6ta Jornada sobre la Biblioteca Digital Universitaria
JBDU 2008

"Los desafíos de la Web Social"

30 y 31 de octubre de 2008
Universidad Nacional de La Plata, ROBLE Red de Bibliotecas
La Plata, provincia de Buenos Aires, Argentina

Plan de Riesgos para la implementación, desarrollo y mantenimiento de componentes de Web 2.0 en Bibliotecas, caso de estudio en una Biblioteca Especializada

Mgter. Lic. Horacio Daniel Kuna ; Asc. Sergio Caballero ; Bibl. Susana Eunice Jaroszczuk ; Prof. Mirta Miranda

Universidad Nacional de Misiones - Facultad de Humanidades y Ciencias Sociales
Departamento de Bibliotecología

RESUMEN

La era tecnológica y la globalización de la economía, ha traído como consecuencia el aumento sustancial de los riesgos en general, y en particular en el proceso software. En estos últimos tiempos la evolución de las aplicaciones tradicionales hacia aplicaciones Web enfocadas al usuario final que se denomina Web 2.0 y la no administración de los mismos puede implicar en cualquier Biblioteca la posibilidad del fracaso del mejor proyecto.

La metodología desarrollada en este trabajo es una herramienta que brinda la posibilidad de efectuar tareas de identificación de riesgos, plan de aversión en base a taxonomías estándar para la implementación de componentes Web 2.0 en bibliotecas especializadas.

PALABRAS CLAVES: PLAN DE RIESGO, WEB 2.0, GESTIÓN DE RIEGOS, TAXONOMÍAS (TIPOLOGÍA), BIBLIOTECA, APLICACIÓN INFORMÁTICA.

1. INTRODUCCIÓN

1.1 Riesgo

Un riesgo es una variable del proyecto que pone en peligro o impide el éxito del mismo. Es la "probabilidad de que un proyecto experimente sucesos no deseables, como retrasos en las fechas, excesos de costes, o la cancelación directa"[1]

Se han producido amplios debates sobre la definición adecuada para riesgo de software, y hay acuerdo común en que el riesgo siempre implica dos características:

- Incertidumbre: el acontecimiento que caracteriza al riesgo puede o no puede ocurrir; por ejemplo, no hay riesgos de un 100 por ciento de probabilidad.
- Pérdida: Si el riesgo se convierte en una realidad, ocurrirán consecuencias no deseadas o pérdidas.

Suele ser común el confundir preocupaciones, riesgos y problemas: mientras que una **preocupación** es cualquier situación sobre la cual existen dudas en algún determinado contexto y que, por lo tanto, será evaluada como un posible riesgo, un **problema** es un riesgo que, efectivamente, se ha producido (véase Figura 1 - Preocupaciones, Riesgos y Problemas).

Figura 1 Preocupaciones, Riesgos y Problemas

1. 2 Gestión de Riesgos

Un efectivo proceso de **gestión de riesgos** es un importante componente en todo proyecto de software exitoso y en el cual la Web 2.0 y sus componentes forman parte del ello; el principal objetivo de dicho proceso constituye posibilitar tanto al proyecto como a las organizaciones el cumplimiento de su misión y de sus propósitos.

---

[1] CAPERS, Jones. Assessment and Control of Software Risk, Upper Saddle River, NJ: Prentice-Hall, 1993.

La gestión de riesgos permite definir en forma estructurada, operacional y organizacional, una serie de actividades para gestionar los riesgos de los proyectos a lo largo de todas las fases de su ciclo de vida de desarrollo de software. En la mayor parte de los casos, esto se traduce en la creación de planes tendientes a impedir que los riesgos se transformen en problemas o a minimizar su probabilidad de ocurrencia o impacto.

1. 3 Propósito del plan de gestión de riesgos

El propósito del plan es identificar los riesgos que se puedan presentar en el desarrollo del proyecto, analizarlos, calcular la exposición y en base a ello poder priorizarlos, para establecer estrategias de control y resolución, que permitan ejercer una correcta supervisión de los mismos.

Es por esta razón que, para que un proyecto de desarrollo pueda llevarse a cabo dentro de los tiempos establecidos y los costos previstos, los riesgos deben ser identificados y controlados, es decir se debe realizar un adecuado "Análisis y Gestión de Riesgos".

Este trabajo pretende ser una herramienta que permita seleccionar e implantar las medidas o 'salvaguardas' para conocer, prevenir, impedir, reducir o controlar los riesgos identificados, y así reducir al mínimo su potencialidad o posibles perjuicios para la implementación de componentes de Web 2.0 en bibliotecas Especializadas.[2]

2. METODOLOGIA

2.1 Inventario de activos:

Se deberá analizar los activos que podrían ser amenazados por algún tipo de riesgo, como ser. Hardware y telecomunicaciones, software y personal.

2.2 Propósitos y Objetivos del análisis de riesgos

En este punto se debe establecer los objetivos generales del análisis de riesgos y establecer claramente los limites que tendrá el proyecto.

---

[2] MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid : Consejo Superior de Informática, Ministerio de Administraciones Públicas, 2006.

2.3 Equipo de Trabajo

Establecidos los limites y objetivos del análisis de riesgo se debe formalizar el equipo de trabajo que realizará la tarea.

2.4 Taxonomía de Riesgos

La clasificación de los riesgos -también denominadas taxonomías de riesgos- puede servir de ayuda para elaborar un enfoque coherente, reproducible y medible. Las listas de clasificación permiten al equipo pensar con mayor amplitud sobre los riesgos que pueden afectar al proyecto dado que se dispone de una lista de áreas del proyecto susceptibles de esconder riesgos.

Existen muchas taxonomías o clasificaciones para los riesgos de proyectos generales de desarrollo de software. Para el presente trabajo se ha escogido la clasificación propuesta por el Software Risk Management (SRM) desarrollado por el Software Engineering Institute. [3]

A continuación se presenta la *Clasificación de los elementos de la taxonomía del software*[4], en el marco del presente proyecto se definen las clase y elementos más importantes y

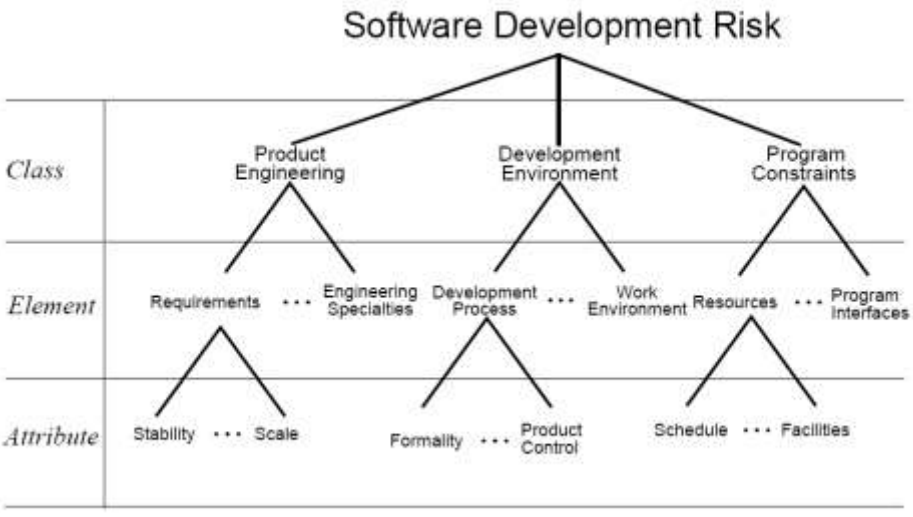

Figura 2 Clasificación de los elementos de la taxonomía del software

[3] HIGUE
Pittsburg
Disponib el 8 de agosto 2008].

[4] CARR, Marvin ; KONDA, Suresh L. ; MONARCH, Ira ; ULRICH, Carol F. ; WLKER, Clay F. Taxonomy-Based Risk Identification. Pittsburgh, Pennsylvania : Software Engineering Institute, Carnegie Mellon University, 1993. Disponible en: www.sei.cmu.edu/pub/documents/93.reports/pdf/tr06.93.pdf. . [Consultado el 8 de agosto 2008].

2.5 Declaración de los Riesgos

Las definiciones genéricas de un riesgo no hacen desaparecer la incertidumbre y dan lugar a distintas interpretaciones del riesgo. Las definiciones que no dejan lugar a dudas permiten a los equipos:

- Asegurarse de que todos los miembros del equipo comprenden el riesgo de la misma forma. Es decir a los informáticos y bibliotecarios que forman parte del proyecto.
- Comprender la causa o causas del riesgo y la relación con los problemas que puedan surgir.
- Disponer de una base para realizar un análisis formal y cuantitativo y planear los esfuerzos.

En las declaraciones de riesgos se definen en forma mas precisa los riesgos identificados, siguiendo un proceso de declaración en dos partes (condición – consecuencia). La primera parte de la declaración de riesgo se denomina **condición** y describe una situación o atributo del proyecto existente que el equipo prevé que puede resultar en una pérdida en el proyecto o en una reducción de beneficios. La segunda parte de la declaración de riesgo se denomina **consecuencia** y describe el atributo o situación no deseable del proyecto. Además se incluyen los **efectos** que tendrían estos riesgos de no controlarse debidamente.

Análisis y prioridad de los riesgos

La meta principal del análisis de riesgos consiste en establecer las prioridades de los elementos de la lista de riesgos y determinar cuál de ellos justifica la reserva de recursos para el planeamiento. Por otro lado la asignación de prioridades a los riesgos permitirá tratar en primer lugar los riesgos más importantes del proyecto.

2.6 Estimación de la probabilidad

La probabilidad del riesgo es una medida que calcula la probabilidad de que la situación descripta en el apartado de consecuencias de los riesgos de la declaración de riesgos llegue a producirse de verdad.

Para cuantificar la incertidumbre acerca de la ocurrencia de los riesgos se emplearán las categorizaciones expresadas en lenguaje natural, en base a un rango de probabilidades establecido en un cuadro de referencia (Ver Tabla 4: estimación de impacto).

2.7 Estimación del impacto

El impacto del riesgo calcula la gravedad de los efectos adversos, la magnitud de una pérdida o el costo potencial de la oportunidad si el riesgo llega a producirse dentro del proyecto.

2.8 Exposición al riesgo

La exposición al riesgo calcula la amenaza general que supone el riesgo combinando la información que expresa la probabilidad de una pérdida real con información que indica la magnitud de la pérdida potencial en un único valor numérico.

La exposición al riesgo se calcula multiplicando la probabilidad de riesgo por el impacto. Luego se utilizará la magnitud de la exposición al riesgo para clasificar los riesgos.

Magnitud de exposición al riesgo:

Aprox. 1 = bajo riesgo.

Aprox. 2 = riesgo medio.

Aprox. 3 = alto riesgo[5]

---

[5] HIGUERA, Ronald P. y HAIMES, Yacov Y., "Software Risk Management", *Technical Report.* Pittsburgh, Pennsylvania : SEI (Software Engineering Institute) ; Carnegie Mellon University, 1996. Disponible en: *www.sei.cmu.edu/pub/documents/96.reports/pdf/tr012.96.pdf*. [Consultado el 8 de agosto 2008].

2.9 Gestión de los Riesgos

2.9.1 Líneas de Acción

Para ejercer una adecuada gestión y supervisión de los riesgos mencionados anteriormente, se elaborará un Plan de Acción y un Plan de Contingencias para cada unos de ellos.

El **Plan de Acción** será utilizado para minimizar los riesgos mediante acciones preventivas. La probabilidad de que un riesgo ocurra así como el impacto que el mismo podría ocasionar en el proyecto pueden ser mitigados encarando los problemas en forma proactiva.

El **Plan de Contingencia**, por el contrario intenta implementar respuestas rápidas para mitigar los efectos en caso de que los riesgos se concreten, es decir reducir el impacto de los mismos mediante una reacción planeada. Este plan, además definirá ciertos indicadores que permitirán poner en marcha las acciones previstas, es decir, en caso que se verifiquen ciertos disparadores se adoptarán las medidas indicadas.

3. EXPERIENCIA

En adelante se expondrá la experiencia realizada en el Centro de Documentación EBY (Entidad Binacional Yacyretá)[6]. Se tomaron como ejemplo siete riesgos, los mismos han sido autorizados por la Empresa para divulgar en el presente artículo, los demás riesgos involucrados en este proyecto se reserva por cuestiones internas de seguridad empresarial.

3.1 - Inventario de activos:

- Hardware y Telecomunicaciones: servidores, computadoras, intranet.
- Software: datos,
- Personas: bibliotecario, informático.
- Costos: adicionales no previstos inicialmente en el proyecto.

3.2 - Propósitos y Objetivos del análisis de riesgos

[6] Mediante trabajos en colaboración por medio de Convenios UNaM-EBY

Implementar componentes Web 2.0 en el Centro de Documentación, previo desarrollo de un adecuado análisis de gestión de riesgos a fin de reducir al mínimo los posibles perjuicios en su implantación.

3.3 Equipo de Trabajo

El equipo de trabajo del proyecto para la implementación componentes Web 2.0 en el Centro de Documentación, está formado por: Jefe de Proyecto, Informáticos, Bibliotecarios.

Las funciones que tienen asignadas cada grupo de los miembros del proyecto son las siguientes:

- Del Jefe de Proyecto:
    - Gestionar el presente plan.
    - Comprobar que el producto satisfaga los requerimientos establecidos.
    - Evaluar con el equipo de gestión de configuración los cambios solicitados en el caso que se presenten.
    - Ordenar al equipo de desarrollo la implementación de los cambios aprobados.
    - Supervisar el cumplimiento de la planificación de desarrollo del proyecto.
    - Adoptar las medidas necesarias tendientes a evitar retrasos en la planificación realizada.
    - Resolver los problemas económicos que se puedan presentar.
    - Interactuar con el equipo de trabajo para detectar tempranamente problemas técnicos o de personal.
    - Gestionar los informes de incidencia
- Bibliotecarios:
    - Relevamiento de los requerimientos Información.
    - Interactuar con los informáticos en el desarrollo de la estructura del proyecto.
    - Administrar el producto software.
- Informáticos:
    - Desarrollar el proyecto software.
    - Mantener el producto software.

3.4 Taxonomía de Riesgos

La siguiente tabla muestra una clasificación de alto nivel de las fuentes de riesgo de los proyectos siguiendo la taxonomía propuesta por la metodología SRM[7] organizadas en tres niveles: clases, elementos y atributos.

ID	Elemento	Riesgo	Fuente
RI-01	Planificación	Errores en la estimación del presupuesto	Jefe de Proyecto
RI-02	Planificación	Cambio de políticas de Gestión.	Dirección de la Biblioteca
RI-03	Planificación	Seguridad del sitio	Jefe de Proyecto Desarrolladores
RI-04	Equipo de Trabajo	Soporte y mantenimiento	Jefe de Proyecto
RI-05	Equipo de Trabajo	Inexperiencia del equipo técnico / bibliotecológico en el desarrollo e implementación del proyecto	Jefe de Proyecto Desarrolladores
RI-06	Equipo de Trabajo	Dificultad de comunicación de la comunicación entre los miembros del grupo de desarrollo del proyecto.	Bibliotecario / Informático
RI-07	Equipo de Trabajo	Desconocimiento o poco conociendo por parte del equipo de desarrollo en la utilización de la herramientas	Bibliotecario / Informático

Tabla 1: taxonomía de riesgos

3.5 Declaración de los Riesgos

RI-01 Errores en la estimación del presupuesto

Condición: errores en los cálculos, no estimar bien los factores que influyen en el cálculo (archivos, funciones, etc.) o el caso contrario la sobre estimación.

Consecuencia: no disponer de los recursos necesarios para terminar el proyecto a tiempo, sobrecarga de tareas al personal.

Efecto: baja calidad del Proyecto, entrega con retraso del proyecto finalizado.

RI-02 Cambio de políticas de gestión

Condición: cambio de políticas de gestión que afectan las metas y objetivos del proyecto. Consecuencia: el proyecto puede sufrir retrasos, cuanto más avanzado este el desarrollo del mismo más crítico será implementar los cambios, y generación de nuevos requisitos.

[7] Idem anterior

Efecto: perdida de tiempo en la reestructuración del proyecto, finalizar el mismo fuera de en los plazos establecidos, no obtener el resultado programado inicialmente en cuanto al producto final.

RI-03 Seguridad del Sitio

Condición: falta de experiencia del personal del proyecto en las cuestiones relacionadas a seguridad Web, control de ingreso malicioso (hackers), seguridad de acceso físico a los equipos, seguridad del software de aplicación, falta de instalación y actualizaciones de programas de seguridad.

Consecuencia: mal funcionamiento de los equipos, ingreso de datos errónea, lentitud en el procesamiento de los datos, perdida de confianza en el proyecto por parte de la Empresa.

Efecto: perdida por borrado, daño y/o robo de la información, infección de virus en la red y en los servidores, perdida de tiempo en el trabajo de reconstrucción del sistema.

RI-04 Soporte y mantenimiento

Condición: garantizar el soporte y mantenimiento del proyecto.

Consecuencia: bajo rendimiento del software, desactualización de los componentes software, bajo rendimiento de hardware, baja calidad de software.

Efecto: falta de adaptación a los cambios por parte del software, error y deficiencia en el acceso a los datos, falta soporte a fallas del equipamiento.

RI-05 Inexperiencia del equipo técnico / bibliotecológico en el desarrollo e implementación del proyecto

Condición: escaso conocimiento y experiencia de los integrantes del proyecto sobre las herramientas utilizadas y los lenguajes de programación.

Consecuencia: destinar mayor tiempo al desarrollo del proyecto, invertir tiempo y recursos económicos en la investigación y capacitación del personal.

Efecto: retrasos en la finalización del proyecto, finalizar el producto con defectos dejando en evidencia la baja calidad del mismo.

RI-06 Dificultad de comunicación entre los miembros del grupo de desarrollo del proyecto

Condición: dificultad de comunicación entre la necesidad del bibliotecario y el lenguaje técnico del informático.

Consecuencia: mala interpretación por parte de informático de las necesidades del bibliotecario, avanzar en el desarrollo de una actividad sin la validación y consenso de ambas partes.

Efecto: producto que no responde a los requerimientos del proyecto, ambiente tenso de trabajo, pérdida de tiempo en la búsqueda de acuerdo en la comunicación, evaluar cambio de personal en caso de no llegar a acuerdos de comunicación. Retraso en la entrega del Proyecto.

RI-07 Desconocimiento o poco conocimiento por parte del equipo de desarrollo en la utilización de la herramientas

Condición: algunos participantes del equipo de desarrollo pueden no contar con la experiencia suficiente en cuanto a utilización de las herramientas de desarrollo, implementación.

Consecuencia: retraso en el desarrollo de actividades definidas por el proyecto, no aprovechar por completo las herramientas técnico informáticas.

Efecto: retraso en la entrega del Proyecto.

3.6 Estimación de la probabilidad

Tabla de Cuantificación de incertidumbre.

Rango de probabilidad	Promedio para el calculo	Expresión de lenguaje natural	Valor numérico
de 1% a 10%	5 %	Baja	1
de 11 % a 25%	18 %	Poco probable	2
de 26% a 55%	40 %	Media	3
de 56% a 80%	68 %	Altamente probable	4
de 81% a 99%	90 %	Casi seguro	5

Tabla 2: estimación de probabilidad

En la siguiente tabla se expresan los riesgos identificados para el proyecto con las probabilidades estimadas subjetivamente para cada uno de ellos.

ID	Riesgo	Expresión	Probabilidad
RI-01	Errores en la estimación del presupuesto	Altamente Probable	5%
RI-02	Cambio de políticas de Gestión.	Poco Probable	40%
RI-03	Seguridad del sitio	Alta	60%
RI-04	Soporte y mantenimiento	Media	30%

RI-05	Inexperiencia del equipo técnico / bibliotecológico en el desarrollo e implementación del proyecto	Altamente Probable	25%
RI-06	Dificultad de la comunicación entre los miembros del grupo de desarrollo del proyecto.	Media	70%
RI-07	Desconocimiento o poco conociendo por parte del equipo de desarrollo en la utilización de la herramientas	Media	20%

Tabla 3: probabilidad de ocurrencia del riesgo

3.7 Estimación del impacto

Para el presente análisis se empleará la escala de medición subjetiva expresada en la siguiente tabla.

Criterio	Retraso en la planificación	Valor numérico
Insignificante	1 semana	1
Marginal	2 semanas	2
Medio	1 mes	3
Crítico	2 meses	4
Catastrófico	Mas de 2 meses	5

Tabla 4: estimación de impacto

En la siguiente tabla se definen el impacto que producirían la ocurrencia de los riegos citados anteriormente:

Riesgo	Impacto
RI-01	Marginal
RI-02	Catastrófico
RI-03	Insignificante
RI-04	Marginal

Riesgo	Impacto
RI-05	Critico
RI-06	Catastrófico
RI-07	Medio

Tabla 5: impacto debido a ocurrencia de los riesgos

3.8 Exposición al riesgo

ID	Riesgo	Probabilidad	Impacto	Exposición
RI-01	Errores en la estimación del presupuesto	5%	1	0.05
RI-02	Cambio de políticas de Gestión.	40%	5	**2**
RI-03	Seguridad del sitio	60%	1	0.60
RI-04	Soporte y mantenimiento	30%	2	0.60

RI-05	Inexperiencia del equipo técnico / bibliotecológico en el desarrollo e implementación del proyecto	25%	4	**1**
RI-06	Dificultad de la comunicación entre los miembros del grupo de desarrollo del proyecto.	70%	5	**3.5**
RI-07	Desconocimiento o poco conociendo por parte del equipo de desarrollo en la utilización de la herramientas	20%	3	0.60

Tabla 6: exposición al riesgo

3.9 Gestión de los Riesgos

a) Riesgo RI-02 Cambio de políticas de Gestión

a.1) Aspectos a considerar:

- **Por que** el riesgo es importante: se pueden modificar el ranking de necesidades de los objetivos del proyecto lo cual llevaría a re adaptación del mismo.
- **Que información** se necesita para seguir el estado del riesgo documentos en donde se explayen oficialmente los objetivos del proyecto.
- **Quien es responsable** de realizar las actividades de control del riesgo: el responsable es el Jefe del proyecto.
- **Que recursos** se necesitan para realizar las actividades de control del riesgo: para realizar las actividades de control del riesgo no se necesitan recursos económicos extras, si una metodología de organización de la documentación del proyecto que abarqué informes periódicos de estados de situación del proyecto.

a.2.) Plan de Acción

- Reformular o re-adecuar el proyecto en base a las nuevas políticas de gestión.

a.3.) Plan de Contingencia

- Disparador: comunicado de las autoridades del cambio gestión, se deberá :
  - Reunión Inmediata con la nueva gestión.
  - Presentación de la Documentación de estado del Proyecto.

b) Riesgo RI-05 Inexperiencia del equipo informático / bibliotecario en el desarrollo e implementación del proyecto.

b.1) Aspectos a considerar:

- **Por que** el riesgo es importante: podría alterar la calidad del producto, provocaría atrasos en el desarrollo e implementación del proyecto.
- **Que información** se necesita para seguir el estado del riesgo:
  - Documentos de estado de avances de trabajos individuales, en donde se explayen las tareas realizadas y las dificultades presentadas y si estas fueron solucionadas con éxito como se solucionaron dichas dificultades.
  - Planilla de informe de Errores y soluciones.
- **Quien es responsable** de realizar las actividades de control del riesgo: el responsable es el Jefe del proyecto, integrantes del equipo de trabajo.
- **Que recursos** se necesitan para realizar las actividades de control del riesgo: para realizar un adecuado control de este riesgo se necesitará personal capacitado para validar las funciones desde el punto de vista técnico/bibliotecológico. Si el control corresponde a una actividad informática, este personal deberá tener amplios conocimientos en cuanto a la tecnología incluida en el proyecto, si el control corresponde a una actividad bibliotecológica este personal deberá tener conocimiento de tecnología aplicables a la bibliotecología.

b.2.) Plan de Acción

- Cursos de capacitación de tecnología Web y administración de componentes Web 2.0 para el personal bibliotecario.
- Realizar talleres y actividades integradoras
- Reuniones semanales entre informáticos y bibliotecarios.
- Contratar personal Informático especializado en:
  - Tecnología Web.
  - Base de Datos.
  - Diseño de Páginas Web.

b.3) Plan de Contingencia

- Disparador: plan de avance no refleja los resultados esperados, falta de calidad en el producto
- Contratar una Consultaría Experta en tecnología Web 2.0

c) Riesgo RI-06 Dificultad de la comunicación entre los miembros del grupo de desarrollo del proyecto.

c.1) Aspectos a considerar:

- **Por que** el riesgo es importante: por que la dificultad en la comunicación provoca la falta de compresión de los actores tanto informáticos como bibliotecarios esto conlleva a un ambiente de trabajo tenso e inseguro por no contar con lenguajes de comunicación comunes a las dos áreas del conocimiento, clima de competencia a fin de hacer prevalecer la opinión profesional que cada miembro asume.
- **Que información** se necesita para seguir el estado del riesgo: presentando informes periódicos grupales de estado de avance, en donde los miembros del proyecto, trabajan en conjunto en la elaboración del informe.
- **Quien es responsable** de realizar las actividades de control del riesgo: el responsable es el Jefe del Proyecto.
- **Que recursos** se necesitan para realizar las actividades de control del riesgo: para realizar un adecuado control de este riesgo se necesitará una metodología que abarqué informes periódicos de estados de situación del proyecto grupales.

c.2) Plan de Acción: para mantener controlado RI-06 deberán adoptar las siguientes medidas de prevención y seguimiento

- Realizar talleres y actividades integradoras.
- Reuniones semanales entre informáticos y bibliotecarios en donde se expresen diferencias de criterios.

- ❖ Controles de la calidad de todo el proyecto, durante el ciclo de vida del mismo.

c.3) Plan de Contingencia

- ❖ Disparador: problemas laborales entre el equipo de desarrollo, deficiencia en la calidad del producto en las fases en donde las actividades sean multidisciplinarias.
  - Contratar un personal capacitado para validar las funciones desde el punto de vista bibliotecario/informático. Este personal deberá tener amplios conocimientos en cuanto a desarrollo software y amplios conocimientos bibliotecológicos.
  - Remover a los miembros del equipo que no posean una predisposición al trabajo en grupo y multidisciplinario.

4. CONCLUSIONES:

El adecuado análisis y gestión de riesgos permitirá que pueda llevarse a cabo un proyecto dentro de los tiempos establecidos y los costos previstos. Consideramos que un Plan de Riesgos constituye un mecanismo formal que permite instalar adecuadamente las tecnologías Web en las bibliotecas.

La metodología presentada en el trabajo, es una herramienta que brinda la posibilidad de efectuar tareas de identificación, administración y mitigación de riesgos en base a taxonomías estándares para la implementación de componentes Web 2.0 en el Centro de Documentación.

Los profesionales de la información debemos ahora aprender a integrar y adaptar las nuevas herramientas informáticas a nuestras necesidades y particularidades, mejorando nuestros servicios y productos, la existencia de componentes Web 2.0 es ya un hecho pero su futuro desarrollo dependerá de las capacidades de los profesionales de la información para adaptarse a las nuevas formas de comunicación y de su capacidad de innovar y, como toda herramienta nueva y en proceso de desarrollo debemos tener en cuenta los riesgos que de ella podría derivarse para que los proyectos tengan éxito.

BIBLIOGRAFIA

1. QUEMADA, Juan. Introducción al Web 2.0 [en línea]. Madrid : Universidad Politécnica de Madrid, 200? 50 p. Disponible en: http://www.slideshare.net/jquemada/introduccion-al-web-20. [Consultado: 02/08/2008]

2. FUMERO, Antonio y Roca, Genís. Web 2.0 [en línea] / con la colaboración de Fernando Sáez Vaca. España : Fundación Orange, 2007. 131 p. Disponible en: http://www.fundacionorange.es/areas/25_publicaciones/publi_253_11.asp. [Consultado: 01/06/2008]

3. COBO ROMANI, Cristóbal y Pardo Kuklinski, Hugo. Planeta Web 2.0 : inteligencia colectiva o medios fast foot [en línea]. México ; Barcelona: Grup de Recerca d'Interaccions Digitals, Universitat de Vic. ; Flacso, 2007. Disponible en: http://www.planetaweb2.net. [Consultado: 01/06/2008]

4. *Active Risk Manager* [en línea]. 2007. Disponible en: http://www.strategicthought.com/ [Consultado: 24/07/2008]

5. *Risk Management Process & Implementation*[en línea]. American Systems Corporation, 2003. Disponible en: http://www.2asc.com. [Consultado: 24/07/2008]

6. *SEI: Software Engineering Institute*. Disponible en: www.sei.cmu.edu/programs/sepm/ [Consultado: 24/07/2008].

7. CAPERS, Jones. Assessment and Control of Software Risk, Upper Saddle River, NJ: Prentice-Hall, 1993.

8. MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid : Consejo Superior de Informática, Ministerio de Administraciones Públicas, 2006.

9. HIGUERA, Ronald P. y HAIMES, Yacov Y., "Software Risk Management*", Technical Report*. Pittsburgh, Pennsylvania : SEI (Software Engineering Institute) ; Carnegie Mellon University, 1996. Disponible en: *www.sei.cmu.edu/pub/documents/96.reports/pdf/tr012.96.pdf*. [Consultado el 8 de agosto 2008].

10. CARR, Marvin ; KONDA, Suresh L. ; MONARCH, Ira ; ULRICH, Carol F. ; WLKER, Clay F. Taxonomy-Based Risk Identification. Pittsburgh, Pennsylvania : Software Engineering Institute, Carnegie Mellon University, 1993. Disponible en: www.sei.cmu.edu/pub/documents/93.reports/pdf/tr06.93.pdf. . [Consultado el 8 de agosto 2008].