# Serie Artículos sobre Gestión de IT y Calidad

# "IT GOVERNANCE & ITIL"

Norberto Figuerola

# IT Governance e ITIL

**Autor: Dr. Norberto Figuerola (PMP)**
Contador Público y Licenciado en Administración (U.B.A.)
Master in Project Management (George Washington University)
ITIL Consultant e ISO 20000 Auditor

---

## IT GOVERNANCE

En el caótico mundo económico actual y las altas fluctuaciones del mercado resulta muy difícil saber que ocurrirá mañana. Las restricciones de acceso al crédito y la recesión han puesto a muchos proyectos de IT bajo presión. Si antes el parámetro de selección era cual es el ROI del proyecto, hoy las empresas se preguntan cuales son las implicaciones en el "cash-flow" o cual es la merma de capital necesario para el inicio del proyecto. Los CIOs son constantemente desafiados a probar el valor de negocio que aporta su organización de IT. Esto se vuelve mucho más exigente cuando las condiciones económicas son difíciles, cuando los presupuestos deben recortarse y los recursos disminuírse, por lo tanto la importancia radica en mostrar la ventaja competitiva de los proyectos de IT y mostrar cómo IT, como organización, esta siendo gobernada.

Después de un período de separación entre la gente de Finanzas y la gente de IT, se nota un trabajo más conjunto entre ambos, por cuanto IT posee una tremenda inversión en activos y es de una importancia estratégica para toda la corporación. Cuando se mide el total de la inversión no sólo se hace referencia al aspecto tecnológico, sino además en la gente y los procesos. En forma sabia ahora antes que pensar en reducir el presupuesto, se debería re-pensar en cambiar los procesos, y pensar de que manera la gente puede hacer sus tareas más eficiente y como innovar. Por eso existen muchas opciones para la explotación de IT para bajar costos, tales como el outsourcing, SaaS, Cloud computing, offshoring y rightsizing de recursos utilizando la estrategia de "demand (or production) resource driven" en donde el plantel es el adecuado para las exigencias del momento y ante cualquier crecimiento imprevisto se recurre a la contratación externa. De todas formas tomar este tipo de decisiones no es simple y requiere conocer muy bien el modelo de negocios y todas las implicaciones que representa hacer un switch a cualquiera de dichas alternativas.

Es muy importante para un Gerente de Proyecto conocer el significado cada vez más difundido del término IT Governance, generalmente junto a otros tales como Portfolio Management, IT Balanced Scorecard, Project Office, etc. Algunos organismos, como OGC, ITGI e ISACA han resaltado la importancia del valor agregado que representa hoy en día el alineamiento de IT a las prácticas y recomendaciones básicas del gobierno de IT. El gobierno adecuado de IT (IT Governance) se ha transformado en un aspecto crítico en toda organización, y aquellas que no lo practican encaran serios riesgos que las pueden colocar en peligro frente a las otras que practican un mejor control y medición. La alineación de la organización IT con la estrategia del negocio es imperativa y esencial. La vieja cultura del oscurantismo respecto de las actividades de IT ya fué reemplazada por una acción mucho más pro-activa y totalmente transparente respecto de su contribución al negocio.

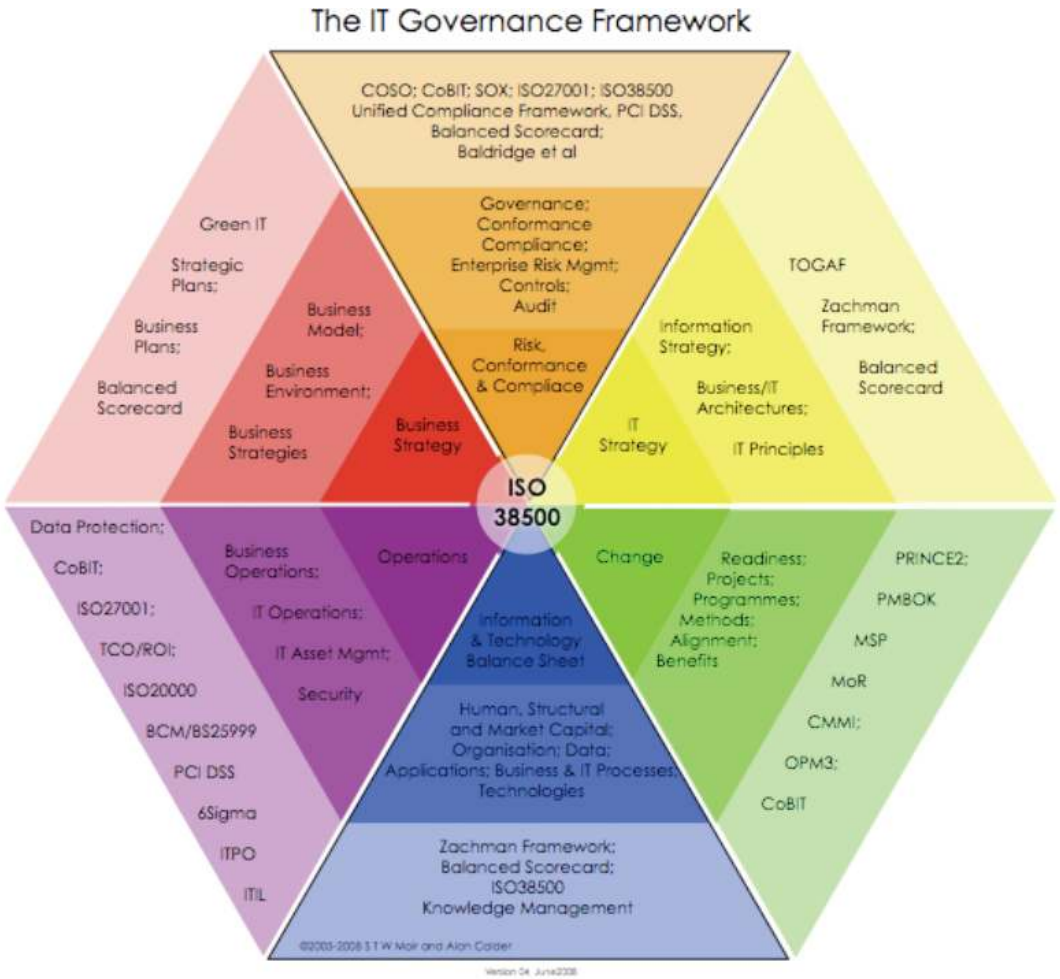
Ya sabemos que la tecnología de la información no es un elemento de apoyo, sino que se trata de un componente esencial para que las organizaciones puedan existir, por lo que la estrategia de IT debe ser parte fundamental de la estrategia del negocio. No se puede separar a una de la otra. En este contexto, ¿cómo hacemos para asegurarnos de hacer bien las cosas en el campo de sistemas? De la misma manera que el gobierno corporativo (Corporate Governance).

***Cómo puede ser definido el concepto de IT Governance ?:*** IT Governance es una metodología o un "framework" que tiene como propósito asegurar el apropiado manejo de los recursos y actividades de IT para asegurar que la organización de IT soporta y facilita el logro de las estrategias y objetivos del negocio. Se logra contestando las siguientes preguntas: La compañía está haciendo las cosas adecuadas? (proyectos de IT que agreguen valor estratégico/económico). Lo está haciendo de la manera adecuada? (enfoque, metodologías, técnicas, herramientas). Está usando eficientemente la tecnología de la información? Se están alcanzando los objetivos deseados?

Los sub-dominios que incluye actualmente una buena metodología de IT governance son:

- Business continuity y disaster recovery
- Cumplimiento de Regulaciones
- Information governance (métricas) y Information security (seguridad) que incluye Cobit e ISO 27000
- IT Service Management (incluye ITIL y Service Level Management)
- Knowledge Management
- Project governance
- Risk management

***Existe un modelo o marco de IT Governance ?*** : El estándar mundial más formal internacionalmente utilizado de Gobierno de IT es el **ISO/IEC 38500**, que se publicó en junio de 2008. Se basó en el trabajo realizado por el Instituto Australiano de Estándares que publicó en el 2005 la AZ 8015. La norma ISO/IEC 38500 establece un marco para el gobierno de IT y de las Telecomunicaciones. La norma es un recurso clave para los profesionales que deseen conocer sobre el tema de gobernabilidad en todo el mundo. Otro modelo bastante completo es el de Calder-Moir, que provee de un framework muy comprensivo de todo lo que integra un modelo de IT governance. Dicho modelo se basa y soporta la implementación de la ISO/IEC 38500, que en definitiva es el estándar internacional de las mejores prácticas para IT governance. La explicación de estos modelos escapa a los objetivos de este documento, sin embargo mucha de la información contenida en el mismo debe ser conocida por el lector.



***Cuáles son los principales aspectos que debe tener en cuenta toda política de IT Governance ?:*** Principalmente giran alrededor de:

1. El cumplimiento de los requerimientos y regulaciones gubernamentales o privadas a distintas industrias.
2. Entender el riesgo operacional que incluye políticas de risk management y de seguridad informática ante la proliferación de amenazas (internas y externas) a la información y datos de IT. ("Risk Governance")
3. La ventaja competitiva lograda por la información a través de IT. ("Data Governance")
4. La necesidad de alinear los proyectos tecnológicos con los objetivos estratégicos organizacionales, asegurando la entrega de lo planificado. ("Project Governance")

**1- Cumplimiento de Requerimientos y Regulaciones**

Mundialmente existen varias regulaciones que deben ser cumplidas y auditadas por IT, algunas con alcance a nivel país y otras que trascienden las fronteras. Varían de acuerdo a la industria pero algunas de ellas son:

El "Combined Code on Corporate Governance" que requiere a una serie de empresas que se encuentran registradas en UK una auditoria anual de todo el material bajo control, incluyendo finanzas, operación y cumplimiento de controles y manejo de riesgos. En el punto específico de riesgos existen muchos requerimientos y regulaciones, el que se combina con el CCCG es el Turnbull que identifica los activos bajo riesgo significativo, incluyendo la información y los procesos de comunicación.

"Sarbanes Oxley" ('SOX') que requiere a una serie de empresas que se encuentran registradas en US tener un sistema de control interno como el framework de COSO, exigiéndole anualmente a las compañías certificar este control interno. Tanto COSO como CoBIT pueden emplearse para asegurar el cumplimiento de dichos requerimientos. SOX no solo exige esto a las casas matrices sino además a cualquier representación fuera de US. Existen varias consultoras que se dedican a auditar el cumplimiento de SOX. Sin embargo no he visto con el mismo énfasis el estudio e implementación de COSO y CoBIT. COSO se focaliza en el control financiero de los procesos y es un framework disponible por el "American Institute of CPA", en cambio CoBIT es un estándar abierto publicado por el ITGI e ISACA cuyo foco es el control y auditoría de IT para el cumplimiento de requerimientos de control y regulatorios y el manejo efectivo de los riesgos.

Las auditorías y consultorías de IT pueden ser realizadas en forma interna, o por terceros. La recomendación es por supuesto un auditor o consultor independiente. ISACA es la organización dedicada a la capacitación de estas personas y la publicación de normas referentes a dicha disciplina. Las certificaciones CISA, CISM y CGEIT se obtienen a través de dicha organización que en la Argentina el capítulo se llama ADACSI. Si usted recibe la revista PM Network por ser miembro del PMI verá un anuncio relativo a dichas certificaciones.

Existen también regulaciones mandatorias para algunas industrias en particular como el caso de las normas de Basilea II para la industria financiera o HIPAA para las transacciones e información de pacientes, enfermos y obras sociales. La información en IT está creciendo a ritmo vertiginoso y mucha está sujeta a regulación. Tanto el gobierno como los clientes, proveedores y demás esperan que la organización sea proactiva y cumpla con dichos requerimientos. Para mencionar otros: la protección de datos personales (en nuestro país Ley 25.326), la firma digital (en nuestro país Ley 25.506), delito informático (en nuestro país aún sin reglamentar), leyes de copyright y legislación sobre transacciones electrónicas en Internet.

**2- Risk management y Seguridad Informática**

"Business continuity" y planificación para "Disaster recovery" son estrategias centrales en la política de risk management de IT. El cumplimiento de estándares para la Continuidad del Negocio tal como el BS25999 demuestran, de alguna forma, un intento genuino de supervivencia ante un inesperado desastre en el negocio.

La proliferación de amenazas sobre la información de IT no son de menor importancia. Son muy amplias y complejas, sin embargo hay que tener en cuenta que los mayores incidentes de seguridad de información son internos y no externos. Los costos indirectos de estos incidentes son superiores a los costos directos reales puesto que el impacto en la reputación de la organización es tremendo.

El desafío para los gerentes de cualquier organización es asegurar que las soluciones para resguardar la seguridad de la información estén disponibles y estén en línea con los objetivos estratégicos y operacionales. El riesgo de la información debe ser controlado dentro del Framework del riesgo empresarial ERM (enterprise risk management). Las decisiones de riesgo afectan a la organización en su conjunto y por lo tanto son decisiones que se toman a nivel top Management y no el departamento de IT solamente.

Referentes típicos de normas relativas a este rubro son las nuevas normas de *PCI Data Security Standard* desarrollado en conjunto por la agrupación de las compañías de tarjetas de crédito más importantes, como una guía que ayude a las organizaciones que procesan o manejan tarjetas de crédito con el fin de prevenir los fraudes de tarjetas de crédito relacionados a los sistemas informáticos y sus riesgos. Las compañías que procesan, guardan o trasmiten datos de transacciones de tarjetas de crédito deben cumplir con el estándar o arriesgan la perdida de sus permisos para procesar las tarjetas de crédito (perdida de franquicias), enfrentar auditorias rigurosas o pagos de multas. Los Comerciantes y proveedores de servicios de tarjetas de crédito, deben validar su cumplimiento al estándar en forma periódica.

El estándar más importante mundialmente referido a seguridad de información sigue siendo la norma ISO/IEC27001. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA. Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution - BSI. La certificación de un SGSI es un proceso mediante el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado.

**3- Ventaja Competitiva**

IT no es una tecnología de bajo costo y bajo impacto sino todo lo contrario, es altamente impactante y requiere fuertes inversiones. La innovación es la regla general, la velocidad de los cambios informáticos y su implementación pueden llegar a resultar críticos para mantener y desarrollar la ventaja competitiva de una empresa. Por lo tanto dentro de las estrategias de IT Governance figuran también las actividades pro-activas hacia los cambios y adaptaciones al mercado para no perder la posición competitiva.

Se menciona fuertemente y con razón que el único propósito de IT es servir al negocio. El alineamiento de IT con los objetivos estratégicos de la compañía y la entrega de servicios y soporte de IT al negocio para alcanzar el éxito competitivo requiere también de un claro liderazgo y políticas de gobierno. Las mejores prácticas de "*IT Service Management"* tal como ITIL juegan un rol altamente significativo en ayudar a las organizaciones para aumentar la efectividad de dichos servicios y soporte de IT.

La valuación de una organización tiene ahora un fuerte componente intangible (muchas veces los intangibles son más valiosos que todos los activos tangibles). Las compañías más exitosas se caracterizan por su habilidad de incrementar sus activos intangibles, inversiones en IT y R&D. La disciplina de "*Knowledge Management"* es un "pibot" fundamental para el éxito hoy en día. La dirección no sólo debe asegurarse que los sistemas e infraestructura de IT son los adecuados para el modelo estratégico de la compañía, sino además garantizar que existan y se actualicen los recursos y el valor agregado de la experiencia y conocimiento adquirido (lesson learned).

**4- Project Governance**

Los Shareholders ya no aceptan más que los proyectos de IT no entreguen lo prometido o terminen fuera de tiempo o presupuesto. Los proyectos de IT exponen a la organización a riesgos significativos tanto financieros como operacionales y competitivos.

Los proyectos de IT solo deberían existir como proyectos de Negocios. La justificación y selección de proyectos es esencial, y debe practicarse junto con una adecuada gestión de los riesgos para tomar las mejores decisiones en términos de ventaja competitiva y entrega de valor agregado.

Un efectivo IT project governance requiere de un feedback continuo al directorio sobre su funcionamiento e implementación. Se deben utilizar Project Managers Profesionales que trabajen con una apropiada metodología y disciplina (tal como PMBOK o Prince2).

***Cómo debe aplicarse IT Governance ?:*** La implementación de un framework adecuado de IT Governance la debe tomar el top management de la organización. La estrategia a seguir debería ser:

1. Designar a un miembro del management responsable de las políticas de IT governance y adoptar un modelo apropiado para la organización y desarrollar la estrategia apropiada tanto al modelo como al negocio.
2. Crear un Comité que tenga participación en todas las actividades de IT, responsable de aprobar y revisar toda la información relacionada con los proyectos, protección de activos y asegurar que el top management reciba regularmente los reportes de rendimiento.
3. Asegurar que el plan corporativo de manejo de riesgos incluya también IT (lo que podría implicar la adopción de ISO27001 information security management system)
4. Trabajar con un Framework que permita auditar y controlar las buenas prácticas en IT (tal como CoBIT)
4. Adoptar un método efectivo (tal como el IT balanced scorecard) para medir el rendimiento de IT.
5. Focalizarse en la entrega de servicios IT alineados con la estrategia del negocio (ITIL)

## INTRODUCCION ITIL

**Cómo se originó ?**

Desarrollada a finales de 1980, la Biblioteca de Infraestructura de Tecnologías de la Información (**ITIL**) se ha convertido en el estándar mundial de facto en la Gestión de Servicios Informáticos. Iniciado como una guía para el gobierno de UK, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software. Hoy, **ITIL** es conocido y utilizado mundialmente. Pertenece a la **OGC**, pero es de libre utilización.

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI.

**Cual es el propósito ?**

Los proveedores de IT ya no pueden permitirse el lujo de centrarse en la tecnología exclusivamente sino que ahora deben considerar la calidad de sus servicios en relación con sus clientes. Se llama "cliente" a cualquier departamento o responsable de la organización a la cual IT le suministra el servicio y el autorizado para dar por finalizado el mismo y, de corresponder, pagarlo. El "usuario" es un nivel menor que cliente y se refiere al empleado que utiliza los servicios de IT para sus actividades diarias. La percepción del cliente es esencial para la provisión de los servicios. Si el servicio cumple o no con las expectativas depende ante todo de cuan eficazmente se acordaron los entregables. Un diálogo continuo con el cliente es esencial para refinar los servicios a prestar y asegurarse que tanto el proveedor como el cliente sepan lo que se espera del servicio. La calidad de un servicio es la capacidad que tiene éste para satisfacer las necesidades y expectativa del cliente, proporcionar una calidad continua es uno de los aspectos más importantes de la industria de los servicios.

Cada vez son más los directivos de las organizaciones que están exigiendo a los CIOs que tengan un Modelo de Gobernabilidad de TI con el objetivo de tener información a través de controles y estructuras que les aseguren que el área TI está actuando como soporte de las estrategias del negocio. Sin una Mejor Práctica como la Gestión de Servicios de TI, estos modelos no pueden funcionar de una manera eficiente. Por un lado, la Gestión de Servicios es clave para la Gobernabilidad de TI, porque se integra a los objetivos del negocio y por otro lado, sin los procesos de ITIL, los indicadores y controles no serían confiables.

Una implementación exitosa de Mejores Prácticas de ITIL define un modelo de procesos sustentado por roles y responsabilidades, entre otros elementos, los cuales al ser implementados a lo largo de toda la organización, generan una nueva forma de trabajo basada en responsabilidades puntuales; de esta manera contribuyen a eliminar los silos en las organizaciones. Por otro lado los procesos de TI con mayor madurez, generan mayor productividad *(menos errores)* y más calidad *(hacer las actividades siempre igual)*, lo cual automáticamente reduce los costos. Se reconoce asi que los servicios que provee el departamento de IT al negocio son clave, estratégicos y un activo organizacional que debe ser eficientemente manejado. Se deben invertir apropiados niveles de recursos para su gestión y para que la entrega, el soporte y el manejo de los servicios que IT presta a la organización sean efectivos

**Como se define ITIL ?**

**ITIL** es un marco público que describe las "***Mejores Prácticas"*** de la gestión de servicios de IT (IT Service Management). Provee de un cuadro genérico para el correcto gobierno de IT y se focaliza en los procesos y servicios necesarios para el negocio y la mejora continua de la calidad de los mismos. Dicho de otro modo ITIL tiene como fin proveer un marco de trabajo para el manejo de la infraestructura, la operativa y el desarrollo de la Tecnología de la Información en la organización, o sea ***"Gestión de los Servicios de IT"***. Donde generalmente se aplica esto? en los centros de cómputos grandes y/o empresas proveedores de servicios del estilo "SaaS".

**Que son "Mejores Prácticas" ?**

Aunque existen diversas definiciones, para efectos prácticos podemos decir que las "mejores prácticas" son un conjunto de prácticas que alguien obtiene analizando y estudiando qué hacen y qué no hacen los mejores exponentes de un tema en particular. La idea es que al terminar el análisis se tendrá un conjunto de prácticas comunes a todos aquellos que están a la vanguardia, y es precisamente ese conjunto el que se recopila y se lanza como "las mejores prácticas" para un tema dado. Así pues, las mejores prácticas no tienen un fundamento matemático o analítico puro, simplemente son obtenidas del mundo real y representan lo que "parece ser lo mejor" hasta el momento. Como tales, las mejores prácticas pueden cambiar con el transcurso del tiempo y, lo que también es muy importante, se debe ser muy cuidadoso al establecerlas para no llegar a conclusiones erradas o ilógicas que lleven a unas "mejores prácticas" absurdas.

**Qué es "Gestión de Servicios IT" ?**

Es el objetivo de ITIL. Para comprender mejor su significado necesitamos entender que se entiende por servicio primero: "un servicio significa la entrega de algo de valor para el cliente (información, reportes, acceso a aplicativos, accesos a redes, PC's, correo, etc.), que con dicho servicio bien prestado pueda cumplir con sus objetivos y sin riesgos"

Un sencillo ejemplo de resultados o servicios que pueden ser facilitados por IT sería cuando la gente de ventas mientras interactúa con sus clientes, a través de su notebook conectada a un servidor en la organización puede acceder a información valiosa para cerrar una operación o resolver cualquier problema. El resultado que el cliente (el representante de ventas de la organización) quiere obtener del servicio es la razón por la cual el lo compraría. El valor que el cliente le otorga al servicio depende de cómo el mismo sea suministrado. El cliente o usuario de TI siempre se preguntará: el servicio que me ofrecen, cumple mis expectativas? Puedo esperar el mismo servicio? Es razonable el costo del servicio?

Gestión de servicios de IT es lo que facilita a un proveedor de servicios (la organización de IT) comprender el servicio que está ofreciendo, asegurarse de que el servicio realmente facilite los resultados que el cliente de negocio de la organización está buscando, comprender el valor que brinda ese servicio y cuan bien está alineado con la estrategia de la compañía y gestionar todos los costos y riesgos del mismo para una eficiente entrega y soporte. Gestión de servicios es entonces un conjunto de capacidades especializadas de la organización para proveer valor a sus clientes en la forma de servicios.

Estos servicios incluyen los procesos, métodos, roles y actividades que el Proveedor de Servicios (Service Provider) utiliza para asegurar la entrega y el soporte de los mismos. La Gestión de Servicios de IT incluye la prestación de los servicios, procesos y componentes de infraestructura IT descriptos en ITIL, su planificación y diseño, estrategia, entrega, soporte y mejora continua. El principal objetivo de la Gestión de Servicios es asegurarse que los servicios de IT estén perfectamente alineados con las necesidades del negocio y que soporten a las mismas.

**Cuales son los beneficios de ITIL ?**

ITIL como vimos provee un marco de las Mejores Prácticas y guías para la Gestión de los Servicios de IT (Services Management). Desde su creación ITIL se ha transformado en la guía mundial más generalmente aceptada para IT Service Management. En las organizaciones ya es reconocido que la información es el recurso y activo estratégico más importante del que dispone. Se reconoce asi que los servicios que provee el departamento de IT al negocio son clave, estratégicos y un activo organizacional que debe ser eficientemente manejado. Se deben invertir apropiados niveles de recursos para su gestión y para que la entrega, el soporte y el manejo de los servicios que IT presta a la organización sean efectivos. Los principales beneficios que aporta la implementación de ITIL a la organización entre otros son:

- Planeamiento de Negocios y Planeamiento de IT
- Integración y alineamiento de las metas de IT con el Negocio
- Medición de la organización de IT (efectividad y eficiencia)
- Optimización de los costos
- Lograr y demostrar un buen retorno de la inversión (ROI)
- Demostrar el valor de negocio que aporta la estructura IT
- Mejora en la entrega y éxito de los proyectos de IT
- Utilización de IT como herramienta y ventaja competitiva
- Entrega de los servicios de IT requeridos y justificados por el Negocio con calidad
- Demostrar un gobierno apropiado de IT
- Aumento de la satisfacción de usuarios y clientes con los servicios de IT
- Mejora en la disponibilidad de los servicios
- Ahorros financieros reduciendo trabajos, pérdidas de tiempo, y mejor uso de recursos
- Mejora del “time-to-market” para nuevos productos o servicios
- Mejora en la toma de decisiones, organización y optimización de los riesgos


***Fecha y lugar de publicación: Buenos Aires, Noviembre de 2008. Queda hecho el depósito que establece la Ley 11.723.***