IMPORTANCIA DE LA GESTIÓN DEL PROCESO DE LA DEMANDA DE TI

Igor Aguilar Alonso
Facultad de Informática
Universidad Politécnica de Madrid,
Campus de Montegancedo. 28660 Boadilla del Monte, Madrid
iaguilar@zipi.fi.upm.es

José Carrillo Verdún
Facultad de Informática
Universidad Politécnica de Madrid,
Campus de Montegancedo. 28660 Boadilla del Monte, Madrid.
jcarrillo@fi.upm.es

Edmundo Tovar Caro
Facultad de Informática
Universidad Politécnica de Madrid,
Campus de Montegancedo. 28660 Boadilla del Monte, Madrid.
etovar@fi.upm.es

Abstract. This paper describes some aspects overall of IT demand management, a key process in the IT governance, which has not been taken into account in companies and now has a very relevant importance in the IT business.
The goal the paper is to describe the problems that have CIOs and IT departments to fulfill his delivery of products/services in the term and established budget and to achieve the success in the business. There are described the importance of demand management, types of the demand, the life cycle of demand, as well as levels of maturity of demand in business.

Palabras Clave Gestión de la demanda TI, tipos de demanda, proceso de la demanda, modelos de madurez de la demanda.

1. INTRODUCCIÓN

La gestión de la demanda TI se define como un megaproyecto, en el que se determina que proyectos de TI deben ser habilitados y ejecutados por el departamento de TI. [1].
La demanda de recursos de TI procede de todas las direcciones y en todas las formas. [2]. Algunas demandas son de rutina, tales como requerimientos “help desk” y o de contratación de empleados, mientras otras demandas son estratégicas y complejas, tales como nuevas aplicaciones para soporte de nuevas oportunidades de negocio. La gestión de la demanda de TI fuerza a que toda ella se produzca a través de un solo punto, en el que se puede consolidar, priorizar y realizar. La gestión de la demanda trabaja de la mano con la gestión del portafolio de TI, para gestionar actuales y futuras inversiones de TI.

2. PRINCIPALES BARRERAS PARA EL ÉXITO DE LAS TI

Una de las más grandes insatisfacciones para los CIOs y los departamentos de TI, es la incapacidad para terminar los proyectos a tiempo y dentro del presupuesto planificado. Esto es debido a que normalmente un departamento de TI tiene muchos proyectos

funcionando simultáneamente y no gestionan adecuadamente la demanda de TI.
Debido a la mala gestión de la demanda de TI muchos proyectos fracasan, causando a la empresa perdida de material, recursos corporativos, incremento en desembolsos de capital adicional para tratar de cumplir con el proyecto, así como la perdida de oportunidades para reducir los costos y mejorar sus ingresos.
Entre las principales barreras con las que se encuentra los CIOs para hacer una buena gestión de la demanda tenemos:

1	**El gran tamaño de requisitos/ proyectos.**
2	**Presupuestos inadecuados**.
3	El corto tiempo para el pensamiento estratégico /planificación.
4/5	**Expectativas poco realista /desconocidas del negocio.**
6	Carencia de destrezas técnicas claves.
7	Rapidez en el cambio tecnológico.
8	Falta **de conocimiento de negocio en TI.**
9	**Carencia de alineación entre esfuerzos de objetivos/ del negocio de TI.**
10	**Dificultad para demostrar el valor de TI.**

Tabla Nº 1. Barreras de los CIOs.

Los planteamientos que se muestran en la Tabla Nº 1; especialmente en los puntos 1, 2, 4, 5, 8, 9, 10, están relacionados con la gestión de la demanda. [3].
Debido a estos inconvenientes y muchos otros factores que se pueden presentar en los departamentos de TI, es necesario gestionar adecuadamente la demanda de TI, ya que tiene una gran importancia y sus resultados se reflejan en el éxito de culminación de los proyectos y en la generación de satisfacción en la empresa y en sus miembros.

3. LA IMPORTANCIA DE LA GESTIÓN DE LA DEMANDA

La importancia de la gestión de la demanda radica en la consecución de beneficios para la empresa y para lograrlos es necesario que estas tengan en cuenta los pasos del ciclo de vida de la demanda, pero en diferentes grados, dependiendo del nivel de madurez de la gestión de la demanda dentro de las organizaciones.
El éxito del departamento de TI radica en el éxito de los proyectos de negocios emprendidos y la culminación a tiempo de estos proyectos de una manera efectiva en coste. Para esto se tendrá en cuenta, la selección acertada de proyectos, su priorización y ejecución de dichos proyectos de TI, los cuales juegan un rol importante en el éxito del departamento de TI. También se tendrá en cuenta la selección de que tipo de proyecto y cuantos proyectos de la lista pueden ser permitidos en el departamento de TI, estos son determinantes críticos para el éxito de los proyectos.
La priorización de proyectos es un proceso complejo que involucra la identificación de los diferentes proyectos y la evaluación de los mismos basándose en factores tales como: valor estratégico, valor financiero, riesgo, adecuación de sistemas existentes, tiempo de ejecución, así como la capacidad de organización y complejidad técnica. Estas evaluaciones son hechas para diferenciar la alta prioridad de los proyectos dentro de una lista de proyectos basados en factores relevantes, particularmente el factor financiero. Estos se utilizan para reflejar con precisión la prioridad de los proyectos de TI que dan soporte a las unidades de negocios prioritarias.
La gestión de la demanda debe de ser "primordialmente responsable de la administración de los negocios" [4] ya que los lideres de los negocios son dueños del valor obtenido de una buena gestión de la misma.
Debido a que la demanda proviene de diferentes direcciones y en diferentes formas, los departamentos de TI están saturados con requerimientos para ser atendidos: Por tal motivo es necesario clasificar dicha demanda.

Craig Symons de Forrester Research, clasifica a la demanda en tres grandes grupos y lo describimos a continuación en el siguiente punto.

4. LOS TIPOS DE DEMANDA.

Cuando se habla de los tipos de demanda esta se segmenta en tres grandes categorías. [5]. La tabla Nº 2, resume brevemente los tipos de la demanda, a saber:

Tipo de demanda	Alto nivel de gestiónde procesos	Sub nivel de gestión de procesos
Demanda Estratégica	Gestión del portafolio de proyectos.	• Identificación clara de los objetivos estratégicos. • Tomar un ciclo de vida completo enfocando a la realización de inversiones y beneficios. • Usar factores basados en procesos para toma de decisiones.
Demanda Táctica	Gestión del portafolio de servicios.	• El catálogo de servicios es el centro del portafolio de servicios. • Automatizar los flujos de trabajo para la ordenación, aprobación y entrega. • Gestión de información para TI y usuarios.
Demanda Operacional	Gestión de activos. --- Gestión del portafolio de aplicaciones.	• Mantener el software y la infraestructura actualizandos. • Cumplir con las normas. • Dar soporte a las aplicaciones. • Mantenimiento del hardware.

Tabla Nº 2. Categorías de la demanda.

4.1. La Demanda Estratégica.

La demanda estratégica es la que se gestiona a través del portafolio de proyectos y es la demanda de nuevos proyectos que introducen la innovación y activan nuevos negocios, productos y servicios. La demanda estratégica "representa la oportunidad mas significativa para incrementar el valor de los negocios". Las presiones internas para mejorar los roles de TI, de los socios del negocio y las presiones externas, tales como regularizar los requisitos y competencia del mercado, requerirá un fuerte vínculo entre el plan estratégico y el proceso de iniciación del proyecto. El administrador del portafolio de proyectos (PPM) ofrece un proceso basado en hechos para evaluar, priorizar y monitorizar proyectos. Las unidades de planeamiento estratégico de procesos, los recursos, la localización de presupuestos, la selección e implementación de proyectos y las métricas "post-mortem" de proyectos, mejoran las buenas prácticas en la organización, saber:

- **Identificando claramente los objetivos estratégicos**. Cada unidad de negocio identifica los objetivos estratégicos clave, y alinea las oportunidades de inversión con los resultados de los negocios, asegurando que la TI y los negocios están involucrando a sus socios. El desarrollo estratégico es altamente colaborativo, e integra a TI y ejecutivos del negocio.
  - **Utilizar un proceso basado en hechos para la toma de decisiones.** Los proyectos son evaluados, seleccionados, priorizados, financiados y revisados basados en sus potenciales riesgos ajustando el valor en el contexto de los objetivos estratégicos organizacionales. Las buenas prácticas organizacionales regularmente revisan proyectos para asegurar que siguen el buen camino para entregar los beneficios esperados y rápidamente cancelarse si no son adecuados. Estas empresas desarrollan un estándar de plantilla para los casos de negocio.
  - **Tomar un enfoque del ciclo de vida completo para la realización de inversiones y beneficios.** El portafolio de inversiones se administra a través del ciclo de vida económico completo para entregar el valor optimo a través de la implementación, adopción y eventuales iteraciones. Las organizaciones de TI a veces erróneamente detienen su participación cuando un proyecto se entrega, a pesar de que la mayoría de los proyectos no entregan su óptimo valor hasta los 6 meses o un año después de que empiezan a utilizarse debido a la adopción típica y curvas de aprendizaje. Además, estas pueden ser oportunidades a lo largo del camino para introducir mejoras incrementales que deben de mejorar el valor del ROI. Las buenas prácticas de las

organizaciones de TI hacen un enfoque de la gestión de un producto: los proyectos tienen un plan del producto que se desarrolla mediante su implementación, entrega, adopción, maduración y el retiro/reemplazo.

4.2. La Demanda Táctica.

La demanda táctica se gestiona mediante el portafolio de servicios.

Muchas de estas peticiones consisten en los requerimientos de cada día de servicios de TI, oscilando desde el centro de llamadas, a petición para la contratación de nuevos empleados. Esto fluye hacia las TI desde muy diferentes direcciones y vía diferentes mecanismos, desde sistemas de la gestión de tickets de viaje, a una simple petición. Fuera de un proceso de petición de servicio de TI formal, la demanda táctica puede abrumar al departamento de TI, ya que es difícil de pronosticar y anticipar.

Las organizaciones líderes están comenzando a capturar y gestionar el costo total de entrega de servicios de TI para implementar la gestión *del portafolio de servicios*. Este portafolio provee operaciones de TI como un proceso para ofrecer una amplia gama de servicios más eficaces y eficientes. También permite a las organizaciones de TI facilitar el servicio a los usuarios con transparencia financiera, referente al coste de los servicios de TI, una calidad del servicio constante y predecible y un enlace directo entre entrega de servicio y valor para el negocio y al mismo tiempo hace que la función de TI sea mas eficaz y eficiente en la entrega de estos servicios.

El portafolio de servicios consta de las siguientes componentes:

- **El catalogo de servicios es el corazón del portafolio de servicios**. Toda la documentación de servicios que este provee, incluyendo soporte, mantenimiento y provisión está en un catalogo estructurado que describe los servicios, el contrato de *acuerdo del nivel de servicio* (SLA) y sus costes. Los usuarios pueden acceder al catálogo de servicios vía un browser basado en una interfase, y este puede ser personalizado para cada usuario para que solamente vea los servicios que han elegido.
- **Flujos de trabajo automatizados para pedidos, aprobación y entrega de servicios**. El portafolio de servicios reduce el coste de entrega de servicios por automatización del flujo de trabajo e incluso la entrega de servicios de TI. Las órdenes son seguidas a través del ciclo de la aprobación de los requerimientos para la apropiada entrega la cual puede incluir a TI así como a proveedores de servicio externos. Por ejemplo, cuando se contrata un nuevo empleado, un administrador tiene que anticiparse para que aquél disponga de una cuenta de correo electrónico y de una computadora, una interfase de Web browser para el catalogo. La petición debe de ser enviada al staff de TI responsable para abrir la cuenta de correo electrónico y configurar la computadora.
- **Información para la gestión de usuarios y TI.** Los datos recogidos acerca de la calidad del servicio y coste; pueden ser enviados a la administración en un informe o mostrarse en un panel de control. La administración de TI puede usar la información para comprender la demanda del servicio, el rendimiento del equipo que presta el servicio y comparar los costos internos de TI, así como identificar el origen de la causa de los problemas de rendimiento. Para la gestión de usuarios finales se puede acceder al panel de control para poder ver la calidad del servicio y poder hacer un mejor pronóstico y regular el consumo. La gestión de usuarios finales nos permite ver en tiempo real la prestación de los servicios de TI y los costes asociados y

poder, de esta manera, hacer comparaciones internas de costes de TI con posibles soluciones outsourcing.

4.3. La Demanda Operacional.

La demanda operacional es la que gestiona la construcción y mantenimiento de la infraestructura de TI. Esta demanda proviene del departamento de TI y de sus propias actividades internas para realizar actividades encaminadas a la gestión de activos clave de TI, que afectan a la capacidad de la empresa para desarrollar sus operaciones de negocio.

La demanda operacional incluye:

- **Gestión de la infraestructura de TI**. La infraestructura de TI se gestiona y actualiza de manera continua suministrándole los medios de TI necesarios, incluyendo servidores, unidades de almacenamiento para los clientes (computadoras, estaciones de trabajo, etc.), redes, sistemas operativos y midleware y retirando sistemas anticuados o redundantes. Se encarga de actualizar otros sistemas y configurar y poner nuevos sistemas en servicio. Hoy en la actualidad, las empresas usan herramientas de gestión de activos para capturar la demanda, abastecerse de hardware y gestionar las licencias.
- **Gestión de parches y actualizaciones de seguridad.** Mantener el software seguro y actualizado, se requieren parches de los proveedores del software. Las herramientas de automatización del centro de datos ayudan a mantener la infraestructura libre de virus, denegación de ataques de servicios y otras amenazas que se dan continuamente.
- **Mantenimiento de aplicaciones software.** Las organizaciones invierten en el desarrollo de aplicaciones software así como en paquetes y sistemas para satisfacer la demanda de aplicaciones realizadas por sus clientes. Este software debe de ser mantenido y gestionado a través de su ciclo de vida. En la actualidad un gran número de empresas están usando la gestión del portafolio de aplicaciones de software para evaluar los costos de mantenimiento de software y captura de información relacionada con peticiones de servicios.

Teniendo en cuenta los tipos de demanda, es necesario resaltar la demanda estratégica, destinada a la creación de nuevos proyectos, nuevos negocios, ideas que son el estado inicial para la creación de nuevas oportunidades de negocio en donde se puede invertir.

En este tipo de demanda es necesario hacer las cosas con una secuencia adecuada, ya que no es una tarea fácil para gestionarlo, por tal motivo describimos el ciclo de vida o los mecanismos que se deben de seguir para facilitar el éxito del proyecto.

5. CICLO DE VIDA DEL PROCESO DE LA DEMANDA

Para gestionar la demanda, tenemos que tener en cuenta el proceso cíclico, [6]. Qué se detalla en la figura Nº 1.

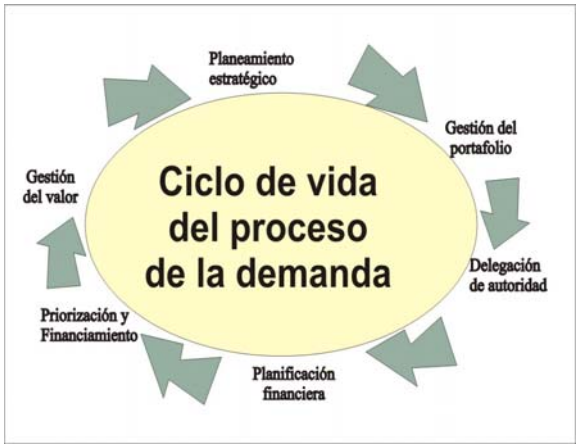

Figura Nº 1. Ciclo de vida de la demanda.

A continuación resumimos brevemente cada uno de estos procesos del ciclo de vida de la demanda.

5.1. Planeamiento Estratégico.

Es el proceso del cual va a depender mucho el éxito del negocio. En este proceso se debe de trabajar con mucho cuidado para tomar las decisiones adecuadas. Es el que nos proporciona la prioridad para todas las inversiones (incluyendo ajuste de estrategias, valores, riesgo y arquitectura). En gran parte de componente va a depender mucho los buenos resultados de una culminación adecuada de un proyecto y lograr el éxito de la empresa.

5.2. Gestión del Portafolio.

Se encarga de traducir la estrategia en categorías de inversión (ejemplos, mejoras del negocio, mantenimiento y cumplimiento); define la asignación financiera, umbrales de riesgo y el retorno objetivo y facilita las revisiones del proyecto.

5.3. Delegación de Autoridad.

Está encargado de la definición del modelo de gobierno para la toma de decisiones correctas y las responsabilidades en el proceso de la gestión de la demanda de TI.

Uno de los principios claves es la autoridad para conducir este proceso dentro de la organización, a la vez que se garantiza el respeto y se asegura la observación del portafolio, la arquitectura, el cumplimiento y estándares de procesos.

5.4. Planificación Financiera.

Determina los fondos necesarios que deben estar disponibles para la inversión en activos de negocio y el presupuesto necesario para mantenerse alineado con el plan estratégico, la gestión del portafolio y la delegación de autoridad y responsabilidades. En adición, la planificación financiera determina el precio de los servicios de TI y como se deben de pagar estos servicios por parte del negocio.

Sin no se fijan los precios "*los usuarios no tienen la información para la gestionar su demanda de recursos de TI*". Esto es importante para no confundir precio y sistemas de tarificación que típicamente resulta un misterio en los informes financieros.

Teniendo en cuenta los sistemas de pago y precios y de otro lado la gestión de la demanda para asegurar la TI y los negocios, estos deben de:

- Trabajar juntos para pronosticar el consumo de los servicios.
- Comprometerse mutuamente en los niveles de servicio y la fijación de precios, y;
- Calcular los pagos haciendo uso del los precio reales que fueron predeterminados.

5.5. Priorización y Financiación.

Las decisiones de priorización y financiación son adoptadas a través de la organización y están relacionadas con los criterios establecidos durante la planificación estratégica, gestión del portafolio y la gestión financiera.

5.6. Gestión del Valor.

Se define como el impacto que un proyecto debe de tener en las entidades externas, particularmente en clientes y proveedores.

Refuerza la responsabilidad para la consecución de beneficios tangibles de los negocios mediante la revisión de proyectos, estableciendo compromisos, monitoreando los resultados y asegurando la capacidad para la entrega del valor, los impactos futuros, las

decisiones de inversión, presupuestos y compensaciones.

6. MODELOS DE MADUREZ DE LA DEMANDA

Como mencionábamos en el punto 4, la demanda esta clasificada en tres grandes categorías (estratégica, táctica y operacional), y para poder gestionarla adecuadamente tiene que cumplir un proceso cíclico, como se menciona en el punto 5.

Pero ahora que esta definido los tipos de la demanda y los ciclos de vida de la demanda, las organizaciones enfrentan el problema de cómo madurar sus prácticas de la gestión de la demanda TI. Por tal motivo es necesario introducir un modelo de madurez de la gestión de la demanda, para que las empresas puedan ubicarse en una determinada etapa y saber si están desarrollando adecuadamente las buenas prácticas de la gestión de la demanda. En la figura Nº 2, ilustramos un esquema como una empresa debe de ir escalando de una etapa a otra en el modelo de madurez de la gestión de la demanda.

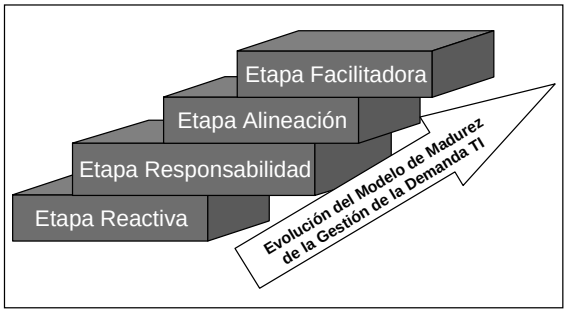

Figura Nº 2. Evolución del Modelo de Madurez de la Gestión de la Demanda.

En el modelo de la madurez del proceso de la demanda podemos encontrar las siguientes etapas, como se observa en la figura Nº 2. [6]. A continuación detallamos cada uno de las etapas del nivel de madurez de la gestión de la demanda dentro de una organización.

Etapa Reactiva.

Es una etapa muy crítica ya que esta caracterizada por niveles de gasto arbitrarios, ya que no se encuentra ningún beneficio, no existen estrategias formales de TI, no se manejan portafolios de TI, los pocos fondos de financiamiento son muy escasos para poder realizar más proyectos.

Etapa de la Responsabilidad.

En esta etapa se introduce el nexo de unión entre administradores y TI, para mediar en la aplicación de planificación y proceso de toma de decisión, según las prioridades del negocio derivadas de las TI desde los planes de negocios existentes y las entrevistas con los líderes del negocio.

En esta etapa ya hay una orientación hacia el negocio, la estrategia de las aplicaciones de TI se desarrolla después del plan del negocio, se define el portafolio de proyectos y se desarrolla el análisis del portafolio. La delegación de la autoridad se delega a través de las políticas de cumplimiento; en esta etapa la asignación de fondos financieros se realiza de una forma más racional, la priorización de proyectos se hacen de una manera más formal.

Etapa de Alineación.

En esta etapa se expande el rol de los administradores para abarcar todos los servicios de TI, integrando los negocios y la planificación de TI, proporcionando una transparencia completa de los servicios de TI y los precios, además se establece un proceso de decisión y responsabilidad que proporciona autonomía a las unidades de negocio mientras se protegen las necesidades de la empresa.

En esta etapa se incrementa el valor de TI, las estrategias de TI se desarrollan en conjunto con los planes de negocio. Es aquí donde se definen más claramente las clases de

portafolio y sus objetivos para todos los productos y servicios. Las unidades de negocio tienen la autonomía para aumentar o reducir sus gastos en TI, los fondos financieros son asignados de acuerdo a las estrategias, según los casos de negocio, estimaciones de consumos; en esta etapa se realiza una priorización formal de todos los proyectos de TI, productos y servicios de una manera mas equilibrada.

Etapa Facilitadora.

En esta etapa se transfiere la responsabilidad primaria de la gestión de la demanda a los negocios, para incrementar la innovación en toda la empresa y hacia abajo.

En esta etapa tenemos el incremento de la innovación, se desarrollan las estrategias de TI dinámicamente junto con el plan del negocio. Se hacen los ajustes dinámicos del portafolio basados en los cambio de la estrategia que se puedan hacer en algún determinado momento, es mas aquí se refina mas el catálogo de servicios para incluir a terceros conocidos por outsourcing.

La etapa facilitadora es el resultado de las buenas prácticas de la gobernanza de TI en la empresa, los ejecutivos de la empresa, así como el personal que trabaja con ellos saben de la importancia de la gobernanza de TI. Los CIOs y los demás ejecutivos de la empresa manejan adecuadamente la gestión de la demanda de TI.

Madurar las prácticas de la buena gestión de la demanda de TI, no es un trabajo tan sencillo, ya que las organizaciones primero deberán hacer una evaluación de cómo están trabajando y luego poder ubicarse dentro de una determinada etapa del modelo de madurez de la gestión de la demanda.

Para pasar de una etapa a otra es necesario que los CIOs entiendan bien las características de las etapas anteriores y cumplan las tareas adecuadas de las buenas prácticas de la gestión de la demanda para cada etapa.

Hoy en día la mayoría de las organizaciones de TI se ubican entre las etapas Reactiva y de la Responsabilidad del modelo de madurez de la gestión de la demanda de TI, por lo que es necesario que entiendan bien las características de estas etapas para poder escalar a la siguiente etapa la de Alineación. Cuando una empresa ha llegado a la etapa Facilitadora se puede decir que esta empresa ha logrado la madurez total dentro del modelo de madurez de la gestión de la demanda TI y cumple de manera adecuada y responsable con las buenas prácticas de la gestión de la demanda.

En la tabla Nº 3, presentamos los estados de madurez de la gestión de la demanda relacionados con el ciclo de vida del proceso de la demanda de TI.

	Reactiva	**Responsabilidad**	**Alineación**	**Facilitadora**
Beneficio	*Ninguna*	*Incremento focalización al negocio*	*Incremento del valor de TI*	*Incremento de la innovación*
Planificación estratégica	No hay estrategia formal de TI.	La estrategia de aplicación de TI se desarrolla después del plan de negocios.	Desarrollo de la estrategia de TI junto con el plan de negocios. Desarrollo de las estrategias de gestión de infraestructura, servicios y activos.	Desarrollo de estrategias de TI dinámicamente junto con el plan de negocio. La estrategia de TI empresarial se consolidada con la TI.
Gestión del portafolio	No existe portafolio de TI (repositorio de proyectos no consolidados)	Definido el portafolio de proyectos de aplicaciones de TI (repositorio simple de proyectos y definición de servicios claves). Inicializar el análisis del portafolio (estrategias, solapamientos, riesgos)	Definidas las clases y objetivos del portafolio para todos los productos y servicios de TI. Portafolio usado en la priorización y gestión del valor.	Ajustes dinámicos del portafolio basado en cambios en la estrategia. Se refina el catálogo de servicios para incluir los de terceros.
Delegación de autoridad	Las delegaciones son desiguales, son muy altas o muy bajas. La gestión de recursos de TI dirige los grupos de aplicaciones. Las TI es responsable de los resultados de las iniciativas de negocio facilitados por las TI	El comité de TI empresarial delega la autoridad en las políticas de cumplimiento. El administrador de recursos de aplicaciones de TI reportan al CIO	Las unidades de negocio tienen autoridad para incrementarse o disminuir sus gastos en TI. La gestión de recursos tiene una dependencia dual. Las TI y los negocios tienen una responsabilidad conjunta.	La gobernanza de TI y RMS están integrados en la gobernanza del negocio. Las unidades de negocio pueden incrementar o disminuir sus gastos en TI. Las unidades de negocio son directamente responsables de los resultados.
Planificación financiera	La asignación de fondos en los proyectos se hace por presiones. En la asignación a las operaciones los fondos son escasos para realizar más proyectos.	Asignación de fondos más racional. Financiación de la infraestructura justificada por proyectos pero administrados separadamente; en las operaciones los fondos son más escasos para realizar más proyectos. Las unidades de negocio de TI aplican un chequeo para ser financiados	Asignación de fondos se deriva de la estrategia. Para las infraestructuras se basan en casos de negocio. En las operaciones se basa en estimaciones de consumos determinados por el análisis de presupuestos basados en actividades.	Asignación de fondos derivada de la estrategia asignación dinámica; funciones y/o unidades de negocio directamente financian sus gastos de TI. Planificación financiera basada en presupuesto cero Gestión del valor para todos los productos y servicios de TI.
Priorización	La aprobación de los proyectos se hacen por presiones o mandatos. Criterios basados en coste.	Priorización formal de proyectos. Se introduce la adaptación a las estrategias y criterios de retorno pero de forma ligera	Priorización formal de todos los proyectos de TI, productos y servicios. Criterios equilibrados (costes, estrategias, riesgos y retornos).	Procesos de priorización dinámicos y muy rigurosos (facilitado por el negocio). Priorización inicial focalizada por la estrategia y los retornos.
Gestión del valor	Desarrollo de casos de negocios complejos de TI, para grandes proyectos, pero no usados después de su aprobación. Baja utilización y seguimiento formal de medidas de rendimiento de las actividades de TI.	Casos de negocio de TI conjuntamente desarrollados para todos los proyectos. Las definiciones de valor se expande para incluir métricas operacionales. Seguimiento de medidas de la realización de la actividad de TI como una clave. Evaluación inicial de riesgos y disponibilidad	El negocio desarrolla los casos de negocios con ayuda de la TI. Las Medidas de valor y riesgo se usan en todos los proyectos, la ejecución de los servicios se miden de punto a punto. La asignación de fondos se basa en las pruebas de valor y mitigación de riesgos. Se realizan auditorias post mortem orientadas al rendimiento del portafolio.	El negocio desarrolla los casos de negocio. Las unidades de negocio y/o funciones son las responsables de demostrar el valor – futuros impactos de los objetivos financieros y operativos. El retorno del portafolio de TI se calcula a nivel de empresa y unidades de negocio/niveles funcionales

Tabla Nº 3. Estados de Madurez de la Gestión de la Demanda TI.

7. CONCLUSIONES

Las conclusiones que podemos sacar son las siguientes:

- La gestión de la demanda de TI aun sigue siendo un proceso critico que no esta bien atendido y los directores no logran entender cual es su importancia.
- La gestión de la demanda es parte de la gobernanza de TI.
- La gestión de la demanda es un problema de comunicación entre los jefes de alto nivel de la organización para ponerse de acuerdo y trabajar conjuntamente en las estrategias de negocio y los objetivos organizacionales.
- Con una buena gestión de la demanda se consigue una mejor transparencia en los costes y el monitoreo de las actividades para poder entregar el servicio o producto en tiempo oportuno.
- Permite desarrollar una cultura de medición y valoración.
- Permite gestionar adecuadamente los recursos internos o externos a la organización.

REFERENCIAS.

[1] John Baschab; Jon Piot; Nicholas G. Carr - The Executive's Guide to Information Technology, Second Edition. Publisher: John Wiley & SonsPub Date: March 23, 2007.

[2] Cray Symons. IT Governance Framework. Best Practices. March 29, 2005.

[3] CIO Magazine´s 2006 State of CIO Survey.

[4] Michael Gerrard, Gartner; defining IT Governance: The IT Demand/Supply Model. October 16, 2006.

[5] Cray Symons. How IT Must Shape And Manage Demand. Best Practices. June 15, 2006.

UN NUEVO MARCO DE CONVERGENCIA Y CALIDAD PARA LA GESTIÓN DE LA SEGURIDAD EN EL SERVICIO DE TI

María Teresa Villalba
Depto. de Sistemas Informáticos, Universidad Europea de Madrid
maite.villalba@uem.es

Luis Fernández
Depto. de Ciencias de la Computación, Universidad de Alcalá
luis.fernandezs@uah.es

José Javier Martínez
Depto. de Ciencias de la Computación, Universidad de Alcalá
josej.martinez@uah.es

Resumen. Dentro del campo de servicios de tecnologías de la información (TI), la gestión de la seguridad tiene una gran importancia. Más allá de las referencias a modelos y estándares, actualmente se han identificado dos grandes demandas para el soporte de la gestión de la seguridad. Por una parte la necesidad de que las organizaciones aborden la convergencia de la gestión de la seguridad en todos sus aspectos y no solamente en el ámbito de las TI. Por otra, la adaptación de los modelos de evaluación y selección de productos software para adecuarlos a las actuales tendencias. En este trabajo, se presentarán el trabajo de los autores en ambos aspectos con referencias a los estándares y modelos relacionados con cada uno de ellos

1. INTRODUCCIÓN

La seguridad es actualmente una de las principales preocupaciones de los responsables de la función informática. El incremento de las amenazas en los últimos tiempos, así como, el aumento en su complejidad ha llevado a directores y gestores de las organizaciones a tener una nueva visión de la seguridad dentro de la estructura de las mismas.

Dentro del modelo de buenas prácticas de la gestión del servicio que supone ITIL [1] la gestión de la seguridad está contemplada en forma de proceso iterativo dentro de la entrega del servicio. Lógicamente incluye importantes actividades de identificación de riesgos, análisis de viabilidad, transformación en SLA (Service Level Agreement) y OLA (Operacional Level Agreement) así como las necesarias acciones de reporting y modificación para completar un típico ciclo PDCA (Plan-Desarrollo-Control-Acción). Por supuesto, a través de las relaciones entre procesos, otras actividades y elementos de otros procesos interactúan con este ciclo de gestión de la seguridad.

No obstante, actualmente, este modelo para la gestión del servicio de las TI necesita contemplar una nueva necesidad: la convergencia de las funciones de gestión de la seguridad dentro de las organizaciones. El aumento en la complejidad de las amenazas y la aparición de nuevas tecnologías, hacen necesaria la combinación de las funciones de seguridad. Aunque en la actualidad todas las organizaciones protegen sus activos físicos y lógicos utilizando gran variedad de mecanismos utilizados por diferentes áreas (departamento de TI, de Seguridad física, Legal, RR.HH., etc.) no existe una

coordinación real entre estas áreas. En los últimos tiempos, este problema se ha manifestado en forma de nuevas amenazas por la adquisición de nuevas tecnologías de protección de la seguridad física que tienen integrado un uso de TI. Es el caso, por ejemplo, de los sistemas de vigilancia basados en circuitos cerrados de televisión (CCTV, Closed-Circuit Televisión) que se están conectando progresivamente a las redes de datos de las organizaciones. Teniendo en cuenta que la información que viaja en ese caso por la red y se almacena posteriormente en los servidores es información sensible, ésta debe protegerse con las medidas de Seguridad Informática necesarias y, además, se debe asegurar que se cumple con la normativa legal vigente manteniendo al mismo tiempo la privacidad. Esto implica, por tanto, la colaboración de los departamentos de Seguridad física, Seguridad Informática y Legal. Todos ellos deben estar perfectamente coordinados para conocer las implicaciones de seguridad que cada decisión en uno de ellos provoca en los otros y así poder aplicar las medidas de protección necesarias.

Con el incremento de amenazas, esta falta de integración deja de ser un simple inconveniente para convertirse en un grave problema al incrementar los riesgos e impedir respuestas coordinadas ante las brechas de seguridad, aumentando así los tiempos de respuesta ante incidentes; limitar los esfuerzos de las organizaciones de establecer estrategias de control centralizado de seguridad y el desarrollo de estrategias de gestión de riesgos integradas; e impedir que se asegure la conformidad con las normativas legales al no disponer del conocimiento de la normativa legal vigente. Abordaremos este tema en el apartado 2.

Sin embargo, no sólo un enfoque estratégico de convergencia es necesario para la adecuada gestión de la seguridad. A un nivel técnico más detallado, los profesionales requieren herramientas de confianza para llevar a la práctica la política de seguridad. Es cierto que la evaluación de la calidad de los productos software y los métodos de selección de los mismos para cada organización o necesidad es una línea de trabajo que ha generado importantes contribuciones desde hace tiempo. No obstante, las peculiares características de estos productos, principalmente COTS (Comercial Off-The-Shelf), y la aparición de estas nuevas tecnologías, no facilitan la aplicación de los modelos generalistas. En el apartado 3, abordaremos las dificultades de evaluación de estos productos así como la necesidad de contar con modelos específicos para software COTS para la seguridad.

2. CONVERGENCIA EN SEGURIDAD TI

2.1. Estado de la cuestión

En Febrero de 2005 ASIS International, ISACA y Systems Security Association (ISSA) fundaron AESRM (Alliance for Enterprise Security Risk Management) una asociación para resolver las cuestiones relacionadas con la convergencia de la seguridad tradicional y la Seguridad Informática. Desde entonces dicha alianza ha realizado diversos estudios relacionados con las necesidades empresariales de Seguridad actuales con el fin de mejorar la Gestión de Riesgos [2, 3]. AESRM define la convergencia como [2]:

"The identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies".

De la definición se extrae, además de la necesaria interrelación entre las diferentes funciones de seguridad anteriormente citada, la necesidad de llevar a cabo un cambio del punto de vista de la seguridad en las organizaciones. Dicha definición refleja los resultados del

estudio llevado a cabo por AESRM entre profesionales del área de seguridad en el que se concluye que es necesario un cambio en la gestión de la seguridad para que pase a tratarse como un valor añadido a la misión global del negocio y no como un centro de coste más. La tendencia internacional pasa por un cambio de la influencia de la seguridad en la visión estratégica empresarial. Por ejemplo, como resultado del citado estudio se deduce que las compañías están involucrando cada vez más a sus directivos de la seguridad en la dirección.

Por otra parte, se han identificado en dicho estudio los diferentes factores que están impulsando la necesidad de la Convergencia en seguridad. Éstos los podemos clasificar en:

1) Aumento de la complejidad estructural de las organizaciones. En la economía global actual, la tendencia es centrarse en el propio negocio y subcontratar los servicios necesarios de apoyo al mismo y esto incluye la seguridad de la organización. Este modelo aumenta la complejidad de la estructura de las organizaciones complicando su gestión y la interrelación entre las diferentes áreas o departamentos de la misma, lo cuál, en el caso de la seguridad, puede derivar en graves agujeros en las fronteras entre unos y otros.

2) Nuevas tecnologías que mezclan funciones tradicionalmente propias de seguridad física con funciones de seguridad informática. En las nuevas tecnologías diseñadas para mejorar la seguridad de las organizaciones, la frontera entre ambos aspectos es cada vez más borrosa. Los nuevos recursos, ya sean físicos o lógicos, tienen cada más riesgo relacionado con ambas áreas. Un ejemplo es el de los sensores de acceso de los armarios para servidores y electrónica de red (comúnmente conocidos como racks) conectados a la red y que emiten una señal a una consola central cuando alguien abre la puerta del rack.

3) Aumento de normativa legal y recomendaciones en respuesta a nuevas amenazas e interacciones de negocio. Debido al incremento y complejidad de las amenazas a la seguridad empresarial, están aumentando las normativas legales que las organizaciones deben cumplir. Esto implica una interacción de los departamentos de seguridad con el departamento legal para la aplicación de las normativas. Es necesario, por tanto, el uso de lenguaje común para un entendimiento de ambas partes. Además, cada vez se da más importancia al cumplimiento de directrices y estándares internacionales por ser un indicador de la calidad de los procedimientos de seguridad implantados en las organizaciones. Algunos de estos estándares, por ejemplo ISO/IEC 27002 [4] (antes ISO/IEC 17799), promueven la gestión integral de la seguridad.

4) Presión continúa en las organizaciones para reducir costes. Es común que las organizaciones se esfuercen por reducir costes en cada una de las operaciones internas llevadas a cabo. En el caso de la seguridad, la comunicación entre los diferentes departamentos relacionados es crítica para la reducción de costes. Por ejemplo, una solución en el departamento de Informática puede significar costes añadidos para el departamento de seguridad física y viceversa. Por otra parte, la integración de las diferentes “seguridades” puede significar una importante reducción de costes ya no sólo por la eliminación de redundancias en la estructura organizativa sino también por la facilidad para integrar soluciones válidas para diferentes áreas (es más fácil justificar inversiones a la dirección si éstas sirven para paliar amenazas en distintos frentes). Un ejemplo de este tipo de soluciones sería el uso de tarjetas electrónicas tanto para el acceso a las instalaciones como para la autenticación y autorización de usuarios a los sistemas de información de la organización.

2.2. Hacia la Convergencia en Seguridad

Para llevar a cabo una respuesta única y global a las amenazas de seguridad física, de la información, operacional, de comunicaciones y de tecnologías de la información, todas ellas deberían verse como una sola seguridad y no

como áreas aisladas. Esta integración bajo el mando del Director de Seguridad no implica un cambio en las funciones de estas áreas sino que todas ellas se convierten en parte de una infraestructura más amplia construida y gestionada dentro de un contexto diferente. Dos son los enfoques más implantados en la actualidad:

1) Creación de un Consejo Directivo de Seguridad centrado en el negocio en el que participen todos los miembros de la alta dirección, además de los responsables de las diferentes áreas de seguridad. Este es sin duda el enfoque más sencillo de implementar pues no requiere cambios en la estructura organizativa: se mantienen las funciones de seguridad como líneas separadas de responsabilidad y se crea un consejo con los directivos de las áreas involucradas que se reúne periódicamente y trabaja conjuntamente en los temas relacionados con la seguridad de la organización. El principal problema de este enfoque, es que su implantación no sea adecuada: dejando fuera a directores técnicos de seguridad o no dando la formación necesaria de dirección de negocio a los responsables de seguridad, algo esencial para que todas las partes involucradas en el consejo hablen el mismo idioma. También es necesario definir una periodicidad de celebración del consejo adecuada y tomar resoluciones que permitan ejecutar acciones.

2) Creación de una nueva figura directiva en la empresa a quien reporten todos los responsables de áreas relacionadas con la seguridad. Esta figura directiva permite coordinar todos los elementos relacionados con la seguridad y recibe los reportes de todos los responsables de áreas relacionadas con la seguridad. El perfil profesional de esta figura debería ser multidisciplinar, es decir, debe tener formación tanto en seguridad física, de TI, de personal y legal, como en áreas de negocio. Los principales inconvenientes de este enfoque son, por una parte, la dificultad de mostrar a la dirección de negocio la necesidad de esta nueva figura, así como, su necesaria introducción en la alta dirección; por otra, la falta de profesionales con este perfil en la actualidad. Según el informe "The Global State of Security Information 2007" realizado por PriceWaterhouseCooper y CXO Media[5] tan sólo el 32% de las empresas encuestadas poseen un profesional de estas características con dicho cargo ejecutivo.

Estos enfoques no son excluyentes entre sí; por ejemplo, puede crearse una nueva figura directiva que englobe todas las "seguridades" de la organización y, al mismo tiempo, tener un Consejo Directivo de Seguridad en el que participen todos los miembros de la dirección incluido el director de Seguridad.

La integración de todas las áreas de la organización relacionadas con la seguridad con la misión del negocio para proporcionar un valor añadido depende en alta medida de la necesaria inclusión de una figura clave: el Director de Seguridad (CSO, Chief Security Officer). Las competencias y habilidades básicas de esta figura son cada vez más críticas para garantizar la protección de todos los activos de la organización y la respuesta correcta ante los incidentes que en la misma se produzcan. Por ello, la figura del CSO en la actualidad debe ubicarse, sin duda, en un nivel ejecutivo y de liderazgo: de esta forma será capaz de garantizar, de forma eficaz, el nivel de riesgo definido como asumible por la dirección, la disponibilidad de las infraestructuras y de los procesos de negocio, la protección de activos, la seguridad de los empleados y la confianza de socios y clientes en la organización.

En la actualidad se está investigando en un plan u hoja de ruta (roadmap) para la implantación progresiva de la convergencia [6] pero, dado que muchas organizaciones europeas tienen implantado el sistema de gestión de seguridad definido en el estándar UNE 71502[7] o ISO/IEC 27001[8], en el caso de la convergencia en seguridad en Europa, una mejor apuesta sería utilizar sistemas de gestión de la seguridad ya existentes o en

proceso y transformarlos y aumentarlos para que sirvan al objetivo de la convergencia. Este enfoque tiene varias ventajas. Por una parte, nos permite apoyarnos en una base ampliamente utilizada y, por tanto, de eficacia probada: el Sistema de Gestión de Seguridad de la Información (SGSI). Además, facilita el cambio en las organizaciones que ya hayan implantado el sistema de gestión reduciendo así el impacto de los cambios. Por otra parte, la norma ISO/IEC 27002[4] ya integra muchos de los conceptos perseguidos por la convergencia al cubrir aspectos organizativos, legales, lógicos (TI) y físicos y requerir su necesaria interrelación en diferentes fases del mismo como, por ejemplo, en la definición de políticas de seguridad.

Otro paso necesario para la convergencia en la seguridad es la formación del personal de seguridad tradicional o física y el de seguridad lógica o de TI. Generalmente las trayectorias formativas y profesionales de ambos perfiles son muy diferentes y, para que sea posible esa necesaria interrelación entre las distintas áreas, es necesario que todos hablen el mismo lenguaje técnico, lo que debería conseguirse a través de una adecuada formación.

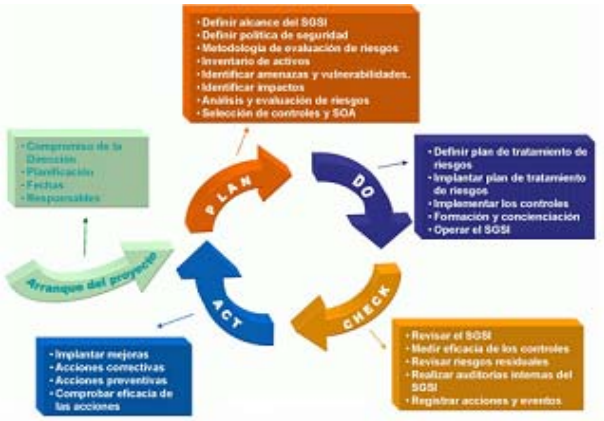

Figura 1. Proceso de implantación de un SGSI (fuente http://iso27000.es)

3. EVALUACIÓN DE PRODUCTOS DE SEGURIDAD

Desde el punto de vista más técnico, es necesario disponer de las herramientas necesarias para implementar las medidas aprobadas por la Dirección en la política de seguridad. El pilar fundamental en el que éstas se apoyan es el software pero el aumento en las amenazas y en la complejidad del mismo, hace que cada vez sea más complicado seleccionar un producto de calidad que cumpla con los requisitos definidos.

Nuestra experiencia como Laboratorio de pruebas de calidad durante el proyecto de investigación (UEM OTRI 2007/02) motivó nuestro interés en la búsqueda de metodologías de evaluación de la calidad aplicables a los productos de Seguridad informática. Para tratar este problema se llevo a cabo un análisis del estado del arte y una evaluación de la aplicabilidad de las metodologías existentes basado en un análisis de los trabajos de investigación en las áreas relacionas, incluyendo estándares de evaluación del software, métodos de evaluación de productos COTS (Commercial Off-The Shelf) y técnicas de pruebas de productos de seguridad. En el caso de los estándares de evaluación, ISO/IEC 14598-5 [9] trata el proceso de evaluación desde el punto de vista de los evaluadores e ISO/IEC 9126 [10] completa este proceso enunciando las características técnicas generales para medir la calidad del software. Otros estándares como ISO/IEC 9241-110 [11] e ISO/IEC 9241-11 [12] extienden estas características. Todos ellos, debido a su naturaleza de estándares, son genéricos y, de ahí, la dificultad de su aplicación directa en la práctica debido al tiempo requerido de adaptación para ajustarlos al dominio de aplicación del producto software a evaluar. Los productos COTS en particular, tienen unas características específicas que los distinguen del software a medida, debido a su naturaleza de caja negra (generalmente no se dispone de

información sobre el código ni su estructura interna), los clientes no están involucrados en el proceso de desarrollo y normalmente se tienen en cuenta en la selección de este tipo de productos otras características distintas de las enunciadas en el ISO/IEC 9126-1, de tipo no técnico, como el coste, el tipo de licencia o el soporte del producto. En un esfuerzo de adaptación para la evaluación de este tipo de productos, ISO/IEC 25051 [13] define el conjunto de requisitos para productos COTS, por lo que es recomendable analizarlo junto con ISO/IEC 14598, de forma que, este último pueda adaptarse a las características específicas de este tipo de productos. Finalmente, ISO/IEC 15408 [14] trata los criterios de evaluación para la evaluación de las propiedades relacionadas con la Seguridad del software.

ISO/IEC 14598-5 se puede utilizar para evaluar cualquier tipo de software. Sin embargo, tal como se comentó anteriormente, los productos COTS tienen características específicas que los distinguen del resto. Por ese motivo, se han publicado diferentes alcances para llevar a cabo el proceso de selección de productos COTS: SPACE (Software Product Advanced Certification and Evaluation) [15], OTSO (Off-The-Shelf Option) [16], STACE (Social Technical Approach to COTS software Evaluation) [17], PORE (Procurement-Oriented Requirements Engineering) [18, 19], CAP (COTS Acquisition Process) [20], RCPEP (Requirements-driven COTS Product Evaluations Process) [21], W-Process [22] or PECA (Planning, Establishing, Collecting, Analyzing) [23]. Aunque estos procesos son una importante contribución al proceso de evaluación de productos COTS, todos ellos se centran en la recogida de requisitos de usuario para su comparación con los productos candidatos. Esto no es aplicable al caso de tener que evaluar un producto individual de forma independiente. Sin embargo, actualmente existe una gran demanda de este tipo de informes. Es el caso, por ejemplo, de los proveedores de software que necesitan conocer las debilidades de sus productos para poder mejorarlas antes de liberarlos en el mercado o con motivos de marketing. También las revistas técnicas de TI utilizan estas evaluaciones en sus publicaciones pudiendo tener una gran influencia sobre los usuarios que leen dichos informes. De ahí, la importancia de disponer de una metodología sistemática que asegure el rigor y exhaustividad de las evaluaciones independientes realizadas. Finalmente, los Criterios Comunes (Common Criteria), normalizados a través del estándar ISO/IEC 15408 [14], asignan lo que denominan nivel de confianza en la evaluación conocido como EAL (Evaluation Assurance Level) que mide el nivel de confianza en la seguridad del producto. Este concepto complica aún más la obtención de una medida final de la calidad global de los productos software dada la necesidad de poder integrar la evaluación de la seguridad obtenida según los Criterios Comunes en la evaluación de la calidad global.

Tras la evaluación del estado del arte se aplicaron los estándares a dos casos prácticos de evaluación [24, 25] obteniendo las siguientes conclusiones:

1) El empleo de estándares en la evaluación de la calidad de productos COTS tiene un alto coste en tiempo y recursos que hace que su aplicación directa no sea práctica.

2) Es necesario disponer de un método que permita integrar la evaluación de Seguridad de los productos en la evaluación global de la evaluación, sin embargo, los estándares no proporcionan ningún mecanismo para llevar a cabo dicha integración.

3) Según el análisis realizado del estado del arte en la evaluación de productos COTS, es necesario tener en cuenta en la evaluación de los mismos los factores no técnicos que influyen en la selección de los productos. Sin embargo, no existe ningún estudio de cuáles son los factores que tienen en cuenta los directores de informática para la selección de productos de Seguridad IT en España.

4) La obtención del modelo de calidad específico para el producto a evaluar es la

actividad con más alto coste en tiempo de la evaluación. Es necesario, por tanto, obtener un modelo de calidad adaptado a los productos de Seguridad IT que minimice el tiempo empleado en la evaluación total.

5) No todas las evaluaciones son iguales: los clientes tienen diferentes requisitos y el objetivo de obtener un informe de calidad puede ser muy diferente de una evaluación a otra. Por ejemplo, no se requiere la misma exhaustividad y rigor cuando el informe de evaluación se va a utilizar para mejorar un producto antes de que éste salga al mercado que aquél que se realiza para publicar un informe funcional en una revista técnica de difusión o el que se requiere para la selección de un producto que se utilizarán en un entorno concreto. Por otra parte, el tiempo y recursos necesarios también depende directamente de la exhaustividad de los informes. Por tanto, es necesario definir diferentes niveles de exhaustividad y acordar con el cliente de la evaluación cómo se llevará a cabo la evaluación y las consecuencias derivadas de utilizar un menor rigor en la evaluación.

4. CONCLUSIONES

En este artículo se han revisado trabajos relacionados con la gestión de la seguridad en dos dimensiones: la estratégica y la táctica. Desde el punto de vista estratégico se concluye con la necesidad de cambiar el modelo actual de organización de la Seguridad dentro de las mismas a fin de realizar una gestión global capaz de incluir todas las áreas relacionadas con la Seguridad. Desde el punto de vista táctico, se han revisado los trabajos existentes en relación con la evaluación y selección de los productos de Seguridad y aplicables a los mismos dada la importancia que el producto utilizado para la implementación de las políticas de Seguridad tiene sobre el resultado final. En esta área se concluye que no existe en la actualidad ningún método práctico de selección y evaluación de productos de Seguridad TIC.

5. REFERENCIAS

[1] Office of Government Commerce OGC. ITIL Managing IT Service: Service Delivery. In Proceedings of (TSO, London, 2001).

[2] The Alliance for Enterprise Security Risk Management. Convergence of Enterprise Security Organizations: International Views., Septiembre 2006.

[3] Deloitte & Touche LLP Canada , The Alliance for Enterprise Security Risk Management The Convergence of Physical y Information Security in the Context of Enterprise Risk Management. Agosto 2007.

[4] ISO 27002 ISO/IEC 27002 Information technology -- Security techniques -- Code of practice for information security management International Styards Organization, Ginebra, 2005.

[5] PriceWaterhouseCooper , CXO Media. The Global State of Security Information 2007, 2008. Available at http://www.pwc.com/extweb/pwcpublications.nsf/docid/114E0DE67DE6965385257341005AED7B/$FILE/PwC_GISS2007.pdf.

[6] Open Security Exchange. Overview & Convergence Council. ADT Financial Services Symposium. Disponible en: www.opensecurityexchange.org/ose_brochure.pdf , Noviembre 2006.

[7] UNE 71502:2004. Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). AENOR, España, 2004.

[8] ISO 27001 ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems -- Requirements International Standards Organization, Ginebra, 2005.

[9] ISO 14598-5 ISO/IEC 14598-5. Information technology -- Software product evaluation -- Part 5: Process for evaluators. International Styards Organization, Ginebra, 1998.

[10] ISO 9126 ISO/IEC IS 9126 - Information technology - Software product evaluation- Quality characteristics y guidelines for their use. International Styards Organization, Ginebra, 1991.

[11] ISO 9241-110 ISO/IEC 9241-110 Ergonomics of human-system interaction -- Part 110: Dialogue principles. International Styards Organization, Ginebra, 2006.

[12] ISO 9241-11 ISO 9241-11 Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability. International Styards Organization, Ginebra, 1998.

[13] ISO 25051 ISO/IEC 25051 Software engineering -- Software product Quality Requirements y Evaluation (SQuaRE) -- Requirements for quality of Commercial Off-The-Shelf (COTS) software product y instructions for testing. International Styards Organization, Ginebra, 2006.

[14] ISO 15408 ISO/IEC 15408. Information technology -- Security techniques -- Evaluation criteria for IT security. International Styards Organization, Ginebra, 2005.

[15] T.; Punter, R. V.; Solingen y J. Trienekens. Software Product Evaluation - Current status y future needs for customers y

industry. In Proceedings of the Proceedings of the 4th IT Evaluation Conference (EVIT-97) (The Netherlys, Delft., 1997).

[16] Jyrki Kontio, Gianluigi Caldiera y Victor R. Basili. Defining factors, goals y criteria for reusable component evaluation. In Proceedings of the Proceedings of the 1996 conference of the Centre for Advanced Studies on Collaborative research (Toronto, Ontario, Canada, 1996). IBM Press.

[17] Douglas Kunda STACE: Social Technical Approach to COTS Software Evaluation.Lecture Notes in Computer Science, Springer-Verlag, 64-84, 2003.

[18] N. A. Maiden, C. Ncube y A. Moore Lessons learned during requirements acquisition for COTS systems. Communications of ACM, 40, 12 1997), 21-25.

[19] N. A. Maiden y C. Ncube Acquiring COTS software selection requirements. Software, IEEE, 15, 2 1998), 46-56.

[20] Michael Ochs, Dietmar Pfahl, G. Chrobok-Diening y B.Nothhelfer-Kolb. A Method for Efficient Measurement-based COTS Assessment y Selection -Method Description y Evaluation Results. In Proceedings of the Proceedings of the 7th International Symposium on Software Metrics (2001). IEEE Computer Society.

[21] Patricia K. Lawlis, Kathryn E. Mark, Deborah A. Thomas y Terry Courtheyn A Formal Process for Evaluating COTS Software Products. IEEE Computer, 34, 5 2001), 58-63.

[22] Teade Punter, Rob Kusters, Jos Trienekens, Theo Bemelmans y Aarnout Brombacher The W-Process for Software Product Evaluation: A Method for Goal-Oriented Implementation of the ISO 14598 Styard. Software Quality Control, 12, 2 2004), 137-158.

[23] Comella-Dorda, J. C.; Dean, E.; Morris y P. Oberndorf. A Process for COTS Software Product Evaluation. In Proceedings of the First International Conference, ICCBSS 2002 (Orlyo, USA, 2002). Springer Berlin / Heidelberg.

[24] Maite Villalba, Luis Fernández Crytosec 2048. e.Security, European Security, 13(June 2007), 78-81.

[25] Maite Villalba, Luis Fernández ISA Server 2006. e.Security, European Security, 14(November 2007), 78-81.

LAS BASE DE DATOS DE GESTIÓN DE LA

CONFIGURACIÓN, EL CORAZÓN DE ITIL

Manuel Pérez Bravo
Indra Sistemas
mperezbra@indra.es

Daniel Rodríguez García
Universidad de Alcalá
daniel.rodriguezg@uah.es

1. INTRODUCCIÓN

Ya desde su definición como concepto, como elemento del proceso ITIL (Information Technology Infrastructure Library) de Gestión de Configuración, la base de datos de configuración (Configuration Management DataBase – CMDB, en sus siglas en inglés). ha despertado mucha expectación entre los diferentes fabricantes de software especializados en ITIL, siendo clasificada como un componente altamente estratégico en todos sus catálogos. La importancia estratégica de la CMDB se explica por su capacidad de colaborar con en el resto de procesos ITSM (IT Service Management) y de la necesidad de tener implementada una buena Gestión de la Configuración antes de aplicar cualquier otro proceso de Gestión. Por esos y otros motivos que explicaremos más en detalle, la CMDB deber ser considerada como el punto de partida hacia la "ITILización" de su empresa.

Este artículo esta estructurado como sigue. La siguientes secciones, explican respectivamente lo que es la CMDB, la necesidad de adaptar el concepto CMDB a las necesidades de una organización y su implantación. En la sección 5, se describe la relación de CMDB con ITSM. Finalmente, se describen las conclusiones más relevantes.

2. ¿QUÉ ES CMDB?

Llamamos Base de datos de Configuración a la base de datos que contiene información específica sobre el estado actual de la configuración de la empresa. Esta base de datos, contiene la información que identifica de forma única a cada elemento de configuración (Configuration Items– CI) y que describe sus atributos, tal y como sucede en las típicas aplicaciones de inventariado. Pero además, muestra sus relaciones con el resto de CI's incluyendo la información generada por el resto de procesos ITIL sobre ese elemento, como cambios, incidencias, informes de disponibilidad, etc. Sobre esta definición consideraremos elemento de configuración a todo componente físico o lógico que forma parte de la infraestructura de la empresa y sobre el que debe existir un cierto control. Más allá de un simple repositorio de datos, o de una base de datos de activos, la CMDB debe ser vista como el elemento de ITIL que permite la interrelación de todos los procesos entre sí, debiendo poder soportar procesos de reconciliación –procesos que sincronizan las diferentes bases de datos que recogen los inputs del resto de procesos ITIL con la propia CMDB–, tener acceso a herramientas descubridoras de nuevos elementos de configuración y capacidad de definir procedimientos de auto auditoría.

De todas las cualidades que puede aportar la CMDB a la organización que la implementa, seguramente la más importante sea la de poder establecer una relación directa entre los CI's y los eventos que se van produciendo durante su gestión desde procesos ITIL. Damos por hecho que cuando una empresa decide aplicar a su negocio las Best Practices de ITIL, estará alineando implícitamente su operativa con las tareas descritas en la guía. Si la CMDB es la central de datos donde se relaciona como está configurada nuestra compañía aplicando un sencillo silogismo podemos deducir que una CMDB bien diseñada, que se adapte a las necesidades específicas de cada negocio, establecerá directamente relaciones entre los ítems que contiene con el rol y dependencia dentro del negocio. Veamos un par de ejemplos a diferentes niveles:

- Imaginemos al personal de soporte en su centro de trabajo, que recibe una notificación sobre un fallo que ha sido producido por cualquier motivo en un servidor de aplicaciones. Con una simple consulta a la CMDB, la persona que en ese momento se encarga del diagnóstico del problema podrá acceder a información específica de ese CI, pero también podrá consultar los cambios que han sido ejecutados sobre ese servidor, quién los realizó, cuando, porqué motivo se hicieron, la incidencias sufridas por ese mismo servidor, componentes a los que estaría afectando el fallo. Una vez que se haya establecido un diagnóstico, se podrán consultar en la CMDB soluciones aportadas anteriormente a problemas similares, facilitando de esta manera el proceso de recuperación, ahorrando costes y mejorando los tiempos de resolución.

- Ahora supongámonos a un director encargado de la gestión del nivel servicio. Gestionar la entrega de un determinado servicio es una tarea que requiere un gran consumo de información, pues los informes que se realizan necesitan incluir muchas variables que determinen el nivel o la calidad del servicio que se está entregando y de cómo se está haciendo. Para estos casos, la CMDB puede ser el repositorio ideal para obtener dicha información. Supongamos que a parte de la relación entre los distintos componentes, hemos diseñado una relación entre un servicio y los componentes que soportan ese servicio, como máquinas, aplicaciones, interfaces, etc. Con esa configuración nuestro director podrá determinar de manera rápida y eficaz las incidencias que sufrieron esos componentes y cómo esas incidencias afectaron a la entrega del servicio, pudiendo establecer los niveles de disponibilidad, capacidad y de usabilidad de cada servicio.

En los ejemplos anteriores se parte de un prerrequisito común, para ambos casos existe por debajo un ente lógico, es decir, un repositorio común capaz de mostrar de manera actualizada y coherente como es una arquitectura de TI, por el que fluye la información de manera bidireccional entre procesos ITSM y repositorio, como en un corazón. Este repositorio es la CMDB.

3. ¿CÓMO ADAPTAR EL CONCEPTO CMDB A LAS NECESIDADES DE UNA ORGANIZACIÓN?

Con la definición de lo que es CMDB se puede adelantar gran parte de la respuesta a esta pregunta. Sabemos de antemano que en la CMDB vamos a almacenar los datos más importantes de cada uno de los activos que tenemos en nuestra compañía y de cómo se relaciona unos con otros. Sin embargo, obviamente quedan cuestiones por resolver, por ejemplo, ¿qué nivel de detalle debemos registrar para cada elemento? ¿Qué familias, tipos, categorías de elementos vamos a

registrar en la base de datos? ¿Cómo puedo mantener íntegros y actualizados estos datos? Evidentemente la CMBD debe estar orientada siempre en línea a los requerimientos básicos del negocio, por lo en las reglas de negocio específicas de su empresa estará la clave del diseño de la CMDB. Por ejemplo, una empresa dedicada a los servicios de telefonía móvil tendrá unas necesidades diferentes a las de una empresa logística. En el primer caso, la infraestructura IT es el negocio, mientras que en la segunda la infraestructura de IT es un soporte, vital pero soporte al fin y al cabo, al negocio. La empresa de Telecomunicaciones necesitará disponer de datos precisos de todos los componentes que integran su arquitectura con un detalle casi milimétrico, de servidores, routers, componentes y aplicaciones, además de contratos de soporte, documentación, etc. ya que su facturación depende de que su arquitectura no se paré, y en caso de parada debe disponer de información extremadamente precisa que le permita saber que parte de IT es la que puede estar comprometida, como afecta al resto del negocio y qué configuración mínima se necesita para reestablecer un servicio TI ("baselines" definidas en el proceso de Continuidad TI). Por ejemplo, no es lo mismo saber que un aplicación esta fallando porque el servidor donde se ejecuta ha sufrido recientemente un cambio en la configuración de su tarjeta de red, que saber simplemente que una aplicación falla por un mal funcionamiento del servidor. Si en la CMDB no hemos definido este componente con ese nivel de detalle, probablemente costará más tiempo identificar el punto de partida del error, por lo que perdemos tiempo y por consiguiente dinero.

Sin embargo, definir un alto nivel de detalle en la estructura de la información no siempre es positivo. Se debe tener en cuenta de que a un mayor número de datos a registrar y controlar, también mayor será el esfuerzo a realizar para diseñar y mantener una CMDB, y a la larga este sobre coste puede lastrar el éxito o fracaso de su proyecto CMDB. Si una empresa no necesita una CMBD "rigurosa" se pueden estar desperdiciando valiosos recursos que pueden hacer falta en otros procesos. Por eso desde el primer momento cualquier persona a cargo del proceso de Control y Gestión de Configuraciones debe tener claro que es lo verdaderamente importante en la empresa y adecuar una CMDB con coste de implantación y mantenimiento en consonancia a los objetivos corporativos: "Primero conozca las necesidades de su empresa, después defina su CMDB".

4. IMPLANTACIÓN DE CMDB

Tras evaluar las necesidades de la empresa, vemos que estas necesidades nos obligan a definir una base de datos de configuración muy elaborada. Usted observa que la cantidad de información a registrar es enorme, y que las relaciones entre los componentes son muy complejas, ¿Estamos ante un reto imposible? Expertos en la materia como Klaas Hofkamp de IBM, con más de 15 años de experiencia en la implantación y definición de CMBD's, recomiendan para estos casos seguir las siguientes directrices.

1- *Establecer los puntos de partida*: ¿Qué problemas estamos intentando solucionar con la CMDB? ¿Necesitamos registrar y controlar los componentes que soportan los servicios? ¿Queremos controlar el ciclo de vida de un activo para evitar excesos en los costes o saber que relación tienen los elementos de la configuración entre sí?. Durante esta fase determine con exactitud cuales serán las prioridades que cubrirá su CMDB.

2- *Identificar los requerimientos de datos*: Investigue quienes son los principales procesos productores de información y cuales son los

consumidores. A posteriori evalué que datos son los más necesarios para optimizar esos procesos.

3- *Controlar la implementación:* A medida que el proyecto va avanzando y que más y más gente va siendo involucrada en la implantación de la CMDB, es muy posible que se le impongan nuevos requisitos de lo que la CMDB "debe hacer". Probablemente todas serán buenas ideas, pero debe conservar el enfoque inicial y esperar a siguientes fases para desarrollarlas. Mantenga ante todo los puntos definidos al principio.

4- *Definir diferentes fases de implantación*: Las soluciones perfectas y únicas no existen. Lo ideal es definir una solución alineada con objetivos parciales, evitando de esta manera posibles bloqueos durante la etapa de análisis. Un enfoque por fases además da la sensación de que el proyecto avanza.

5- *Utilizar estándares en la identificación de componentes:* La implantación de una CBMD es una tarea que involucra a muchas y diferentes partes de la empresa. Usted como promotor de la CMDB debe estimular el uso de una nomenclatura común, apoyada si es posible, por estándares, y será su deber el que todo el mundo la conozca y la utilice.

6- *Definir los Servicios IT:* Todo evento que ocurra dentro de la infraestructura IT, debe ser registrado hacia el servicio del que forma parte. Si su empresa no tiene definido un catalogo de Servicios IT, difícilmente usted podrá relacionar los elementos de configuración con sus servicios. Como ya se ha dicho anteriormente, uno de los grandes beneficios de la CMDB es vincular los componentes con los servicios que soportan, por lo tanto, si no hay definido un catalogo de servicios, implique a la compañía para hacerlo.

7- *Establecer un equipo de proyecto*: El equipo del proyecto de CMDB debe estar formado por personal de las diferentes áreas afectadas por el control de la configuración, como personal de control de cambios, de control de activos, de resolución de Incidencias, etc. aunque limitado en su número. No es conveniente grandes equipos, ya que se puede perder mucho tiempo en discusiones como por definición de nomenclatura.

8- *Busque el compromiso de la dirección*: La implicación directa de la dirección proveerá y reforzará las políticas de Gestión de la Configuración. Para logarlo demuestre desde el inicio del proyecto los beneficios latentes de la CMDB, prepare datos, demostraciones y maquetas que apoyen y confirmen su trabajo.

9- *Preparar formación para el "cambio cultural":* Cada vez que se producen cambios o que se implantan aplicaciones nuevas, los métodos de trabajo, procedimientos y tareas diarias sufren importantes modificaciones. Ante este reto es necesario preparar al personal de la compañía. Sea proactivo y anticipe el cambio cultural antes de que se produzca, defina desde los inicios del proyecto quién, como y cuando debe cambiar su "modus operandi".

10- *Elaborar un plan de comunicación:* Como si fuera una campaña de marketing, usted debe comunicar los objetivos y beneficios de su proyecto. Un empleado será mucho más receptivo ante los cambios si es consciente los beneficios que le reportará la nueva herramienta en su trabajo. Su implicación con el proyecto aumentará y usted dispondrá de valiosos aliados para llevar a cabo su objetivo con éxito.

5. CMDB Y SU RELACIÓN CON EL ITSM

Ya tenemos por un lado un repositorio global donde guardar los componentes de la infraestructura IT, y por otro lado tenemos los procesos que forman parte del ITSM (Information Technology Service Management). Además de la relación entre componentes, otro tipo de relación a definir en una CMDB es la relación entre ítems de configuración y los datos que se van generando con cada uno de los procesos de Gestión. Veamos ahora que procesos generan qué tipo de información y como se relacionan esos datos con la Base de Datos de Configuración.

Gestión de Incidencias y CMDB.

La Gestión de Incidencias tiene como objetivo informar y registrar eventos que interrumpan la operativa normal de la empresa con el fin de resolverlos a la mayor rapidez posible. Cada vez que sucede un incidente, se debe crear un registro donde se informe que componente tiene el problema, además de detalles varios que ayuden a su diagnóstico. Desde ese momento CMDB y Gestión de incidencias deben tener una comunicación fluida, pues dentro de la CMDB se establecerá la relación entre la incidencia generada y el componente afectado.

Pero Gestión de Incidencias no sólo es un proveedor de información a la base de datos de Configuración. En la mayoría de las ocasiones, recuérdese el caso del operador de Service Desk, es consumidor. La información contenida en la CMDB se utiliza para agilizar el diagnóstico (durante la fase de análisis) y la recuperación (durante el la fase de resolución). Pero quizás, la información más importante que recupere Gestión de Incidencias de la CMDB sea el impacto que tiene una incidencia sobre un elemento. El impacto es un atributo que se tiene que establecer a todos y cada uno de los CI's que hay en la CMDB y cuyo valor se determina durante la fase de implantación de la CMDB o ya dentro de las tareas especificadas para el proceso de Gestión de la Configuración. El impacto indica como de grave es un incidente ocurrido en ese CI, debido a su peso dentro de un servicio o por las relaciones que el componente tiene con otros. A mayor impacto, mayor será la celeridad con la que se debe resolver un problema.

Gestión de Problemas y CMDB

Gestión de problemas destaca por ser un proceso proactivo que busca la reducción de los incidentes que ocurren de manera recurrente en la empresa. Imagínese que usted es miembro del equipo de control de errores, y debe investigar porqué siempre después de un cambio, una determinada aplicación tiene incidencias en determinadas funcionalidades. ¿Dónde buscará usted los datos que le ayuden a iniciar la investigación? Obviamente, en la CMBD y con esos datos se podrá investigar quién es el responsable del elemento y advertirá al grupo implicado acerca de las incidencias que ocurren cuando realizan un cambio de en su sistema. Otros datos importantes que la Gestión de problemas suele consultar son el estado en el que se encuentran los componentes durante la investigación o datos de problemas anteriores.

Gestión del Cambio y CMDB

Cualquier compañía dedicada a la prestación de servicios, es consciente de que en el trabajo diario tienen y deben suceder cambios. Los cambios pueden surgir por nuevas necesidades o como respuesta a problemas que han ocurrido en la empresa. Sea cual fuere el motivo, el control que se debe establecer sobre el elemento de configuración que se modifica debe ser extremadamente riguroso. Desde el momento en que se crea un cambio, esa entidad cambio debe ser registrada en la CMDB y relacionada con todos los componentes que van a ser modificados. De manera recíproca, el personal involucrado en el cambio debe extraer de la CMDB, durante la elaboración del documento oficial, aquellos elementos de la configuración que estarían relacionados –sea cual sea el tipo de relación– con ese componente (¡qué útil puede ser, conocer de antemano que un cambio en la configuración un router puede afectar a toda una subred de servidores, verdad?!) Identificadas, gracias a la CMDB, las relaciones de los CI, se podrá determinar con mayor exactitud el impacto que tiene dicho cambio sobre la arquitectura global y sobre la entrega del servicio a los clientes, movilizando recursos y estableciendo las medidas preventivas necesarias.

Gestión de la Entrega y CMDB

Gestión de la entrega es el proceso que se encarga de distribuir en paquetes, un determinado número de cambios autorizados y de archivar físicamente copias de ese software hasta que se deja de utilizar en la empresa. Durante el ciclo de vida de una entrega, ya desde la fase de planificación se debe establecer un vínculo entre la versión de software que se va a distribuir y los componentes que verán afectados por la distribución. Obviamente este vínculo se definirá siempre a nivel de CMBD.

Gestión de la Disponibilidad y CMDB

La disponibilidad es uno de los pilares básicos sobre los que descansa el mundo de los servicios IT. Un servicio 24x7 debe ser ante todo fiable, que no falle nunca o casi nunca, y que su disponibilidad sea muy alta. Para evaluar la disponibilidad de un determinado servicio se tiene que investigar la disponibilidad de todos los componentes que lo soportan, utilizando para ello ratios como por ejemplo el tiempo de recuperación después de fallo o tiempo transcurrido entre incidencias. Como se ha comentado anteriormente, la CMDB debe de contener información acerca del número de incidencias que un determinado elemento lleva sufridos durante su ciclo de vida y si esas incidencias provocaron una interrupción del servicio. Recuperada esa información podremos calcular cuanto tiempo se ha invertido para su recuperación. Gracias a esto la CMDB pasa por ser una herramienta fundamental para el proceso de Gestión de la Disponibilidad. La información contenida en la CMDB es vital para el proceso, pues gracias a ella, se puede analizar como y cuanto de disponible ha estado un determinado servicio para nuestros clientes durante un periodo de tiempo, y poder así diseñar las políticas adecuadas de mejora o mantenimiento de la disponibilidad.

Gestión Financiera de IT y CMDB

Puede darse el caso de que usted necesite para su organización un proceso de gestión Financiera de IT capaz de determinar el verdadero coste de un servicio IT y así poder repercutir esos costes hacia nuestros clientes. Para estos casos puede resultar necesario que la CMDB almacene dentro de un componente de configuración, nuevos atributos que guarden información de índole económica. Suponemos que un determinado servicio IT está integrado por múltiples componentes tanto de origen software como hardware. Si por ejemplo, en nuestra CMBD hemos añadido datos sobre el

precio de adquisición o cálculos de amortización, Gestión Financiera de IT podrá fijar el valor de utilización de un servicio en función del coste de desgaste de los componentes utilizados. A más datos de carácter económico guardemos en la CMDB, con mayor exactitud se podrá determinar cuanto vale un servicio.

Gestión de Continuidad IT y la CMDB

La continuidad IT establece los mecanismos necesarios para restablecer unos servicios IT básicos en caso de un problema generalizado en los sistemas. Esa configuración básica (component baseline) debe estar especificada siempre por componente dentro de la CMDB.

Gestión del nivel del Servicio y CMDB

En uno de los ejemplos que se describió al principio del artículo, el director que necesita elaborar un informe de entrega de servicio, se ve la relación que existe entre CMDB y Gestión de SLA (Service Level Agreement). Cuando usted ofrece un servicio IT a una compañía externa, o su a propia empresa de manera interna, necesita saber como y de calidad está prestando ese servicio. Para medir la calidad, se realizan una serie de monitorizaciones y seguimientos sobre los CI's que haya registrados en la CMDB, comparando los datos obtenidos con lo que se haya acordado en los SLAs. Los SLA son contratos de facto firmados entre cliente y proveedor que indican los niveles esperados, y las penalizaciones en caso de no llegar a esos niveles, que un servicio IT debe ofrece. Por tanto su CMDB también le puede proporcionar la foto sobre como está prestando su servicio.

6. CONCLUSIONES

En estos días en los que se habla continuamente de la necesidad de aumentar la productividad del factor trabajo, del elemento diferenciador en nuestros servicios con respecto a nuestros competidores, de la mejora continua de la calidad, ahora más que nunca usted debe pensar en ITIL como marco de referencia. Dentro de un entorno empresarial excepcionalmente dinámico (y hostil), donde las necesidades, los requerimientos, las oportunidades de negocio cambian, es más importante que nunca controlar qué es lo que tenemos en nuestra empresa y como lo gestionamos. Las buenas prácticas que ITIL describe nos muestran el camino a seguir para controlar nuestros servicios, incrementar nuestra productividad y reducir el impacto que tienen todos estos cambios en la arquitectura IT. Tal y como hemos expuesto durante este artículo esas buenas prácticas tienen siempre un punto de partida, la implementación de la Gestión de la Configuración, y de la CMDB. Con una única la palabra, "relaciones", podemos describir el valor fundamental que guarda toda CMDB. Relaciones entre componentes, y relaciones con las entidades propias de los procesos de gestión.

Finalmente, implantar una CMDB en cualquier compañía es siempre un proyecto muy ambicioso, aunque ya sabemos que el camino hacia la calidad y la excelencia nunca fue sencillo. Por eso debe implicar desde el primer momento a todo el personal de su empresa, a los directivos para que apoyen el proyecto, y a los empleados para que entiendan que las mejores practicas de ITIL suponen una mejora en sus métodos de trabajo.

7. REFERENCIAS

[1] Malcom Fry "ITIL Functions Supported by the CMDB" BMC Software, View Point.

[2] Klass Hofman "Lessons Learned on CMDB", BMC Software, Focus on CMDB.

III CONGRESO INTERACADÉMICO DE ITSMF 2008 EN LA UNIVERSIDAD CARLOS III

Madrid, 19 de Mayo de 2008.- El III Congreso Interacadémico ITIL 2008, organizado en Madrid por itSMF España y por el Departamento de Informática de la Universidad Carlos III de Madrid, contó en esta edición con más de 300 asistentes procedentes del mundo empresarial, académico y de la Administración Pública, certificando así el progresivo interés que despierta en España el valor que las mejores prácticas ITIL de gestión de la tecnología pueden reportar a las empresas y Administraciones Públicas.

En el congreso se trataron temas relacionados con la gestión del servicio de TI como: casos prácticos, gobierno de las TI, ISO20000, acuerdos de nivel de servicio, gestión de la configuración, etc. A lo largo del congreso se constató como las TI están evolucionando a buen ritmo desde un rol focalizado en automatizar las operaciones a un papel de liderazgo en los negosios. A lo largo de las veintiuna ponencias presentadas se profundizó en los conceptos de: orientación al servicio, aportación al negocio y excelencia en la operación. Dentro de la orientación al servicio se presentaron ideas novedosas sobre el diseño de mapas de servicios o la forma de medir los Acuerdos de Nivel de Servicio. Dentro de la orientación al valor se profundizó en como optimizar el proceso de Planificación Estratégica de las TI o como diseñar modelos eficientes de Gobierno y Gestión de las TI. La excelencia de la operación contó con interesantes aportaciones sobre la evolución de la gestión de la configuración (autodescubrimiento, reconciliación, federación, etc) o como mejorar la usabilidad de los procesos. También se analizó el como las certificaciones TI de las organizaciones y de los profesionales ayudan a la consecución de la excelencia.

En el encuentro se dieron cita un gran número de profesionales, investigadores y estudiantes interesados en las mejores prácticas de la Gestión de Servicio de las TI. En el Congreso Interacadémico, también participaron las Facultades y Escuelas de Informática de: Universidad de Alcalá, Universidad Nacional de Educación a Distancia, Universidad Antonio de Neblija, Universidad Politécnica de Madrid, y Universidad Rey Juan Carlos, así como la Escuela de Ingeniería de Telecomunicaciones de la Universidad Pompeu Fabra. El congreso también permitió a los estudiantes de últimos cursos de ingeniería tecnológica el tomar contacto con el mundo empresarial e investigador. El congreso fue abierto por Mark Gemmell vicepresidente de itSMF España y Belén Ruiz Mezcua Vicerrectora Adjunta de Investigación para el Parque Científico Universidad Carlos III de Madrid.

Ponencias presentadas.

Por parte de Abast Grup, Jorge Fernández y Antonio Valle, partiendo de un análisis crítico de como generar valor en las TI, realizaron un planteamiento de despliegue de un plan estratégico de sistemas que optimiza la toma de decisiones. En la segunda ponencia, Jorge presentó el trabajo de investigación desarrollado dentro de la Universidad

Politécnica de Cataluña consistente en un modelo denominado Agile BI Governance para evitar los fracasos de los proyectos de Business Intelligence. Miguel García Menéndez de Atos Consulting trato la publicación de la norma ISO/IEC 38500:2008 y cómo dicha norma ayuda a un correcto Gobierno de las TI mediante una definición clara de conceptos y una asignación correcta de responsabilidades. Por su parte la Universidad Rey Juan Carlos por medio de Eugenio Fernández, repasando la bibliografía del Gobierno de las TI, expuso un modelo unificado que sigue el ciclo de vida de las TI y que fue implantado en su universidad.

El empleo del catálogo de servicios como herramienta clave para alinear las TI con el negocio fue tratado por Cristina Gordillo y José Manuel Cao de HP de una forma práctica con ejemplos del mapa de servicios y dando indicaciones de como monitorizarlo de forma eficaz. La correcta visión del servicio TI su forma de plasmarlo en acuerdos de nivel de servicio y la tipología de indicadores a emplear estuvieron defendidos por José Luis Benito, consultor y formador independiente en la gestión de las TIC. En la misma temática, una visión práctica de cómo monitorizar los SLA considerando los tiempos transcurridos de una forma diferenciada dentro de un mismo grupo de soporte o entre dos estados, fue el tema elegido por Javier García Arcal de IT Deusto y profesor de la Universidad Antonio de Nebrija.

Otro de los puntos clave de una óptima gestión del servicio es la gestión de la configuración, Jesús Garcia Romanos y Álvaro García Merchan de IBM dieron ejemplos de sistemas de gestión de la configuración incidiendo en la integración de diferentes fuentes y su sincronización con la gestión de cambios. La importancia de la CMDB como aspecto clave del éxito de los proyectos ITIL fue también el tema tratado por Manuel Pérez y Daniel Rodríguez de la Universidad de Alcalá. La alineación negocio y sistemas en las Telcos mediante la convergencia de dos estándares como eTOM e ITIL, fue la ponencia defendida por Álvaro Torres y Ángel Sánchez de Everis. Douglas Wagner de TQS, tras un análisis de los cambios acontecidos en el área informática, disertó cómo gestionar de forma adecuada los riesgos inherentes a los procesos TI mediante un mapa de procesos y un modelo de gestión.

Alfonso Gutiérrez de Accenture presentó un modelo pensado para crear valor y hacer evolucionar las organizaciones desde una perspectiva de industrialización a una perspectiva de integración con el negocio en que las TI sean un facilitador estratégico. Por parte de la Universidad Politécnica de Madrid, José A. Calvo-Manzano y Gerzón Gómez disertaron sobre un estudio que analizando las dependencias entre procesos ITIL establecen una secuencia de implementación.

Para paliar la escasez de datos sobre el estado de las implantaciones ITIL en España, el comité del observatorio de itSMF por medio de Raquel Paz de GMV, Paula Fernández de GFI, Luis Morán de Telefónica y Antonio Folgueras de la UC3M, presentaron los resultados de una encuesta masiva que centra sus objetivos en analizar el rol de las TI así como el grado de utilización de los diferentes estándares y las estrategias de outsourcing. Aparte de dicho análisis sobre encuestas del sector, en un congreso académico no podían faltar ponencias relativas a cómo alcanzar la excelencia en la docencia de ITIL y dentro de esta última área Jorge Infante presentó la experiencia de la Universidad Pompeu Fabra.

El tema de la evaluación de los procesos ITIL fue tratado por Sandra Gomes de Balmes Konsulting que tras un análisis de los beneficios y de los pasos a realizar en una evaluación ITIL, proporcionó ejemplos de plantillas empleadas en casos reales. Pasando del enfoque de evaluación de la madurez a un enfoque de normativa, Carlos Manuel Fernandez de AENOR y Magdalena Arcilla de la Universidad Nacional de Educación a Distancia dieron un repaso a todos los aspectos clave de la norma ISO20000 desde los beneficios, las consideraciones clave en cada proceso ITIL, para terminar hablando del proceso de certificación. Pasando de las certificaciones de las organizaciones a las certificaciones de

profesionales, Luis Miguel Rosa Nieto de EXIN analizó que aportan las certificaciones a los profesionales que las obtienen, cuales son las más conocidas en el ámbito de las TI en España y la demanda que existe en el mercado por parte de las empresas de profesionales certificados.

Dos fueron los grupos de trabajo de itSMF España que expusieron sus avances. El grupo de estrategia del servicio representado por Oscar Rozalén, David Bathiely, Miguel Angel Fernández y Manuel Caño, desgranaron el proceso de planificación estratégica orientado al servicio de las TI así como la utilización del Cuadro de Mando Integral para TI como ayuda al despliegue de los objetivos estratégicos. El grupo de trabajo de gestión de proyectos representado por Inés López, Ramón Batista y Juan Carlos Vigo que se encargó de analizar cómo conseguir el cambio cultural en la implantación de ITIL, apoyándose para ello en los dos estándares más reconocidos en la gestión de proyectos: PMBOK y PRINCE2. Otra variante de la parte humana de los sistemas de la información la aportó Borja Peñuelas de ISC, que analizó los factores y conceptos que componen la usabilidad de los procesos de TI y el valor y beneficio que su adecuada usabilidad aporta.

Mesa redonda.

El cierre del congreso y punto álgido del evento se materializó en una mesa redonda en donde se contó con un plantel compuesto por reconocidas personalidades relacionadas con el mundo de los estándares TI: Carlos Manuel Fernández (AENOR), Ana Mª Rodríguez de Viguri (AETIC), Manuel Monterrubio (ALI), Francisco Antón Vique (ASTIC) y Luis Fernández Sanz (ATI). En dicha mesa redonda moderada por Marlon Molina de New Horizons, se discutió el papel de los estándares y mejores prácticas en el papel del ingeniero tecnológico y el importante papel que en la adopción de estándares juegan las Administraciones Públicas. A lo largo de la mesa redonda también se dio fe de la dificultad para encontrar profesionales tecnológicos y la importancia de asociarse y ser parte activa de las asociaciones que representan un sector que mueve un porcentaje muy significativo del PIB de España. El congreso además fue seguido vía remota por Internet en varias universidades españolas. Tanto las presentaciones como los videos pueden bajarse desde la web de itSMF España (www.itsmf.es).

Artículos anteriores publicados en RPM-AEMES

Nombre	Autor/es	Vol	Nº	Fecha
Estimación de variables en proyectos de desarrollo de software (PDS)	J. Aroba, I. Ramos, C. Riquelme	1	2	Agosto 2004
Una propuesta para la verificación de Requisitos basada en métricas	B. Bernárdez , A. Durán, M. Toro, M. Genero	1	2	Agosto 2004
Modelos segmentados de estimación del esfuerzo de desarrollo del Software: Un caso de estudio con la base de datos ISBSG	J. Cuadrado-Gallego, D. Rodríguez, M.A. Sicilia	1	2	Agosto 2004
Proceso y herramientas para la productividad en el aseguramiento y medición de calidad en desarrollos java	L. Fernández, P. Lara	1	2	Agosto 2004
Lecciones aprendidas al determinar el estado actual del área de proceso de gestión de requisitos utilizando el CMMI	J. Calvo-Manzano, G. Cuevas, T. San Feliu, A. Serrano, M. Arcilla	1	3	Diciembre 2004
Mejora de la calidad en desarrollos orientados a objetos utilizando especificaciones UML para la Obtención de precedencia de Casos de Prueba	L. Fernández, P. Lara, J. Cuadrado-Gallego	1	3	Diciembre 2004
Modelado dinámico y aprendizaje automático aplicado a la gestión de proyectos software	HERACLES	1	3	Diciembre 2004
Un procedimiento de medición de tamaño funcional: diseño y aplicación	N. Condori-Fernandez, S. Abraão, O. Pastor, S. Martí	1	3	Diciembre 2004
Estimación del esfuerzo de implantación en sistemas ERP	A. Cano, J. Tuya	2	1	Marzo 2005
Un enfoque de modelado y simulación para la comprensión del proceso de diseño centrado en el usuario	N. Hurtado, M. Ruíz, J. Torres	2	1	Marzo 2005
Estimación del esfuerzo de un proyecto software utilizando el criterio mdl-em y componentes normales n-dimensionales	Miguel Garre Rubio, Mario Charro Cubero	2	1	Marzo 2005
Optimización de Métrica Versión 3 en entornos orientados a objetos	J. L. López-Cuadrado, Á. García-Crespo, B. Ruiz-Mezcua, I. González-Carrasco	2	2	Agosto 2005
Experiencias de las administraciones públicas españolas en los procesos de gestión de requisitos y gestión de subcontratación	J.A. Calvo-Manzano, G. Cuevas, I. García, T. San Feliu, A. Serrano, F. Arboledas, F. Ruiz de Ojeda	2	2	Agosto 2005
El factor humano: instrumentos de medida competencial y estimación software	R. Colomo Palacios, E. Tovar Caro, J. Carrillo Verdún	2	2	Agosto 2005
El Papel de la Organización en la Gestión de Riesgos en Proyectos Software Aeroespaciales	Bernard, P., Salvador, L	2	3	Diciembre 2005
Evaluación de la exactitud de un nuevo método de estimación ágil	Fernando Machado, Luciana Calcagno	2	3	Diciembre 2005
Utilización de QFD en la toma de decisiones para la estructuración de una familia de productos	Montse Ereño, Rebeca Cortazar	2	3	Diciembre 2005
Indicadores Empíricos Formales y muy Tempranos de Complejidad Esencial de Sistemas de Gestión Intensiva de Datos: Un Modelo Conceptual	Pedro Salvetto, José Carrillo, Oscar Marbán, Julio Fernández, Juan Carlos Nogueira, Javier Segovia	3	1	Abril 2006
Project Management Improvement in Extreme Programing	Houda Zouari Ounaies, Yassine Jamoussi2, Mohamed Ben Ahmed	3	1	Abril 2006
Quality Through Test Management in Production Management Vision on Software Production Lines	Giovani Salvadori	3	1	Abril 2006
MECHDAV: un modelo y su herramienta para la evaluación técnica de la calidad de las herramientas RAD para ambientes visuales	L.S. Vargas, A. G. Gutiérrez, E. M. Felipe	3	2	Septiembre 2006
Applying Software Process Metrics in Business Process Models	E. Rolón, F. Ruiz, F. García, M. Piattini	3	2	Septiembre 2006
Desarrollo de productos de software seguros en sintonía con los modelos SSE-CMM, COBIT e ITIL	Edmundo Tovar C., José Carrillo V., Vianca Vega Z., Gloria Gasca H.	3	2	Septiembre 2006
Recomendaciones para el desarrollo del capital	Ricardo Colomo Palacions, Edmundo	4	1	Enero 2007

Nombre	Autor/es	Vol	Nº	Fecha
humano desde la perspectiva de la mejora del proceso software	Tovar Caro, Juan M. Gómez Berbis, Ángel García Crespo			
Team Software Process (TSP): mejoras en la estimación, calidad y productividad de los equipos en la gestión del software	Bayona, S., Calvo Manzano, J., Cuevas, G., San Feliu, T.	4	1	Enero 2007
Desde ISO 9001 hacia CMMI, pasos para la mejora de los procesos y métricas	Rolando Armas Andrade, Arturo Chamorro Gómez, Maite Montes Beobide, José A. Gutiérrez de Mesa	4	1	Enero 2007
Contribución de los estándares internacionales a la gestión de procesos software	Francisco J. Pino, Félix Garcia, Mario Piattini	4	2	Abril 2007
Asociacion tecnica de cajas de ahorros(ATCA): un plan de mejora basado en el modelo CMMI	Pablo Serrats Suárez, Alberto Villuendas Hereza, Pilar Meneses Ballestar,	4	2	Abril 2007
EXHAUSTIF®: Una herramienta de inyección de fallos por software para sistemas empotrados distribuidos heterogéneos	Antonio da Silva, José F. Martínez, Lourdes López , Luis Redondo	4	2	Abril 2007
Análisis de Fiabilidad de Sistemas Aplicando Técnicas de Crecimiento de Fiabilidad del Software	Dña. Amaya Atencia Yépez, D. Luis Redondo López	4	3	Septiembre 2007
Definición de Métricas de Calidad en el Procesos de Parametrización de Sistemas ERP	Carmen Pages, Luis de-Marcos, José-Javier Martínez, José-Antonio Gutiérrez	4	3	Septiembre 2007
Análisis del Valor de un Proyecto en el Marco del Método Parker	Helena Garbarino1 José Carrillo Verdún	4	3	Septiembre 2007
Benchmarking is an essential control mecanism for management	Ton Dekkers	4	4	Octubre 2007
Changing from fpa to cosmic a transition framework	H.S. van Heeringen	4	4	Octubre 2007
Modelo de gobierno de una factoría software	Aurelio Gandarillas Cordero, Mamdouh El Cuera	4	4	Octubre 2007
Case study of a successful measure-ment program	Pam Morris	4	4	Octubre 2007
Cuadro de mando para la gestión integrada	Douglas Wagner	4	4	Octubre 2007
Increase ict project success with concrete scope management	Carol Dekkers, Pekka Forselius	4	4	Octubre 2007
Capacitación de recursos testing	Miguel Ángel García Palomo, Mamdouh Elcuera	4	4	Octubre 2007
Calidad en modelos conceptuales: un análisis multidimensional de modelos cuantitativos basados en la iso 9126	Beatriz Marín, Nelly Condori-Fernández, Oscar Pastor	4	4	Octubre 2007
Kemis: entorno para la medición de la calidad del producto software	Moisés Rodríguez, Marcela Genero, Javier Garzás, Mario Piattini	4	4	Octubre 2007
Análisis del valor de un proyecto de TI en el marco del método Parker	Helena Garbarino, José Carrillo Verdún	5	2	Enero 2008
Gobierno de la externalización del proceso software	Ángel Sánchez, Jezreel Mejía,Gonzalo Cuevas	5	2	Enero 2008
Gestión de los riesgos tecnológicos	Luis Martín Romeral, Álvaro Torres Gallego	5	2	Enero 2008

Llamada a la participación Revista Procesos y Métricas

Uno de los principales objetivos de esta revista es que aquellas entidades y organizaciones interesadas **participen** en ella. Y por ello le instamos tanto a usted como a su institución para que realicen contribuciones, o envíen sus comentarios y sugerencias. Actualmente estamos abiertos a la recepción de trabajos para el próximo número que cubra los siguientes tópicos:

- Artículos académicos.
- Casos prácticos o casos de éxito (success histories) de aplicación de métricas y procesos de tecnologías de la información en organizaciones
- Artículos de difusión que traten conceptos teóricos, básicos, novedosos, etc… explicados de forma amena, o que traten aspectos relacionados con la difusión y empleo de ciertas técnicas, métricas o procesos.
- Información sobre noticias, eventos, etc…

La revista se edita en formato electrónico y papel (ambas con ISSN propio), y es accesible a través de su web: http://www.aemes.fi.upm.es/rpm/rpm.php. Consulte la 'Guía para Autores' publicada en este número o visite la web para más información sobre el formato de las contribuciones.
Esperamos sus contribuciones en: rpm@aemes.org

Información sobre el congreso "Sólo Requisitos"

Que se celebra en Madrid del 16 al 20 de Junio, y que organizamos desde el portal www.CalidaddelSoftware.com.
La asistencia a las Jornadas del 19 y 20 de Junio es GRATUITA para las inscripciones recibidas hasta el 9 de Junio, comunicadas por correo electrónico a soloreq2008@CalidaddelSoftware.com indicando en el asunto "Inscripción gratuita en SoloReq2008", y confirmadas por la organización telefónicamente entre el 10 y el 13 de Junio a cada inscrito. Aforo limitado. Como agradecimiento a la difusión que AEMES haga entre sus ASOCIADOS:

- Los ASOCIADOS de AI2 tendrán un descuento del 20% en su inscripción en cursos y jornadas técnicas del evento.
- Como entidad colaboradora, incluiremos su banner en el brochure de "Sólo Requisitos" que tendrá una difusión a través del portal y otros medios estimada en 10.000 descargas

"Sólo Requisitos 2008" tendrá lugar en Madrid del 16 al 20 de Junio. Durante las jornadas de experiencias, tendrá lugar la presentación de 12 ponencias, además , la celebración de una Mesa Redonda sobre "La Gestión de requisitos clave para el éxito de la externalizacion del software" y una Ponencia Magistral "Un enfoque práctico en la interpretación de las recomendaciones de CMMI para los procesos de gestión y desarrollo de requisitos". En el programa destacan las ponencias técnicas sobre:

"La gestión de requisitos en la subcontratación de proyectos. Recomendaciones de CMMI-ACQ"
"Los procesos de requisitos y las metodologías ágiles: un caso basado en SCRUM".

El programa actualizado se puede descargar desde:
http://www.calidaddelsoftware.com/modules.php?name=News&file=article&sid=279

Las jornadas SLO REQUISITOS 2008 (JORNADAS PRÁCTICAS SOBRE GESTIÓN E INGENIERÍA DE REQUISITOS DEL SOFTWARE Y EL MODELO DE MEJORA CMMI®. LOS REQUISITOS Y EL OUTSOURCING DEL SOFTWARE) se celebrarán en el Auditórium de Atos Origin en la calle Albarracín 25 de Madrid durante los 19 y 20 de Junio, mientras que los tres días anteriores se impartirán seminarios de formación específica sobre CMMI, métricas, reutilización, pruebas y CobiT. Adicionalmente se ha programado una edición del seminario de "Introducción a la Ingeniería de Requisitos" el día 24 de Junio.

ASOCIACIÓN ESPAÑOLA DE MÉTRICAS DE SISTEMAS INFORMÁTICOS AEMES
Facultad de Informática de la UPM. Campus de Montegancedo. 28660-Boadilla del Monte (Madrid)
Teléfono: 91 336 66 08. Fax: 91 336 74 12. E-mail: admon@aemes.org

FORMULARIO DE INSCRIPCIÓN A AEMES

Información Personal
Apellidos: Nombre:
Teléfono: e-mail:
Dirección Personal:
Empleo:

Inscripción Institucional o Empresarial
Institución o Empresa: C.I.F.:
Dirección:

Datos Bancarios
Número de Cuenta:
Titular:

Autorizo a AEMES a cargar a la cuenta arriba indicada la cuota Anual de inscripción que asciende a 360 € + la cuota de inscripción que asciende a 150 €

Fecha y Firma

FORMULARIO DE INSCRIPCIÓN A RPM (Revista de Procesos y Métricas)

Información Personal
Apellidos: Nombre:
Teléfono: e-mail:
Dirección Personal:
Empleo:

Inscripción Institucional o Empresarial
Institución o Empresa: C.I.F.:
Dirección:

Datos Bancarios
Número de Cuenta:
Titular:

Autorizo a AEMES a cargar a la cuenta arriba indicada la cuota Anual de subscripción a RPM que asciende a 60 € + Gastos de Envío

Fecha y Firma