

Gestión de Riesgos



Proyecto Ingeniería del Software 2008/09
Casino Online

Tabla de Cambios

Fecha	Autor/Autores	Comentario
Gabriela Ruiz	26/02/2009	Revisión de Gonzalo
Alberto Fernández	28/01/2009	Revisión y seguimiento
David Fernández y Alberto Fernández	11/12/2008	Revisión de Gonzalo
Alberto Milán, David Fernández y Alberto Fernández	13/11/2008	Generación del documento inicial



Índice

1. Introducción.....	4
2. Identificación, análisis y planificación	4
2.1 Riesgos Tecnológicos	4
2.2 Riesgos de Personal.....	5
2.3 Riesgos de Organización	6
2.4 Riesgos de Herramientas.....	6
2.5 Riesgos de Requisitos	7
2.6 Riesgos de Estimación	7
3. Seguimiento.....	7
3.1 Riesgos superados.....	7
3.2 Nuevos riesgos	8



Gestión de Riesgos

1. Introducción

Se entiende por riesgo a cualquier dificultad o complicación que pudiera suceder a lo largo de la especificación, diseño, implementación y/o desarrollo en general de un proyecto.

Por cada riesgo considerado hay que tener en cuenta su probabilidad de aparición (Alta, Moderada, Baja) y efectos (Catastróficos, Serios, Tolerable, Insignificante) y posibles estrategias para evitar los riesgos en la medida de lo posible.

2. Identificación, análisis y planificación

2.1 Riesgos Tecnológicos

- El servidor ha de tener un ancho de banda mínimo capaz de soportar una alta carga de usuarios.

Probabilidad: Moderada. **Efectos:** Tolerable. **Estrategias:** Mejorar el protocolo de comunicación para minimizar el tráfico de la aplicación. Como último motivo, se podría solicitar más ancho de banda ó requerir mejor equipamiento hardware.

- La latencia ha de ser suficientemente baja como para ofrecer un buen servicio en tiempo real.

Probabilidad: Baja. **Efectos:** Tolerable. **Estrategias:** Compactar los posibles mensajes, reduciendo el número de comunicaciones por mensaje. Realizar un estudio del retardo de cada cliente al realizar login a la aplicación. Si el retardo es superior a un máximo establecido se le comunicará con un mensaje de *Imposibilidad de juego*. Como última solución, solicitar una mejora en la conexión.

- La base de datos usada en el sistema no puede procesar tantas peticiones por segundo como se había estimado.

Probabilidad: Moderada. **Efectos:** Serio. *Estrategias:* Establecer prioridades en las peticiones sobre el SGBD. Como última solución cabe solicitar una mejora de hardware en el equipo servidor y/o probar alternativas de SGBD.

- Privacidad en la comunicación cifrada entre servidor y cliente.

Probabilidad: Alta. **Efectos:** Catastrófico. *Estrategias:* Salvaguardar con copias incrementales el sistema de manera que sea fácilmente recuperable, analizar posibles soluciones a fallos de seguridad, como seleccionar otro método de cifrado que no posea dichas vulnerabilidades (u otras).

- Falta de privacidad en ciertos contenidos de la Base de Datos susceptibles de contener información personal. Incumplimiento de la Ley de Protección de Datos.

Probabilidad: Alta. **Efectos:** Catastrófico. *Estrategias:* Estudio detallado de los contenidos que han de ser cifrados y del algoritmo de cifrado. Estudiar disociaciones entre los posibles datos contenidos. Además, puede añadirse la redacción de un documento Log escrito por el servidor que almacene todas las transacciones realizadas sobre la BBDD, para poder localizar en qué punto se ha infringido dicha ley.

2.2 Riesgos de Personal

- Es imposible encontrar uno o varios desarrolladores con las habilidades necesarias para la realización de una tarea concreta del proyecto.

Probabilidad: Baja. **Efectos:** Catastrófico. *Estrategias:* Si la obtención de información y/o documentación por medio escrito u online no da resultado, se solicitará ayuda a un tutor/guía que pueda facilitarnos la adquisición del conocimiento necesario. En caso de no superarse, se modificará dicha tarea, o incluso puede descartarse si no fuese indispensable, hasta encontrar desarrolladores capaces.

- Falta de personal. Ello incluye la falta de personal por distintos motivos: enfermedad, época de estudios (exámenes), sobrecarga de trabajo ajeno al proyecto, motivos personales...

Probabilidad: Alta. **Efectos:** Serio. *Estrategias:* Evaluar las razones de incapacidad del personal y realizar un reajuste en la planificación modificando los plazos de entrega intermedios, reasignar el trabajo entre el personal disponible y capacitado; además el miembro incapacitado debe recuperar el tiempo perdido, en cuanto sea posible, incrementando el tiempo de dedicación necesario para la recuperación, a menos que no sea necesario, por haber sido realizado por otro miembro del equipo.

- Nuevas incorporaciones en el equipo de diseño/desarrollo.

Probabilidad: Moderada. **Efectos:** Tolerable. *Estrategias:* Estructurar correctamente el trabajo y realizar una buena documentación para simplificar a las nuevas incorporaciones una integración rápida a la información ya desarrollada. Se puede incluir, si es necesario, un pequeño tiempo de adaptación a las tecnologías utilizadas manteniendo eventualmente los niveles de trabajo de los miembros antiguos.

2.3 Riesgos de Organización

- Falta de estructura jerárquica en el grupo del proyecto.

Probabilidad: Moderada. **Efectos:** Serio. **Estrategias:** La toma de decisiones se hace de forma consensuada, debiendo informar a todo el personal de proyecto y, guardando y documentando las decisiones tomadas. Así mismo, la asignación de tareas debe discutirse entre todos los miembros, siendo flexibles y estando motivados para realizar la labor asignada.

- Problemas económicos.

Probabilidad: Baja. **Efectos:** Catastrófico. **Estrategias:** No existe estrategia de resolución, al no existir presupuesto básico de proyecto. Se asumirán los costes o se abordarán desde alternativas aceptables.

- Falta de coordinación entre los miembros del equipo.

Probabilidad: Alta. **Efectos:** Serio. **Estrategias:** Marcar objetivos temporales y realizables, controlando el desarrollo individual desequilibrado. Se realizarán reuniones semanales en el laboratorio, y habrá una comunicación constante a través del Google code y groups. En todo caso que lo requiera, las tareas se distribuirán en grupos, haciendo posible el cumplimiento de los objetivos a pesar de que existan otros riesgos que superar (por ejemplo, falta de personal).

2.4 Riesgos de Herramientas

- La herramienta utilizada genera código ineficiente.

Probabilidad: Moderada. **Efectos:** Tolerable. **Estrategias:** Realizar pruebas del código generado y probar nuevas herramientas de desarrollo y/o compiladores.

- No se puede utilizar alguna herramienta que estaba pensada usar por problemas de integración con el resto del sistema.

Probabilidad: Alta. **Efectos:** Tolerable. **Estrategias:** Realizar un estudio sobre los posibles problemas que puede presentar el uso de una herramienta antes de comenzar su desarrollo en la misma. Tener preparadas herramientas alternativas por si durante el desarrollo hubiera problemas con las seleccionadas.

- Hibernate en la base de datos: Nuevo riesgo surgido debido al deseo del equipo de desarrollo.

Probabilidad: Baja. **Efectos:** Tolerable. **Estrategias:** Se intentará realizar gracias a los conocimientos de varios miembros del equipo de desarrollo en este campo. En caso de no ser realizable, posiblemente la estrategia que se adoptaría sería la de abandonar la idea, aunque es poco probable que esto se produzca.

2.5 Riesgos de Requisitos

- Cambios en los requisitos que requieren un rediseño de la aplicación grande.

Probabilidad: Alta. **Efectos:** Serio. **Estrategias:** Intentar definir de forma concreta todos los requisitos con la intención de realizar un diseño que sea capaz de afrontar cambios y minimizar el impacto. La modularización del código generado y la división del proyecto en varias partes puede ayudar al rediseño de una parte determinada sin que afecte a las demás.

- El usuario o cliente cree que un cambio significa una pequeña modificación en los requisitos.

Probabilidad: Alta. **Efectos:** Serio. **Estrategias:** Escribir un documento con los posibles cambios *a priori* para informar al usuario de la envergadura de la modificación y poder estudiarlos llegado el caso de que interesen.

2.6 Riesgos de Estimación

- Se ha infravalorado el tiempo requerido para desarrollar el proyecto.

Probabilidad: Moderada. **Efectos:** Catastróficos. **Estrategias:** Adquirir partes del proyecto ya desarrolladas (componentes).

3. Seguimiento

3.1 Riesgos superados

- Falta de personal:

Todos los miembros del equipo de desarrollo han demostrado su valía en los distintos campos asignados. Aún a falta de realizar las implementaciones de los distintos módulos de los que constará el casino podemos afirmar que el grupo es organizado y competitivo en todos los aspectos habiendo un entendimiento más que aceptable entre sus componentes.

- Conexión entre cliente y servidor:

Este riesgo tecnológico ha aparecido cuando no se pensaba que pudiese ocasionarse. Ha sido correctamente solucionado y superado.

- Conexión con la base de datos:

La base de datos diseñada, aunque sigue expuesta a alguna modificación mínima, ha demostrado su fiabilidad en las conexiones y su funcionamiento correcto.

- Estructura del equipo de desarrollo:

Se ha conseguido que una estructura lineal en la que las decisiones se toman de manera medianamente consensuada y se realizan votaciones funcione correctamente sin ocasionar ningún problema hasta el momento.

- Herramientas usadas:

Las herramientas software utilizadas han mostrado una perfecta solvencia en la realización del prototipo. El espacio de almacenamiento del proyecto *subversion* está a la altura de las expectativas y realiza el trabajo deseado de manera eficaz.

- Incorporaciones de nuevos miembros:

Se tuvo una incorporación de última hora en el primer cuatrimestre, la cual no resulto problema alguno. El nuevo miembro se adaptó perfectamente a la filosofía de trabajo y demostró motivación y disponibilidad por ayudar. Pueden surgir nuevas incorporaciones en el segundo cuatrimestre, las cuales se esperan solventar de la misma manera.

- Falta de coordinación entre los miembros del equipo.

De forma leve, entre los miembros, no quedo aclarado cuando debía hacerse el envío, del trabajo realizado para su continuación, entre los mismos, produciéndose a su vez un cierto nivel de incapacidad del personal, siendo solventado incrementando el tiempo dedicado a las tareas incompletas.

- Pérdida de herramientas.

Robo de un portátil, solventado mediante la comunicación entre el equipo y el apoyo y cooperacion en el desarrollo de las tareas encargadas a dicho miembro, por parte de otros miembros del equipo.

3.2 Nuevos riesgos

- Pérdida de herramientas. Ello incluye el robo o extravío de herramientas y puede desembocar en pérdida de información.

Probabilidad: Moderada. **Efectos:** Serio. **Estrategias:** La pérdida de información se palea mediante el uso de un repositorio, para que, en caso de sufrir perdidas de equipos o dispositivos de trabajo (portatil, memoria usb,...), la información pérdida sea mínima, mientras que los equipos/dispositivos perdidos pueden sustituirse. Si la sustitución no pudiese ser inmediata, surgiría la falta de personal (cuya solventación esta prevista).

- Pérdida de personal. Ello incluye la pérdida de personal por distintos motivos: abandono de estudios (asignaturas), sobrecarga de trabajo ajeno al proyecto, motivos personales...

Probabilidad: Moderada. **Efectos:** Catastróficos. **Estrategias:** Reestructurar correctamente el trabajo restante y modificar la futura documentación a desarrollar. Se puede incluir, si es necesario, un incremento en el tiempo dedicado al proyecto por parte de todos los miembros del equipo.