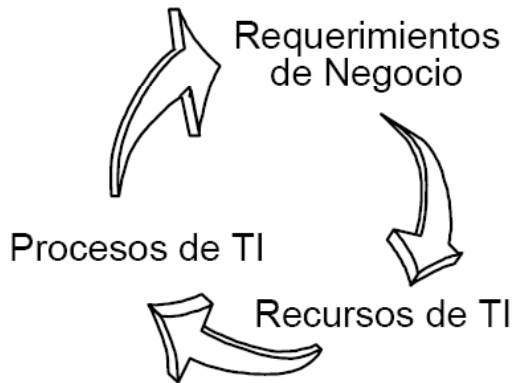


Control **OB**jectives for **I**nformation and related **T**echnology

LOS PRINCIPIOS DEL MARCO REFERENCIAL

Existen dos clases distintas de modelos de control disponibles actualmente, aquéllos de la clase del “modelo de control de negocios” (por ejemplo COSO) y los “modelos más enfocados a TI” (por ejemplo, DTT). *COBIT* intenta cubrir la brecha que existe entre los dos. Debido a esto, *COBIT* se posiciona como una herramienta más completa para la Administración y para operar a un nivel superior que los estándares de tecnología para la administración de sistemas de información.. **Por lo tanto, COBIT es el modelo para el gobierno de TI.**

El concepto fundamental del marco referencial *COBIT* se refiere a que el enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI.



Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que *COBIT* hace referencia como *requerimientos de negocio para la información*. Al establecer la lista de requerimientos, *COBIT* combina los principios contenidos en los modelos referenciales existentes y conocidos:

Requerimientos de calidad	Calidad Costo Entrega (de servicio)
Requerimientos Fiduciarios (COSO)	Efectividad & eficiencia de operaciones Confiabilidad de la información Cumplimiento de las leyes & regulaciones

Requerimientos de Seguridad	Confidencialidad Integridad Disponibilidad
------------------------------------	--

La Calidad ha sido considerada principalmente por su aspecto ‘negativo’ (no fallas, confiable, etc.), lo cual también se encuentra contenido en gran medida en los criterios de Integridad. Los aspectos positivos pero menos tangibles de la calidad (estilo, atractivo, “ver y sentir”¹⁴, desempeño más allá de las expectativas, etc.) no fueron, por un tiempo, considerados desde un punto de vista de Objetivos de Control de TI. La premisa se refiere a que la primera prioridad deberá estar dirigida al manejo apropiado de los riesgos al compararlos contra las oportunidades. El aspecto utilizable de la Calidad está cubierto por los criterios de efectividad. Se consideró que el aspecto de entrega (de servicio) de la Calidad se traslapa con el aspecto de disponibilidad correspondiente a los requerimientos de seguridad y también en alguna medida, con la efectividad y la eficiencia. Finalmente, el Costo es también considerado que queda cubierto por Eficiencia.

Para los requerimientos fiduciarios, *COBIT* no intentó reinventar le rueda – se utilizaron las definiciones de COSO para la efectividad y eficiencia de operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones -. Sin embargo, confiabilidad de información fue ampliada para incluir toda la información – no solo información financiera.

Con respecto a los aspectos de seguridad, *CobIT* identificó la confidencialidad, integridad y disponibilidad como los elementos clave, fue descubierto que estos mismos tres elementos son utilizados a nivel mundial para describir los requerimientos de seguridad.

Comenzando el análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad más amplios, se extrajeron siete categorías distintas, ciertamente superpuestas.

¹⁴ **Ver y Sentir** (*look and feel*)

A continuación se muestran las definiciones de trabajo de COBIT:

Efectividad	Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
Eficiencia	Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
Confidencialidad	Se refiere a la protección de información sensible contra divulgación no autorizada.
Integridad	Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
Disponibilidad	Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
Cumplimiento	Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.
Confiabilidad de la información	Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Los recursos de TI identificados en COBIT pueden explicarse/definirse como se muestra a continuación:

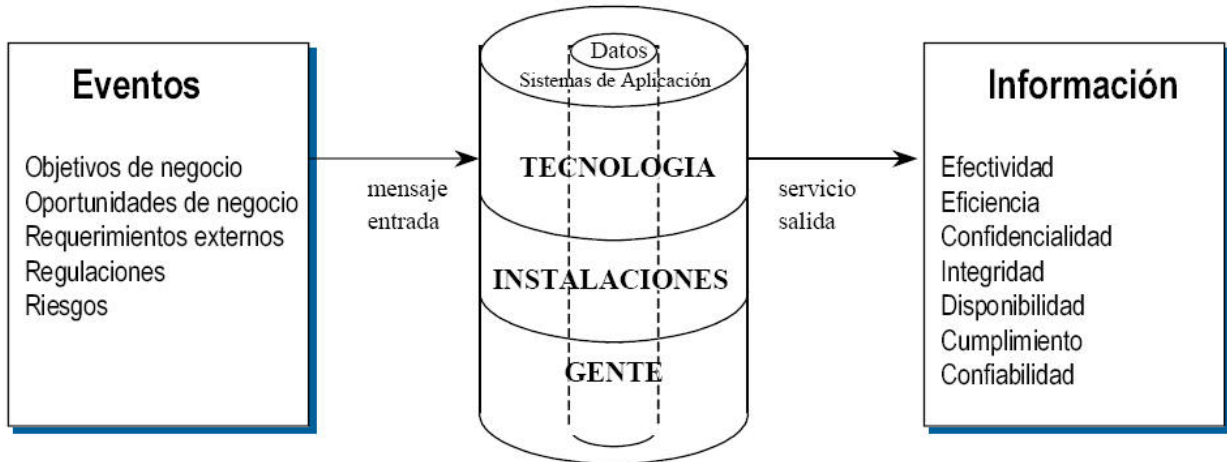
Datos	Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.
Aplicaciones	Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados
Tecnología	La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
Instalaciones	Recursos para alojar y dar soporte a los sistemas de información
Personal	Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información

El dinero o capital no fue considerado como un recurso para la clasificación de objetivos de control para TI debido a que puede definirse como la inversión en cualquiera de los recursos mencionados anteriormente y podría causar confusión con los requerimientos de auditoría financiera.

El Marco referencial no menciona, en forma específica para todos los casos, la documentación de todos los aspectos “materiales” importantes relacionados con un proceso de TI particular. Como parte de las buenas prácticas, la documentación es considerada esencial para un buen control y, por lo tanto, la falta de documentación podría ser la causa de revisiones y análisis futuros de controles de compensación en cualquier área específica en revisión.

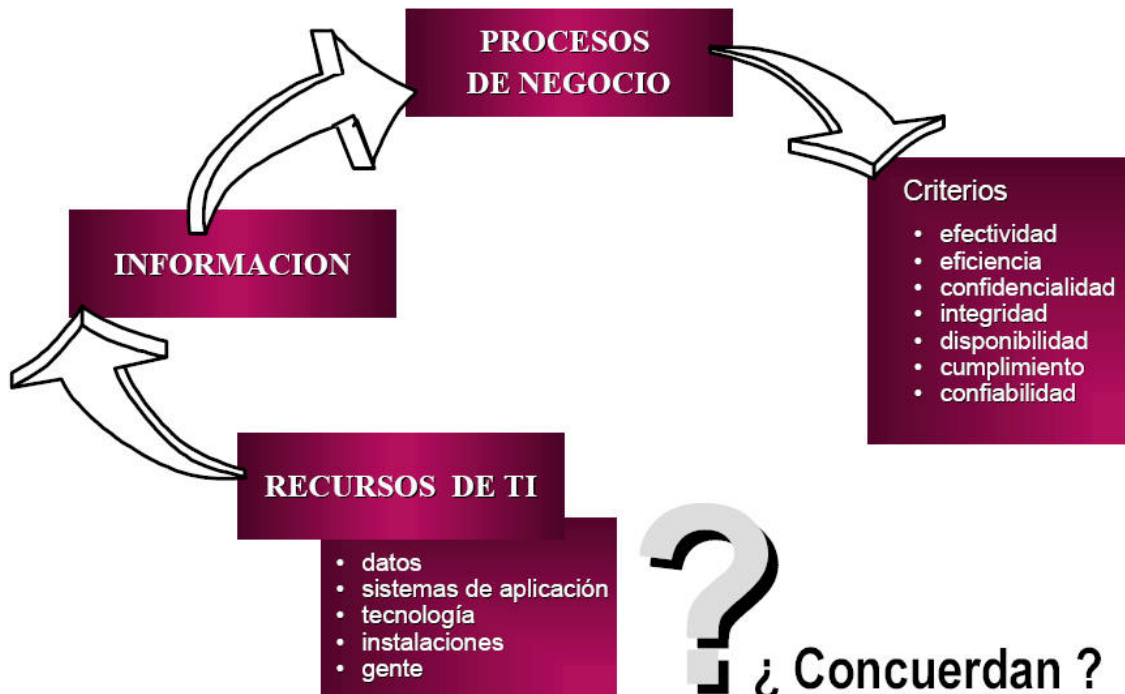
OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

Otra forma de ver la relación de los recursos de TI con respecto a la entrega de servicios se describe a continuación:



La información que los procesos de negocio necesitan es proporcionada a través del empleo de recursos de TI. Con el fin de asegurar que los requerimientos de negocio para la información son satisfechos, deben definirse, implementarse y monitorearse medidas de control adecuadas para estos recursos.

¿Cómo pueden entonces las empresas estar satisfechas respecto a que la información obtenida presente las características que necesitan? Es aquí donde se requiere de un sano marco referencial de Objetivos de Control para TI. El diagrama mostrado a continuación ilustra este concepto.



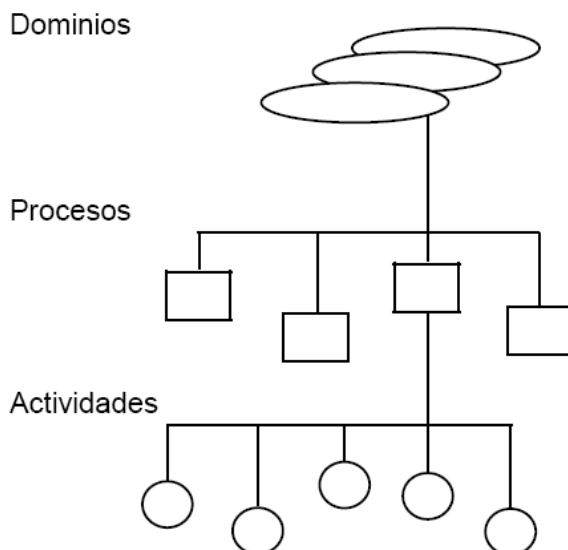
OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

El marco referencial consta de Objetivos de Control de TI de alto nivel y de una estructura general para su clasificación y presentación. La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI al considerar la administración de sus recursos.

Comenzando por la base, encontramos las actividades y tareas necesarias para alcanzar un resultado medible. Las actividades cuentan con un concepto de ciclo de vida, mientras que las tareas son consideradas más discretas. El concepto de ciclo de vida cuenta típicamente con requerimientos de control diferentes a los de actividades discretas. Algunos ejemplos de esta categoría son las actividades de desarrollo de sistemas, administración de la configuración y manejo de cambios. La segunda categoría incluye tareas llevadas a cabo como soporte para la planeación estratégica de TI, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño.

Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con "cortes" naturales (de control).

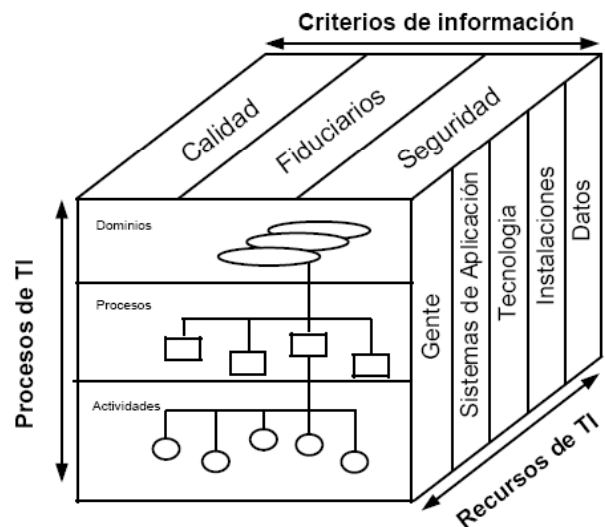
Al nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI.



Por lo tanto, el marco referencial conceptual puede ser enfocado desde tres puntos estratégicos: (1) recursos de TI, (2) requerimientos de negocio para la información y (3) procesos de TI. Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente.

Por ejemplo, los gerentes de la empresa pueden interesarse en un enfoque de calidad, seguridad o fiduciario (traducido por el marco referencial en siete requerimientos de información específicos). Un Gerente de TI puede desear considerar recursos de TI por los cuales es responsable. Propietarios de procesos, especialistas de TI y usuarios pueden tener un interés en procesos particulares. Los auditores podrán desear enfocar el marco referencial desde un punto de vista de cobertura de control.

Estos tres puntos estratégicos son descritos en el Cubo COBIT que se muestra a continuación:



Con lo anterior como marco de referencia, los dominios son identificados utilizando las palabras que la gerencia utilizaría en las actividades cotidianas de la organización –y no la "jerga"¹⁵ del auditor -. Por lo tanto, cuatro grandes dominios son identificados: planeación y organización, adquisición e implementación; entrega y soporte y monitoreo.

¹⁵ Jerga (jargon)

**Planeación y
organización**

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

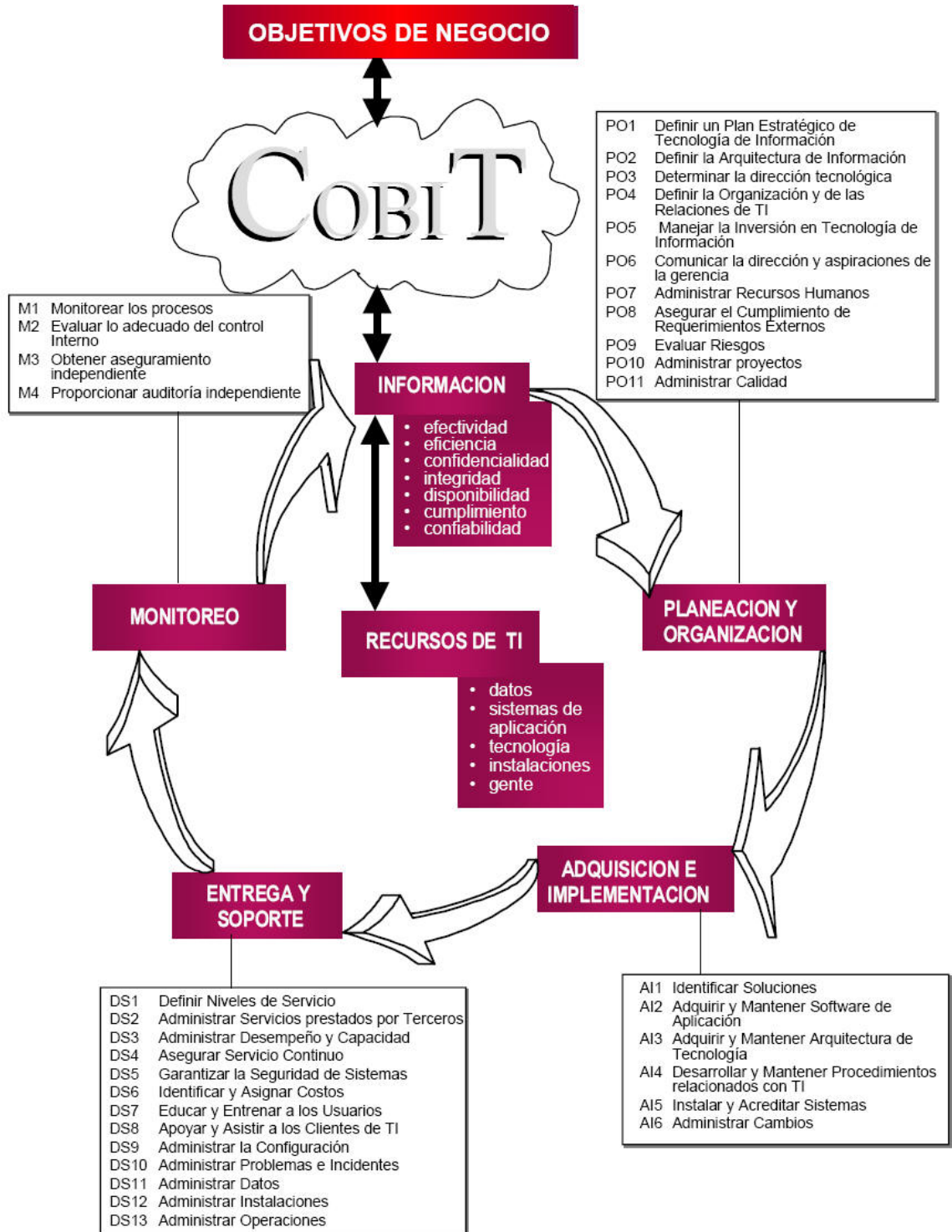
**Adquisición e
implementación**

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

**Entrega y
soporte**

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. *Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación*

PROCESOS DE IT DE COBIT DEFINIDOS DENTRO DE LOS CUATRO DOMINOS



Debe tomarse en cuenta que estos procesos pueden ser aplicados a diferentes niveles dentro de una organización. Por ejemplo, algunos de estos procesos serán aplicados al nivel corporativo, otros al nivel de la función de servicios de información, otros al nivel del propietario de los procesos de negocio.

También debe ser tomado en cuenta que el criterio de efectividad de los procesos que planean o entregan soluciones a los requerimientos de negocio, cubrirán algunas veces los criterios de disponibilidad, integridad y confidencialidad. – en la práctica, se han convertido en requerimientos del negocio. Por ejemplo, el proceso de “identificar soluciones automatizadas” deberá ser efectivo en el cumplimiento de requerimientos de disponibilidad, integridad y confidencialidad.

Resulta claro que las medidas de control no satisfarán necesariamente los diferentes requerimientos de información del negocio en la misma medida. Se lleva a cabo una clasificación dentro del marco referencial *COBIT* basada en rigurosos informes y observaciones de procesos por parte de investigadores, expertos y revisores con las estrictas definiciones determinadas previamente.

Primario	es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.
Secundario	es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.
Blanco (vacío)	podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

Similarmente, todos las medidas de control no necesariamente tendrán impacto en los diferentes recursos de TI a un mismo nivel. Por lo tanto, el Marco Referencial de *COBIT* indica específicamente la aplicabilidad de los recursos de TI que son administrados en forma específica por el proceso bajo consideración (no por aquellos que simplemente toman parte en el proceso). Esta clasificación es hecha dentro el Marco Referencial de *COBIT* basado en el mismo proceso riguroso de información proporcionada por los investigadores, expertos y revisores, utilizando las definiciones estrictas indicadas previamente.

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

TABLA RESUMEN

La siguiente tabla proporciona una indicación, por proceso y dominio de TI, de cuáles criterios de información tiene impacto de los objetivos de alto nivel, así

como una indicación de cuáles recursos de TI son aplicables.

DOMINIO	PROCESO	Criterios de Información							Recursos de TI					
		efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad	recursos	sistemas de aplicación	tecnología	instalaciones	datos	
Planeación y Organización	PO1	Definir un plan estratégico de sistemas	P	S						<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	PO2	Definir la arquitectura de información	P	S	S	S					<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
	PO3	Determinar la dirección tecnológica	P	S								<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	PO4	Definir la organización y sus relaciones	P	S						<input checked="" type="checkbox"/>				
	PO5	Administrar las inversiones (en TI)	P	P					S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	PO6	Comunicar la dirección y objetivos de la gerencia	P					S		<input checked="" type="checkbox"/>				
	PO7	Administrar los recursos humanos	P	P						<input checked="" type="checkbox"/>				
	PO8	Asegurar el apego a disposiciones externas	P					P	S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
	PO9	Evaluar riesgos	S	S	P	P	P	S	S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	PO10	Administrar proyectos	P	P						<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	PO11	Administrar calidad	P	P		P			S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Adquisición e Implementación	AI1	Identificar soluciones de automatización	P	S							<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	AI2	Adquirir y mantener software de aplicación	P	P		S		S	S		<input checked="" type="checkbox"/>			
	AI3	Adquirir y mantener la arquitectura tecnológica	P	P		S						<input checked="" type="checkbox"/>		
	AI4	Desarrollar y mantener procedimientos	P	P		S		S	S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	AI5	Instalar y acreditar sistemas de información	P			S	S			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	AI6	Administrar cambios	P	P		P	P		S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Entrega de servicios y Soporte	DS1	Definir niveles de servicio	P	P	S	S	S	S	S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	DS2	Administrar servicios de terceros	P	P	S	S	S	S	S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	DS3	Administrar desempeño y capacidad	P	P			S			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	DS4	Asegurar continuidad de servicio	P	S				P		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	DS5	Garantizar la seguridad de sistemas			P	P	S	S	S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	DS6	Identificar y asignar costos		P					P	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	DS7	Educar y capacitar a usuarios	P	S						<input checked="" type="checkbox"/>				
	DS8	Apoyar y orientar a clientes	P							<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
	DS9	Administrar la configuración	P				S		S		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	DS10	Administrar problemas e incidentes	P	P			S			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	DS11	Administrar la información				P			P					<input checked="" type="checkbox"/>
	DS12	Administrar las instalaciones					P	P					<input checked="" type="checkbox"/>	
	DS13	Administrar la operación	P	P		S	S			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Monitoreo	M1	Monitorear el proceso	P	S	S	S	S	S	S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	M2	Evaluar lo adecuado del control interno	P	P	S	S	S	S	S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	M3	Obtener aseguramiento independiente	P	P	S	S	S	S	S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	M4	Proporcionar auditoría independiente	P	P	S	S	S	S	S	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>