Unidad 1: Introducción y Definiciones

La primera norma internacional que trata sobre el concepto de Gobierno TI es ISO/IEC-38500 (http://www.iso.org/iso/catalogue_detail?csnumber=51639). La norma busca asesorar a quienes tienen responsabilidades sobre el correcto funcionamiento de las organizaciones, en relación al papel que les toca jugar respecto de las TI , definiendo y detallando unos principios generales para el buen Gobierno Corporativo de las TI: responsabilidad, estrategia, inversión, conformidad, rendimiento y comportamiento.

Respecto a las metodologías, no existe una metodología unificada para la Gobernanza de TI. Existen metodologías que ayudan y facilitan un buen Gobierno de TI, destacando principalmente ITIL y COBIT por los años que llevan incorporando las mejores prácticas en Gestión y Gobierno de TI.

- ITIL es un marco de trabajo basado en mejores prácticas. En su nueva Versión 3 se centra en integrar las TI con el negocio, incorporando mejores prácticas para el Gobierno TI y adoptando un punto de vista más estratégico, reforzándolo con la ampliación de los procesos de Estrategia de Servicio. Se ha convertido en un estándar de facto. http://www.itil-officialsite.com/
- CoBIT en su versión 4.1 es un marco de trabajo aceptado internacionalmente como una buena práctica para el control de la información TI y los riesgos que conllevan. Permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio. Realza la importancia en cuanto a regulaciones, estando implantado en grandes empresas que cotizan en bolsa y prácticamente imprescindible para las que cotizan en Wall Street.

También hay marcos de trabajo que tratan más específicamente algunos aspectos relativos al Gobierno de las TI. Entre ellos cabe destacar:

- Val IT que se concentra en la gestión del portafolio de iniciativas de TI para generar valor a la organización y proveer un marco de trabajo para el gobierno de las inversiones en TI.
- RISK IT establece un marco de trabajo para las organizaciones para identificar, gobernar y administrar los riesgos asociados a las iniciativas en TI.

Cobit 5 intenta integrar o relacionar todos los marcos e iniciativas de ISACA (Val IT, Risk IT, BMIS, ITAF y Board Briefing) así como conectar con el resto de iniciativas y estándares en la comunidad TI (ITIL, ISO, etc.)

En este curso nos centraremos en COBIT 4.1.

ANTECEDENTES HISTORICOS

Para poder entender mejor cual es el origen de COBIT es necesario revisar los antecedentes históricos que le dieron origen. A continuación del libro Sistemas de Control Interno para Organizaciones de Oswaldo Fonseca Luna, primera edición, Lima 2011, en el cual relata como fue que se dio inicio al tema de las normas de control interno.

LEY SARBANES-OXLEY Y EL CONTROL INTERNO

La Gran Depresión se inicio en 1929 y duró casi una década, siendo una de las recesiones económicas mas profundas que afectó a los Estados Unidos y a otros países industrializados. Aunque sus posibles causas todavía son un tema de intenso debate, algunos expertos sostienen que uno de los factores que contribuyeron a su aparición fue la especulación bursátil ocurrida en los Años 30, caracterizada por el gran desequilibrio en el poder adquisitivo de la gente, sobre todo, el día de la caída dramática del precio de las acciones en la Bolsa de Valores de Nueva York (29/10/1929).

Dos piezas importantes de la legislación fueron promulgadas en aquella época por el Presidente Franklin D. Roosevelt, para regular el mercado de valores e imponer controles sobre las compañías: Securities Act de 1933, y la Securities Exchange Act de 1934 que creó la Securities And Exchanges Commission (SEC). En adelante, la SEC inicio su tarea de proteger a los inversionistas, estableciendo controles adicionales, especialmente, con posterioridad a 1987 en que se produjo otra crisis en el mercado de valores.

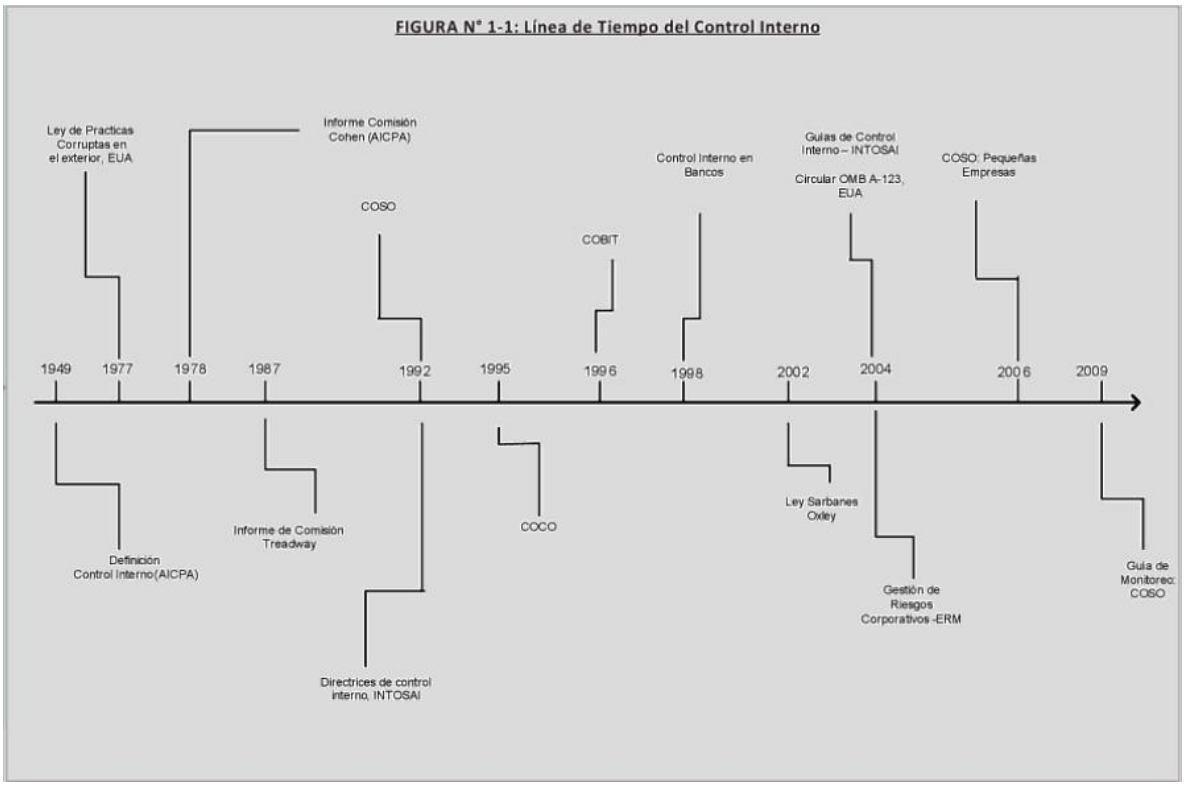
Mientras los escándalos financieros envolvían en Europa a PARMALAT en Italia y AHOLD en los países bajos, en los primeros años del siglo XXI, el Washington Post, el New York Times y el Wall Street Journal exponían ante la opinión pública los entretelones del fraude corporativo a gran escala perpetrado por grandes conglomerados ubicados en el ranking de Fortune 100, como por ejemplo: ENRON y WORLDCOM. Ambos acontecimientos pusieron en evidencia la perdida de confianza de los inversionistas y del público en general en los organismos reguladores y en las compañías que listan acciones en Bolsa y, por cierto, en los estados financieros de emisores, dictaminados por auditores independientes. Con mucha razón algunos

analistas financieros al evaluar los acontecimientos comenzaron a preguntarse ¿Dónde estaban los Auditores?

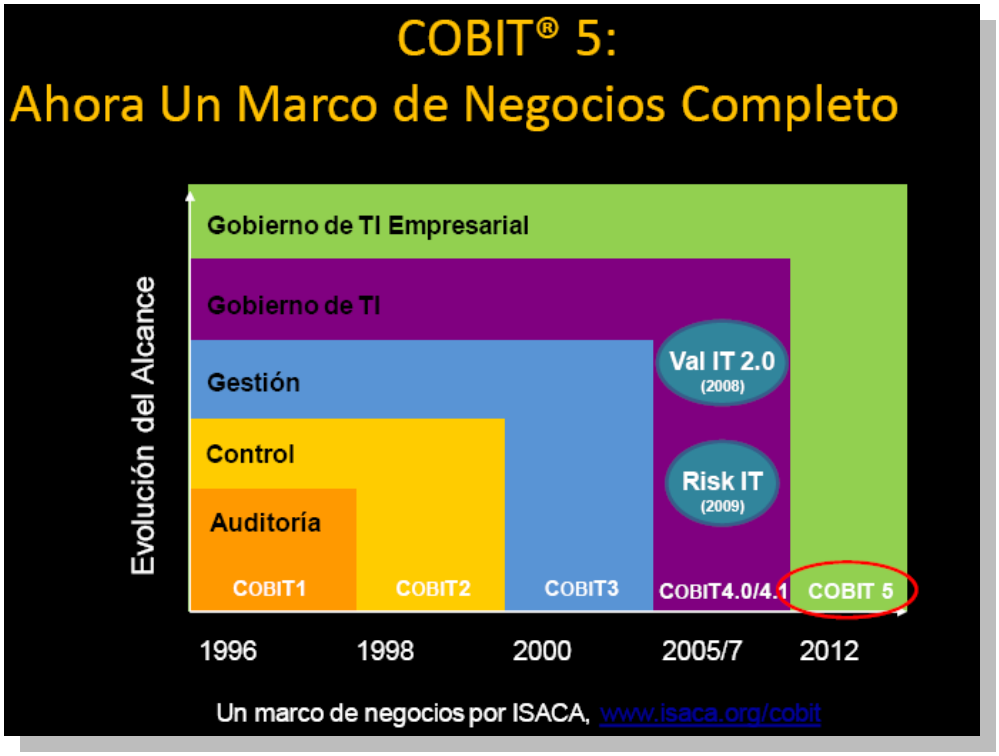
Estos escándalos financieros sacaron a la luz las prácticas usadas por grandes corporaciones para maquillar sus estados financieros, una de las cuales arrastro en su caída a su auditor externo – Arthur Anderson– quién por el caso ENRON fue exilado del mundo de los negocios. Estas malas prácticas podrían resumirse en:

- Fallas en la conducción corporativa en grandes compañías y en las retribuciones a directores y funcionarios por rentabilidad en su desempeño.
- No inclusión en los estados financieros consolidados de las operaciones con partes relacionadas.
- Liberalidad extrema y cuestionable en la aplicación de los principios contables requeridos para la preparación de estados financieros, y para la declaración de las utilidades.
- Reconocimiento de ingresos ficticios en los estados financieros.
- Destrucción y manipulación y alteración de documentación contable.
- No revelación en los dictámenes de los auditores independientes de hechos sobre la marcha del negocio examinado.

En respuesta a la quiebra de las grandes corporaciones, el Congreso americano sanciono la ley promovida por el Senador Paul Sarbanes y el Representante Michael Oxley, cuya iniciativa estuvo dirigida a todas las compañías públicas y, por cierto a todos los despachos de contabilidad que auditaban emisores públicos. La Ley Sarbanes – Oxley (o ley SOx), fue promulgada por el Presidente Bush en Julio del 2002.



Tomado de Sistemas de Control Interno para Organizaciones de Oswaldo Fonseca Luna
HISTORIA DE COBIT



Como pudimos ver anteriormente la importancia de un entorno controlado, en nuestro caso para este curso nos interesa el tema de control en la gestión de TI.

Alineación con los Objetivos de Negocio

Las empresas actualmente hacen grandes inversiones en recursos de tecnología de información para apoyar los procesos de negocio. El valor significativo y relevante que el uso de la información tiene para las organizaciones, determina que todos los procesos relativos a la producción, administración y uso de servicios de Tecnologías de Información (TI) deben ser óptimamente gestionados y controlados para asegurar la calidad de la información como soporte de los objetivos de negocio.

Los procesos de datos e información producto de las operaciones y procesos de negocio, requieren la aplicación de técnicas y medidas de control en el marco de un sistema de gestión que garantice la prestación de los servicios y la reducción de vulnerabilidad a amenazas generadoras de riesgo que pongan en peligro la estabilidad del sistema operacional, organizacional y del sistema macro del negocio. Hasta hace unos años el objetivo principal de una empresa era la rentabilidad, pero las lecciones aprendidas con los escándalos financieros de grandes compañías como Enron llevaron a la reflexión que para poder generar rentabilidad es sumamente importante asegurar la permanencia de la empresa. Esto ha llevado a una creciente preocupación hoy en

día en la alta dirección de todas las organizaciones, públicas o privadas, acerca de las actividades de la función de TI. Así mismo, la dirección se ve en la necesidad de justificar el valor de las importantes inversiones en las TICs, asegurar el cumplimiento normativo, a la vez que minimizar los riesgos.

Todos estos factores han propiciado la aparición de modelos, metodologías y prácticas dirigidas a garantizar un mejor gobierno o un rendimiento óptimo de las TIC en las organizaciones. Algunas de estas prácticas han sido desarrolladas por la propia dirección de las áreas de TI mientras que otras externas tienen como propósito el control externo de las propias unidades TIC. Entre las prácticas más aceptadas podemos situar a COBIT.

Los objetivos de Control para la Información y la Tecnología relacionada (conocidos generalmente por su acrónimo COBIT®) brindan un conjunto de buenas prácticas a través de un marco de trabajo basado en procesos, y presenta las actividades de una estructura manejable y lógica. Las buenas prácticas de COBIT están enfocadas fuertemente en el control y menos en la ejecución, es decir, indican más qué se debe conseguir sin focalizarse en el cómo.

Una de las características de COBIT es que esta orientado al negocio, vinculando las metas de negocio con las metas de TI, proporcionando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los propietarios de los procesos de negocio y de TI.

Otra característica es su enfoque hacia los procesos, mediante un modelo que subdivide TI en 34 procesos de acuerdo a cuatro áreas de responsabilidad (Planear, Construir, Ejecutar y Monitoreo) que básicamente coinciden con el conocido ciclo de Deming (Plan-do-check-Act).

De manera más general, el empleo de un marco como COBIT satisface las necesidades de la Dirección y aporta una serie de beneficios que facilitan que se logren tanto los objetivos de la TI como los del negocio. Esto lo logra:

- Asegurando una mejor alineación, basándose en su enfoque en el negocio.
- Facilitando la implantación de políticas, procedimientos, prácticas y estructuras organizativas, para garantizar los objetivos perseguidos y prevenir eventos no deseados.
- Facilitando una medición objetiva sobre el estado actual de las TIC en una organización y facilitando el asesoramiento para determinar dónde se requieren mejoras. Así la dirección posee información que le permitirá tomar decisiones frente a riesgos, de forma rápida y asegurando el éxito.

- Proporcionando a la Dirección una visión más clara sobre lo que hace la unidad de TI.
- Definiendo la propiedad y la responsabilidad de los diferentes procesos TI de la organización.
- Facilitando una evaluación de la capacidad de dichos procesos, basada en sus modelos de madurez.
- Optimizando las inversiones realizadas en las TI.
- Facilitando el entendimiento de todos los participantes, al basarse en un lenguaje común.

Los objetivos de una buena gestión de TI son:

- Proporcionar una adecuada gestión de calidad
- Aumentar la eficiencia
- Alinear los procesos de negocio y la infraestructura de TI.
- Reducir los riesgos asociados a los Servicios de TI.
- Generar negocios.

Las áreas de enfoque de gobierno de TI describen los tópicos en los que la dirección ejecutiva requiere poner atención.

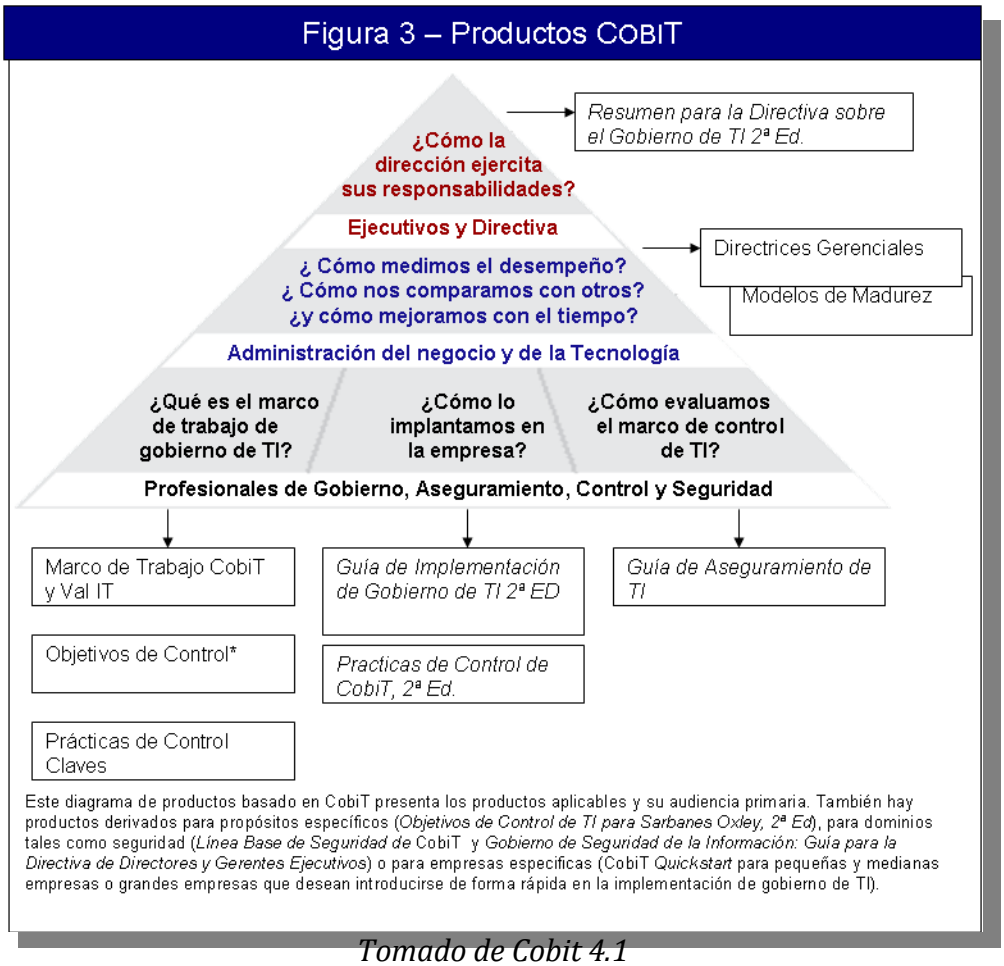
Figura 2 – Áreas de Enfoque del Gobierno de TI

•**Alineación Estratégica** se enfoca en garantizar la alineación entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.
•**Entrega de Valor** se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.
•**Administración de Recursos** se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI: , aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.
•**Administración de Riesgos** requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del apetito de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.
•**Medición del Desempeño** rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas medibles más allá del registro convencional.

Tomado de Cobit 4.1

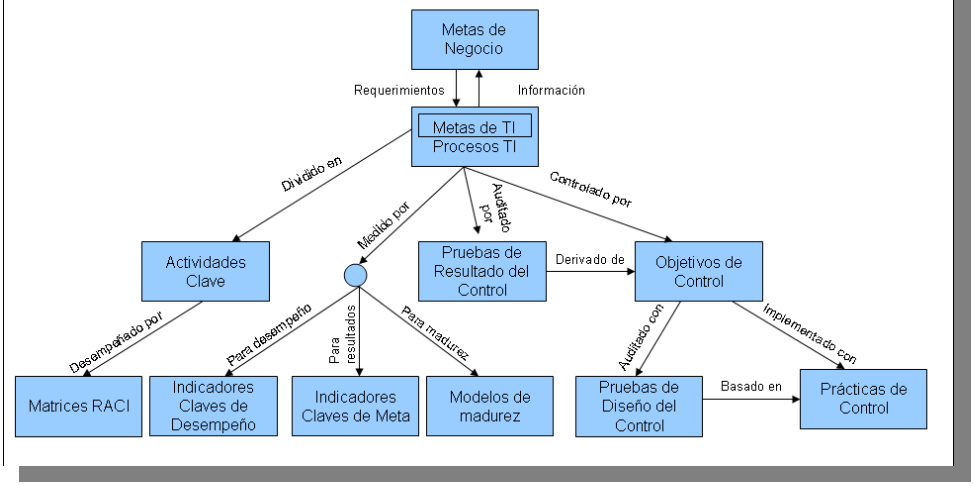
COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas

técnicos y riesgos del negocio, y comunicar ese nivel de control a los Interesados (Stakeholders).



Tomado de Cobit 4.1

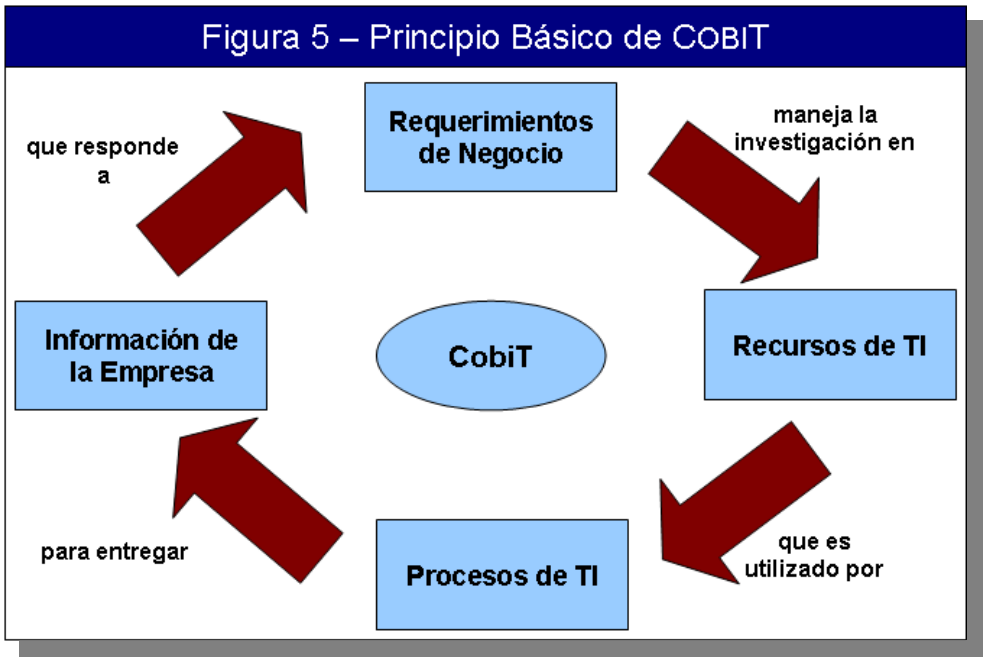
Figura 4 – Interrelaciones de los componentes de COBIT



En el capítulo Marco de trabajo vamos ver como este proporciona a la alta gerencia un entendimiento más detallado de los conceptos clave y principios de COBIT e identifica los cuatro dominios de COBIT y los correspondientes 34 procesos de TI. Se explica él porque necesitamos de un marco de trabajo. Nos permite identificar para quienes, con todo el tema de manejo de involucrados. Y por último el Que.

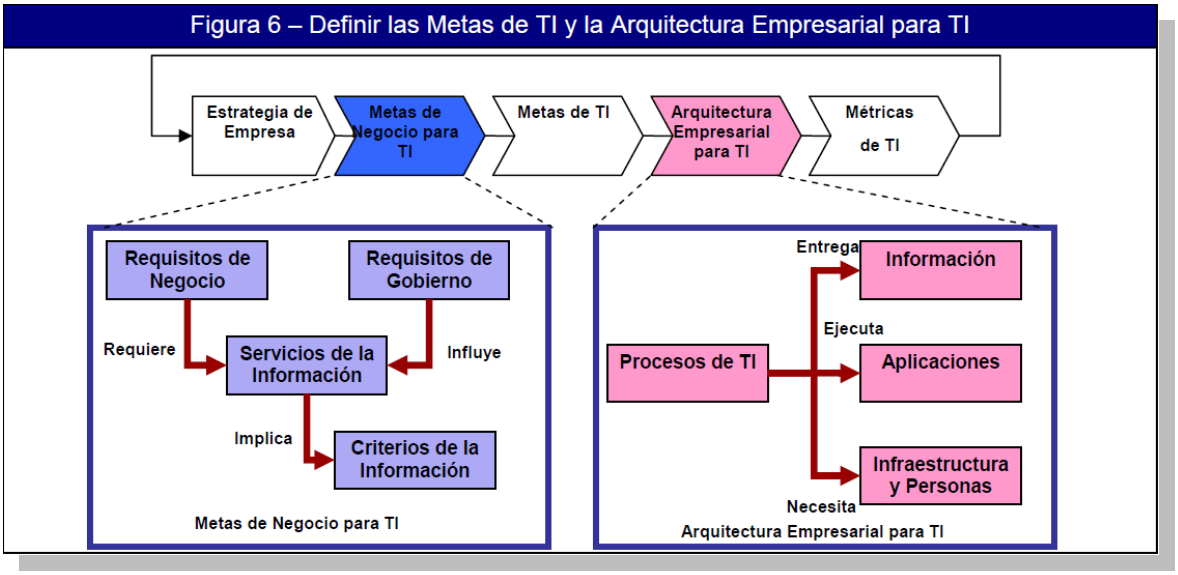
COBIT es orientado al Negocio.

Figura 5 – Principio Básico de COBIT

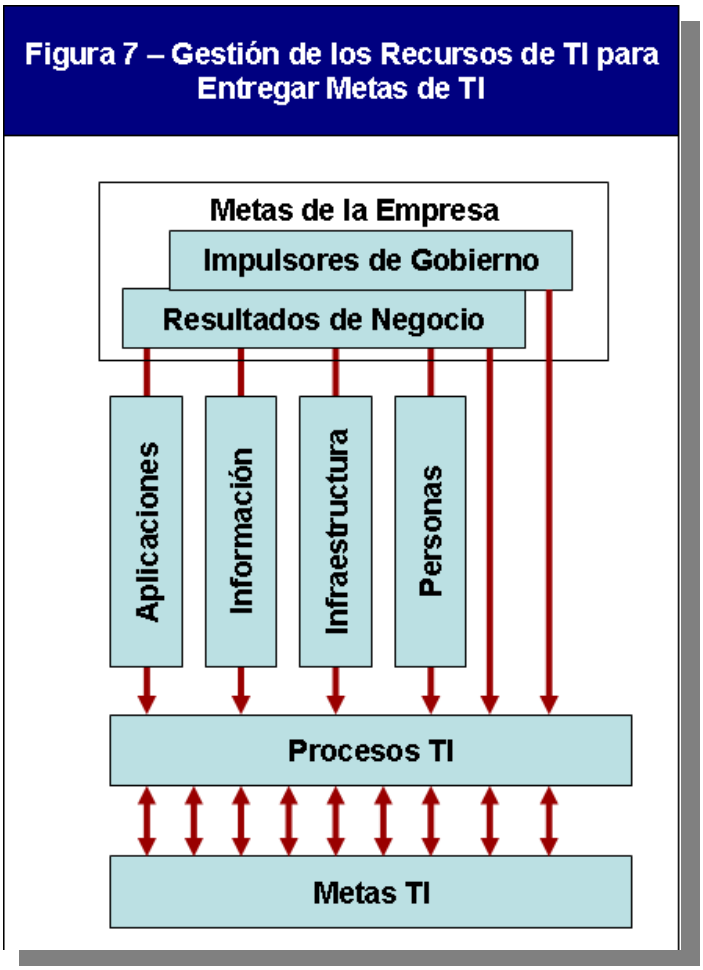


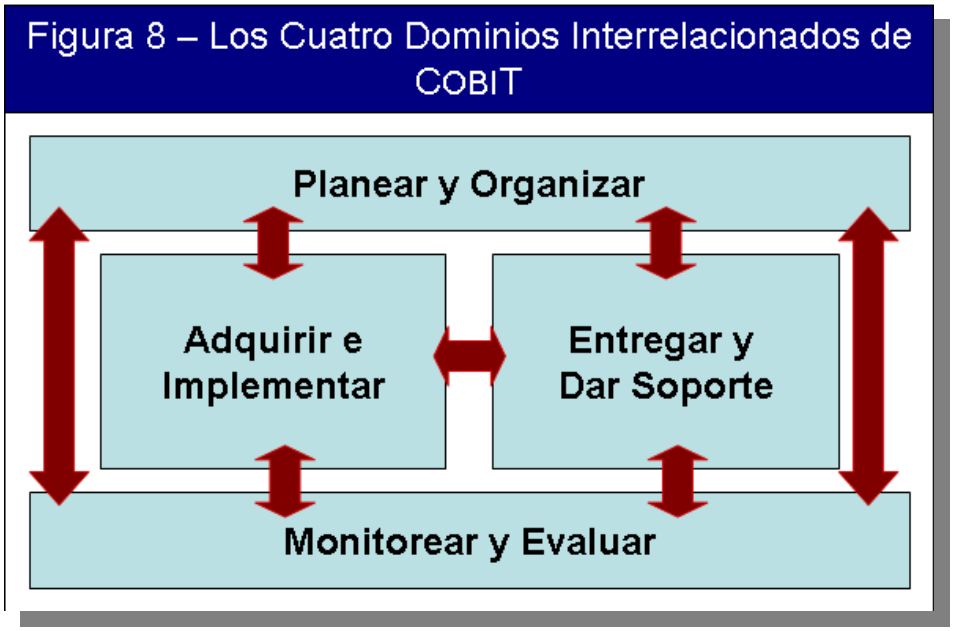
Definir metas

Figura 6 – Definir las Metas de TI y la Arquitectura Empresarial para TI

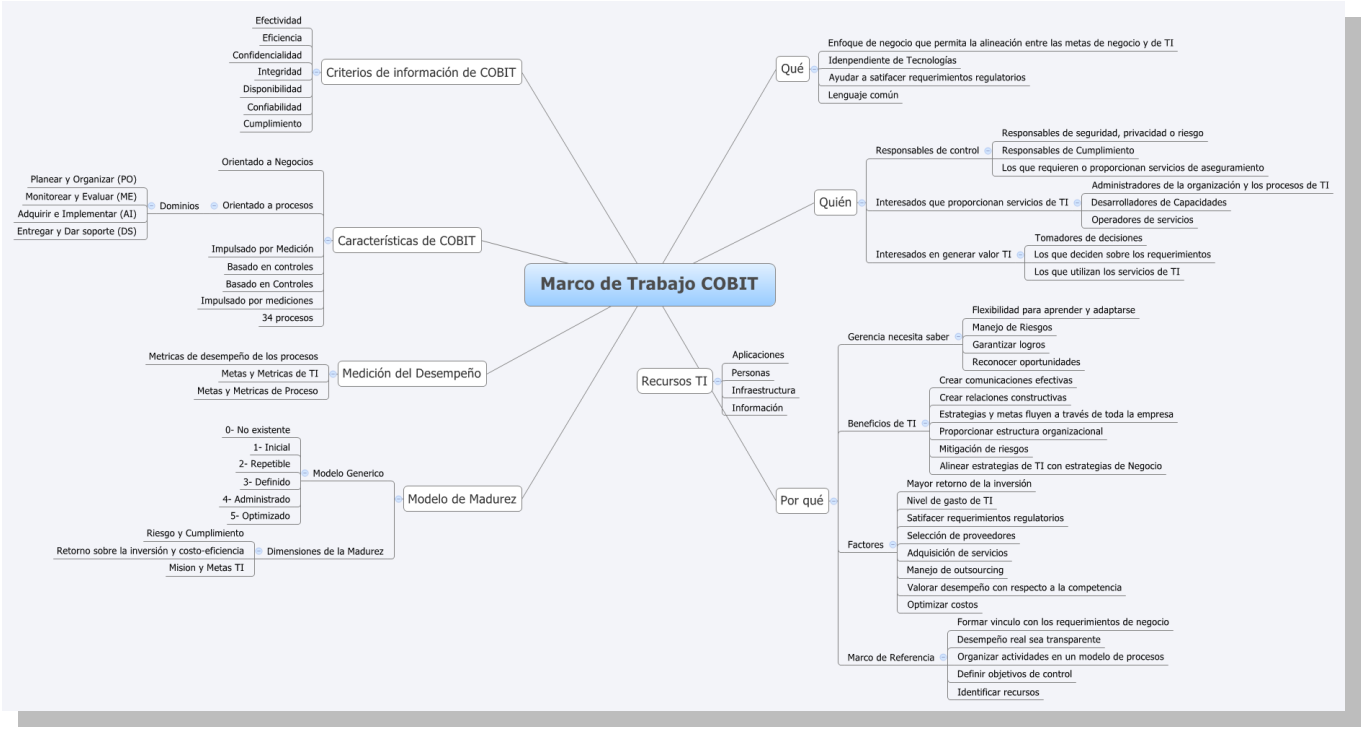


Orientado a procesos:





El siguiente diagrama resume el Marco de Trabajo de COBIT:



Dentro de la provisión de información, las Tecnologías de Información requieren de recursos para poder implementar, brindar, monitorear y asegurar la provisión de la información de la información. El Marco referencial de COBIT distingue los siguiente Recursos:

- Datos: Que son los contenedores de información almacenados en su estructura de información.
- Aplicaciones: Sistemas de Información que permiten ingresar y presentar los datos al negocio en base a los requerimientos del mismo; pero de forma automatizada.
- Tecnología: Que cubre todos los componentes de hardware, software, sistemas base, sistemas de almacenamiento de información. También incluyen la infraestructura de comunicaciones, como redes, enlaces, etc.
- Instalaciones: Son las facilidades físicas, para alojar a los datos, aplicaciones, tecnologías, aptitudes para administrar, gestionar y proveer los servicios de tecnologías de información.
- Personal: Son todos los integrantes de TI, con su conocimiento, experiencias, aptitudes para administrar, gestionar y proveer los servicios de tecnologías de información.

Los Procesos de TI

Los procesos de TI, son todo el conjunto de actividades que involucra el manejo y gestión de las tecnologías de la información, para lograr la provisión de los servicios de información.

COBIT propone alinear los procesos en base a un control de los mismos a través de la creación de Objetivos de Control que permitan administrar y entender el riesgo de los procesos y los recursos que se requieren para el manejo exitoso de los mismos.

Un punto muy importante es el modelo de Madurez de COBIT, en cada uno de los procesos viene definido las pautas para evaluar el nivel de madurez en la organización.

Del PDF COBIT 4.1 leer el capítulo MARCO DE TRABAJO. Página 11 a la Página 28

2: Dominio "Planear y Organizar"

Vamos a estudiar el primer dominio que es Planear y Organizar. 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 de negocio. Este dominio cubre los siguientes cuestionamientos:

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las siguientes necesidades de negocio?

Objetivos:

1. Estudiar el primer dominio de COBIT "Planear y Organizar"
2. Analizar los 10 procesos asociados a este dominio.

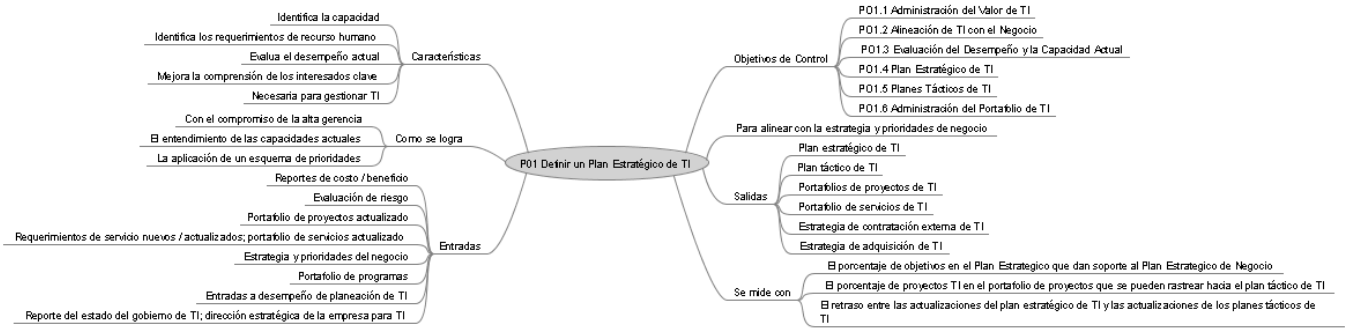
Cada proceso es estructurado de la siguiente forma:

- Definición
- Como se logra
- Entradas
- Salidas
- Objetivos de Control
- Como se mide

A continuación mapas conceptuales de cada proceso:

PO1 Definir un Plan Estratégico de TI

Sostener o extender los requerimientos de gobierno y de la estrategia del negocio, al mismo tiempo que se mantiene la transparencia sobre los beneficios, costos y riesgos enfocándose en la incorporación de TI y de la gerencia del negocio en la traducción de los requerimientos del negocio a ofertas de servicio, y el desarrollo de estrategias para otorgar estos servicios de una forma transparente y rentable.

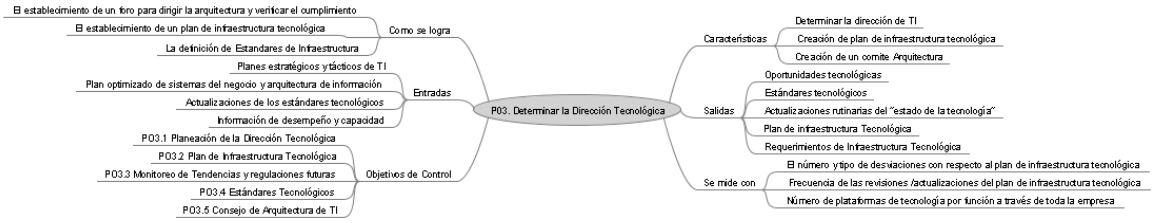


PO2 Definir la Arquitectura de la Información

Agilizar la respuesta a los requerimientos, proporcionar información confiable y consistente, para integrar de forma transparente las aplicaciones dentro de los procesos del negocio enfocándose en el establecimiento de un modelo de datos empresarial que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos

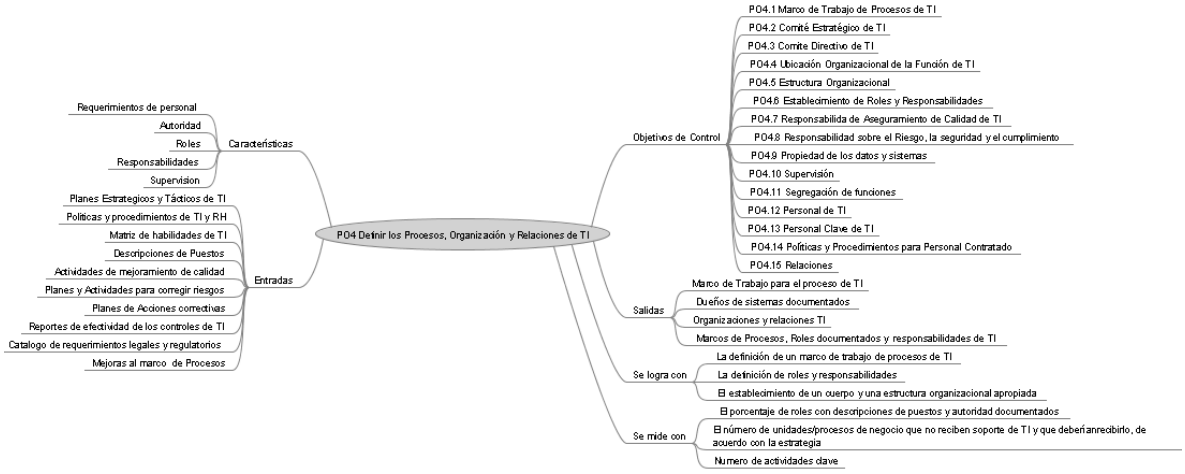
PO3 Determinar la Dirección Tecnológica

Contar con sistemas aplicativos estándar, bien integrados, rentables y estables, así como recursos y capacidades que satisfagan requerimientos de negocio actuales y futuros enfocándose en la definición e implantación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas.



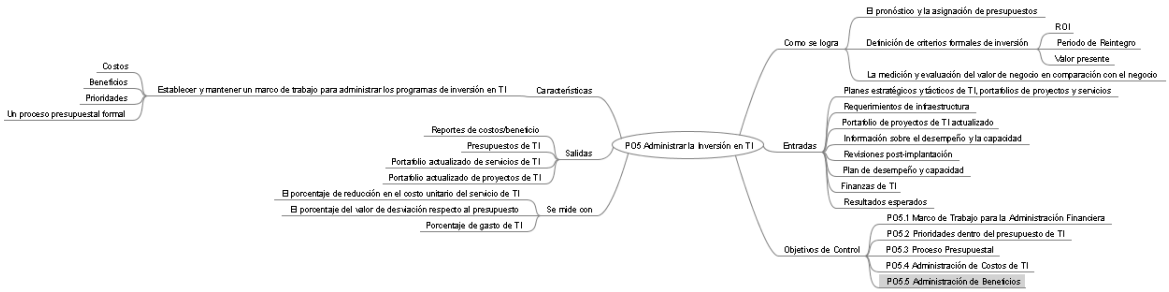
PO4 Definir los Procesos, Organización y Relaciones de TI

Agilizar la respuesta a las estrategias del negocio mientras al mismo tiempo cumple con los requerimientos de gobierno y se establecen puntos de contacto definidos y competentes enfocándose en el establecimiento de estructuras organizacionales de TI transparentes, flexibles y responsables, y en la definición e implantación de procesos de TI con los propietarios, y en la integración de roles y responsabilidades hacia los procesos de negocio y de decisión.



PO5 Administrar la Inversión de TI

Mejorar de forma continua y demostrable la rentabilidad de TI y su contribución a la rentabilidad del negocio con servicios integrados y estandarizados que satisfagan las expectativas del usuario enfocándose en decisiones de portafolio e inversión en TI efectivas y eficientes, y por medio del establecimiento y seguimiento del presupuestos de TI de acuerdo a la estrategia de TI y a las decisiones de inversión.

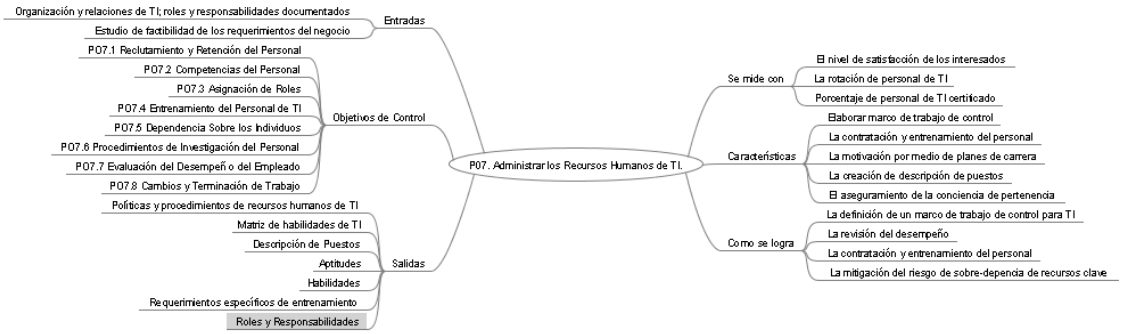


PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia

Comunicar de una manera precisa y oportuna, la información sobre los servicios de TI actuales y futuros, los riesgos asociados y las responsabilidades enfocándose en proporcionar políticas, procedimientos, directrices y otra documentación aprobada, de forma precisa y entendible y que se encuentre dentro del marco de trabajo de control de Ti a los interesados.

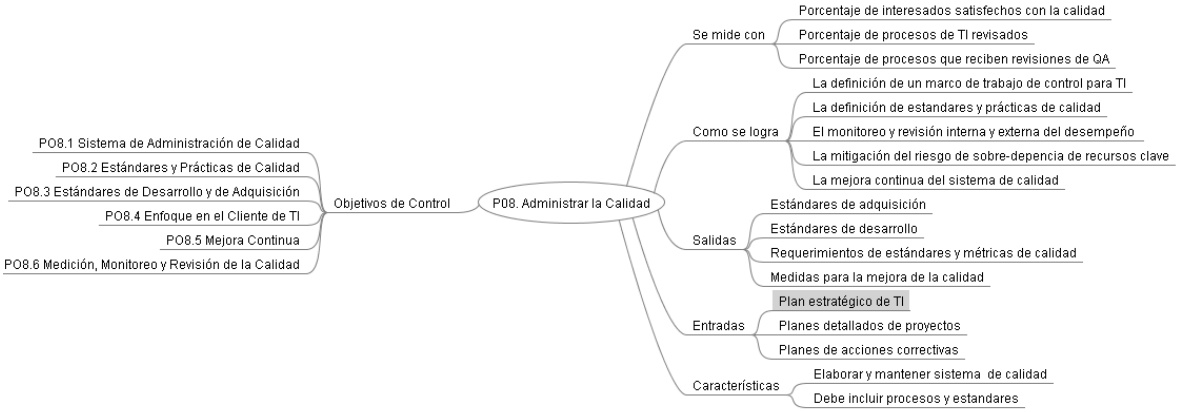
PO7 Administrar los Recursos Humanos de TI

Administrar los recursos humanos de TI para formar personas competentes y motivadas para crear y entregar servicios de TI enfocándose en la contratación y entrenamiento del personal, la motivación por medio de planes de carrera claros, la asignación de roles que correspondan a las habilidades, el establecimiento de procesos de revisión definidos, la creación de descripción de puestos y el aseguramiento de la conciencia de la dependencia sobre los individuos.



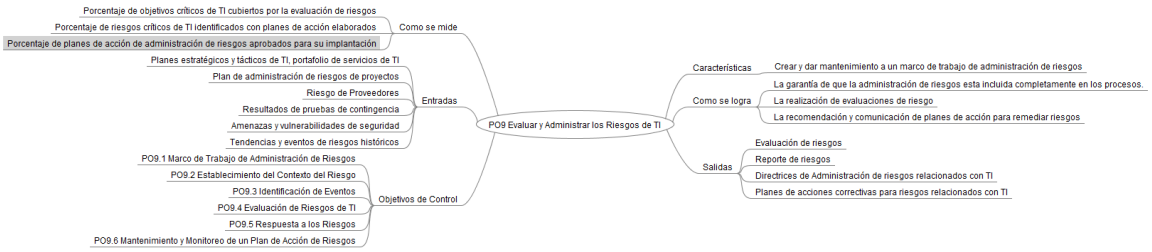
PO8 Administrar la Calidad

Administrar la calidad para la mejora continua y medible de la calidad de los servicios prestados por TI enfocándose en la definición de un sistema de administración de calidad (QMS, por sus siglas en inglés), el monitoreo continuo del desempeño contra los objetivos predefinidos, y la implantación de un programa de mejora continua de servicios de TI.



PO9 Evaluar y Administrar los Riesgos de TI

Analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de negocio enfocándose en la elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales.



PO10 Administrar Proyectos

Administrar proyectos para generar la entrega de resultados de proyectos dentro de marcos de tiempo, presupuesto y calidad acordados enfocándose en un programa y un enfoque de administración de proyectos definidos, el cual se aplica a todos los proyectos de TI, lo cual facilita la participación de los interesados y el monitoreo de los riesgos y los avances de los proyectos.