View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by El Servicio de Difusión de la Creación Intelectual

Coloured Petri Nets como apoyo a la Gestión de proyectos de Continuidad del Negocio

Sergio Machuca[1], Gabriela A. Sasco[1],

[1] Telemática, Eduardo Acevedo 1622,
11200, Montevideo, Uruguay
{ smachuca, gsasco}@telematica.com.uy

Resumen. Las tecnologías de la información son clave en el éxito de las organizaciones. Su utilización requiere complejas infraestructuras que incluyen gran número de componentes (aplicaciones, servidores, etc.). Esto implica que los impactos y riesgos motivados por fallas o indisponibilidades crecen con cada nueva aplicación, mejora de la red o actualización de los mismos.
COBIT, ITIL e ISO 27000 plantean la necesidad de conocer los riesgos que puedan afectar la continuidad del negocio y contar con planes adecuados y alineados con los objetivos de la organización. Se debe asegurar que los servicios críticos estén disponibles ante cualquier evento que pueda afectar la organización.
El Análisis de Impacto al Negocio (BIA) es el punto de partida de todo proyecto de Continuidad de Negocio.
En este artículo se presenta como representar la infraestructura utilizando Coloured Petri Nets. Se describe como aplicar esta representación en el BIA para conocer los recursos involucrados en los servicios.

Keywords: Business Impact Analysis, Business Continuity Management, Coloured Petri Nets, Continuidad del Negocio

1 Introducción

Las tecnologías de la información son actualmente un factor determinante en el éxito de las organizaciones y su utilización impacta los procesos del negocio requiriendo a menudo infraestructuras de TI muy complejas.

Los sistemas de información se han vuelto críticos, pues son los que sustentan los procesos de negocio. Por ello, las organizaciones deben disponer de planes para asegurar la continuidad de dichos sistemas, que permita mantener sus servicios operativos en caso de situaciones imprevistas.

Los impactos y riesgos motivados por fallas o indisponibilidades crecen con cada nueva aplicación, mejora de la red o actualización de los sistemas o aplicaciones. Cualquier interrupción de los servicios si no es conocida de antemano o es muy prolongada, puede convertirse en una situación catastrófica para la organización.

Los responsables de TI deben encontrar formas de mitigar o minimizar, en la medida de lo posible y de forma rentable, los riesgos y efectos de las interrupciones imprevistas. Los directivos por su parte deben tener la garantía de que sus activos de información, datos y aplicaciones, estarán disponibles.

Los estándares más difundidos y aceptados como COBIT [1], ITIL [2], ISO 27000 [3] aportan una guía a la solución a este problema introduciendo la necesidad de la gestión de la continuidad (BCM).

La **gestión de la continuidad del negocio** (Business Continuiry Management - BCM) [11],[12],[13] es un proceso interno de una organización cuyo objetivo es asegurar que los procesos de negocio críticos estén disponibles para clientes, proveedores y otros stakeholders que necesiten acceder a ellos. Entre las actividades necesarias se pueden mencionar gestión de proyectos, backups, gestión de cambios, etc. Los principales objetivos son: Preparar la organización para afrontar adversidades; Garantizar ante cualquier evento la Continuidad de las operaciones críticas, integridad de empleados, activos, imagen empresarial, reputación, así como también brindar un servicio a los clientes de nivel aceptable y cumplir con acuerdos y compromisos con terceros; Proveer confianza para stakeholders internos y externos; Contar con procesos de documentación y mejora continua; etc.

Es necesario establecer procedimientos operativos y medidas de seguridad con el objetivo de salvaguardar la operación, el centro de cómputos, la infraestructura física, el personal, los procedimientos operativos, la información y documentación contra cualquier evento que, intencional o accidentalmente, pueda afectar la organización.

Para establecer políticas de continuidad se requiere de un Análisis de Impacto al Negocio (Business Impact Analysis - BIA) [10],[11],[12],[13],[14] que permita disponer de un inventario de todos los procesos de la Organización, y de los recursos de TI que los soportan para clasificarlos de acuerdo a su prioridad de recuperación.

Ninguna de las metodologías mencionadas define como modelar la infraestructura. En [4],[5],[6] se presentó como representar la infraestructura de TI utilizando ASDG y Coloured Petri Nets (CPNets). Se mostró la forma de utilizar esas representaciones como apoyo en la gestión de cambios en componentes de infraestructura y en la gestión de la disponibilidad. En [7] y [8] se observan propuestas similares. Todos estos trabajos, proponen analizar el impacto en los servicios (procesos de negocio) a partir de fallas en componentes individuales (ej. calcular la disponibilidad analizando impactos ante fallas en componentes [5],[8]; analizar el impacto de la falla en un componente previo a realizar un cambio [6]; realizar análisis de riesgo a partir del estudio de la correlación de amenazas y vulnerabilidades [7]).

En [6] se propuso utilizar CPNets para representar la infraestructura de TI como apoyo en la gestión de cambios. Se optó por CPNets, porque permiten modelar diversas configuraciones que con ASDG no era posible.

En este artículo se presenta como aprovechar esa representación con CPNets, para brindar apoyo a proyectos de Continuidad (BCM).

En particular, el objetivo es utilizar la representación en el BIA, paso esencial en un proyecto de Continuidad del Negocio (BCM) que requiere de un inventario actualizado de todos los procesos de la Organización, así como los recursos tecnológicos en los que se soportan tales procesos para luego poder clasificarlos.

El artículo se organiza como sigue: primero una introducción a los principales modelos de gestión, luego conceptos básicos de la gestión de la continuidad.

Posteriormente se describe la forma de utilizar CPNets para representar la infraestructura de TI y apoyar la gestión de cambios y disponibilidad. También como adaptar esa representación para conocer la infraestructura involucrada en un proyecto de BCM.

2 Modelos de Gestión

En este documento nos enfocamos en tres estándares específicos, ampliamente adoptados a nivel global COBIT, ITIL e ISO 27000.

COBIT ® 4.1 [1]: Publicado por el ITGI (IT Governance Institute) es un marco de referencia de alto nivel para el control y el gobierno de TI. Su misión es "investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores".

COBIT hace énfasis en la orientación al negocio y fue diseñado no solo para ser utilizado por usuarios y auditores, sino también, para ser utilizado como una lista de verificación detallada para los propietarios de los procesos de negocio. En el Marco Referencial de COBIT se proporcionan herramientas a los propietarios de procesos de negocio que facilitan el cumplimiento de sus responsabilidades. El marco referencial comienza con la premisa "*Con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos de TI agrupados en forma natural"*.

COBIT define 34 objetivos de control de alto nivel, uno para cada proceso de TI, agrupados en: planeación & organización, adquisición & implementación, entrega (de servicio) y monitoreo. En particular se pueden mencionar los siguientes: DS1 Definir Niveles de Servicio, DS3 Administrar Desempeño y Capacidad, DS4 Garantizar la Continuidad del Servicio, DS9 Administrar la Configuración.

DS4 Garantizar la Continuidad del Servicio. La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio [16].

Por su parte ITIL [2],[9]: Publicado por la OGC (Office of Government Commerce) del gobierno británico proporciona un marco de referencia de mejores prácticas para la gestión de servicios de TI. ITIL ofrece un marco para todas las actividades de TI, como parte de la entrega de servicios. Las actividades se dividen en procesos, que proporcionan el marco para gestionar los Servicios TI en forma más madura.

ITIL provee "mejores prácticas" para la gestión de TI las cuales proveen: Guías para alinear los servicios de TI con los requerimientos de negocio; Un lenguaje común para TI y el negocio; Un marco referencial, no una metodología; Un conjunto de mejores prácticas neutral a los proveedores; Guías, no un como hacerlo paso a paso para que una organización implemente procesos de gerenciamiento de TI.

Además del modelo de procesos se encuentran: Guías en la planificación e implementación; Sugerencias de organización, roles y habilidades requeridas; Sugerencias para la educación y el entrenamiento; Descripción de atributos clave en herramientas; Ejemplos de políticas y procedimientos

ITIL define que la gestión de la continuidad de los servicios debe controlar los riesgos que podrían impactar los servicios de TI. La Gestión de la Continuidad del Servicio de TI (IT Service Continuity Management, ITSCM) debe considerar que quienes proveen los servicios de TI, estén siempre en condiciones de proveer un nivel aceptable del servicio, reduciendo el riesgo de eventos a niveles aceptables. El objetivo es disponer de un plan de recuperación de servicios de TI. La ITSCM debe diseñarse para que apoye la gestión de la continuidad del negocio.

Por último, la ISO/IEC 27002:2005, derivada de la norma BS 7799 del gobierno británico, renombrada ISO/IEC 17799:2005, proporciona un marco de referencia para la gestión de seguridad de información [3], establece las guías y principios generales para comenzar, implementar, mantener y mejorar la Gestión de la Seguridad en una organización. Sus objetivos proveen una guía general sobre las metas comúnmente aceptadas para la Gestión de la Seguridad de la Información. El dominio 14 de este estándar, establece guías para gestionar la continuidad:

14.1 Aspectos de seguridad de la información en la gestión de continuidad del negocio. [3],[11]

Objetivo: Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y asegurar su recuperación oportuna.

El objetivo es el de implementar un proceso de gestión de la continuidad del negocio para minimizar el impacto y la recuperación por perdida de activos de información en la organización (la cual puede ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación. En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

A grandes rasgos, las 3 hacen énfasis en identificar, controlar y mantener todos los componentes de TI, como forma de gestionar adecuadamente la continuidad de la operación de los servicios. [13]

3. Continuidad del Negocio

Continuidad del Negocio está compuesta por la **Planificación para Recuperación de Desastres (DRP)** y la **Planificación para el Restablecimiento del Negocio. DRP** es la capacidad de afrontar una interrupción de los servicios de una organización mediante un plan para restablecer los procesos críticos [11],[12],[13].

Análisis y Clasificación de los Procesos del Negocio Todo proyecto de BCM o DRP debe comenzar con un Análisis de Impacto al Negocio (BIA) [10],[11],[12], [13],[14]. Es esencialmente un informe que muestra el costo de la interrupción de los

procesos de negocio, con el cual la organización tiene la capacidad de clasificar los mismos en función de su criticidad y establecer la prioridad de recuperación (o su orden). Incluye un inventario actualizado de los recursos humanos, tecnológicos y materiales en los que se soportan tales procesos.

En el **BIA** se elabora un inventario de los recursos humanos, tecnológicos y materiales que soportan los procesos críticos, lo que permite enfocar los esfuerzos de prevención y recuperación sobre los elementos críticos de la infraestructura.

En grandes organizaciones, donde existe gran número de aplicaciones y equipamiento con complejas interoperabilidades, suele ser muy difícil disponer de un inventario completo. Armar dicho inventario, clasificarlo y medir el impacto de eventos y su probabilidad de ocurrencia, suele insumir un tiempo considerable y requerir de la disponibilidad de muchos recursos humanos.

El objetivo de este trabajo es definir una metodología que apoye en la etapa del BIA, para conocer los recursos involucrados en un servicio (recursos de TI, servidores, aplicaciones, etc). Esta metodología permitirá disminuir los tiempos de confección del inventario. El BIA identificará cuales son los servicios esenciales para el negocio y cuales son los componentes de TI requeridos para brindarlos. A partir de la información generada se arma el plan de recuperación.

4. Especificación

Los objetivos que se persiguen con la especificación son los siguientes:

1. Conocer el impacto (usuarios afectados, administradores, aplicaciones, servicios, conexiones, etc.), cuando un componente de la infraestructura (red, hardware, software de aplicación, eléctrico, etc), deje de funcionar ya sea por un cambio programado o por falla del mismo [4],[5],[6].
2. Conocer los recursos tecnológicos involucrados en el soporte de un determinado servicio o proceso de negocios.

Para resolver ambos objetivos, se necesitan conocer los componentes de infraestructura de TI, su relación con otros componentes quienes son los usuarios de los servicios y quienes son los administradores de los distintos componentes, etc.

4.1 Metodología

En [6] se propuso utilizar Coloured Petri Nets (CPNets) para representar la infraestructura de TI. Con ellas se pudo representar diversas configuraciones que en trabajos anteriores con ASDG [4],[5] no fue posible. En esos trabajos, se analizó como realizar estudios de impacto previos a la realización de un cambio en la infraestructura y como estudiar la disponibilidad de los servicios teniendo en cuenta los impactos de las fallas en componentes.

Se representó la infraestructura de TI como una CPNet [16], donde los recursos de TI (servidores, dispositivos de red, software de base, aplicaciones, dispositivos eléctricos) y usuarios, son nodos (Places) y sus relaciones de dependencia, conexiones físicas y eléctricas, son conexiones (transitions) entre ellos.

Analizar el impacto de un cambio o falla de un componente se traduce en encontrar los nodos alcanzados en una ejecución de la CPNet partiendo de ese componente.

En este artículo, se muestra como realizar un análisis inverso, o sea, conocer los recursos involucrados en la prestación de un servicio. Para ello **no se puede utilizar el procedimiento anterior**, pues no es posible recorrer la CPNet en forma inversa. Por ello, se define una CPNet simétrica. De esta forma, encontrar los recursos involucrados en un servicio, consiste en conocer los nodos alcanzados en una ejecución de la CPNet simétrica a partir del servicio analizado

4.2 Petri Nets [15]

Una Red es definida formalmente como una tripleta N = (S, T, F) tal que:

S y **T** son conjuntos disjuntos (los elementos de S son llamados *S-elementos* y los de T, *T-elementos*)

F $\subseteq$ (S * T) $\cup$ (T * S) es una relación binaria entre **S** y **T**.

Una *marcación* es una asignación de tokens a los S-elementos que define el estado de una red. El número y posición de los tokens puede cambiar durante la ejecución .

La ejecución es controlada por el número y distribución de los tokens. Una red se ejecuta disparando transiciones. Una transición se dispara removiendo tokens de los S-elementos de entrada y creando nuevos en los de salida, pudiendo ser disparada cuando se encuentra habilitada, es decir cuando en cada S-elemento de entrada hay al menos un token por cada arco de entrada de la transición.

A partir de esta definición, es posible definir diversos tipos de interpretaciones de las redes de Petri, permitiendo especificar colas y tokens con identidad, de manera de simplificar la cantidad de Places y Transiciones, así como especificar tiempos.

Place/Transition nets (P/T nets).

En esta clase de redes de Petri se llaman «Places» a los *S-elementos* y «*Transitions*» a los *T-elementos*. Son las comúnmente llamadas *Petri Nets* y básicamente es a partir de estas que surgen las distintas extensiones.

Coloured PetriNets (CPNets) [16]

Son una extensión de las anteriores en que las marcas pueden pertenecer a un tipo determinado (coloreado), lo cual permite diferenciar distintas marcas.

Las principales diferencias con las P/T Nets son: los “Places” de una CPNet pueden contener marcas de un tipo determinado; los arcos de una CPNet poseen expresiones de arco, y las transiciones pueden tener una condición de habilitación.

4.3 Especificación con Petri Nets

Para representar la infraestructura de TI con Petri Nets se consideran los componentes como nodos ***“S”*** y las dependencias como nodos ***“T”*** de la misma. La Petri Net se define de la siguiente manera:

$$PN = (C, T, FF) \quad (1)$$

Donde: **C** son los componentes de la infraestructura

T y **FF** son transiciones que representan las relaciones entre los componentes

T es el conjunto de transiciones de la Red de Petri, y **FF** representa las relaciones entre los "S" elementos y los "T" elementos. Ambos nos permiten modelar las relaciones entre componentes. (Ver Fig. 1).

Se utilizan tokens diferenciados para modelar situaciones como clusters, balanceadorees de carga, dependencias temporales, etc.

Fig. 1. Ejemplo de relación entre recursos

4.4 Petri Net Simétrica

La Petri Net simétrica queda definida de la siguiente manera:

$$PNSimétrica = (C, T, FFSimétrica) \quad (2)$$

C y **T** son las los mismos que PN.

FFSimétrica por su parte queda definida como sigue. (Ver ejemplo Fig. 2).

$$FF = \forall s_i t_j \in FF \Rightarrow t_j s_i \in FFSimétrica \quad (3)$$
$$\forall t_i s_j \in FF \Rightarrow s_j t_i \in FFSimétrica$$

Fig. 2. PN Simétrica

4.5 Análisis

En [4],[5],[6] se mostró como realizar un análisis de impacto, partiendo de fallas en componentes para analizar servicios afectados. Este análisis es utilizado como apoyo en la gestión de cambios y en la gestión la disponibilidad.

En un proyecto de BCN se requiere lo opuesto, o sea conocer los recursos involucrados en un determinado servicio (recursos de TI, servidores, aplicaciones, etc). En el BIA se identificará cuales son los servicios esenciales para el negocio y con esta metodología se conocerá cuales son los componentes de TI requeridos para brindarlos. Con la información generada se puede armar el plan de recuperación.

Análisis de componentes de un servicio

La CPNet (PN) definida originalmente, contiene los servicios ofrecidos, los componentes de TI y las relaciones y dependencias entre ellos. Para conocer el impacto de una falla en un componente se realiza un análisis de impacto (análisis de alcance) a partir del nodo afectado.

Como se mencionó anteriormente, no se puede utilizar el procedimiento anterior para conocer los componentes de un servicio, pues no es posible recorrer la Petri Net en forma inversa y por ello se debe utilizar la ***PN Simétrica***.

En nuestra representación, los servicios son representados por los usuarios.

Para conocer los componentes involucrados en un servicio, se marca el "*usuario del servicio*", a analizar. Se construye el árbol de alcance en la ***PN Simétrica***. El resultado es la lista de todos los componentes involucrados en la prestación del servicio (recursos de TI, servidores, aplicaciones, etc).

Esta información permite planificar la recuperación de los servicios.

4.6 Caso de Estudio

Consideremos ahora la siguiente realidad representada gráficamente en la figura 3. En ella se pueden apreciar los componentes (hardware, aplicaciones, etc) y los usuarios que dependen de ellas. Se utiliza una infraestructura simple que permita observar fácilmente las relaciones. Sin embargo en organizaciones complejas, la red puede llegar a contener cientos o miles de componentes.

De la misma forma, en la figura 4 se observa la ***PN Simétrica.*** En ella figuran los mismos usuarios y componentes, pero las dependencias son simétricas a la anterior.

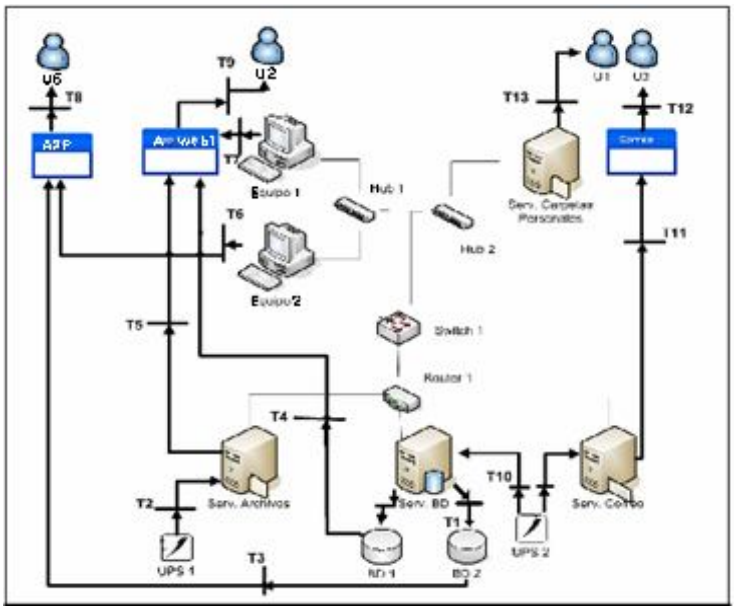

Fig. 3. PN Ejemplo

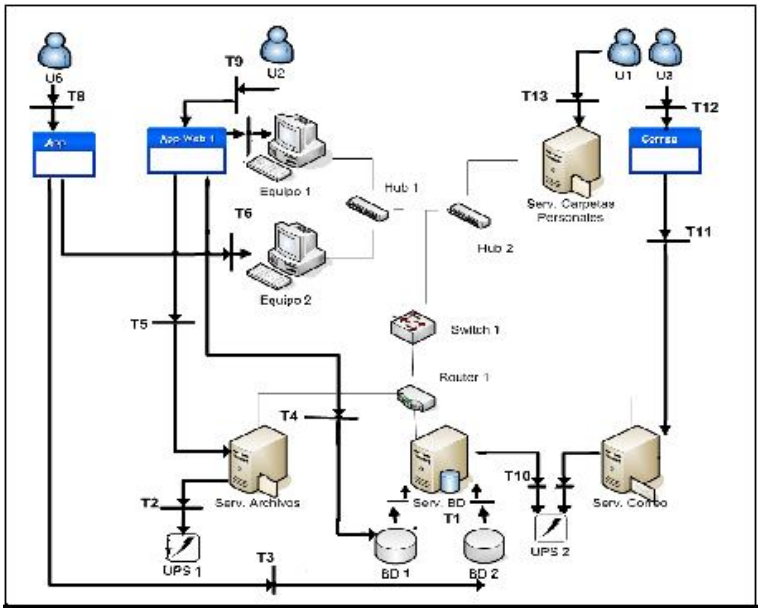

Fig. 4. PN Simétrica Ejemplo

El ejemplo anterior es muy simple, pero permite observar claramente la representación y el análisis.

Sin embargo, en grandes organizaciones, donde se tiene cientos de equipos y aplicaciones y donde existe una intrincada relación entre aplicaciones (webservices, N-Tier, etc).la realidad puede ser muy compleja y el análisis es complicado.

Análisis de componentes de un servicio

El servicio ofrecido por la aplicación ***APP*** es utilizado por el usuario ***U6***. Como ya comentamos en nuestra representación, un *usuario* se corresponde con un *servicio*, por lo que el estudio lo realizaremos a partir del usuario ***U6***.

En la siguiente figura, podemos observar, que el servicio utilizado por ***U6*** depende de ***APP***, quien a su vez depende de ***BD2*** y ***Equipo2***. Siguiendo con el análisis se observa que ***BD2*** depende de ***ServidorBD*** y de ***UPS2.***

Esta información, nos permite conocer los componentes involucrados en el servicio y planificar los planes de recuperación.

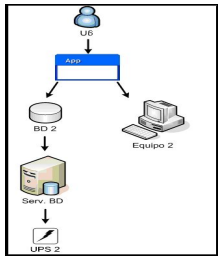

Fig5. Arbol de alcance desde servicio U6

5 Conclusión y Trabajos Futuros

Se analizó la problemática de la gestión de la continuidad de los servicios de TI y la necesidad del BIA para conocer los componentes involucrados en los servicios.

Se utilizó una propuesta que modela la infraestructura de TI con CPNets, representando los componentes de hardware y software y sus dependencias. En esta CPNet, se realizan análisis de impactos para conocer los componentes afectados por la falla de un componente. El análisis fue utilizado para coordinar los cambios en la infraestructura y la gestión de la disponibilidad de los servicios.

Se adaptó esa representación, y se construyó una CPNet simétrica que permite un recorrido inverso para conocer los componentes involucrados en un servicio. La salida de este análisis se utiliza en el Análisis de Impacto al Negocio (BIA).

Referencias

1. COBIT. http://www.isaca.org.
2. http://www.itil.org/en/vomkennen/itil/servicedesign/servicedesignprozesse/itservicecontinuitymanagement.php (ITIL Service Continuity Mangement). Ult. acc. 2012.
3. ISO 27000. http://iso27002.wiki.zoho.com/14ContinuidaddeNegocio.html. Ult. acc. 2012.
4. S.Machuca, G.Sasco, N.Chiaro: Modelo de grafos para el estudio de la disponibilidad y la gestión de los niveles de servicio en servicios de IT, MVD TELCOM 2006 (I Congreso Regional de Telecomunicaciones).
5. S.Machuca, G.Sasco,. Modelo de grafos para el estudio de la disponibilidad y la gestión de los niveles de servicio en servicios de IT, CACIC 2007.
6. S.Machuca, G.Sasco, IT Change Management using Coloured Petri Nets, ALIO/INFORMS International Meeting 2010.
7. P. Stephenson, A Formal Model for Information Risk Analysis Using Colored Petri Nets. CPN 2004 – 5th Annual Workshop on Colored Petri Nets.
8. N. Milanovic, B.Milic and M. Malek. Modeling business process availability. IEEE International Workshop on Methodologies for Non-functional Properties in Services Computing (MNPSC), Hawaii, July 2008.
9. G. Kemmerling, D.Pondman. Gestion de servicios TI – Una introducción a ITIL. ISBN 90-77212-18-3, 2004.
10. J. L. Barry Lyons IV, Preparing For A Disaster: Determining the Essential Functions That Should Be Up First, SANS Institute
11. Alejandro Cerezo H, Soportando y Auditando la Gestión de la Continuidad del Negocio (BCM), ISACA Capítulo Monterrey
12. Manuel Ballester, Continuidad del Negocio, FIST Madrid 2005
13. Alvaro Rodríguez de Roa, Modelos de madurez en Business Continuity Management paso a paso hacia la excelencia, ISACA Latin CACS 2011
14. José Angel Peña, COBIT aplicado para asegurar la continuidad de las operaciones, ISACA Latin CACS 2005
15. Reisig W., Petri Nets, an introduction (EATCS Monographs on the Theoretical Computer Science Vol 4), Berlin Springer-Brlag, 1985.
16. K. Jensen: A Brief Introduction to Coloured Petri Nets. In: E. Brinksma (ed.): Tools and Algorithms for the Construction and Analysis of Systems. Proceeding of the TACAS'97 Workshop, Enschede, The Netherlands 1997, Lecture Notes in Computer Science Vol. 1217, Springer-Verlag 1997, 203-208.