ISSN: 1698-2029 Volumen 5 Número 3

OCTUBRE 2008

Revista de

Procesos y Métricas

de las tecnologías de la información

CONTENIDOS

EL BUEN GOBIERNO DE LA SEGURIDAD. *Miguel Ángel Thomas* ……...…*57*

GOBERNADOR DE TI: NACE UN NUEVO PUESTO EN EL NIVEL DIRECTIVO *Miguel García Menéndez* …….……..…….....*64*

LA GESTIÓN CUANTITATIVA EN CMMI. RELACIÓN CON SPC Y SEIS SIGMA. *Anabel Manchón Diez*……...……...……...……..*67*

DE LA GESTIÓN POR PROCESOS AL B.P.M. *Dr. Montgomery Lee, PDF , Ignacio Fernández*……...……...……...*72*

ENTERPRISE AND IT ARCHITECTURE: LAS CLAVES DEL GOBIERNO DE TI *Ángel Sánchez*……..……...…….....*77*

PRUEBAS DE SEGURIDAD EN EL MARCO DE UNA FACTORÍA DE CALIDAD DE PRODUCTO SOFTWARE. *Jesús Pérez Cristóbal*……..……...…...*82*

Revista de Procesos y Métricas de las Tecnologías de la Información

Volumen 5 Número 3

Revista fundada por la Asociación Española de Métricas del Software (AEMES)

<http://www.aemes.org>

ISSN: 1698-2029
Nº Depósito: M23879-2006

Maquetación
Luis de Marcos
Ana Belén Sánchez Díaz

Impresión
Imprenta UAH

Asociación Española de MÉtricas del Software (AEMES)

1. Propósito de la Sociedad

La Asociación Española de Métricas de Sistemas Informáticos (AEMES) es una asociación sin ánimo de lucro y con plena capacidad de obrar y personalidad jurídica y patrimonial y con un funcionamiento plenamente democrático, tal y como exige el artículo 7.1 g) de la ley orgánica 1/2002 de 22 de marzo.

La Asociación AEMES tiene por finalidad última contribuir a la difusión de los métodos y técnicas relacionados con la gestión cuantitativa de las Tecnologías de la Información y en particular con aquellos aspectos relacionados con la mejora del proceso de desarrollo del software y su gestión económica, en las empresas e instituciones que las desarrollan o utilizan, promoviendo el uso de indicadores, métricas y cuadro de mando en las mismas.

Con este fin dirige sus actuaciones a:

a) Promover, coordinar y desarrollar actividades relacionadas con las medidas de los procesos de las Tecnologías de la Información.

b) Favorecer el intercambio de información y experiencia entre los profesionales relacionados con este tema.

c) Relacionarse con otras organizaciones internacionales afines.

d) Difundir información al público en general sobre la gestión económica de las Tecnologías de la Información.

e) Crear comités y grupos de trabajo especializados en estos temas.

f) Canalizar la formación de especialistas en este campo, facilitando el acceso a titulaciones específicas y en concreto las promovidas por el International Function Points Users Group.

g) Canalizar las peticiones de certificaciones de puntos función y de otras métricas del software relativas a aplicaciones solicitadas por empresas.

h) Homologar y mantener un registro de profesionales, material docente y otros que puedan ser utilizados para los fines de la asociación.

2. Asociados

La asociación se compone de dos clases de asociados: Miembros de Número y Miembros Honoríficos.

Los Miembros de Número son las personas físicas o entidades que participan regularmente en las actividades de la asociación. La asociación está abierta, sin discriminación, a todas las personas físicas o entidades, sean estas organizaciones públicas o privadas, que están interesadas en promover los fines y actividades de la asociación.

Los miembros de Número ingresan en la asociación previa solicitud dirigida a la junta directiva (El formulario se encuentra las páginas finales de esta revista).

3. Beneficios de la Asociación

Los miembros de Número gozan de la plenitud de derecho en orden a participar en los Órganos de Gobierno de la asociación, tanto en la Asamblea General como en la Junta Directiva, siempre con sujeción a lo previsto en los estatutos y de acuerdo con las directrices y normas fijadas por la Junta Directiva.

Los miembros de Número tienen derecho a participar en las actividades y actos sociales en la forma, en que cada caso, disponga la Junta Directiva.

Los miembros de Número tienen derecho a recibir sin coste alguno las publicaciones periódicas realizadas por la asociación.

4. Publicaciones de la Asociación

Boletín de la Asociación Española de MÉtricas de Sistemas informáticos.
Publicación de periodicidad trimestral cuyo contenido está centrado fundamentalmente en la actividad interna de la asociación. Se describen también nuevos recursos como libros o herramientas software de interés para los asociados. También se comentan aquellos eventos de especial relevancia relacionados con la gestión de los Procesos de las Tecnologías de la Información y las Comunicaciones.

Revista de Procesos y Métricas de las Tecnologías de la Información.
Publicación de periodicidad cuatrimestral cuyo contenido está formado por artículos científicos revisados por pares y enfocados en las áreas de interés de la asociación.

EL BUEN GOBIERNO DE LA SEGURIDAD

Miguel Ángel Thomas

Resumen: La seguridad en los sistemas de información y la organización entorno a la misma es una preocupación creciente en las empresas y organizaciones actualmente. El presente artículo explica la evolución actual del Gobierno de la Seguridad en las empresas, el ciclo de vida del programa de seguridad así como los principios y áreas de gobierno. El enfoque del artículo se basa en nuestra experiencia real en la implantación del Gobierno de la Seguridad dentro de grandes organizaciones.

Abstract: Information Systems security procedures and supporting organization is becoming an increasing concern among enterprises. This paper deals with the evolution of the IT Security Governance in different organizations, the Security Program Lifecycle and the fundamental application areas and principles. The approach displayed in this article is based on our experience in several project engagements, deploying Security Governance framework in big corporations.

Palabras clave: Gobierno de las Tecnologías de la Información, Seguridad Informática, Gestión de Riesgos Tecnológicos.

1. SITUACIÓN ACTUAL

La evolución actual del Gobierno de la Seguridad en las empresas, generalmente representados por los departamentos de Seguridad, se centra principalmente en el concepto de "Seguridad Distribuida". En la práctica el ámbito de la seguridad dentro de una organización abarca normalmente todas las áreas y departamentos:

- **desde la propia infraestructura técnica** (hardening, parcheado sistemas, segmentación de redes, …)
- **pasando por el ciclo de vida del SW (**toma de requerimientos de seguridad en las primeras fases, desarrollo de módulos seguros, buenas prácticas de codificación, pruebas de seguridad).
- **teniendo en cuenta los aspectos legales y regulatorios de aplicación a toda la organización** (LOPD, LSSI, SOX, MIFiD, etc)**.**
- **llega incluso a tomar de decisiones estratégicas a nivel comercial** (uso de certificados digitales, implementar la seguridad como un valor diferencial por ejemplo en dispositivos móviles, etc.)

Por lo tanto, es realmente difícil que un único departamento de Seguridad sea capaz de ejecutar directamente todas las iniciativas en cada uno de los ámbitos de aplicación.

En la práctica, las tareas diarias que realizan los departamentos de Seguridad dependen directamente del nivel al que reporten y dónde estén ubicados. Por ejemplo no es lo mismo un departamento de Seguridad que está dentro del área de TI y reporta a la dirección de sistemas que un departamento de Seguridad que reporta directamente al CEO y está a la 'altura' de las direcciones de Negocio.

No obstante, generalmente el Gobierno de la Seguridad en una organización suele centrarse en dos tipos de actividades claramente diferenciadas:

- Por un lado, existe una primera etapa en dónde se define un framework de Seguridad para toda la organización y se definen una serie de controles que se deben de cumplir en la mima. Tras esa etapa, el área de Seguridad se ocupa de 'controlar' que el resto de áreas y departamentos de la organización implementan y cumplen dichos controles. Es

decir, el área de seguridad coordina, controla, supervisa y da soporte al resto de áreas para que la seguridad se implemente correctamente.

- Además suelen existir un conjunto de proyectos que ejecuta directamente (o subcontrata) y que son únicamente de su competencia. Ejemplos pueden ser los Sistemas de Gestión de la Seguridad (ISO27001) o implementaciones de Sistemas de Gestión de Identidades o Consolas Centralizadas de logs, etc.

Otro dato importante que hay que tener en cuenta dentro del ámbito del Gobierno de la Seguridad, es que en la actualidad, cada vez más se están creando departamentos de Seguridad con personal especializado. Además muchos de estos cuentan con apoyo externo a la propia organización.

2. PROCESOS DE GOBIERNO

El Gobierno de la Seguridad debe dar cobertura a todos los componentes básicos de un programa de seguridad, cubriendo las tareas básicas solicitadas por las áreas de negocio y la alta dirección de la organización.

Actualmente la norma más extendida que indica los diferentes puntos de control sobre la seguridad en cualquier organización, sin lugar a duda es la ISO27001/ISO27002.

Alrededor de este modelo se debería estructurar el Gobierno de la Seguridad, no obstante debe ser siempre una guía que ayude a la organización y nunca debe llegar a convertirse en un elemento que complique u obstaculice la seguridad. También me gustaría indicar que el hecho de utilizar la ISO27001 como modelo de referencia no tiene porqué implicar que la organización 'tenga que' certificarse contra esta norma.

Es preferible ir implementando paulatinamente los controles más necesarios y si llega el momento plantearse la certificación. El camino contrario es más costoso y penoso, no garantizando llegar a gestionar correctamente la seguridad.

El gráfico que a continuación se muestra indica el proceso de gestión, a alto nivel que debería realizar el Área de Gobierno de la Seguridad:

Figura 1. Ciclo de Vida del Programa de Seguridad.

- **Estrategia.** A partir de la propia estrategia de negocio de la organización se deben identificar los nuevos objetivos y estrategias de seguridad. Esta estrategia debe estar soportada en los estándares de gestión de la seguridad y debe cumplir con la normativa y regulación actual, además de evidentemente dar soporte a los objetivos del negocio.
- **Política.** El área de seguridad debe crear, revisar y mejorar la política, normas y procedimientos de seguridad de la organización en base a estándares y buenas prácticas reconocidas internacionalmente y a las directivas del negocio.
- **Concienciación.** Un tema imprescindible que debe promover directamente el área de seguridad es la concienciación, sensibilización y formación. Debe promover el conocimiento y utilización

de los recursos de seguridad entre los usuarios de los sistemas de la organización diseñando y desarrollando planes de formación y concienciación y liderando iniciativas encaminadas a la implantación de dichas medidas.

- **Implementación.** Debe realizar tareas de gestión en la implementación de los proyectos asignados al área de seguridad de la información. Realizar tareas de detección de desviaciones, soporte técnico y análisis de seguridad, proponiendo las medidas preventivas y/o correctivas que se estimen oportunas. Gestionar las actividades encaminadas a la implantación de los controles de Seguridad definidos por la organización interactuando con las áreas de negocio y tecnología implicadas.
- **Monitoreo.** Una función muy importante que debe realizar el área de seguridad son las revisiones del funcionamiento de los procesos de seguridad ya implantados. Es imprescindible disponer de métricas y cuadros de mando que permitan conocer en todo momento el estado y la eficacia de los controles implantados.
- **Cumplimiento.** Detectar, proponer e implantar las acciones necesarias para cumplir con el marco legal vigente que afecta al desarrollo del negocio de la organización desde el punto de vista del área de seguridad.

3. PRINCIPIOS DEL BUEN GOBIERNO

De acuerdo a los requisitos de alto nivel expresados anteriormente, es importante establecer una serie de criterios que deberemos tener en cuenta en la definición de la función de seguridad:

- **Principio de independencia.** La función de seguridad no debe estar condicionada en el nivel táctico y operativo por otras funciones dentro de la organización.
- **Principio de resolución de intereses.** La función de seguridad debe estar definida de tal manera que se garantice el no conflicto de intereses, y en el caso de que esto se presenten en alguna de sus funciones, debe proveer los mecanismos necesarios para solventarlo.
- **Principio de autoridad.** La función de seguridad debe disponer de la autoridad necesaria para ejercer sus funciones con las garantías correspondientes.
- **Principio de universalidad.** La función de seguridad debe tener carácter global y único dentro de la organización.
- **Principio de responsabilidad.** La función de seguridad será la responsable de todos los aspectos relacionados con la seguridad dentro de la organización.

4. ÁREAS DE GOBIERNO

Otro modo de enfocar el gobierno de la seguridad, en vez de a nivel de procesos, es hacerlo según las competencias que deba de asumir en la organización. Evidentemente, y tal y como se ha presentado al inicio del presente artículo, estas competencias dependerán mucho del nivel de interlocución que tenga en la organización.

No obstante, y de un modo genérico las competencias se podrían agrupar como sigue:

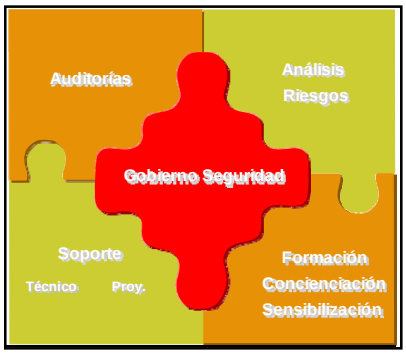

Figura 2.

El área de **Gobierno de la Seguridad** trabaja en temas relacionados con los estándares, políticas, procedimientos de Seguridad, incluyendo la vertiente legal. Aquí se muestran una serie de tareas que podría realizar:

- Definir y mantener la Política de Seguridad que será de aplicación a toda la organización.
- Definir las Normas y Estándares de Seguridad que aplicarán a todos los equipos involucrados en la definición, implantación y mantenimiento de la Seguridad (normas de desarrollo de SW, normas de securización de máquinas, normas de control de accesos, salida de soportes, etc…).
- Selección de Controles ISO27002, PCI-DSS, ISO15408, SOX, LOPD/RMS, etc. que aplicarán a toda la organización. Validación de los controles con la Dirección la organización y redacción del SOA (lista de controles aplicables).
- Revisión y aprobación de los procedimientos de seguridad asociados a los diferentes equipos (manuales de instalación de SW, HW, etc…).

El **área de Auditorías** se ocupa fundamentalmente de la revisión de la implantación del framework definido. También, dentro del ámbito de la legislación Española trabaja en la auditoría de LOPD, auditorías de vulnerabilidades e implantación de las medidas exigidas en el Reglamento de Medidas de Seguridad. Aquí se muestran una serie de tareas que podría realizar:

- Crear el programa de Auditoría y seguimiento de controles.
- Crear la metodología asociada a las auditorías.
- Realizar auditorías de cumplimiento normativo legal: LOPD y LSSI.
- Realizar auditorías de cumplimiento normativo de estándares: ISO27001, ISO 15408 y PCI-DSS.
- Realizar pruebas de vulnerabilidades de las plataformas.
- Seguimiento y soporte a las acciones correctivas.

El área de **Análisis de riesgos** trabajará con todos los temas relacionados con el análisis y gestión de riesgos de los Sistemas de Información, generalmente trabaja con las metodologías como Magerit, CRAMM o ISO 13335-3, ISO27005. Aquí se muestran una serie de tareas que podría realizar:

- Inventario y clasificación de activos.
- Análisis de vulnerabilidades de los sistemas.
- Identificación de amenazas.
- Ejecución de BIA (Análisis de Impacto en el Negocio) para evaluar el impacto.
- Selección de Salvaguardas.
- Evaluación del Riesgo.
- Gestión de Riesgo (implantación y seguimiento de controles).

El área **Formación, Concienciación y Sensibilización** tiene como uno de los principales objetivos que todos los proveedores y el propio personal de la organización, conozcan y estén sensibilizados en materia de confidencialidad, requerimientos legales y técnicos de obligado cumplimiento por la normativa en materia de protección de datos de carácter personal y en Seguridad en general. Aquí se muestran una serie de tareas que podría realizar:

- Presentaciones divulgativa de la importancia de la Seguridad y de saber qué tiene que hacer cada persona en caso de tratar ficheros con datos personales, detectar incidentes de seguridad y de las implicaciones de no hacerlo.
- Creación de trípticos auto explicativos.

- Creación de tests para que cada persona pueda conocer si sabría cómo actuar en caso de un incidente de seguridad (esta tarea, aunque sea genérica permite que el usuario 'reclame' formación).
- Elaborar mensajes estándar de correo electrónico para que sean divulgados.
- Jornadas de formación sobre las políticas, estándares y procedimientos de trabajo en materia de protección de datos y medidas de seguridad. Estos mensajes serán diferentes en función de los perfiles que se determinen como audiencia objetivo, en principio se plantearían tres tipos de perfiles: perfiles directivos (alta dirección), perfiles gestores y perfiles usuarios/operadores.

El **área de Soporte** se ocupa del soporte, tanto técnico como a nivel de desarrollo de las aplicaciones, generalmente tiene amplios conocimientos en aspectos relacionados con la instalación y configuración de firewalls, antivirus, sistemas de detección de intrusos, desarrollo seguro, etc. Las principales tareas que realiza son las siguientes:

- Gestión de los requisitos de Seguridad, su objetivo principal es el estudio de todos los requisitos de Seguridad: ver como se 'empaquetan' en las diferentes implantaciones (planificación de los requisitos de seguridad, gestión de alcance para nuevos requisitos de seguridad, gestión de los cambios de alcance en las releases e implantaciones existentes, evaluar los análisis funcionales y diseños técnicos para identificando el impacto en la Seguridad)
- Realizar el aseguramiento de la Seguridad de los desarrollos implicados en los diferentes entornos, asegurar el conocimiento y aplicación de los estándares de desarrollo definidos (mantenimiento y aplicación de estándares y mecanismos de aseguramiento de la seguridad establecidos por el área de Gobierno, control y seguimiento de los ciclos de pruebas, etc…).
- Gestión de los entornos y evoluciones tecnológicas de la Seguridad (gestión de la configuración de la seguridad, estudios de viabilidad de mejoras de la aplicación y evolución tecnológica de los entornos en materia de seguridad, coordinación del paso a producción de los sistemas de seguridad como antivirus, firewalls, ids, etc...)
- Coordinación de las líneas de trabajo entre los entornos no productivos y productivos.
- Diseño, configuración y monitorización del sistema de detección de intrusiones, consola de logs, instalación y configuración de las herramientas para el análisis de vulnerabilidades, etc

5. INTEGRACIÓN DEL GOBIERNO DE SEGURIDAD EN EL CICLO DE VIDA DE LOS PROYECTOS

Por último y a modo de ejemplo, vamos a mostrar cómo se puede integrar el Gobierno de la Seguridad en el Ciclo de Vida de los Proyectos. Las competencias que asumirá el Gobierno de la Seguridad, en este caso, están orientados a cubrir las necesidades de gestión de proyectos de seguridad y de resolución de incidencias o dudas dentro del ámbito de la seguridad de una organización.

En este sentido, la gestión de proyectos de Seguridad se realizará en función del estado del ciclo de vida de los proyectos (viabilidad de proyectos, proyectos nuevos y mantenimientos) y de la interrelación existente entre los mismos:

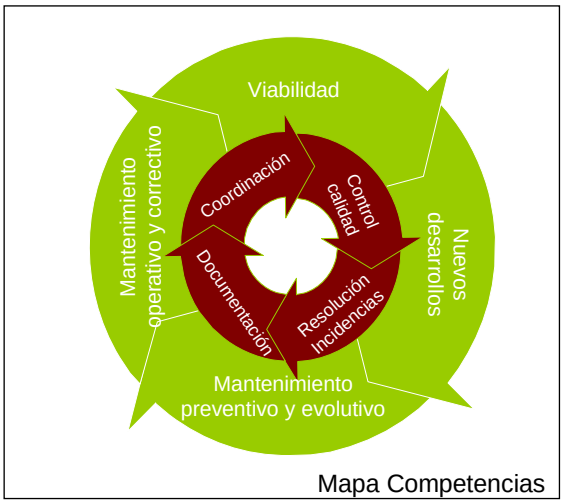

Figura 3. Mapa de Competencias.

- **Viabilidad de Proyectos - Análisis de proyectos.** En este caso el área de Seguridad realiza tareas de análisis de viabilidad de los requisitos de seguridad para los proyectos solicitados por los responsables del negocio o técnicos. Se identifican los requerimientos técnicos y funcionales de Seguridad necesarios y se propone su viabilidad para la integración en la arquitectura de seguridad existente.
- **Nuevos desarrollo.** Los responsables de la organización plantean al área seguridad los proyectos nuevos que se desean ejecutar, describiendo los requerimientos técnicos y funcionales de los mismos y su propuesta del nivel de seguridad que pretendan dotarles, a alto nivel.

Partiendo de esta información y del conocimiento que dispone el área de seguridad de la arquitectura de aplicaciones de la organización, el área de seguridad analizará los requerimientos individuales de seguridad y su integración en la arquitectura de seguridad ya desplegada (SAS 70, SOX, LOPD, LDAP, TIM, PKI, comunicaciones, etc.) y propondrá los controles necesarios para conseguir el nivel de seguridad propuesto.

Para los controles propuestos se adjuntarán las estimaciones a alto nivel de coste/beneficio con el fin de ayudar a los responsables a seleccionar los controles más adecuados en cada momento para cada nuevo desarrollo.

- **Mantenimiento preventivo y evolutivo.** Para las aplicaciones/sistemas ya existentes se revisa su nivel actual de seguridad y los controles que están implantados. Se analiza su grado de efectividad y el beneficio que aporta. Se toma como referencia los requerimientos de seguridad planteados internamente por la normativa de seguridad vigente y se priorizan las iniciativas de seguridad para cada sistema/aplicativo.

El área de seguridad se encarga de realizar el seguimiento de los proyectos en donde está involucrados los requerimientos de seguridad y colaborando en las pruebas que sean necesarias.

Además, el área de seguridad se encarga de la supervisión de los pasos a producción de los controles, gestionando los recursos necesarios y proponiendo las fechas más convenientes para minimizar el impacto de los mismos y asegurar su correcto funcionamiento.

- **Mantenimiento operativo y correctivo.** El área de seguridad realiza las tareas de gestión del mantenimiento operativo y correctivo de la misma forma que el mantenimiento preventivo y evolutivo pero teniendo en cuenta las características de este tipo de proyectos.
- **Coordinación de actividades.** Realiza funciones de coordinación de proyectos multi-sistema, independientemente de los equipos y/o proveedores implicados. Estos proyectos tienen como elemento común la seguridad.

- **Control de calidad.** El área de seguridad realiza las tareas de revisión de calidad siguiendo los estándares y metodologías proporcionadas por el marco de seguridad de la organización de forma que se garantiza la calidad de los proyectos en los que intervenga el área de seguridad.

Revisa la calidad de los entregables relacionados con los entornos productivos de forma que evaluará su validez en función de los estándares fijados y su cumplimiento con los requerimientos de seguridad solicitados. Colaborará definiendo planes de pruebas y ejecutando las pruebas que sean necesarias para aprobar los pasos a producción desde el punto de vista de seguridad.

- **Documentación.** El área de seguridad se encarga de generar la documentación requerida para realizar el seguimiento de las tareas que realiza utilizando los formatos estándares de la organización. Toda la documentación generada queda a disposición de la organización en los repositorios que ésta designe.
- **Escalado y resolución de incidencias.** El área de seguridad se encarga de la gestión de las incidencias dando el soporte necesario a los responsables de la organización, tanto internos como externos, que se puedan ver involucrados en la resolución de las mismas.

6. REFERENCIAS.

[1] "CISM, Certified Information Security Manager, Review Manual 2008" ISACA.

[2] JTC 1/SC 27. "ISO/IEC 27001:2005", International Standards for Business, Government and Society.

[3] "COBIT 4.1", IT Governance Institute

[4] "Governing for Enterprise Security Implementation Guide", CERT

GOBERNADOR DE TI: NACE UN NUEVO PUESTO EN EL NIVEL DIRECTIVO

Miguel García Menéndez
Atos Consulting
miguel.gmenendez@atosorigin.com

Resumen: "El IT Governance está aquí para quedarse". Como ya ocurriera a principios de esta década con la Seguridad, hoy la palabra de moda es, sin duda, Gobernanza. Eso, al menos, parecen indicar todas las alarmas, a la vista del creciente interés sobre el tema que ha venido observándose, en el último año y medio, en el mercado español. Bajo esa premisa, el presente artículo propone la creación de una nueva figura en las organizaciones: el Gobernador de las TIC, y describe un posible perfil para estos nuevos directivos. A partir de ahí, se plantean una serie de dudas: ¿están los actuales responsables de Tecnología preparados para asumir ese nuevo papel?, ¿constituye, para ellos, una oportunidad única de ascender al nivel directivo? ¿cabría pensar que el perfil descrito debería ser, también, el de los profesionales que asesoran a las organizaciones en este ámbito? ¿Existe algún tipo de iniciativa formativa orientada a ayudar a moldear a los actuales profesionales en la horma de la nueva figura?

Abstract: Information Systems security procedures and supporting organization is becoming an increasing concern among enterprises. This paper deals with the evolution of the IT Security Governance in different organizations, the Security Program Lifecycle and the fundamental application areas and principles. The approach displayed in this article is based on our experience in several project engagements, deploying Security Governance framework in big corporations.

Palabras clave: Buen gobierno corporativo de las TIC, Gobernador de TI, CGO, CGEIT.

1. INTRODUCCIÓN

Los Consejos de Administración y las Direcciones Generales han comprendido, desde hace tiempo, la necesidad de establecer marcos de buen gobierno corporativo. Esto se hace particularmente evidente si se tienen en cuenta las crecientes obligaciones en materia de conformidad regulatoria.

Más aún, los Sistemas de Información, y las Tecnologías de la Información y las Comunicaciones que los sustentan, han adquirido una gran relevancia en el logro de los objetivos corporativos y en la entrega de beneficios. Ello ha llevado a un importante número de organizaciones a darse cuenta de que la *gobernanza* ha de extenderse también al ámbito tecnológico; hasta tal punto, que, hoy en día, el buen gobierno de las TI es considerado una parte integrante de la gobernanza corporativa, como medio de apoyar y reforzar las estrategias y objetivos de la organización.

Este escenario (con una creciente demanda, por parte del negocio, de la aportación que ofrece la tecnología; y con una superior concienciación sobre la importancia de contar con buenas prácticas y modelos) abre un claro camino hacia el desarrollo y despliegue de la **Gobernanza de TI**.

Como parte de este "despliegue", y dado que la dirección (gobierno) de las TI ya no ha de verse como una preocupación exclusiva de la Dirección de Informática, sino de la alta dirección en su conjunto, está surgiendo una nueva figura a nivel directivo: el **Gobernador corporativo de TI** (*Chief [IT] Governance Officer*, o CGO, como recogería la bibliografía anglosajona).

Como ventaja añadida, el establecimiento de un puesto tal, dentro de la organización, supondrá una demostración palpable del compromiso de aquella con la excelencia en las buenas prácticas de gobernanza de TI.

2. CON LA MIRA PUESTA EN EL NEGOCIO

En el nuevo contexto, la misión del gobernador de TI será proporcionar el debido apoyo al Consejo de Administración y a la Dirección General, maximizando la contribución hecha por las Tecnologías de la Información al éxito de la organización y, al mismo tiempo, gestionando y mitigando los riesgos derivados del uso que se hace de la propia tecnología.

3. EL PERFIL

Entre las responsabilidades (o, dicho de otro modo, habilidades) de los profesionales que desarrollen su actividad entorno a la gobernanza de las TI en sus respectivas entidades, cabe descatar las siguientes:

- deberán conocer las actuales tendencias, así como los principales modelos organizativos y de dirección de TI, y saber armonizar y canalizar su valor para la entidad. Esta meta se alcanzará mediante el **establecimiento de procesos de implantación y despliegue de dichos marcos de referencia para el gobierno, la dirección y el control de las TI** a lo largo y ancho de la organización;
- deberán ser capaces de asegurar que las TI actuan como catalizador para el logro de los objetivos del negocio, mediante la integración de los planes estratégicos de TI con los planes estratégicos de la organización y mediante la sincronización de los servicios prestados desde TI con las operaciones de la compañía para optimizar los procesos de negocio. A ello contribuirá el **desarrollo de una estrategia tecnológica de la empresa**;
- deberán, asimismo, encargarse de garantizar que, tanto TI, como las áreas de negocio, cumplen con sus responsabilidades sobre la gestión del valor: esto es, que las nuevas inversiones en actividades apoyadas en tecnología producen el beneficio esperado y aportan un valor al negocio, medible, tanto invididual, como colectivamente; que las capacidades (soluciones y servicios) son entregados en tiempo y coste; y que los servicios y otros activos de TI contribuyen de manera contínua al valor del negocio. Todo ello, mediante el **desarrollo de un proceso de gobierno del valor**;
- adicionalmente, los gobernadores de TI deberán asegurar la existencia y puesta en marcha de marcos apropiados, alineados con las normas y modelos de referencia, para identificar, evaluar, mitigar, gestionar, comunicar y supervisar los riesgos del negocio relacionados con las TI, como una actividad más del buen gobierno de la empresa. Todo ello, mediante el **desarrollo, mejora y mantenimiento de un proceso contínuo y analítico de gestión de los riesgos empresariales**;
- estos nuevos directivos deberán ocuparse de que el área de TI disponga de recursos suficientes, competentes y capaces de ejecutar los objetivos estratégicos presentes y futuros, y de responder a las demandas del negocio, a través de una optimización de la inversión, del uso y de la ubicación de los activos tecnológicos (aplicaciones, información, infraestructuras y personal). Todo ello, mediante la **puesta en marcha de un proceso contínuo de planificación, gestión optimizada y evaluación de recursos**;
- igualmente, deberán asegurar que se establecen metas e indicadores para las TI, de apoyo al negocio, en colaboración con las partes interesadas; y que se fijen, supervisen y evaluen ciertos obje-

tivos medibles. Todo ello, mediante **procesos contínuos de gestión y evaluación del rendimiento**;

- finalmente, deberán ser capaces de actuar como impulsores del cambio cultural y organizativo dentro de la entidad; a lo cual se llegará, a través de la **activación del oportuno programa de comunicación y gestión del cambio** que habrá de mantenerse en el tiempo y en paralelo a la implantación de las nuevas prácticas y procesos adoptados dentro de la organización.

Se trata, en definitiva, de habilidades y actividades directamente relacionadas con **la definición, el establecimiento y/o el mantenimiento de un marco de referencia para la gobernanza de las TI** (materializada en liderazgo, estructuras organizativas y procesos) para: asegurar la sincronización con el buen gobierno de la entidad; controlar el entorno de TI y la información de negocio mediante la puesta en marcha de las mejores prácticas; y garantizar la conformidad con los requisitos externos.

4. UNA REFLEXIÓN FINAL

Pero, acaso, el perfil descrito ¿se corresponde solamente al esperado de un directivo encargado del buen gobierno de las TI, dentro de su organización?; o, de hecho, ¿no se tratará, también, de un catálogo de competencias con las que debería contar toda la comunidad de asesores y consultores que prestan sus servicios en el ámbito de referencia?

Tal vez la respuesta venga dada por la creciente oferta académica de postgrado que, sobre el Buen Gobierno de las TIC, diversas entidades públicas y privadas están poniendo en marcha en los últimos tiempos. La última iniciativa en este sentido, llega, una vez más, de la mano de ISACA (www.isaca.org) y su Instituto para el Buen Gobierno de las TI (www.itgi.org): bajo el acrónimo CGEIT (*Certified in the Governance of Enterprise IT*) (www.isaca.org/cgeit) propone una nueva certificación profesional, con la que tratará de reconocer las competencias y habilidades mínimas, requeridas en aquellos profesionales del sector encargados de asesorar a las organizaciones en la puesta en marcha y el mantenimiento de marcos de gobernanza de TI que permitan a sus equipos directivos atajar las actuales diferencias existentes entre los objetivos del negocio, los objetivos de la función informática y sus procesos; y comprender el modo de enfrentarse a los riesgos de la empresa que se deriven del creciente empleo de la tecnología.

5. REFERENCIAS.

[1] ISO/IEC 38500:2008. Corporate Governance of Information Technology. International Organization for Standardization, 1-6-2008.

[2] Val IT 2.0. Enterprise Value. Governance of IT Investments. IT Governance Institute, 2008.

[3] CobiT 4.1. Control Objectives for Information and related Technology. IT Governance Institute, 2007.

[4] Audit programs currently in alignment with ISACA's Model Curriculum. http://www.isaca.org/Content/NavigationMenu/Students_and_Educators/Model_Curriculum/Programs_in_Alignment/Audit_Programs_Currently_in_Alignment_with_the_Model_Curriculum.htm

[5] CGEIT, Certified in the Governance of Enterprise IT. http://www.isaca.org/Template.cfm?Section=CGEIT_Certification&CONTENTID=43651&TEMPLATE=/ContentManagement/ContentDisplay.cfm

[6] CGEIT, Certified in the Governance of Enterprise IT. Exam reference material. http://www.isaca.org/Template.cfm?Section=CGEIT_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=36126

[7] García Menéndez, Miguel. "Towards a new C-level player". IT Strategy and Technology Newsletter. Atos Consulting. August, 2007.

[8] García Menéndez, Miguel. "Gobernador de TI: Nuevo garante de la calidad de las TIC dentro de la organización". Calidad. Asociación Española de la Calidad. Febrero, 2008.

LA GESTIÓN CUANTITATIVA EN CMMI. RELACIÓN CON SPC Y SEIS SIGMA

Anabel Manchón Diez.
Sopra PROFit.

1. INTRODUCCIÓN

CMMI es uno de los modelos más conocidos y empleados a nivel mundial, y cada día más y más empresas lo emplean como estándar para implementar Mejoras en sus Procesos Software.

Con el nacimiento de las nuevas constelaciones CMMI, este modelo abarca no sólo las actividades del desarrollo de software (CMMI for Development), sino también la prestación de los servicios (CMMI for Services) y la adquisición del software por terceros (CMMI for Acquisistion), convirtiéndose así en un modelo de buenas prácticas con cobertura total para las empresas de TI. CMMI mantiene su estructura de niveles de madurez, así como la denominación de los mismos en todas sus constelaciones.

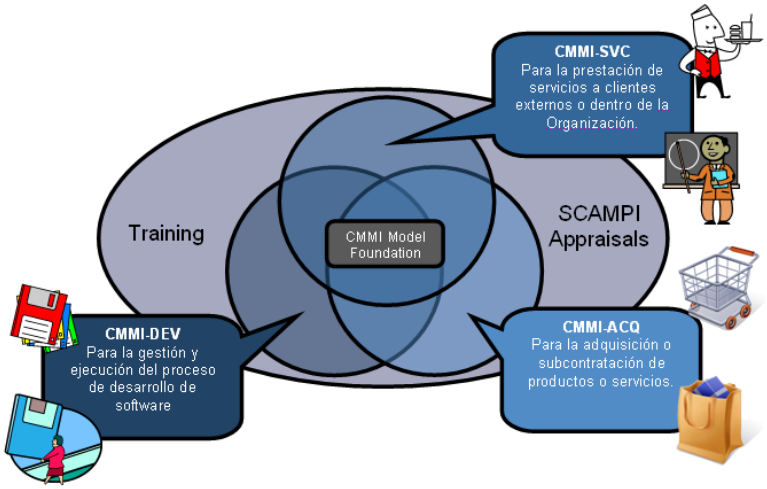

Figura 1.

Aunque los niveles de madurez 2 y 3 son los más empleados tanto en el ámbito nacional como internacional, cada día está más en auge el empleo de los niveles 4 y 5, conocidos como Niveles de Alta Madurez, donde la Gestión Cuantitativa, basada en el empleo de técnicas estadísticas, es la clave para obtener los Modelos de Rendimiento y Líneas Base a seguir por los procesos clave del negocio, que permitirán mejorarlos y obtener mejores rendimientos que redunden en la mejora de los beneficios de la compañía.

Las organizaciones que se encuentran en un **nivel 4**, establecen objetivos cuantitativos para calidad y ejecución de los procesos y

les usan como criterios en la gestión de procesos y proyectos. Los objetivos se basan en las necesidades de los clientes, usuarios finales, organización e implantadores de los procesos. La calidad y efectividad de los procesos se miden en términos estadísticos y se eliminan las causas especiales de variación para predecir su rendimiento.

En el **nivel 5**, la organización mejora sus procesos en base a una comprensión cuantitativa de las causas comunes de variación inherentes en los procesos y se enfoca sobre la mejora continua de la eficacia del proceso, a través tanto de la mejora incremental, como de la innovación tecnológica.

2. ¿CUÁNDO APLICAR UNA GESTIÓN CUANTITATIVA?

Para poder realizar una Gestión Cuantitativa de los Procesos y Proyectos de la organización, es necesario que se den una serie de premisas:

- **Los procesos son estables**, se puede establecer su rendimiento, sus límites de control y de especificación.
- **Se dispone de un repositorio de métricas maduro**, que permite establecer modelos de comportamiento y líneas base de los procesos.
- **Se conocen las relaciones entre las diferentes variables** que influyen en los procesos, por lo que se pueden evaluar estas relaciones y conocer aquellas que son significativas.

Pero quizá la dificultad surge cuando se cumplen estas premisas, pero no sabemos **qué herramientas emplear, cuándo y cómo**. Entre las posibles herramientas que nos pueden ayudar a realizar una gestión estadística de nuestros procesos y proyectos, destacan dos:

- **SPC (Statistical Control Process)**
- **Seis Sigma**

3. ¿QUÉ ES SPC?

SPC (Statistical Process Control) es un conjunto de técnicas estadísticas empleadas para realizar un control sobre los procesos. Entre estas técnicas destacan las "7 Magníficas":

- Gráficos de Control
- Histogramas
- Hoja de Control
- Diagrama de Procesos
- Diagrama causa-efecto
- Diagrama de Pareto
- Diagrama de Dispersión

Muchas de estas herramientas son grandes conocidas en la mayoría de las empresas, pero muy pocas son utilizadas para la resolución de problemas o la identificación de dependencias y tendencias. Además de las "7 Magníficas", hay otras herramientas en el marco de SPC:

- Variación del Sistema de Medida: R&R (Repetibilidad & Reproducibilidad)
- Capacidad de Proceso
- Gráficas de Evolución: Run Chart
- Boxplot
- Ensayos de Hipótesis
- Diseños de Experimentos: DOE
- Diagramas de Efectos Principales
  - Diagramas de Interacciones
  - ANOVA

Si no se dominan las técnicas estadísticas ni la orientación óptima de estas herramientas, SPC puede llegar a asustar a quien se plantea emplearlo: ¿Qué herramienta utilizar?, ¿cuándo?, ¿cómo interpretar los resultados?,…

Seis Sigma, a diferencia de SPC, plantea una secuencia lógica de actividades asociadas al

empleo de herramientas, que ayudan a la organización a la utilización correcta de las mismas.

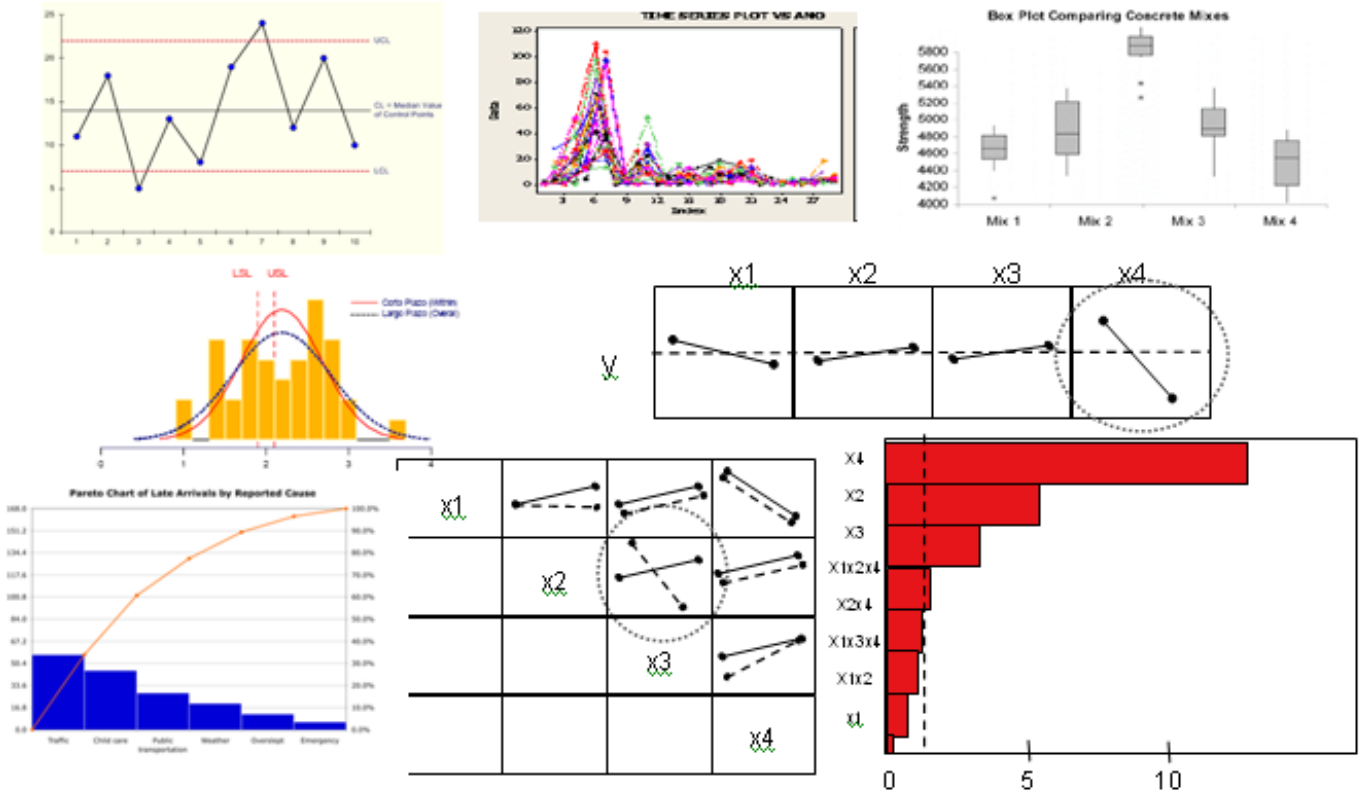

Figura 2.

4. SEIS SIGMA COMO INSTRUMENTO DE MEJORA

Seis Sigma fue ideada por Bill Smith, Jefe de Calidad de Motorola, comenzando su implementación en 1987. Es una metodología orientada a la mejora de los procesos productivos, cuya filosofía es **trabajar mejor** llevando a la **reducción del número de fallos en los productos**. Su objetivo es **aumentar la satisfacción del cliente** mediante la prevención y eliminación de defectos, teniendo como resultado la mejora del **rendimiento económico** de la organización.

"**Sigma**" se refiere a la desviación típica, una medición de la variación de los procesos, de su capacidad, y el estándar Seis Sigma se refiere a un proceso que tiene 6 desviaciones típicas, 6σ, entre el objetivo y el límite de especificación más cercano.

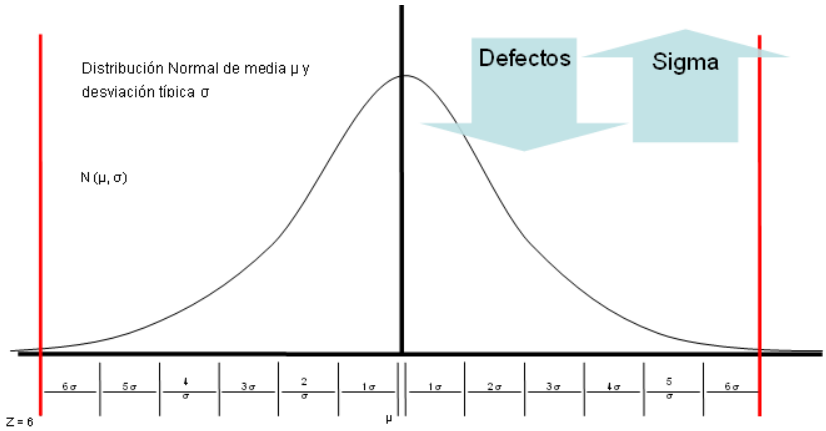

Figura 3.

La Sigma del Proceso, su capacidad, está ligada al rendimiento que obtenemos de él, que está asociado a los defectos o errores que se detectan, los **DPMO** (Defectos por Millón de Oportunidades). Así, un proceso de capacidad 6Sigma equivale a un rendimiento del 99,9997% y sólo 3,4 defectos por cada millón de oportunidades, DPMO.

En la tabla adjunta puede verse la relación entre la capacidad de los procesos (su sigma), el rendimiento que se obtiene de él y el número de defectos que se espera encontrar por cada millón de oportunidades (DPMO).

Rendimiento	DPMO	Sigma
99,9997%	3,4	6
99.976%	6	5
99.4%	233	4
93%	66.807	3
65%	308.537	2
50%	500.000	1

Tabla 1.

Un ejemplo puede darnos una idea de las implicaciones:

*Supongamos una compañía eléctrica, cuyo proceso de encendido de las luces fuera **4Sigma**, esto equivaldría a que las luces estarían apagadas casi **1 hora a la semana** debido a problemas o defectos en el suministro, si la compañía mejorara la capacidad de este proceso hasta **6Sigma**, los cortes de luz debidos a errores en el suministro, se reducirían a sólo **2 segundos por semana**.*

La metodología 6Sigma presenta un Ciclo de Mejora, denominado **ciclo DMAIC** (**D**efine, **M**easure, **A**nalyze, **I**mprove, **C**ontrol), cada una de las etapas se centran en:

- **Define:** la Definición del problema o situación que se quiere mejorar
- **Measure:** la Medida de esta situación y recopilación de datos históricos
- **Analyze:** el Análisis de los datos recopilados
- **Improve:** establecer el Plan de Mejora de la situación o problema

- **Control:** garantizar que se mantienen las mejoras implantadas.

Asociada a cada una de estas etapas del ciclo DMAIC, 6Sigma propone el empleo de las herramientas estadísticas (SPC) más adecuadas para cubrir el objetivo, con lo que minimizamos podemos dar respuesta a las preguntas que nos surgían al emplear solamente SPC: ¿Qué herramienta utilizar? , ¿cuándo? , ¿cómo interpretar los resultados?,…

ETAPA	HERRAMIENTAS
Define	▪ QFD/Casa de la Calidad ▪ Diagrama de Proceso ▪ Diagrama Causa Efecto/ Ishikawa ▪ Diagrama de Pareto
Measure	▪ Diagrama de Proceso ▪ Evaluación del Sistema de Medida (R&R) ▪ Capacidad de Proceso

Analyze	▪ Herramientas gráficas:
	  ▪ Boxplot
	  ▪ Time Series
	  ▪ Diagramas de Efectos Principales
	  ▪ Diagramas de Interacciones
	  ▪ etc.
	▪ Gráficos de Control
	▪ Ensayos de Hipótesis

Improve	▪ Gráficos de Control ▪ Ensayos de Hipótesis ▪ Diseño de Experimentos (DOE)
Control	▪ Gráficos de Control ▪ Auditorías ▪ Métodos conductuales ▪ Métodos a prueba de error

Tabla 2.

DE LA GESTIÓN POR PROCESOS AL B.P.M

Dr. Montgomery Lee,
PDF

Ignacio Fernández,
Gas Natural Informática

Cuando presentamos en Barcelona mi primer libro editado en castellano, *Ya sé quien tiene tu queso*, en una escuela de negocios, EADA, creo recordar, el presentador hizo mucho énfasis en el subtítulo del libro, una frase ingeniosa a la vez que provocativa: "Las cosas se pueden hacer bien ó como siempre"

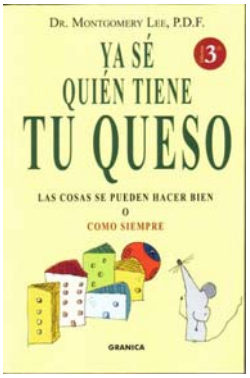

Figura 1.

La discusión sobre la frase derivó al final en una acalorada discusión acerca de lo que quiere decir hacer las cosas bien. Sí, porque pese a que todo el mundo utiliza esa sentencia, muy pocos (o ninguno) son capaces de definir con un mínimo de precisión su significado real.

Porque vamos a ver, cuando decimos que hacemos las cosas bien, ¿queremos decir que las hacemos bonitas? ¿ó baratas? ¿Quizá de forma más rápida?..., pero claro, también podría ser con una mayor carga de diseño, o pensándolo mejor... ¿quizá de más utilidad?...no obstante... ¿no querremos decir hacerlas más fiables? ... ¿o más duraderas?....

En fin, es fácil decir que hacemos las cosas bien, pero no es tan fácil explicarlo.

No se les ocurra buscar en las enciclopedias el significado, y mucho menos en Internet. Yo lo hice, y las conclusiones fueron cuando menos sorprendentes: Hacer las cosas bien es patrimonio casi exclusivo del fútbol, a excepción hecha de la primera referencia de todas, que es de Hacienda, lo cual no es ninguna sorpresa, porque es evidente que esta gente sí que sabe hacer las cosas bien...

En definitiva, si pensamos un poco, llegaremos a la conclusión que hacer las cosas bien significa hacerlas cada vez con menos recursos, sin que ello implique sacrificar calidad ni prestaciones.

Pero... ¿Por qué hacer las cosas bien, si podemos hacerlas como siempre? ¿Para qué complicarnos la vida? Mi insigne colega, el Dr. José María Cervelló, profesor de derecho, historiador y bibliófilo, nos brinda la respuesta: "Hay que hacer las cosas bien por hacerlas bien y porque es rentable"

Toda esta disquisición, aparte de ser una cuña publicitaria acerca de mi libro, el cual les recomiendo encarecidamente, creo que ilustra perfectamente el tema de la gestión por procesos, porque esta filosofía no deja de ser un aproximación a hacer las cosas bien, de hecho cada vez mejor, cambiando los viejos *modus operandi* con los que hemos venido funcionando toda la vida en nuestros procesos de negocio.

Estos conceptos de gestión, en los procesos industriales de de fabricación se aplican de forma masiva desde finales de la segunda guerra mundial, aunque seguramente tuvieron su inicio a finales del siglo XIX, a partir de las teorías de Frederic Taylor, el padre de los métodos y tiempos, y difusor de lo que se vino en llamar el *Management Científico*.

Lo que se buscaba con todo esto era optimizar los procesos de fabricación, eliminando aquellas complejidades innecesarias, los cuellos de botella, las acumulaciones de stocks intermedios, etc., de forma que los flujos de producción fueran lo más claros y directos posibles, optimizando de este modo todos los medios de producción empleados, incrementando obviamente el beneficio de fabricación.

Figura 2.

En definitiva, se trataría de pasar de los procesos de fabricación artesanales, poco formalizados, basados en las habilidades y conocimientos del trabajador, con una baja capacidad de producción y repetibilidad, a las modernas cadenas de montaje, en las que las piezas se producen en serie con un alto nivel de fiabilidad, con procesos de montaje automatizados y en muchos casos robotizados, con la máxima reducción de los *stocks* intermedios, ajustando al máximo la productividad de todos los recursos, humanos y materiales, implicados en el proceso de fabricación.

Figura 3.

Estas filosofías de mejora de procesos de fabricación fueron concebidas en los Estados Unidos, fundamentalmente a partir de los estudios de Demming y Juran, pero su implantación de forma efectiva se realizó en Japón, país en el que se aplicaron con éxito y se perfeccionaron; todo ello debido a la necesidad de reconstruir un país devastado por la guerra. De hecho, su máximo impulso se obtuvo en la industria automovilistica nipona, y este hecho dio origen a muchos modelos de referencia ampliamente implantados en la actualidad como son el *Lean Manufacturing, Just-in-time* y modelos de calidad total, entre otros. De hecho, se formalizaron y aplicaron con éxito las filosofías de mejora continua, como el *KAIZEN*, de igual manera que se consiguió la implicación de todo el personal en la consecución de la mejora en la productividad y calidad de los productos fabricados, mediante lo que se vino en llamar los *Círculos de Calidad*

En definitiva, todos estos modelos de calidad, al igual que sus sucesores, como podría ser el caso de *Six Sigma*, se basan en la definición, medición y control del proceso productivo, como base para su optimización posterior.

Ahora bien, todo esto que se ha aplicado con éxito demostrado a los procesos de fabricación...¿es exportable a aquellos procesos de negocio que no son de fabricación, es decir, a los procesos de soporte ó a los procesos de servicio? ¿es posible pasar de la "ejecución artesana" de los procesos administrativos ó de desarrollo de sistemas, por ejemplo, a procesos "industrializados" de soporte y servicios? ¿Se puede crear "una cadena de montaje" en la tramitación de un pedido? ¿es posible industrializar el desarrollo y mantenimiento de aplicaciones? ¿Se pueden eliminar los tiempos muertos en la tramitación de cualquier solicitud administrativa interna en una empresa?

Figura 4.

En definitiva... ¿podemos "industrializar" todos aquellos procesos que realizamos en nuestras empresas que no sean estrictamente de fabricación?

Y si la respuesta es afirmativa, deberíamos plantearnos cual debería ser el resultado esperado, que no es más que la realización de dichos procesos de forma normalizada, lo cual permitirá facilitar su repetitividad, su medición y,a través de ésta, determinar las posibilidades de optimización del proceso en cuestión, ya sea simplificando los puntos de control, eliminando algunas de las tareas implicadas y, finalmente, evaluando la viabilidad técnica y económica de su automatización.

Para todo ello, deberemos proceder de la misma manera que haríamos en una cadena de montaje, definiendo los pasos ó actividades que componen el proceso y para cada uno de ellos, identificar qué es lo que entra ó sale, quién interviene, qué o quién ó en donde se frena el flujo de trabajo, y, en definitiva, el valor añadido que todos y cada uno de los que intervienen en el paso aportan al mismo, y si este valor se puede incrementar. Para ello, convendría que nos formuláramos las siguientes preguntas:

- ¿Quién hace qué?
- ¿Cuál es el coste de nuestros procesos?
- ¿Dónde están los cuellos de botella?
- ¿Cuál es la lógica de la secuencia de avance del proceso?
- ¿Qué conocimientos se utilizan?
- ¿Qué datos se administran?
- ¿Qué sistemas de información se utilizan y qué procesos respaldan?

Responder a estas preguntas es, ni más ni menos, la definición de un proceso, o dicho en otras palabras, un *proceso* es cualquier secuencia repetitiva de *actividades* que una o varias *personas* desarrollan para hacer llegar una salida a un destinatario, a partir de unos *recursos* que se utilizan o se consumen. Es decir, para definir un proceso necesitamos conocer la secuencia de actividades que lo conforman, los recursos implicados, ya sean materiales ó humanos, los sistemas y herramientas que se utilizan, los procedimientos y normas que aplican, y finalmente las métricas e indicadores que nos mostrarán el comportamiento del proceso.

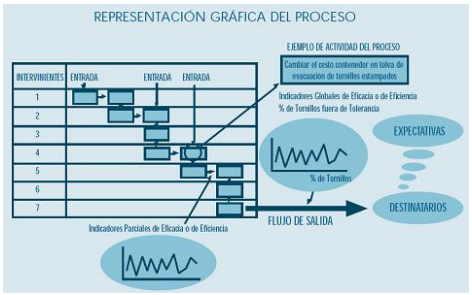

Figura 5.

Resumiendo, implantar la gestión por procesos implica, en primer lugar, identificar todos los procesos relevantes, describirlos y analizarlos, eliminar los puntos débiles, reforzar los cuellos de botella, eliminar los pasos innecesarios, en definitiva optimizarlos. Además se debe crear una organización orientada a procesos, en la cual cada uno de ellos tenga un propietario que se responsabilice de su control y optimización, de la misma forma que una cadena de fabricación tiene siempre su responsable. Además debe asegurarse la integración de los sistemas de información que dan soporte al proceso y garantizar que la infraestructura que los soporta proporciona los tiempos de respuesta adecuados para que ésta no se constituya en un cuello de botella, pero sobre todo, es necesario establecer los mecanismos de seguimiento y monitorización, imprescindibles para conocer la

estabilidad del proceso y los resultados de las acciones de optimización.

Todo esto en cuanto a la gestión por procesos, pero quizá es un término anticuado. En estos tiempos que corren nos bombardean con multitud de siglas que empiezan por BP, desde el BPM(Business Process Management) al BPM (Business Process Monitoring), pasando por el BPM (Business Process Modelling), por no hablar del BPA (Business Process Automation), ó el BPA (Business Process Analysis) y sin olvidar el BPR (Business Process Reengineering). Toda esta ensalada de siglas no hace más que sembrar la confusión entre el respetable. Porque....¿qué significa BPM? ¿Es un cambio de paradigma en la gestión empresarial? ¿Una filosofía de mejora continua? ¿Un conjunto de herramientas para conseguir lo anterior? ¿Herramientas sofisticadas para pintar procesos? ¿Ó quizá una suite de herramientas de automatización de procesos?

En primer lugar, debemos distinguir entre filosofía y tecnología. BPM como filosofía es lo que anteriormente hemos llamado gestión por procesos, es decir, la industrialización de los procesos no productivos.

En muchas actividades empresariales, no es necesario reinventar la rueda, puesto que existen modelos de referencia que proponen una estandarización de los procesos basada en las mejores prácticas de la industria. Entre ellos podemos destacar el modelo ISO, que proporciona diferentes modelos de referencia para la gestión de la calidad.

En el mundo de las tecnologías de la información, existen varios modelos de referencia. En primer lugar, el modelo ITIL (Information Technology Infrastructure), el cual define un marco de trabajo de las mejores prácticas destinadas a la entrega de servicios de T.I; recientemente ha aparecido la versión 3 de este modelo.

En segundo lugar, el Modelo CMM (Capacity Maturity Model), desarrollado por el Software Engineering Institute de la Carnegie-Mellon University, proporciona un conjunto de prácticas y procesos clave en el desarrollo de software, estableciendo diferentes estadios de madurez que se alcanzan a través de la puesta en práctica de determinados procesos claves en cada nivel. Se considera el modelo de referencia en calidad de desarrollo de software, hasta el punto que las mayores empresas de outsourcing de desarrollo están certificadas en el nivel 5 de CMM, que es el máximo alcanzable.

Finalmente, el modelo COBIT (Control Objectives for Information and Related Technology) establece un marco de gobierno para las organizaciones de tecnologías de la información, y tiene como objetivo reducir el espacio existente entre las exigencias de control, las cuestiones técnicas y los riesgos del negocio. COBIT permite la buena práctica para el control de TI en todas las áreas de una organización.

En cuanto a la tecnología, debemos distinguir fundamentalmente entre las herramientas y los motores. Entre las herramientas podemos distinguir aquellas que permiten modelizar los procesos, las que permiten su automatización y las que permiten establecer los mecanismos de seguimiento, aquellas que presentan los resultados en cuadros de mandos llenos de gráficos, indicadores y relojes, al estilo del *tablier* de un coche, por ejemplo. Los motores son las herramientas que permiten automatizar el flujo de actividades dentro de los sistemas de información, como son los motores de workflow, que proporcionan la facilidad de automatización de la ejecución de los diferentes pasos de un proceso en base a las transacciones informáticas implicadas en el mismo, ó los *middleware* de Integración, que permiten la integración de los diferentes sistemas informáticos a través del traspaso de información, que puede ser transformada ó no, en base a reglas del negocio programables.

Las herramientas de modelización, que son la base para cualquier proyecto de automatización basado en herramientas BPM, permiten dia-

gramar los procesos de negocio, identificando todos los agentes que intervienen. Dado que siempre están soportadas por una base de datos, proporcionan funcionalidades de búsqueda y análisis de procesos.

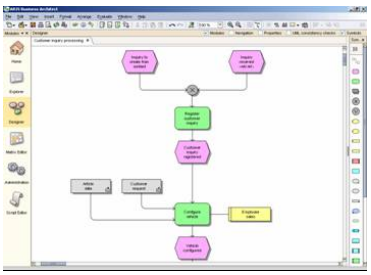

Figura 6.

En cuanto a las herramientas de simulación, se basan en las anteriores, que les proporcionan los modelos de procesos, a los que agregan características de capacidad, velocidad de ejecución y demás limitaciones, lo que permite simular el comportamiento de un proceso, identificar los cuellos de botella y evaluar la efectividad de los cambios producidos en un proceso.

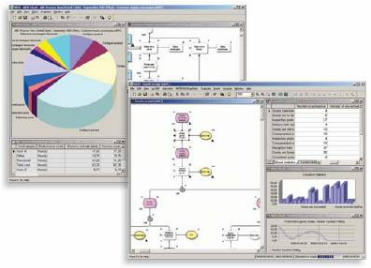

Figura 7.

Por último, las herramientas de análisis y monitorización proporcionan amplias capacidades gráficas para el análisis del comportamiento de un proceso, la evolución de sus métricas de control y la plasmación gráfica, tanto de los resultados de la simulación como de las mejoras y optimizaciones propuestas.

Figura 8.

Para concluir, creo que es imprescindible distinguir entre la filosofía BPM y la tecnología que comparte siglas. Además, cualquier proyecto de implantación de herramientas BPM debería pasar por implantar antes la filosofía de gestión por procesos, puesto que es de todos conocidos que no se puede mejorar lo que no se mide y que automatizar un desastre solamente proporciona un desastre automático.

“Locura es hacer más de lo mismo y pretender alcanzar distintos resultados" - Albert Einstein

“Si buscas resultados distintos, no hagas siempre lo mismo” - Albert Einstein

“La mejor estructura no garantizará los resultados ni el rendimiento. Pero la estructura equivocada es una garantía de fracaso” Peter Drucker (1909-2005) Escritor y consultor estadounidense

“El progreso y el desarrollo son imposibles si uno sigue haciendo las cosas tal como siempre las ha hecho” - Wayne W. Dyer (1940-?) Escritor estadounidense

El Dr. Montgomery Lee P.D.F. es profesor universitario, conferenciante y escritor de reconocido prestigio. En España se ha publicado dos de sus obras, Ya sé quien tiene tu queso (Granica 2006) y El efecto Riverside (Granica, 2007)

Ignacio Fernández es ingeniero industrial y actualmente es el responsable de modelos de referencia en Gas Natural Informática.

ENTERPRISE AND IT ARCHITECTURE: LAS CLAVES DEL GOBIERNO DE TI

Ángel Sánchez
Pº de la Castellana, 141 – planta 9
28046 Madrid
www.everis.com

Resumen: Una de las principales preocupaciones de las áreas de sistemas es el alineamiento con los procesos de negocio, así como el uso eficiente de sus recursos TI o, de una manera más general, de sus activos de proceso. Estos dos objetivos se pueden cumplir simultáneamente usando los principios y métodos de las Enterprise Architectures (EA), que persiguen la replicación y uso eficiente de los recursos tecnológicos y del negocio siguiendo las necesidades de las áreas de negocio. Una estrategia de EA empieza con la identificación de todo aquel elemento candidato a ser replicado a otras localizaciones o áreas organizativas o, simplemente, susceptible de ser mejorado en la búsqueda de la eficiencia. Estos "bloques" se componen de hardware TI, datos, aplicaciones y procesos de negocio. La gestión apropiada de estos elementos, así como su identificación es una tarea compleja que requiere de equipos específicos y herramientas adecuadas. Este artículo proporciona una visión general de los principios de las EA y sus beneficios, todo ello desde un punto de vista práctico a partir de experiencias reales en proyectos.

Abstract: One of IT Departments main concern is the alignment with business processes and trends as well as the efficient use of IT resources or, in general, IT processes' assets. These two goals can be simultaneously achieved by using the principles and methods of the Enterprise Architectures (EA), which aim the replication and efficient use of IT and business resources following the needs of the business areas. An EA strategy starts with the identification of any element candidate to be replicate to other locations or organizational units or, merely, improved seeking efficiency. These "building blocks" are composes of IT hardware, data, application and business processes. The appropriate management of such elements, as well as their identification is a difficult task which requires specific teams and adequate tools. This article provides and overview of EA principles and benefits from a practical point of view based on actual project experiences.

Palabras clave: Gobierno de TI, Enterprise Architectures, Organización TI.

1. INTRODUCCIÓN - ¿QUÉ ES UNA ENTERPRISE ARCHITECTURE?

Llevamos muchos años hablando sobre el alineamiento entre negocio y sistemas, es como un *mantra* que se repite, que oímos en todo tipo de reuniones, mesas redondas y, en general, cualquier foro al que asistimos los profesionales de la Gestión de las Tecnologías de la Información (quienes quiera que seamos y somos muchos). De tanto oírlo nos hacemos los sordos. Basta una pregunta, ¿Cuántos directores de sistemas (CIOs) forman parte del Consejo de las principales compañías? La respuesta: pocos, muy pocos. Sin embargo, hay un nuevo concepto que se está abriendo paso que pude ser la solución, parcial probablemente, a ese divorcio entre negocio y sistemas. El concepto se denomina *Enterprise Architecture* (EA) y se puede entender como el conjunto de procesos, recursos humanos, materiales y sistemas de información que soportan una organización.

Una particularidad de las EA son las arquitecturas más relacionas con las áreas de TI, que en este caso denominaremos "Arquitectura TI" y será en las que nos centremos (para una revisión del tema es recomendable el trabajo de J.Ross, "Enterprise Architecture: Deriving

Business Benefits from IT", MIT Center for Information Systems Research, abril de 2006).

Estás arquitecturas van más allá del concepto de modelo de procesos, no se trata de levantar o "pintar", como se dice en el argot, los procesos de un área y los distintos elementos que lo soportan, sino de establecer un repositorio que recoja de forma sencilla, operable y mantenible dichos procesos y su relación con las aplicaciones que los soportan, la información que manejan y las personas afectadas. Desde este punto, pocas son las empresas que han abordado un proyecto de arquitectura y lo que predominan son iniciativas parciales. Por ejemplo, se abordan proyectos de gestión del servicio y se implanta ITIL (Information Technology Infrastructure Library), simultáneamente alguien instala herramientas de gestión del portafolio y, para completar el cuadro, el responsable de desarrollo decide que todo sea SOA (Service Oriented Architecture) concepto ubicuo que no suele faltar en las áreas de sistemas. El resultado: confusión y pobre retorno de esas inversiones que en el mejor de los casos acaban convertidas en vistosas presentaciones "powerpoint" en las mesas de quienes lanzaron estas iniciativas a bombo y platillo.

Pero como hemos comentado hay una forma de hacerlo mejor, de ordenar los activos (personas, información, procesos y aplicaciones) que conforman un área de sistemas: aplicando los modelos de Arquitectura TI.

2. DE LAS EA Y ARQUITECTURAS TI AL GOBIERNO DE TI

Según se ha explicado en la sección anterior, las Arquitecturas TI (como concreción al área de sistemas del concepto más amplio de de EA) permiten estructurar claramente los activos del área de sistemas y por lo tanto gestionarlos mejor. No debemos de olvidar que un marco de Gobierno de TI debe de ayudar a movilizar los recursos de un departamento de la forma más eficiente obedeciendo a necesidades:

1) Normativas, como pueden ser los marcos regulatorios (ahora de nuevo en primera plana) como Sarbanes-Oxley, CobIT, CMMi, etc.
2) Operativas, la tan comentada eficiencia.
3) Del negocio. Por ejemplo, planes de gestión de la demanda.

Evidentemente, para poder hacer los tres puntos anteriores, logrando una operación de nuestros sistemas de información que minimice los riesgos, generando la confianza que el negocio (y los clientes) requiere, es necesario conocer de qué material esta hecho nuestra organización, cuáles son los activos clave, su relación, etc. Y lo que es más, como se relaciones con los procesos de negocio… Este marco de relaciones es lo que hemos denominado Arquitectura TI, entendiendo que es parte de la EA y que se encuentra íntimamente relacionada con las actividades del negocio, tal y como se ilustra en la figura 1:

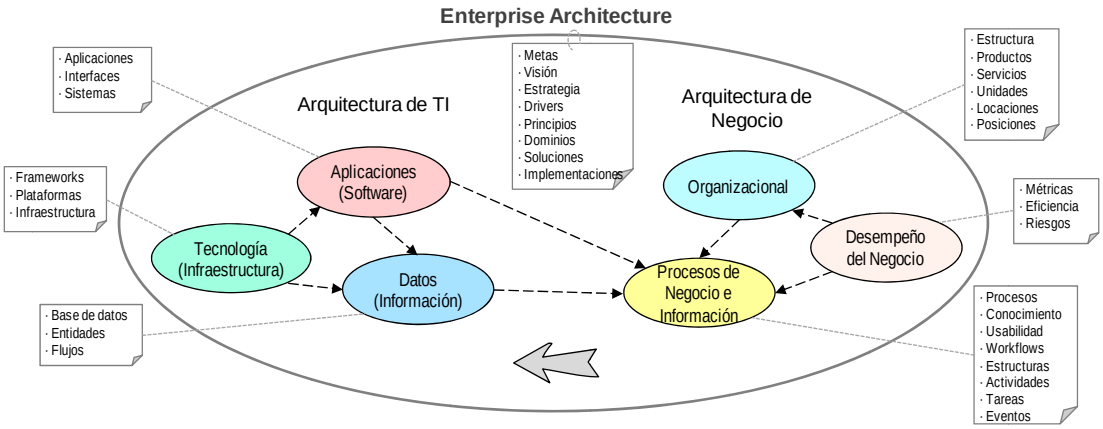

Figura 1. : Las Arquitecturas TI y del Negocio como elementos constitutivos de las EA.

Por otro lado, siguiendo las ideas de Ross (anteriormente citado), una vez que la organización dispone de un marco común para la ejecución de sus procesos o servicios (lo que se denomina en inglés "Foundation for Exceution"), el modelo operativo de la compañía, su Arquitectura TI y el modelo de Gobierno está íntimamente relacionados:

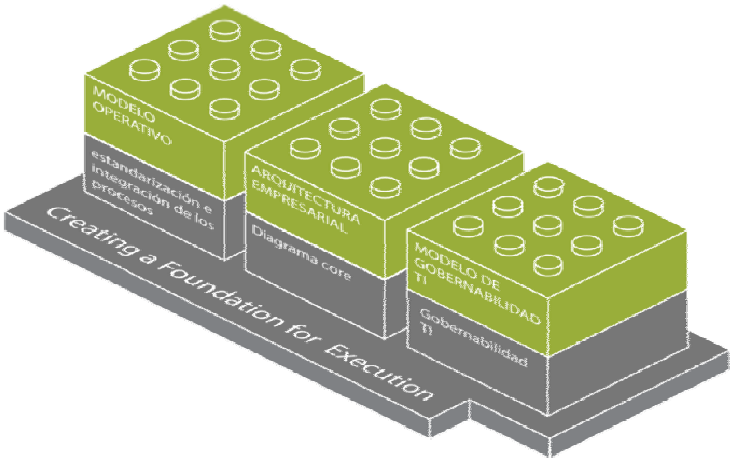

Figura 2. : Modelo operativo, EA y modelo de Gobierno como bloques constitutivos del área de sistemas y soporte de la organización.

3. DEMOS UNA VISIÓN DE CONJUNTO

Imaginemos que podemos pararnos a pensar y ordenar todos los activos que componente una Arquitectura TI, siguiendo una típica visión de "abajo a arriba". En primer lugar nos encontramos con todas las infraestructuras tecnológicas, inmediatamente por encima se encuentran las funciones de gestión del servicio TI, donde el modelo ITIL marca la referencia. Llegados a este punto nos encontramos con activos básicamente tecnológicos, los procesos que soportan el servicio que esta tecnología presta y las

personas entrenadas para ello. A muchos "pisos" por encima, se encuentran los procesos de negocio soportados por las aplicaciones desarrolladas a tal efecto. Lo normal es que no se vaya más allá y que estos dos niveles o agrupaciones de activos se encuentren separados, sin un mecanismo que permita visualizarlos de forma integrada. Entonces, ¿cómo debemos proceder? Vayamos paso a paso:

- En primer lugar se modelan los procesos de negocio, es decir, aquellos que van orientados a satisfacer un resultado concreto de la actividad de la empresa y se documentan con una herramienta de EA (ARIS, System Architect y Provision entre otras), indicando los indicadores y métricas asociados; así como los perfiles e integrantes de la organización afectados. Concluido este ejercicio podemos dar por finalizada la Arquitectura de Negocio. Este modelado, favorecido por el uso de herramientas, se puede llevar a cabo empleando notación estándar como BPMN (Business Process Modeling Notation). En este caso, tal y como describe la figura 3, nos encontramos dentro del ámbito de la estrategia y el análisis de procesos de negocio.
- En segundo lugar se modelan los datos y aplicaciones que soportan los procesos anteriormente descritos y diseñados. El uso de BPMN y herramientas adecuadas permite pasar de la especificación de un proceso a la de un servicio IT (p.e., Web Services) mediante un intérprete denominado BPEL (Busines Process Excution Language). Es decir, gracias a los principios de Arquitectura TI y al uso notación estándar se pueden unir de forma elegante el modelado de negocio con el de sistemas, en otras palabras, sentar las bases del Diseño Detallado.
- Finalmente, tras modelar el negocio y los interfaces de los servicios TI, es necesario integrar los dos mundos: negocio y sistemas. Esta vinculación es todavía más eficaz en escenarios SOA, donde previamente las aplicaciones se han analizado para determinar cuales son los servicios de aplicación que poseen y agrupado en servicios de negocio. Dichos servicios se suelen catalogar e inventariar gracias a herramientas que proporcionan la función de "repositorios de servicios". Las herramientas de Arquitectura TI permiten integrar estos repositorios con los procesos de negocio y los datos a gestionar, permitiendo tener en una única ubicación lógica todos los activos relacionados con el modelado de una determinada actividad.

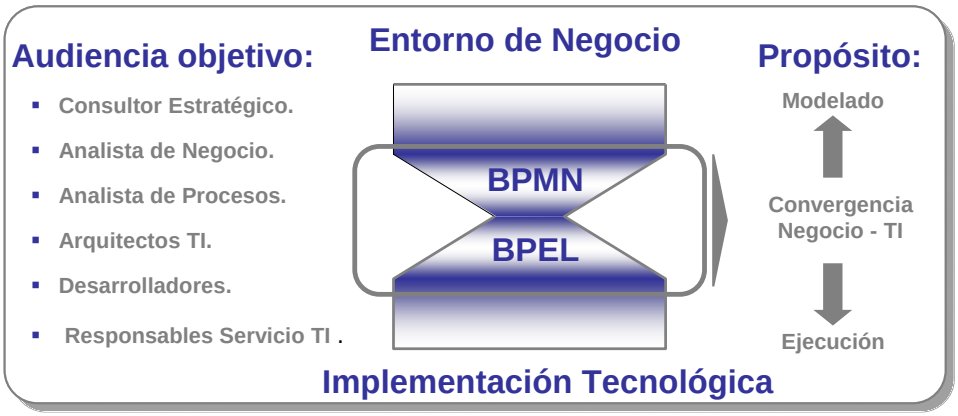

Figura 3. : Convergencia negocio – TI a través de los métodos de EA

Es importante destacar que la adopción del paradigma SOA tiene más implicaciones en la definición de procesos, es decir, en las áreas negocio que en las técnicas. En efecto, SOA supone un cambio radical pues la idea de aplicación que soporta a uno o varios procesos se pierde. En su lugar lo que tenemos es un conjunto de servicios, adecuadamente inventariados y expuestos, que bien agrupados con la ayuda de alguna solución de integración darán soporte a los procesos de negocio. Si el análisis y exposición por parte de las áreas de técnicas se hace correctamente, son los analistas de negocio los que deben sacar el máximo partido a dichos servicios mediante un correcto modelado.

4. CONCLUSIONES

A modo de conclusión, destacaría que pese a su inmadurez actual, los principios, técnicas (como el cuadrante Zachman o el modelo TOGAF) y herramientas de Arquitectura TI nos abren las puertas a un nuevo mundo en el que analistas de negocio (procesos) y sistemas (arquitectos) se confundan, siendo difícil establecer la distinción entre unos y otros pues ambos trabajarán sobre los mismos activos de información, usando las mismas técnicas. Esto no es Ciencia Ficción, está a la vuelta de la esquina y las oportunidades para los negocios serán muy significativas, permitiendo al fin la tan manida convergencia entre las áreas de negocio y sistemas.

Por otro lado, el conocer y ordenar adecuadamente los activos del área de sistemas permite desplegar modelos de Gobierno TI, o lo que es más, se la base de los mismo, ligando la gestión de los activos con su gobierno.

5. REFERENCIAS.

[1] J.Ross, 2006. “Enterprise Architecture: Deriving Business Benefits from IT”, MIT Center for Information Systems Research, abril de 2006.JTC 1/SC 27. “ISO/IEC 27001:2005”, International Standards for Business, Government and Society.

[2] N.G. Carr, 2003. “IT dosen’t Matter”, Harvard Business Review.

[3] M. Curley, 2004. "Managing Information Technology for Business Value", INTEL Press

PRUEBAS DE SEGURIDAD EN EL MARCO DE UNA FACTORÍA DE CALIDAD DE PRODUCTO SOFTWARE

Jesús Pérez Cristóbal
Consultor Senior de Calidad de SW y Procesos TI
Métodos y Tecnología
jesus.perez@mtp.es
http://www.mtp.es

Resumen El artículo presenta una visión de las pruebas de seguridad dentro del marco de estandarización de procesos que representa el modelo de factoría de pruebas. Dicha visión es fruto de la experiencia de MTP. Dentro de este ámbito se realiza un análisis general sobre cuestiones tales como metodologías utilizadas, cuadros de mando, procesos de calidad, utilización de herramientas especializadas o modelos de riesgo.

1. INTRODUCCIÓN

El paradigma de la factoría software está tomando auge gracias a la tendencia actual de buscar modelos de fabricación de software que tiendan a esquemas más industriales y que se alejen de las formas artesanales que han dominado por mucho tiempo este sector (y que han ocasionado no pocos perjuicios). Recordemos que, como diversos autores han señalado, las características esenciales de las factorías software son la estandarización de sus procesos, productos y servicios como camino para mejorar la calidad del software, reducir los tiempos de desarrollo e incrementar la productividad.

Pero el creciente éxito del modelo de factoría software no debe entenderse de forma aislada. Otras tendencias asentadas en la economía actual han servido de revulsivo a este modelo. Algunas de estas tendencias son: la externalización de servicios por parte de las empresas (outsourcing), que dota a las empresas de mayor flexibilidad o la creciente deslocalización como importante factor de reducción de costes. Otra tendencia destacable sería la búsqueda por parte de las empresas de las economías de escala (basado en el fenómeno comprobado de que a medida que la producción en una empresa crece, sus costes por unidad producida se reducen).

Dentro de este contexto favorable están surgiendo diferentes variedades de factoría software. Algunas clasificaciones atienden a criterios como la modalidad de outsourcing (off-shore, near-shore, on-shore). Otra clasificación es la que distingue las factorías software según el ámbito concreto del ciclo de vida del software en el que se especializan. Por ejemplo existen factorías que cubren todo el ciclo de vida del software pero otras se han especializado en fases concretas como la fase de construcción, la fase de mantenimiento o la fase de pruebas. Es esta última modalidad de factoría la que nos interesa en este artículo: la factoría de calidad de producto software, comúnmente denominada como factoría de pruebas o de testing.

El éxito del modelo de factoría de pruebas se basa en explotar al máximo los beneficios de la especialización de recursos humanos, y en general de una elevada volumetría. Esto puede suponer importantes beneficios para el cliente: mejora de la calidad y de la eficiencia en las pruebas, disminución de costes fijos por unidad

de producción, mejora en los cálculos de estimación de costes y tiempo, disminución del riesgo en proyectos novedosos, etc.
Una factoría de pruebas poseerá un catalogo de servicios que los clientes pueden contratar. Típicos servicios serán por ejemplo pruebas funcionales, pruebas de aceptación, pruebas de prestaciones, pruebas de regresión… Entre este tipo de servicios (quizás como un protagonismo menor) también se encontrara probablemente las pruebas de seguridad.

El contexto actual desde la perspectiva de la seguridad es ciertamente preocupante: todavía existe un gran desconocimiento sobre temas de seguridad en el ámbito del desarrollo software y esto propicia la consiguiente debilidad estructural del sector informático en este campo. No es por tanto casualidad que las estadísticas de incidentes de seguridad muestren un alza continuada en los últimos años y que diferentes encuestas reflejan que uno de los mayores inhibidores a la expansión del comercio electrónico en la red sea el miedo a la inseguridad.

Una solución eficaz a esta problemática descrita sería integrar las pruebas de seguridad en el ciclo de vida del software, y huir de soluciones reactivas (esto es actuar tras el conocimiento de incidentes de seguridad). Esto conllevaría, entre otras aspectos, unos adecuados requisitos de seguridad y una eficaces pruebas se seguridad.

2. PRUEBAS DE SEGURIDAD EN UNA FACTORÍA SOFTWARE: BASE METODOLÓGICA

Dada la estandarización y formalización del desarrollo software en base a modelos reconocidos por el mercado, es factible especializar y estandarizar el proceso de pruebas de seguridad. Desde este punto de vista la factoría de pruebas puede ser el marco idóneo para la realización de este proceso de pruebas.

El punto de partida para que una factoría de pruebas oferte este servicio debería ser el contar con un marco metodológico sólido, preferentemente basado en estándares reconocidos y respetados internacionalmente. En el contexto de las pruebas de seguridad de aplicaciones Web (que representan la mayoría de las aplicaciones que se construyen actualmente) una metodología muy reputada es la del proyecto OWASP (Open Web Application Security Project, en inglés 'Proyecto de seguridad de aplicaciones Web abiertas'). Este proyecto se adapta perfectamente a las necesidades que podría tener una factoría software ya que cuenta con requisitos genéricos de seguridad, una metodología para realizar las pruebas, herramientas para la realización de pruebas de seguridad, extensa documentación sobre el proceso, una gran comunidad de usuarios, y numerosos subproyectos dentro del mismo área de seguridad.

La metodología OWASP cubre la seguridad en todo el ciclo de vida del software, aunque se centra principalmente en las pruebas de intrusión web. El objetivo de tal metodología es que las pruebas de seguridad sean consistentes, reproducibles, y de calidad. También es exhaustiva en el sentido de que busca analizar todas las vulnerabilidades conocidas. Su enfoque principal es el de una aproximación de caja negra donde los técnicos que realizan las pruebas sólo necesitan poseer una mínima información sobre la aplicación que va a ser testeada.

La metodología OWASP señala dos fases en las pruebas:

- **Modo pasivo:** los auditores intentan comprender la lógica de la aplicación y recopilar la información relevante (la utilización de un proxy http para observar todas las peticiones y respuestas http puede ser de gran utilidad). Al final de esta fase los auditores deberían comprender cuales son todos los puntos

de acceso de la aplicación (por ejemplo cabeceras HTTP, parámetros, cookies).

- **Modo activo:** en esta fase los auditores a cargo de la comprobación empiezan a realizar las pruebas usando la metodología específica para las diferentes categorías de vulnerabilidades (por ejemplo pruebas de autenticación, de validación de datos, de gestión de sesiones, de denegación de servicio…)

3. CALIDAD, COSTE Y PLAZOS ANTICIPADOS

La factoría de pruebas debería anticipar al cliente la calidad, el coste y los plazos en que va a obtener el servicio. Esto supone que:

- Antes de la ejecución de las pruebas se debe acordar el **alcance** de tales pruebas. Dicho alcance lo podemos medir a través de la amplitud y la profundidad de las pruebas. La amplitud corresponde a los diferentes módulos o partes de la aplicación que se quiere testear. La profundidad corresponde al nivel de pruebas de seguridad que se quiere ejecutar o a su tipo (revisión de código o pruebas de penetración).
- Para obtener una **estimación de tiempo y costes** de la evaluación, la factoría deberá tener en cuenta el alcance de las pruebas y los puntos función de la aplicación a testear. A través de esta información se debe utilizar una metodología adecuada para hallar tiempo y costes. Un posible modelo de estimación podría ser una adaptación del modelo genérico Cocomo II con el factor correctivo de los datos históricos que la factoría pudiera poseer. Es importante señalar que sólo a través de una planificación adecuada será posible para la factoría de pruebas cumplir en costes y tiempo las estimaciones previstas. Y que esta planificación deberá estar explicitada en el plan de pruebas de seguridad, que detallará el alcance, las fases, las actividades, los recursos, los tiempos, y las técnicas a aplicar.
- La **calidad** de la evaluación se comprueba a través de la información sobre las métricas de proceso y los entregables por parte de la factoría software. Las métricas nos dan valiosa información sobre la realización de las pruebas y el resultado de tales pruebas. Tales métricas deben mostrar que el nivel de desempeño está alineado con el Acuerdo de nivel de servicio (SLA). Los entregables además del informe final serán productos de trabajo como informes de herramientas, documentos intermedios, ficheros de logs...

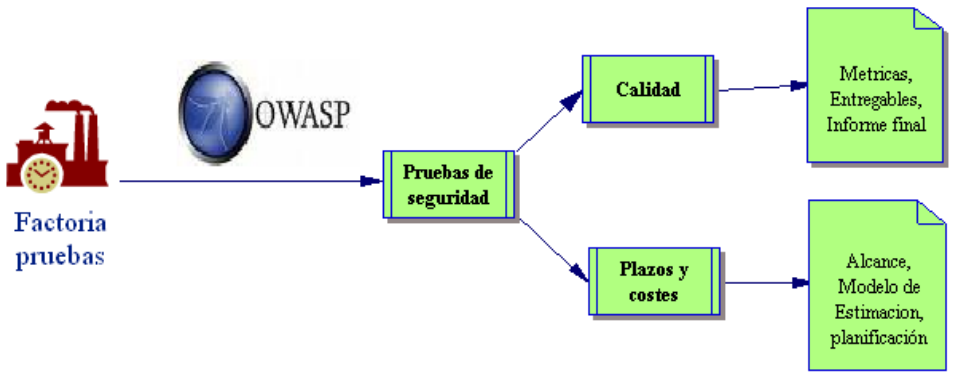

Figura 1.

4. CUADROS DE MANDO

Como en el resto de pruebas, las de seguridad deben formar parte de un proceso definido, documentado y medido para poder ser gestionado. En el ámbito de la medición dentro de una factoría software son esenciales los cuadros de mando operacionales que permiten la monitorización en vivo de determinadas métricas seleccionadas por su importancia en el proceso.

Marcos de referencia como Cobit, principalmente, e Itil, nos pueden ayudar a diseñar cuadros de mandos para los procesos de gestión de pruebas en general y de gestión de pruebas de seguridad en particular (conjuntamente con la metodología OWASP).

Existirán dos tipos de cuadros de mando: el interno, diseñado para los responsables de la factoría de pruebas, y el cuadro de mando externo, creado para los clientes de la factoría y que forma parte del interfaz externo que la factoría proporciona a estos.

Las métricas utilizadas en los cuadros de mando de la fase de pruebas de seguridad, junto con las técnicas de estimación adecuadas, nos deben permitir controlar información tal como la duración de las pruebas, los recursos dedicados, o el tiempo medio entre vulnerabilidades encontradas. Además pueden existir otros indicadores que recojan información sobre la calidad del proceso. Ejemplos de tales métricas pueden ser: esfuerzo total del proyecto (horas hombre), esfuerzo total en cada fase, número de vulnerabilidades encontradas en cada fase, vulnerabilidades críticas halladas…

5. AUTOMATIZACIÓN DE PRUEBAS

La estandarización del proceso de pruebas de seguridad pasa por la utilización de herramientas de seguridad que proporcionen automatismo en las tareas a realizar. Por ello la factoría de pruebas debe desarrollar una estrategia de automatización de pruebas. Esta estrategia debe definir qué actividades se pretenden automatizar, qué categorías de herramientas de pruebas se utilizaran, qué acciones serán necesarias llevar a cabo.

Finalmente se debe definir cuáles son los costes y beneficios esperados de la estrategia de automatización.

Un subgrupo de estas herramientas son las que proporcionan automatismo en las búsquedas de vulnerabilidades. Hay dos tipos de estas:

- **Herramientas automáticas de intrusión**: suelen funcionar como proxies intermedios entre el cliente web y el servidor. Retienen la información intercambiada y a partir de ahí son capaces de lanzar gran cantidad de pruebas automáticas. Estas pruebas pueden ahorrar gran cantidad de tiempo a los técnicos que realizan pruebas manuales de penetración.
- **Herramientas automáticas de análisis de código**: a partir del código fuente permiten descubrir posibles vulnerabilidades de seguridad. Puede ser de una gran ayuda en las revisiones de código manuales.

Son obvias las ventajas que aporta la automatización: rapidez, exhaustividad, permite realizar pruebas de manera repetitiva, y a largo plazo reduce los costes. Sin embargo este tipo de herramientas de análisis y comprobación de seguridad automatizadas tienen grandes limitaciones. En primer lugar estas herramientas son genéricas, por lo que no están diseñadas para aplicaciones específicas, sino para aplicaciones en general. Por lo que aunque pueden encontrar determinadas vulnerabilidades genéricas, no tienen el conocimiento suficiente sobre una aplicación específica como para permitirles detectar la mayoría de los agujeros de seguridad. Además en una gran parte de los casos las

vulnerabilidades de seguridad más serías son aquellas no genéricas.

Por tanto podemos decir que las herramientas que proporcionan automatismo resuelven con relativo bajo coste la localización de las vulnerabilidades más conocidas. Sin embargo para conseguir niveles mayores de seguridad es necesario diseñar y ejecutar pruebas de seguridad adaptadas a las características del producto software a evaluar. Una factoría de pruebas, debido a su especialización, aporta mayores ventajas en cuanto a cobertura de vulnerabilidades y en cuanto a los plazos de ejecución.

6. INFORME DE PRUEBAS DE SEGURIDAD

El producto final de la evaluación de seguridad por parte de la factoría de pruebas es el informe de pruebas de seguridad que normalmente estará inserto en el informe global de pruebas realizadas.

Dicho informe de seguridad deberá ser fácilmente comprensible, señalar todos los riesgos encontrados en la evaluación de seguridad y dirigirse tanto al personal técnico como a los responsables ejecutivos de la empresa cliente.

Más concretamente, dicho informe podría contar con un resumen ejecutivo no técnico que describa el nivel de riesgo, un resumen destinado a los responsables técnicos del cliente y por último un apartado que incluya detalles técnicos sobre las vulnerabilidades encontradas, y las consideraciones necesarias para que estas sean resueltas.

Es importante reseñar que para que un informe refleje una percepción correcta de los riesgos encontrados la factoría de pruebas debe contar con un modelo de análisis de riesgos, ya que descubrir vulnerabilidades en aplicaciones software es importante, pero igualmente importante es ser capaz de estimar el riesgo asociado que conllevan tales vulnerabilidades. El mayor problema que se plantea al establecerse un modelo de riesgos en una factoría software es que este modelo debe ser lo más genérico posible al testearse aplicaciones de muy diversos clientes que pueden pertenecer a diferentes sectores de la economía.

Tal modelo genérico de análisis de riesgo puede partir de la conocida valoración estándar de riesgo:

Riesgo = Probabilidad de ocurrencia * Impacto

Probabilidad de ocurrencia: medida aproximada de lo probable que es que la vulnerabilidad sea descubierta y explotada por un atacante.

Impacto: consecuencia de la materialización de una amenaza.

Ante las vulnerabilidades halladas por el equipo de la factoría software un acertado modelo de análisis de riesgos descompondrá los factores que intervienen en la "probabilidad de ocurrencia" y en el "impacto" para la seguridad de las aplicaciones, y mostrará como combinarlos para determinar la severidad global para el riesgo.

Como resumen de todo el informe de evaluación de pruebas sería interesante proporcionar una métrica global que sintetizará el estado de la aplicación desde la perspectiva de la seguridad. La idea básica consistiría en clasificar las vulnerabilidades descubiertas según su criticidad y a partir de criterios objetivos (se utilizaría el modelo de riesgo). Podríamos definir por ejemplo vulnerabilidades de criticidad máxima, alta, media y baja. Por cada vulnerabilidad de cada tipo la métrica se incrementaría un cierto valor. Por último existirían unos rangos de valores de la métrica que definirían el estado de la seguridad de la aplicación. De esta forma podríamos hablar, por ejemplo, de estado crítico, grave, medio, bajo, muy bajo y óptimo.

7. PROCESO DE PRUEBAS DE SEGURIDAD

La estandarización del proceso de pruebas de seguridad supone que es un proceso definido claramente, documentado en su vertiente interna (subprocesos, actividades, procedimientos y tareas de trabajo), como en su vertiente externa (SLAs, cuadros de mando).

Normalmente será un proceso cíclico, donde la responsabilidad final de aceptar o no los riesgos encontrados en la evaluación pertenece siempre al cliente.

En el siguiente diagrama se ha utilizado el estándar BPMN para formalizar como ejemplo un proceso simplificado de pruebas de seguridad en el marco de una factoría de pruebas.

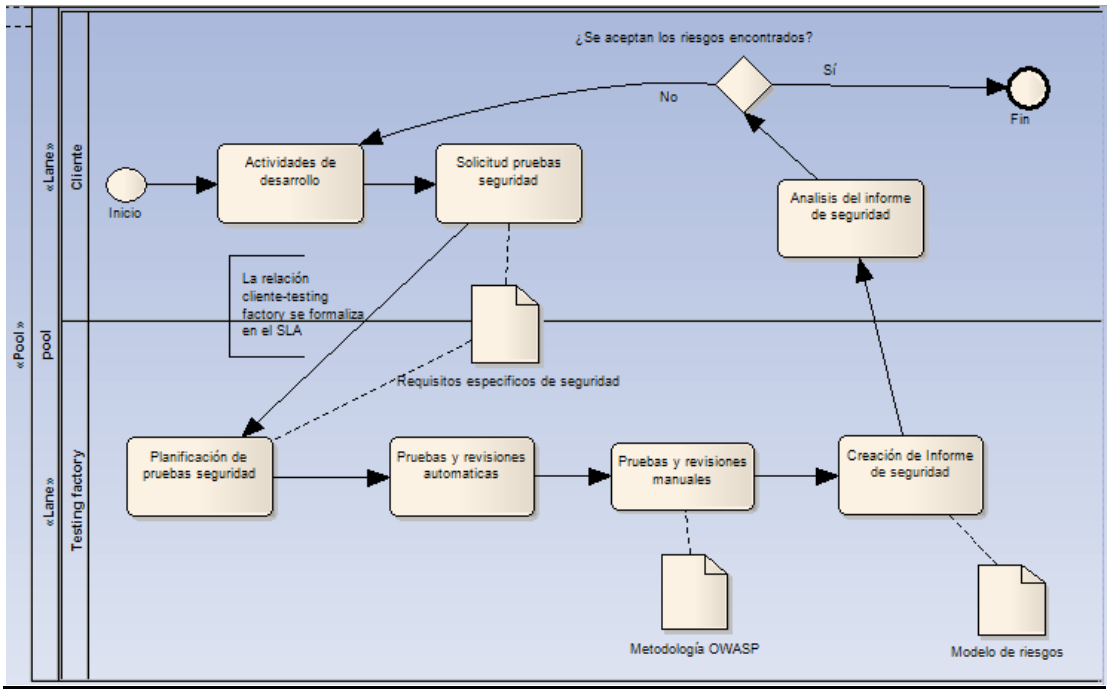

Figura 2.

8. CONCLUSIONES

- Dada la estandarización y formalización del desarrollo software en la actualidad en base a modelos reconocidos y atendiendo a los beneficios de la externalización de procesos especializados, es factible estandarizar el proceso de pruebas de seguridad en el marco de una factoría de software.
- La utilización de una metodología reconocida internacionalmente (como por ejemplo OWASP) puede proporcionar las bases adecuadas al proceso.
- La factoría de pruebas debe anticipar al cliente la calidad, el coste y los plazos en los que se realizaran las pruebas de

seguridad y esta información debe ser integrada en el plan de pruebas.

- La factoría de pruebas debe contar con un modelo de análisis de riesgo para que el cliente puede entender en la lógica de su negocio la información encontrada en el proceso de pruebas de seguridad. Puede ser útil la utilización de una métrica síntesis de la evaluación de seguridad.

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 humano desde la perspectiva de la mejora del	Ricardo Colomo Palacions, Edmundo Tovar Caro, Juan M. Gómez Berbis,	4	1	Enero 2007

Nombre	Autor/es	Vol	Nº	Fecha
proceso software	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	1	Enero 2008
Gobierno de la externalización del proceso software	Ángel Sánchez, Jezreel Mejía,Gonzalo Cuevas	5	1	Enero 2008
Gestión de los riesgos tecnológicos	Luis Martín Romeral, Álvaro Torres Gallego	5	1	Enero 2008
Importancia de la gestión del proceso de la demanda de TI.	Igos Aguilar Alonso, José Carrillo Verdún, Edmundo Tovar Caro	5	2	Mayo 2008
Un nuevo marco de convergencia y calidad para la gestión de la seguridad en el servicio de TI.	María Teresa Villalba, Luis Fernández, José Javier Martínez	5	2	Mayo 2008
Las bases de datos de gestión de la configuración, el corazón de ITIL.	Manuel Pérez Bravo, Daniel Rodríguez García	5	2	Mayo 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

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

Guía para Autores

Se recomienda a los autores enviar los artículos electrónicamente utilizando la dirección de correo electrónico rpm@aemes.org . Por favor dirigir los artículos al Editor de la Revista de Procesos y Métricas de las Tecnologías de la Información o a la Asociación Española de Métricas de Sistemas Informáticos. El artículo debe ser enviado para el proceso de revisión en formato Microsoft Word o PDF.
En el caso de envíos de artículos en papel, se deben enviar tres copias al Editor de la Revista de Procesos y Métricas de las Tecnologías de la Información o a la Asociación Española de Métricas de Sistemas Informáticos. Facultad de Informática - Universidad Politécnica de Madrid, Campus de Montegancedo, Boadilla del Monte. Madrid - 28660.
Los artículos se deberán enviar sin indicar en el documento en el que se describa el trabajo presentado los autores del mismo. Para cada artículo enviado se deberá enviar en un documento adjunto el nombre y la filiación completa (incluida dirección, teléfono y correo electrónico) de los autores del artículo, y se indicará cual de ellos se deberá considerar como autor de contacto a efectos de comunicación.
El envío de un artículo implica que el trabajo descrito no ha sido publicado previamente (excepto en el caso de una tesis académica), que no se encuentra en ningún otro proceso de revisión, que su publicación es aceptada por todos los autores y por las autoridades responsables de la institución donde se ha llevado a cabo el trabajo y que en el caso de que el artículo sea aceptado para su publicación, el artículo no será publicado en ninguna otra publicación en la misma forma, ni en Español ni en ningún otro idioma, sin el consentimiento de la Asociación Española de Métricas del Software.
Una vez recibido un artículo se enviará al autor de contacto, por correo ordinario, una carta de recepción del artículo, tanto si este ha sido enviado por correo electrónico como si lo ha sido por correo ordinario.
Todos los artículos recibidos para ser considerados para su publicación serán sometidos a un proceso de revisión. La revisión será realizada por tres expertos independientes. Para asegurar un proceso de revisión lo más correcto posible los nombres de los autores y los revisores permanecerán confidenciales.
Una vez revisado un artículo se enviará por correo ordinario una carta con los resultados de la revisión, tanto si este ha sido enviado por correo electrónico como si lo ha sido por correo ordinario. En el caso de que el artículo haya sido rechazado se adjuntarán las valoraciones de los revisores.
El proceso de revisión está libre de costes para los autores.
Una vez que un artículo haya sido aceptado, se solicitará a los autores que transfieran los derechos de autor del artículo a la Asociación Española de Métricas de Sistemas Informáticos. Recibida la transferencia, se solicitará a los autores el envío de una versión del artículo lista para publicación que se deberá enviar en formato Microsoft Word.
La publicación de un artículo en la revista está libre de costes para los autores.

Guía para la preparación de manuscritos
El texto deberá estar escrito en un correcto castellano (Uso Español) o en Inglés (Uso Británico). Excepto el abstract que deberá estar escrito en un correcto Inglés (Uso Británico).
Abstract y Resumen. Se requiere un abstract en inglés con un máximo de 200 palabras. El abstract deberá reflejar de una forma concisa el propósito de la investigación, los principales y resultados y las conclusiones más importantes. No debe contener citaciones. Se debe presentar a continuación del abstract en inglés una traducción del mismo al castellano bajo el epígrafe Resumen.
Palabras clave. Inmediatamente después del Resumen se proporcionarán un conjunto de 5 palabras clave evitando términos en plural y compuestos, tampoco se deben usar acrónimos o abreviaturas a no ser que sean de un uso ampliamente aceptado en el campo del artículo. Estas palabras claves serán utilizadas a efectos de indexación.
Subdivisión del artículo. Después del Abstract y el Resumen, que no llevarán numeración, se debe dividir el artículo en secciones numeradas, comenzando en 1 y aumentando consecutivamente. Las subsecciones se numerarán 1.1 (1.1.1, 1.1.2, etc.), 1.2, etc. No se deben incluir subdivisiones por debajo del tercer nivel (1.1.1). Cada sección o subsección debe tener un título breve que aparecerá en una línea separada.
Apéndices. Si hay más de un apéndice, se deben identificar como A, B, etc. Las ecuaciones en los apéndices tendrán una numeración separada: (Eq. A.1), (Eq. A.2), etc.
Agradecimientos. Se deben situar antes de las referencias, en una sección separada.
Tablas. Se deben numerar las tablas consecutivamente de acuerdo con su orden de aparición en el texto. Se deben poner títulos a las tablas debajo de las mismas.
Figuras. Se deben numerar las figuras consecutivamente de acuerdo con su orden de aparición en el texto. Se deben poner títulos a las figuras debajo de las mismas.
Referencias. Se debe verificar que cada referencia citada en el texto se encuentra también en la lista de referencias y viceversa. Los trabajos no publicados o en proceso de revisión no pueden ser citados.
-*Citaciones en el texto*: Un solo autor. El primer apellido del autor, seguido de una coma y la primera inicial, seguida de un punto, a continuación, tras una coma, el año de publicación. Todo entre corchetes. Dos o más autores. Los nombres de los autores, siguiendo el formato de un solo autor, separados por puntos y comas y el año de publicación. Lista. Las listas deberán ser ordenadas, primero de forma alfabética y luego, si fuera necesario, de forma cronológica. Si hay más de una referencia del mismo autor en el mismo año deben ser identificadas por las letras “a”, “b”, etc., situadas después del año de su publicación.
-*Referencias*. Véase Volumen 1 Número 1 de esta publicación. Apartado 2.8.2.
Formato
-*Tamaño de la Página*: Deberá ser Carta (21,6 cm de ancho por 27,9 de largo). Las páginas irán sin numeración.
-*Tipo de Letra*: Deberá ser Times New Roman
-*Tamaño y Formato de la letra y el texto*: Título: 18 Negrita. Texto Centrado. Título de Sección: 14 Negrita. Alineación Izquierda. Espaciado Anterior y Posterior 12. Título de Subsección: 12 Negrita. Alineación Izquierda. Espaciado Anterior y Posterior 6. Título de Sub-Subsección: 12 Normal. Alineación Izquierda. Espaciado Anterior y Posterior 6. Texto: 12 Normal. Justificado. Espaciado Anterior y Posterior 0. Sangría en Primera Línea 1
-*Interlineado*: 1 Línea
-*Columnas*: 2. Todo el texto excepto el título, datos de los autores, abstract y resumen debe presentarse a 2 columnas

Socios Institucionales

ALCAMPO S.A.
ALI
AI2
ASOCIACIÓN TÉCNICA DE CAJAS DE AHORROS
ATOS ORIGIN
BANCO DE ESPAÑA
BBVA
CAELUM INFORMATION & QUALITY TECHNOLOGIES
CARE TECHNOLOGIES S.A.
CAST SOFTWARE ESPAÑA
C.E.C.A.
CENTRO DE CÁLCULO DE ALAVA, S.A.
COMPUTER ASSOCIATES ESPAÑA
COMPUWARE, S.A.
CORITEL, S.L.
DELOITTE, S.L.
EL CORTE INGLÉS
ELITE SISTEMAS DE CONTROL
ENDESA SERVICIOS
EUROPEAN SOFTWARE INSTITUTE
EVERIS
EWORK-LINE TECHNOLOGY SERVICES, S.A.
GAS NATURAL INFORMÁTICA
GESEIN
IBERDROLA
IBERIA
ICM
IEE
INDRA SISTEMAS S.A.
INDRA SOFTWARE LABS, S.L.
INSA
IT·DEUSTO, S.L.
LA CAIXA
LEDA CONSULTING, S.L.
LINEA DIRECTA ASEGURADORA
MAPFRE INTERNET
MTP
NESS PRO SPAIN
ONCE
OPTIMYTH SOFTWARE TECHNOLOGIES
SADIEL
SOFTWARE AG, ESPAÑA, S.A.
SOGETI ESPAÑA, S.L.
SOPRA PROFIT, SAU
TECNOLOGÍA Y CALIDAD DE SOFTWARE, S.A.
TELEFÓNICA DE ESPAÑA, S.A.U.
UNIVERSIDAD CARLOS III
UNIVERSIDAD DE ALCALÁ DE HENARES
UNIVERSIDAD DE DEUSTO
UNIVERSID OBERTA DE CATALUNYA
UNIVERSIDAD POLITÉCNICA DE MADRID
UNIVERSIDAD POLITÉCNICA DE VALENCIA

AEMES
Asociación Española de Métricas de Sistemas Informáticos
(N.I.F. G-81 76 73 86)

12 y 13 de noviembre de 2008

IX Conferencia Anual de la Asociación Española de Métricas de Sistemas Informáticos.

GESTIÓN DEL SERVICIO DE TI: GOBIERNO, INDICADORES, MÉTRICAS Y FINANZAS

PATROCINADORES PLATA

MÉTODOS Y TECNOLOGÍA

POLITÉCNICA

PATROCINADORES BRONCE

gesein