MODELOS DE DESARROLLO PARA GOBIERNO TI

Models of development for IT government

RESUMEN

Con el entorno y dinámicas competitivas de la actualidad, contar con tecnología de información y comunicaciones no supone por sí misma una ventaja competitiva para las organizaciones. Es la gestión de esa tecnología la que puede dar una ventaja o marcar factor diferencial para el éxito de estas. De acuerdo a esto, apropiarse de un modelo de gobierno IT, para esta gestión, es un elemento clave para el cumplimiento de los objetivos de la empresa

PALABRAS CLAVES: COBIT, Gerencia de TIC, Gestión de TIC, Gobierno IT, ITIL, Modelos de gobierno IT, Serie ISO 27000

ABSTRACT

With the surroundings and dynamic competitive of the present time, to count on technology of information and communications it by itself does not suppose a competitive advantage for the organizations. It is the management of that technology the one that can give an advantage or mark to factor differential for the success of these. According to this, to take control of a model of IT government, for this management, is a key element for the fulfillment of the objectives of the company

KEYWORDS: COBIT, IT Government, ITIL, Management of ICT, Models of IT government, ISO 27000 Series

CARLOS EDUARDO MARULANDA ECEHEVRRY
Ingeniero Industrial, MBA. Profesor Auxiliar Universidad de Caldas, Profesor catedrático Asociado Universidad Nacional
carlose@ucaldas.edu.co

MARCELO LÓPEZ TRUJILLO
Ingeniero Sistemas, Magíster en Educación, Ph.D (c) en Sociedad de la información y del conocimiento.
Profesor Asociado Universidad de Caldas
mlopez@ucaldas.edu.co

CARLOS ALBERO CUESTA IGLESIAS
Ingeniero Sistemas, doctorando en Ingeniería del Software. Profesor Asociado Universidad de Caldas
cacuestai@gmail.com

1. INTRODUCCIÓN

En un mundo globalizado, dinámico e incierto como el de hoy, las Tecnologías de Información y Comunicaciones TIC juegan un papel preponderante y fundamental para el desarrollo de las organizaciones desde diferentes ámbitos como el tecnológico, económico, financiero, de servicios y de producción entre otros, es fundamental una adecuada preparación y formación desde una óptica corporativa, hasta una enfoque de lo que llamamos hoy gobierno de Tecnología de Información (Gobierno T), con el fin de dar a respuesta a los innumerables requerimientos de estas, porque más allá de los elementos puramente técnicos y tecnológicos, es primordial reconocer la organización como un todo, integral, holístico y con una sinergia propia que procura el cumplimiento de sus objetivos enmarcados en aumentar la rentabilidad y las ganancias al máximo.

En este artículo se exploran los diferentes desarrollos de gobierno IT, los más utilizados en el mundo y que han marcado una pauta importante en el desarrollo organizacional.

2. CONTENIDO

2.1 MODELO BÁSICO DE GERENCIA TI

Con el avance e inversión en TIC en las organizaciones, los grupos directivos y gerentes esperan resultados rentables para la empresa, que la coloquen a la vanguardia en los mercados. Sin embargo los casos de la vida diaria muestran ejemplos como: fracasos en la implantación de soluciones TIC, tecnología inadecuada u obsoleta, procesos incompletos, falta de visión, presupuestos excedidos etc. Paul Strassmann, conocido consultor norteamericano, señala que no hay una relación directa entre la inversión de las empresas en TIC y el retorno que consiguen de esa inversión [1]. Fundamentalmente el manejo de TIC debe apuntarle a lo siguiente:

- La alineación de sus objetivos con los objetivos de la organización
- Aprovechamiento de oportunidades y generación de mayor rentabilidad
- Uso equilibrado, equitativo y justo de los recursos destinados a TIC
- Minimización del riesgo

Considerando el concepto de ventaja competitiva el cual evalúa la medida en que la tecnología proporciona una ventaja sostenible para el negocio[2]. En términos de Porter [3] una estrategia en costo, diferenciación o enfoque, como se aprecia en la figura 1:

Fecha de Recepción: 26 de mayo de 2009.
Fecha de Aceptación: 12 de abril de 2009.

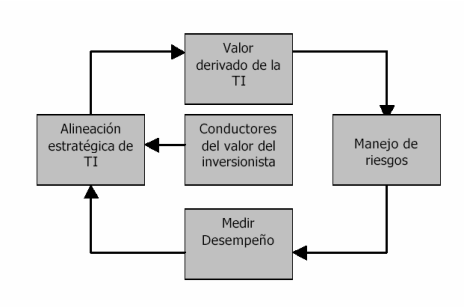

Figura 1. Gerencia de TI

En cuanto a la alineación estratégica fundamentalmente se persigue: una alineación con las estrategias del negocio, prestar un servicio fundamental para el logro de los objetivos organizacionales, desarrollar inversiones justas para el mejoramiento de la rentabilidad de la empresa y contar con información precisa y oportuna para la toma de decisiones

En cuanto al valor derivado se persigue: mantener estándares de tiempo entrega adecuados, hacer uso adecuado y justo de los presupuestos y satisfacción del cliente.

En lo pertinente a la medición del desempeño: uso de sistemas como Balance Score Card, medición de resultados y uso de indicadores

Para el manejo de riesgos: definición de políticas para el manejo de riesgos, inclusión del sistema de control interno y el establecimiento de planes de contingencia

2.2. MODELO ITIL

ITIL son las siglas de la metodología desarrollada a finales de los años 80's por iniciativa del gobierno del Reino Unido, específicamente por la OGC (Office of Goverment Comerce), Oficina Gubernativa de Comercio Británica. Las siglas de ITIL significan Information Technology Infrastructure Library o Librería de Infraestructura de Tecnologías de Información [4][5], incluyendo redes de computadores y comunicación, hardware, software y documentación. Esta metodología es una aproximación a la gestión de servicios de Tecnologías de Información en todo el mundo. ITIL Proporciona una descripción detallada de una serie de buenas prácticas, con una amplia lista de roles, tareas, procedimientos y responsabilidades que pueden adaptarse a cualquier organización de TIC [6].

2.2.1. Forma de uso de ITIL en Managed Services

ITIL postula que el servicio de soporte, la administración y la operación se realiza a través de cinco procesos: manejo de incidentes, manejo de problemas, manejo de configuraciones, manejo de cambios y manejo de entregas

2.2.2. Proceso de manejo de incidentes

Su objetivo primordial es restablecer el servicio lo más rápido posible para evitar que el cliente se vea afectado, esto se hace con la finalidad de minimizar los efectos de la operación.

2.2.3. Proceso de manejo de problemas

El Objetivo de este proceso es prevenir y reducir al máximo los incidentes. Ayudando a proporcionar soluciones rápidas y efectivas para asegurar el uso estructurado de los recursos.

2.2.3.1. Control del problema

Implica identificar el problema, clasificación de los problemas, en caso de ser conocido, se recurre al procedimiento de solicitud de servicio, en caso de no ser conocido se tendría que hacer una fase de investigación para determinar la causa del problema y luego hacer un diagnostico e implementar la solución y finalmente se hacer una evaluación para observar si se resolvió el problema de raíz. En caso de que funcione la solución se pasa a la documentación.

2.2.3.2. Control del error

Que implica identificación el error, registro para clasificar el error, evaluación del daño generado o el efecto que puede generar el error, resolución o corrección del error y determinar que problemas están asociados o como es que al momento de cambiar algo al sistema, se cambia de forma uniforme y no se altera el fin del mismo.

2.2.4. Proceso de manejo de configuraciones

Su objetivo es proveer con información real y actualizada lo que se tiene configurado e instalado en cada sistema del cliente. Este proceso es uno de los más complejos ya que se mueve bajo cuatro vértices que son: administración de cambios, administración de liberaciones, administración de configuraciones y administración de procesos diversos.

2.2.5. Proceso de control de cambios

El objetivo de este proceso es reducir los riesgos tanto técnicos, económicos y de tiempo al momento de la realización de los cambios. Lo que implica: registro y clasificación del cambio, monitoreo y planeación y si el rendimiento es satisfactorio se da la aprobación del cambio, en caso contrario se pasa a la fase de reingeniería y se aprueban los cambios, se construyen prototipos o modelos en los que se van a hacer las pruebas, se hacen las pruebas pertinentes para ver las capacidades del sistema, se da la autorización e implementación; ya implementado se observa que no se hayan tenido desviaciones y se ajusta a las necesidades actuales que también se le considera como revisión post-implementación

2.2.6. Proceso de manejo de entregas

Su objetivo es planear y controlar exitosamente la instalación de Software y Hardware bajo tres ambientes: ambiente de desarrollo, ambiente de pruebas controladas y ambiente real. Este proceso marca la transición de acuerdo a los ambientes por los que se va dando la evolución del proyecto.

2.3. MODELO COBIT

La necesidad del aseguramiento del valor de las TIC, la administración de los riesgos asociados a las TIC, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del gobierno de la empresa. El valor y el riesgo se definen como la posibilidad que un evento adverso, desgracia o contratiempo pueda manifestarse produciendo una pérdida, de ahí lo critico del control para el gobierno de TIC [7].

El enfoque hacia procesos de COBIT subdivide las TIC en 34 procesos de acuerdo a las áreas de responsabilidad: planear, construir, ejecutar y monitorear; ofreciendo una visión de punta a punta de las TIC. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas. COBIT da soporte al gobierno de TIC, al brindar un marco de trabajo que garantiza que: TIC está alineada con el negocio, TIC capacitan el negocio y maximiza los beneficios, los recursos de TIC se usen de manera responsable y los riesgos de TIC se administren apropiadamente

Los productos COBIT se han organizado en tres niveles diseñados para dar soporte a: administración y consejos ejecutivos; administración del negocio y de las TIC; profesionales en gobierno, aseguramiento, control y seguridad.

2.3.1. Procesos orientados

Aunque existen bastantes metodologías y técnicas para la mejora de procesos como los mencionados en [8] y [9], metodologías como SPICE [10], desarrollado por ISO y CMMI [11], COBIT define las actividades de TIC en un modelo genérico de procesos en cuatro dominios. Estos dominios son planear y organizar, adquirir e implementar, entregar y dar soporte, monitorear y evaluar. Los dominios se equiparan a las áreas tradicionales de TIC de planear, construir, ejecutar y monitorear. Para gobernar efectivamente las TIC, es importante determinar las actividades y los riesgos que requieren ser administrados. Éstos se pueden resumir como sigue:

2.3.1.1. **Planear y organizar (PO)**

Este dominio cubre las estrategias y las tácticas identificando la manera en que las TIC puedan contribuir de la mejor manera al logro de los objetivos del negocio. Además de la realización de la visión estratégica, se requiere planear, comunicar y administrar desde diferentes perspectivas. Finalmente se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

2.3.1.2. **Adquirir e implementar (AI)**

Para llevar a cabo la estrategia de TIC, las soluciones de TIC necesitan ser identificadas, desarrolladas o adquiridas así como la

implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

2.3.1.3. **Entregar y dar soporte (DS)**

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.

2.3.1.4. **Monitorear y evaluar (ME)**

Todos los procesos de TIC deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

2.3.2. Basado en controles

2.3.2.1. Los procesos requieren controles

Los objetivos de control detallados se identifican por dos caracteres que representan el dominio más un número de procesos y un número de objetivos de control. Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCn, que significa número de control de proceso. Se deben tomar como un todo junto con los objetivos de control del proceso para tener una visión completa de los requerimientos de control.

PC1 Dueño del proceso: Asignar un dueño para cada proceso COBIT de tal manera que la responsabilidad sea clara.
PC2 Reiterativo: Definir cada proceso COBIT de tal forma que sea repetitivo.
PC3 Metas y objetivo: Establecer metas y objetivos claros para cada proceso COBIT para una ejecución efectiva.
PC4 Roles y responsabilidades: Definir roles, actividades y responsabilidades claros en cada proceso COBIT para una ejecución eficiente.
PC5 Desempeño del proceso: Medir el desempeño de cada proceso COBIT en comparación con sus metas.
PC6 Políticas, planes y procedimiento: Documentar, revisar, actualizar, formalizar y comunicar a todas las partes involucradas cualquier política, plan ó procedimiento que impulse un proceso COBIT.

2.3.3. Medición del desempeño

Las métricas y las metas se definen en COBIT a tres niveles:

- Las metas y métricas de TIC que definen lo que el negocio espera de estas (lo que el negocio usaría para medir las TIC)
- Metas y métricas de procesos que definen lo que el proceso de TIC debe generar para dar soporte a los objetivos de TIC (cómo sería medido el propietario del proceso de TIC)
- Métricas de desempeño de los procesos (miden qué tan bien se desempeña el proceso para indicar si es probable alcanzar las metas)

2.4. SERIE ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. La seguridad puede ser vista como una medida de robustez de un sistema, respecto a una política de seguridad [12]

2.4.1. Origen

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (*British Standards Institution*), es responsable de la publicación de importantes normas como: 1979 Publicación BS 5750 - ahora ISO 9001, 1992 Publicación BS 7750 - ahora ISO 14001, 1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas

prácticas para la gestión de la seguridad de su información. En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007 manteniendo el contenido así como el año de publicación formal de la revisión.

2.4.2. La serie 27000

A semejanza de otras normas ISO, según (Organization, 2008) la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van desde 27000 a 27019 y de 27030, 27044, pasando por 27001, 27002, 27003, 27004, 27005, 27006, 27007, 27011, 27031, 27032, 27033, 27034 y 27799

2.4.3. Elementos básicos para su desarrollo

Básicamente el desarrollo del proceso para la implementación del modelo ISO 27000, se fundamenta en los elementos que aparecen en la figura 2:

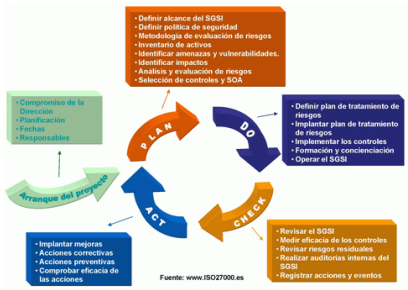

Figura 2. Modelo ISO 27000

2.4.4. Arranque del proyecto

Inicialmente se deben tener en cuenta las siguientes fases:

1. Compromiso de la Dirección
2. Planificación, fechas, responsables

2.4.5. Implementación

La cual se puede dar teniendo en cuenta los siguientes elementos: definir plan de tratamiento de riesgos, implantar plan de tratamiento de riesgos, implementar los controles, formación y concienciación, desarrollo del marco normativo necesario, gestionar las operaciones del SGSI y todos los recursos que se le asignen e implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

2.4.6. Seguimiento

Se dimensiona de la siguiente manera: ejecutar procedimientos y controles de monitorización y revisión, revisar regularmente la eficacia del SGSI, medir la eficacia de los controles y revisar regularmente la evaluación de riesgos así:

1. Realizar regularmente auditorías internas:
2. Revisar regularmente el SGSI por parte de la Dirección
3. Actualizar planes de seguridad
4. Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI:

2.4.7. Mejora continua

Como resultado de la implantación de los pasos anteriores se procura el mejoramiento continuo así:

1. Implantar mejoras
2. Acciones correctivas
3. Acciones preventivas
4. Comunicar las acciones y mejoras
5. Asegurarse de que las mejoras alcanzan los objetivos pretendidos

3. CONCLUSIONES Y RECOMENDACIONES

En el entorno y dinámica competitiva actuales, la posesión de tecnología no supone por sí misma una ventaja competitiva para las organizaciones. Es la gestión de esa tecnología la que puede darle una ventaja competitiva o un factor diferencial con especial énfasis en la gestión de los riesgos derivados del uso de Tecnología de la Información.

Desde la experiencia de los autores, es claro que los gerentes de TI, deben ser formados no sólo en el ámbito tecnológico y metodológico de las tecnologías de información, sino además en ,o referente a la gerencia de las TI

Es importante utilizar algún modelo de desarrollo de gobernanza TI, como los expuestos en este artículo, pero siempre considerando los elementos esenciales de una organización

La implantación de cualquiera de los modelos expuestos requieren del entendimiento que las organizaciones son un todo y que siempre lo que se realice tendrá algún efecto en la misma.

La gobernanza en TIC cada vez esta mas alineada con la estrategia organizacional, la aplicación de los estándares que presentamos se debe articular con la gestión por proyectos y competencias en el ámbito organizacional para direccionar las organizaciones en la economía del conocimiento de nuestros tiempos.

4. BIBLIOGRAFÍA

[1] Strassmann, P.: "Getting better value from information management" Information Economics Journal, 2003.

[2]. **Parker, Marilyn, M** , (1988) "Information Economics", book New Jersey: Prentice Hall.

[3] Porter, Michael E., "Competitive advantage: creatng

and sustaining superior performance", book The Free Press, New York, 1985.

[4] Jhon D. Hwang, Information Resources Management, , New Era, New Rules. IEEE IT, Pro November – December 2002, pp 9 – 17

[5] Wing Lam, Ensure Bussines Continuity, IEEE IT, Pro, may – june 2002, pp 19 – 25

[6] Kemmerling, G.; Pondman, D**.**, 2004, Gestión de Servicios TI, una introducción a ITIL,O. o. G. C. I. S. Support

[7] Pressman, R. (2001). *Ingeniería del software. Un enfoque práctico",* 5a ed. McGraw-Hill.

[8] Koomen T. y Pol, M., Test Process Improvement: a practical step by step guide to structured testing, Addison-Wesley, 1999.

[9] Swinkels, R., Technical Report 12-4-1-FP. A comparison of TMM and other test process Improvement Models, Frits Philips Institute, 2000.

[10] Chrissis M. B., Konrad, M. y Schrum, S., CMMI: Guidelines for Process Integration and Product Improvement. Addison-Wesley, 2003.

[11] El Emam, K., Drouin, J.N. y Melo W., SPICE: the theory and Practice of Software process Improvement an capability Determination. Wiley IEEE Computer Siciety Press, 1997.

[12] Viega J.; McGraw, G., 2001, Building Secure Software: How to avoid security problems the right way,

OTRAS REFERENCIAS

BON VAN JAN et al, 2003. IT Service Management, An Introduction. itSMF-Australia.
OGC, Office of Government Commerce, 2003. ITIL´s Books, Service Supports Book. Sixth version. The Stationary Office, TSO.
Information Systems Audit and control Foundation (2001). "COBIT. Governance, control and audit for information and related technology". 3a ed.
COBIT., COBIT, 3ª. Edición. Comité Directivo de COBIT y la Information Systems Audit And Control Foundation., 2001.