**Sistema de Pasantías Empresariales**

**Lista De Riesgos**

**Versión 2.0**

**Historia de Revisión**

|  |  |  |  |
| --- | --- | --- | --- |
| **Fecha** | **Versión** | **Descripción** | **Autor** |
| 19/02/16 | 2.0 | *Unificación de documentos.* | *Hexacode, InnovaTech, Sist+, S&Q\_Solutions* |

**Tabla de Contenidos**

1. Introducción 7

1.1 Propósito 7

1.2 Alcance 7

1.3 Definiciones, Acrónimos y Abreviaturas 7

1.4 Referencias 7

1.5 Vista Global 7

2. Riesgos 8

2.1 Dependencia 8 2.1.1 Magnitud del Riesgo 8

2.1.2 Descripción 8

2.1.3 Impactos 8

2.1.4 Indicadores 8

2.1.5 Estrategia de Mitigación 8

2.1.6 Plan de Contingencia 8

2.2 Planificación inadecuada 8

2.2.1 Magnitud del Riesgo 8

2.2.2 Descripción 8

2.2.3 Impactos 8

2.2.4 Indicadores 9

2.2.5 Estrategia de Mitigación 9

2.2.6 Plan de Contingencia 9

2.3 Pérdida de datos 9

2.3.1 Magnitud del Riesgo 9

2.3.2 Descripción 9

2.3.3 Impactos 9

2.3.4 Indicadores 9

2.3.5 Estrategia de Mitigación 9 2.3.6 Plan de Contingencia 10

2.4 Aprendizaje y uso de herramientas 10

2.4.1 Magnitud del Riesgo 10

2.4.2 Descripción 10

2.4.3 Impactos 10

2.4.4 Indicadores 10

2.4.5 Estrategia de Mitigación 10

2.4.6 Plan de Contingencia 10

2.5 Restricciones por parte de la DST 10

2.5.1 Magnitud del Riesgo 11

2.5.2 Descripción 11

2.5.3 Impactos 11 2.5.4 Indicadores 11 2.5.5 Estrategia de Mitigación 11

2.5.6 Plan de Contingencia 11

2.6 Ausencia (temporal o definitiva de integrantes) 11

2.6.1 Magnitud del Riesgo 11

2.6.2 Descripción 11

2.6.3 Impactos 11

2.6.4 Indicadores 11

2.6.5 Estrategia de Mitigación 12

2.6.6 Plan de Contingencia 12

2.7 Falta de explicación por parte de la CCT o DEX 12

2.7.1 Magnitud del Riesgo 12

2.7.2 Descripción 12

2.7.3 Impactos 12

2.7.4 Indicadores 12

2.7.5 Estrategia de Mitigación 12

2.7.6 Plan de Contingencia 12

2.8 Detenimiento repentino en las actividades académicas de la universidad 12

2.8.1 Magnitud del Riesgo 12

2.8.2 Descripción 12

2.8.3 Impactos 13

2.8.4 Indicadores 13

2.8.5 Estrategia de Mitigación 13

2.8x.6 Plan de Contingencia 13

2.9 Problemas de Comunicación entre Líderes de los Equipos 13

2.9.1 Magnitud del Riesgo 13

2.9.2 Descripción 13

2.9.3 Impactos 13

2.9.4 Indicadores 13

2.9.5 Estrategia de Mitigación 13

2.9.6 Plan de Contingencia 13

2.10 Ataques informáticos 13

2.10.1 Magnitud del Riesgo 13

2.10.2 Descripción 13

2.10.3 Impactos 14

2.10.4 Indicadores 14

2.10.5 Estrategia de Mitigación 14

2.10.6 Plan de Contingencia 14

2.*11* Distribución inadecuada de actividades 14

2.*11*.1 Magnitud del Riesgo 14

2.*11*.2 Descripción 14

2.*11*.3 Impactos 14

2.*11*.4 Indicadores 14

2.*11*.5 Estrategia de Mitigación 14

2.*11*.6 Plan de Contingencia 14

2.*12* Restricciones de tiempo 15

2.*12*.1 Magnitud del Riesgo 15

2.*12*.2 Descripción 15

2.*12*.3 Impactos 15

2.*12*.4 Indicadores 15 2.*12*.5 Estrategia de Mitigación 15

2.*12*.6 Plan de Contingencia 15

2.13 Insatisfacción por parte de los clientes 15

2.13.1 Magnitud del Riesgo 15

2.13.2 Descripción 15

2.13.3 Impactos 15

2.13.4 Indicadores 16

2.13.5 Estrategia de Mitigación 16

2.13.6 Plan de Contingencia 16

2.14 Caída de los servidores 16

2.14.1 Magnitud del Riesgo 16

2.14.2 Descripción 16

2.14.3 Impactos 16

2.14.4 Indicadores 16

2.14.5 Estrategia de Mitigación 16

2.14.6 Plan de Contingencia 16

2.15 Inexperiencia en labores de desarrollo de software en equipo 17

2.15.1 Magnitud del Riesgo 17

2.15.2 Descripción 17

2.15.3 Impactos 17

2.15.4 Indicadores 17

2.15.5 Estrategia de Mitigación 17

2.15.6 Plan de Contingencia 17

2.16 Ignorar riesgos 17

2.16.1 Magnitud del Riesgo 17

2.16.2 Descripción 17

2.16.3 Impactos 17

2.16.4 Indicadores 17

2.16.5 Estrategia de Mitigación 17

2.16.6 Plan de Contingencia 18

2.17 Entradas malformadas en la base de datos 18

2.17.1 Magnitud del Riesgo 18

2.17.2 Descripción 18

2.17.3 Impactos 18

2.17.4 Indicadores 18

2.17.5 Estrategia de Mitigación 18

2.17.6 Plan de Contingencia 18

2.18 Desuso 18

2.18.1 Magnitud del Riesgo 18

2.18.2 Descripción 18

2.18.3 Impactos 18

2.18.4 Indicadores 18

2.18.5 Estrategia de Mitigación 19

2.18.6 Plan de Contingencia 19

2.19 Ausencia de servidores 19

2.19.1 Magnitud del Riesgo 19

2.19.2 Descripción 19

2.19.3 Impactos 19

2.19.4 Indicadores 19

2.19.5 Estrategia de Mitigación 19

2.19.6 Plan de Contingencia 19

2.20 Mala comunicación o requerimientos mal definidos por parte de la CCT 20

2.20.1 Magnitud del Riesgo 20

2.20.2 Descripción 20

2.20.3 Impactos 20

2.20.4 Indicadores 20

2.20.5 Estrategia de Mitigación 20

2.20.6 Plan de Contingencia 20

**Lista de Riesgos**

1. **Introducción**

En este documento se ofrece una lista detallada de los riesgos que el equipo de desarrollo del proyecto considera pueden afectar - directa o indirectamente - el desarrollo exitoso, y la posterior implantación del Sistema de Administración y Gestión de Pasantías (SAGP).

**Propósito**

Este documento tiene como propósito principal servir de herramienta para evaluar los riesgos que pudiesen presentarse durante el desarrollo del sistema, y establecer un plan de detección y ataque frente a los mismos, con el fin de evitar que afecten de forma irreversible el desarrollo y culminación satisfactoria del sistema.

**Alcance**

El alcance de este documento es explorar y analizar los distintos riesgos que podrían presentar tanto el sistema en sí, como el proceso de desarrollo del mismo, a fin de lograr el propósito explicado en el punto anterior. Para lograr esto se propone analizar los siguientes aspectos en cada uno de los riesgos existentes: escala, descripción, impactos sobre el sistema, indicadores de que el riesgo está ocurriendo, estrategias de mitigación y los planes de contingencia.

**Definiciones, Acrónimos y Abreviaciones**

* USB: Universidad Simón Bolívar.
* DEX: Decanato de Extensión
* CCT: Coordinación de Cooperación Técnica.
* DST: Dirección de Servicios Telemáticos.
* CAS: *Central Autification System* (Sistema de Autenticación Centralizado).
* Sistema Beta: Sistema de Administración de Pasantías actualmente en uso.
* Stakeholders: Término utilizado para referirse a los diferentes sujetos o entidades afectadas o involucradas en la realización del proyecto.

**Referencias**

Para esta entrega del documento, no se hacen referencias a otros documentos.

**Vista Global**

En este documento, se presenta un listado de los riesgos en orden descendente de magnitud (gravedad e impacto). Para cada riesgo se detalla su magnitud (indica el nivel de impacto en el sistema o su desarrollo), descripción, impacto (en qué aspectos, y cómo, afecta el riesgo), indicadores (describe cómo monitorear y detectar que el riesgo está a punto de ocurrir), estrategia de mitigación (describe que se está haciendo actualmente para evitar el riesgo), y plan de contingencia (describe cuál será el procedimiento a seguir en caso de que el riesgo se materialice).

1. **Riesgos**
   1. **Dependencia**
      1. *Magnitud del Riesgo: Alta.*
      2. *Descripción*

Se deberá medir el grado de dependencia que existe en el lugar de trabajo, en este caso la CCT, luego de la implantación del sistema de información, es decir, hay que plantearse la pregunta ¿Qué pasaría si se el sistema no está disponible? ¿Seguiría todo funcionando?

* + 1. *Impactos*

Si el lugar de trabajo es altamente dependiente del sistema y se presenta una falla técnica o de otra naturaleza que inhabilite el uso del sistema, la CCT se vería involucrada en serios problemas por verse incapacitada de brindar los servicios que presta actualmente en el área de pasantías.

* + 1. *Indicadores*

Si se ha migrado totalmente del método manual al método sistematizado planteado por el equipo de desarrollo del proyecto, muy probablemente, los empleados del CCT se deshicieron de los documentos con los cuales solían trabajar. Esto hace que se tenga el riesgo de una alta dependencia del sistema una vez se encuentre totalmente funcional, por no contar con los documentos para atender eventualidades, de forma manual, en caso de fallas del sistema.

* + 1. *Estrategia de Mitigación*

Para reducir el riesgo de dependencia, se propone plantear a la CCT que una vez implantado el sistema se debe contar con formatos de documentos que permitan el trabajo manual para que sean utilizados en caso de una eventualidad.

* + 1. *Plan de Contingencia*

En caso de ocurrir algo inesperado con el funcionamiento del sistema luego de que se encuentre completamente implantado, queda en manos del encargado de administración del sistema de la CCT solventar el problema lo más rápido posible para que esta dependencia regrese a la normalidad. Mientras tanto no se solvente la situación se usarán formatos manuales, los cuales, luego de sobrepuesta la problemática serán vaciados en el sistema para tener toda la información digitalizada. Adicionalmente, se puede contar con manuales de respaldo para emergencias que expliquen al personal cómo desarrollar el trabajo de forma manual.

**2.2 Planificación Inadecuada**

*2.2.1 Magnitud del Riesgo: Alta.*

*2.2.2 Descripción*

Con planificación inadecuada se hace referencia particularmente a la elaboración de un cronograma de actividades que en un principio parecen factibles, pero que en la práctica se hacen imposibles de seguir.

*2.2.3 Impactos*

Este riesgo conlleva a que ocurra lo siguiente: desorganización dentro del equipo, incumplimiento de las actividades y compromisos establecidos, acumulación de trabajo para las semanas previas o entregas posteriores, no alcanzar el objetivo final del proyecto. Afecta la imagen y compromete a la empresa.

*2.2.4 Indicadores*

Se logra detectar con cierta facilidad si el riesgo está ocurriendo. Dado que existen entregas semanales y mensuales de documentos y avances del sistema, fallas en las entregas acordadas podrían indicar que el equipo no está bien encaminado. Adicionalmente, durante la semana se realizan reuniones informativas entre los miembros del equipo desarrollador donde se manifiestan los compromisos y logros de cada miembro, falta de cumplimiento en los plazos de entrega pueden indicar que el equipo está desenfocado.

*2.2.5 Estrategia de Mitigación*

Para reducir la probabilidad de que este riesgo ocurra, se designa a un líder de equipo que se encarga de mantener a los miembros de su equipo al pendiente de las actividades que se deben ejecutar en la semana y priorizarlas. Adicionalmente, se pide compromiso a los miembros del equipo para generar confianza en el ambiente de trabajo y afianzar el sentido de cumplimiento de los roles y asignaciones de cada miembro.

*2.2.6 Plan de Contingencia*

Si se llega a materializar el riesgo, se manejaría la situación convocando a una reunión de los miembros del equipo lo antes posible. En dicha reunión se discutiría la posible elección de un nuevo líder y/o la re-planificación de actividades. Adicionalmente, se hablaría con los miembros acerca de las razones de la falta de interés y se propondrían soluciones que permitan aumentar la productividad, motivación y/o eficacia.

**2.3 Pérdida de Datos**

*2.3.1 Magnitud del riesgo: Alta.*

*2.3.2 Descripción*

Este riesgo viene a ser importante debido a que en los datos reside toda la información. El sistema de información almacena todos los datos obtenidos a través de formularios, ubicados en las páginas, en bases de datos alojadas en algún servidor.

*2.3.3 Impactos*

La materialización de este riesgo implica pérdida de información vital para el DEX, con lo cual no podrían operar con normalidad. Esto afecta las actividades diarias del Decanato y, adicionalmente, no permite la realización de los seguimientos rutinarios y obtención de datos estadísticos de interés.

*2.3.4 Indicadores*

Se observa la posibilidad de perder datos si al servidor donde se almacena la base de datos no se le realizan respaldos de manera rutinaria y si no se revisa los datos obtenidos por el uso del sistema.

*2.3.5 Estrategias de Mitigación*

La manera de reducir la probabilidad de pérdida de datos es realizando respaldos rutinarios de los datos existentes. Estos respaldos deberían hacerse, tanto en la base de datos donde está almacenado el sistema como en una computadora distinta, si es posible, en otra locación geográfica. Otra manera, sería llevar un registro en físico de las cosas de vital importancia que se automatizan con el sistema, ya sean copias o impresiones que permitirían tener un respaldo importante de la información del sistema. Adicionalmente, es importante contar con una persona capacitada para la gestión de la base de datos.

*2.3.6 Plan de Contingencia*

Luego de la pérdida de datos se pueden encontrar dos posibles escenarios: si existe un respaldo reciente en buen estado o si no existe un respaldo reciente. En caso que no se encuentren disponibles respaldos recientes, la CCT restaura los datos por medio de la última versión disponible y se procedería a llenar de nuevo, de existir registros en físico, los datos que sean de alta importancia para la coordinación. En caso contrario, simplemente se restaura la información.

**2.4 Aprendizaje y Uso de Herramientas**

*2.4.1 Magnitud del riesgo: Alta.*

*2.4.2 Descripción*

La falta de experiencia en el manejo de herramientas (lenguajes de programación, lenguajes informáticos, sistemas de control de versiones, frameworks, etc.) por parte de los encargados de desarrollar el sistema requiere una inversión de tiempo y esfuerzo extra para comprender su funcionamiento. Podría ocurrir que el aprendizaje de las herramientas se haga más lento de lo esperado, debido a lo compleja que puedan llegar a ser. Además se habla sobre la adaptación de los *stakeholders* (en el área de mantenimiento del sistema) con las herramientas seleccionadas para el desarrollo.

*2.4.3 Impactos*

La cantidad de tiempo destinado a investigación y aprendizaje sobre el uso de las herramientas, así como para corregir errores productos del aprendizaje podría imposibilitar culminar el proyecto en el lapso de tiempo esperado. También, puede suceder que los *stakeholders* no se sientan cómodos con las herramientas seleccionadas, ya sea porque es compleja o muy diferente a la que están acostumbrados a usar, así como por lo que tardan en adaptarse y conocer los beneficios que estas pueden brindarles.

*2.4.4 Indicadores*

Avance lento en cuanto a la implementación del sistema. Fallas en el funcionamiento de las partes del sistema que ya han sido implementadas. En cuanto a la adaptación de las personas que mantienen el sistema, se puede notar su bajo aprendizaje cuando éstos tengan dudas o que su trabajo en vez de hacerse más fácil se vuelva tedioso.

*2.4.5 Estrategias de Mitigación*

La mejor manera de evitar este riesgo es destinar tiempo para la investigación, práctica, consulta con profesores y reuniones grupales que favorezcan y aceleren el aprendizaje sobre el manejo de las herramientas. Para los *stakeholders* se debe mostrar en cada avance del desarrollo cómo se utilizaron las herramientas y las restricciones que provee. De esta manera se va haciendo una idea del funcionamiento del nuevo sistema.

*2.4.6 Plan de Contingencia*

En caso de complicarse mucho el aprendizaje de las herramientas, se propone recurrir a consultas adicionales con profesores, estudiantes y preparadores o alguna de las dependencias que la USB que manejen dichas herramientas. En cuanto a los *stakeholders* se deben realizar reuniones para mostrar el funcionamiento del sistema y diversos ejemplos que apliquen a su trabajo rutinario y así demostrarles el uso de las herramientas.

**2.5 Restricciones por parte de la DST**

*2.5.1 Magnitud del riesgo: Alta.*

*2.5.2 Descripción*

Los desarrolladores del proyecto no poseen conocimiento acerca de la estructura del sistema de identificación CAS, utilizado por la DST para la USB, por lo que es necesario solicitar una serie de permisos a la DST. Además, se deben llevar a cabo los procedimientos burocráticos para obtener la información necesaria.

*2.5.3 Impactos*

Empleo de tiempo en realizar los procedimientos necesarios para acceder a la información, y en la espera de respuestas por parte de la DST.

*2.5.4 Indicadores*

Retraso en el desarrollo del sistema, ocasionado por el período de espera de respuestas por parte de la instancia mencionada.

*2.5.5 Estrategias de Mitigación*

Plantear a los clientes y a los profesores la necesidad de comunicación con la DST para obtener los permisos pertinentes para la realización del sistema.

*2.5.6 Plan de Contingencia*

Buscar soluciones con un menor grado de dependencia a la DST para la identificación de los usuarios que tendrán acceso al sistema, a saber: la creación de un módulo de administrador encargado de asignar roles a los usuarios del sistema. Con esto, se abordaría la dependencia a la DST en una última fase del desarrollo del sistema.

**2.6 Ausencia (temporal o definitiva) de integrantes**

*2.6.1 Magnitud del riesgo: Alta.*

*2.6.2 Descripción*

Los integrantes del equipo podrían no estar disponibles por diversas razones: enfermedad, problemas familiares, retiro de la asignatura, obstrucción de las vías de comunicación (por razones climáticas o de otra naturaleza), o simplemente por no no compartir el objetivo de cumplir con las responsabilidades tanto dcon el equipo como con el cliente.

Este riesgo es de mucha importancia ya que si llega a ocurrir el desarrollo del sistema podría verse comprometido, dado que si algún(os) miembro(s) deja(n) de ejercer el rol asignado el equipo se desequilibrará, haciendo que se acumule más trabajo y que los miembros restantes tengan que encargarse de más responsabilidades de las que pueden soportar.

*2.6.3 Impactos*

El impacto que implica este riesgo es crítico, puesto que aumenta la carga de actividades sobre los otros miembros del equipo. Podría generar retrasos en las entregas, y en caso extremo, no cumplir con las entregas. Esto haría que no se culmine el proyecto o que se culmine pero no cumple con las expectativas del cliente.

*2.6.4 Indicadores*

Algunos indicadores de que un miembro está indispuesto son la ausencia de la persona en las clases de la asignatura, evasión de conversaciones con otros miembros del equipo, no contestar correos o mensajes de texto, no atender llamadas, obtener bajas calificaciones en la asignatura (lo que puede conllevar un retiro de ésta), etc. En general, la falta de interés.

*2.6.5 Estrategia de mitigación*

Motivar y propiciar la comunicación entre los miembros del equipo. Procurar mantener un ambiente de trabajo agradable, evitando la tensión entre los integrantes. Fomentar el sentido de compañerismo y unidad, haciendo así que no se quiera dejar el proyecto por muy complicado que sea, puesto que se sentirá un compromiso de culminarlo con éxito.

*2.6.6 Plan de contingencia*

Despido d la persona si ésta no se reporta para informar su situación. En el momento en que el miembro deja temporal o permanentemente el equipo, deberá hacerse una reunión de extrema importancia para conversar lo ocurrido y delegar el rol abandonado y abordar la posible redistribución de las actividades (entre los miembros restantes) para cubrir la el vacío que deja el integrante que abandona el equipo.

2.7 **Falta de explicación por parte de la CCT o DEX**

*2.7.1 Magnitud de Riesgo: Alta*

*2.7.2 Descripción*

Puede ocurrir que la persona encargada de explicar los requerimientos del sistema al equipo de desarrollo no se explique bien, u omita algún detalle.

*2.7.3 Impactos*

El equipo avanza en el desarrollo del sistema a medida que captura los requerimientos en las pertinentes reuniones con el cliente. En caso de alguna falla u omisión, es posible que no pueda volver atrás y el cliente pueda verse afectado, ya que el sistema puede tener alguna funcionalidad distinta a la pensada.

*2.7.4 Indicadores*

Insatisfacción del cliente ante la demostración de funcionalidades completadas durante cada iteración.

*2.7.5 Estrategias de mitigación*

Tener un buen plan de comunicación y asignar a personas con buenas aptitudes sociales para interactuar con el cliente

*2.7.6 Plan de contingencia*

Reformulamiento de la parte externa del plan de comunicación

2.8 **Detenimiento repentino en las actividades académicas de la universidad.**

*2.8.1 Magnitud de Riesgo: Alta*

*2.8.2 Descripción*

La situación precaria de la universidad (y del país en general) tanto en el ámbito político/administrativo como en la disponibilidad de recursos, generan la posibilidad del cese de actividades en la universidad, bien sea por un paro convocado, o por la imposibilidad de continuar actividades debido a falta de uno o varios servicios básicos (transporte, agua, comedores, etc.)

*2.8.3 Impactos*

El desarrollo del proyecto se detendría casi por completo, solo aquellas funcionalidades que ya fueron comenzadas podrían continuar, pero no habría manera de comunicarse con el cliente para verificarlas, ni de comenzar a desarrollar funcionalidades nuevas.

*2.8.4 Indicadores*

El ambiente político en el país, el cumplimiento actual de los servicios en la universidad, las acciones que tomen las diferentes instituciones que agrupan a los obreros y/o profesores.

*2.8.5 Estrategias de mitigación*

Sale del alcance del estudiante.

*2.8.6 Plan de contingencia*

Nuevo plan de comunicación, planificar nuevos espacios para el desarrollo del proyecto, continuación del proyecto cuando se estabilice la situación.

**2.9 Problemas de Comunicación entre los líderes de los equipos**

*2.9.1 Magnitud de Riesgo: Alta*

*2.9.2 Descripción*

Cada equipo desarrollará un subsistema del sistema. Una vez que estén implementados, éstos han de integrarse. Por esa razón, se han de acordar previamente los protocolos de comunicación entre los mismos. De no haber comunicación entre los líderes de los equipos, no se puede asegurar que los mismos sean compatibles.

*2.9.3 Impactos*

Retrasos importantes en la última etapa del desarrollo del proyecto.

*2.9.4 Indicadores*

Interfaces muy dispares entre los componentes. No se hace uso del plan de comunicaciones.

*2.9.5 Estrategia de Mitigación*

Facilitar la comunicación entre los líderes de equipos usando una gran variedad de medios. En la mayoría de los casos, los líderes sólo se comunicarían en persona. De resultar imposible, ellos pueden usar videoconferencias o correos electrónicos. De cualquier forma, es menester que ellos sigan el plan de comunicaciones.

*2.9.6 Plan de Contingencia*

En el mejor de los casos, sólo sería necesario modificar las interfaces entre los componente producidos para que éstos se puedan integrar.

**2.10 Ataques informáticos**

*2.10.1 Magnitud del riesgo: Media a Alta.*

*2.10.2 Descripción*

Se refiere al método por el cual algún usuario puede causar daños o problemas a un sistema intentando tomar el control, desestabilizar o dañar.

*2.10.3 Impactos*

Los daños que puede ocasionarse son: corromper el sistema, eliminación de información, afectación de módulos y subsistemas, modificar datos, caida de servidores por saturación de peticiones.

*2.10.4 Indicadores*

Algunas maneras de vislumbrar un posible ataque al sistema es si se presentan algunos puntos vulnerables como: poseer servidores externos que establecen comunicación con destinos peligrosos, comunicación con enlaces extrernos a través de puertos no estándar, alertas que se detectan fuera del horario estándar.

*2.10.5 Estrategias de Mitigación*

La manera de evitar que ocurra este riesgo es revisando los puntos vulnerables del sistema, por lo que se debería contar con un equipo que desarrolle pruebas de ataques al sistema.

*2.10.6 Plan de Contingencia*

La cadena de acciones a tomar es: solucionar lo antes posible el daño al sistema causado por el ataque y recuperar la información borrada (siempre y cuando aplique). Adaptar el sistema para que no permita fallos de este estilo nuevamente.

**2.11 Distribución Inadecuada de Actividades**

*2.11.1 Magnitud del riesgo: Media a Alta.*

*2.11.2 Descripción*

Este riesgo engloba no solo la asignación no equitativa de trabajo entre los miembros del equipo sino también el hecho de que algunos miembros sean responsables de tareas que involucran herramientas que desconocen, tareas que no son de su agrado, etc.

*2.11.3 Impactos*

Mal desempeño de los integrantes del equipo a la hora de realizar sus tareas (ya sea por falta de experiencia o interés en el área en que fueron asignados). Esto afecta la calidad del producto final, cuya culminación podría verse comprometida por razones de tiempo y desempeño ya que no se realizan las actividades según lo planificado.

*2.11.4 Indicadores*

Si se presenta alguna falla de cumplimiento de las tareas semanales por parte de los integrantes del equipo se podría estar evidenciando una mala distribución de las actividades.

*2.11.5 Estrategias de Mitigación*

Llegado el momento de la distribución de actividades, entre los integrantes del equipo, se debe llegar a un acuerdo en cuanto a los roles que cada uno jugará, para asegurarse que cada miembro se sienta a gusto con su papel. Además, es importante permitir la rotación de los roles entre los miembros del equipo de desarrollo, para asegurarse de que cada uno encuentre ese rol con el que se siente más cómodo.

*2.11.6 Plan de Contingencia*

Realizar una reunión para redistribuir los roles del equipo, de modo que se garantice la realización de cada una de las tareas según la planificación que se tenga.

**2.12 Restricciones de Tiempo**

*2.12.1 Magnitud del riesgo: Media a Alta.*

*2.12.2 Descripción*

Este riesgo viene dado cuando el trabajo que se quiere realizar requiere más tiempo de lo que puede invertirse. Generalmente se tiene a un personal asignado casi exclusivamente al desarrollo de un proyecto. Sin embargo, los equipos responsables de la formación de este sistema están compuestos por alumnos que tienen otras responsabilidades y obligaciones asociadas a su carga académica o actividades laborales fuera de la universidad. En consecuencia, se dispone de un tiempo limitado para trabajar y dedicarle al desarrollo del sistema.

*2.12.3 Impactos*

Molestias por parte del cliente, puesto que no se cumplen sus expectativas y molestias por parte del equipo desarrollador por la presión que esta situación genera. Además, se obtiene un avance lento o inexistente en el desarrollo del proyecto y se genera una disminución en la calidad del sistema en formación, debido a la falta de atención en los detalles.

*2.12.4 Indicadores*

Aplazamiento de las diversas responsabilidades asignadas a los miembros de los equipos. Necesidad de realizar actividades relacionadas con el proyecto a altas horas de la noche.

*2.12.5 Estrategias de Mitigación*

Realizar una distribución equitativa de las responsabilidades y tareas a realizar durante el avance del proyecto, donde cada miembro debe estar pendiente de sus actividades y notificar si existe algún inconveniente para no realizarla. Fomentar la cooperación entre miembros del equipo con fines de aligerar lo más posible la carga delegada a los integrantes y lograr que el tiempo a invertir, necesario para el proyecto, disminuya y pueda ser efectivo.

*2.12.6 Plan de Contingencia*

Analizar la asignación de roles y responsabilidades de cada miembro de modo que se pueda redistribuir las tareas de acuerdo a la disponibilidad de cada quien.

**2.13 Insatisfacción por parte de los Clientes**

*2.13.1 Magnitud del riesgo: Media a Alta.*

*2.13.2 Descripción*

En cada reunión en el que se le muestre al cliente el estado actual del sistema, éste debe dar a conocer cuál es su postura frente a los avances mostrados. Existe la posibilidad en el cual su apreciación a este sea negativa, puesto a que no le gustó o debido a que faltan requerimientos.

*2.13.3 Impactos*

Desmotivación y frustración entre los miembros del equipo de trabajo y retrasos en el desarrollo del sistema en desarrollo debido a que deben rehacerse o modificarse partes del sistema. En el peor de los casos pudiera perderse el sistema completo, y con éste todo el esfuerzo invertido en él.

*2.13.4 Indicadores*

Desánimo por parte del cliente, malos entendidos entre el cliente y el equipo encargado de la elaboración del sistema. Manifestación por parte del cliente, defendiendo su postura y opinión frente a los avances del proyecto en elaboración.

*2.13.5 Estrategias de Mitigación*

Una estrategia para que se trate de evitar que esto suceda es mantener contacto continuo con el cliente, utilizando los diferentes medios de comunicación disponible (reunión, correos electrónicos, conversaciones, etc.) tratando que quede lo más claro posible para los involucrados en el desarrollo, la dirección hacia la que apunta el sistema. Adicionalmente, llevar constancia de cada reunión mediante minutas para darle fe a los acuerdos concretados.

*2.13.6 Plan de Contingencia*

Revisión continua del flujo de trabajo para identificar el punto que genera el conflicto entre los medios. Luego, verificar la causa (si fue un punto errado o mala comunicación por parte del cliente o si fue una mala interpretación del equipo) y finalmente asumir responsabilidades de acuerdo a lo sucedido.

**2.14 Caída de los Servidores**

*2.14.1 Magnitud del riesgo: Media.*

*2.14.2 Descripción*

La caída de los servidores de la USB hace imposible el acceso de los *stakeholders* a los formularios y datos de importancia para la CCT.

*2.14.3 Impactos*

Retraso en las actividades de la CCT debido a que se podría acceder a la información actualizada del sistema. También existirían conflictos al momento de realizar pruebas del sistema por parte de los desarrolladores, para hacer las pruebas concernientes del mismo.

*2.14.4 Indicadores*

Más allá de las fuertes lluvias y/o apagones (que generalmente causan caída de los servidores) es difícil saber con exactitud cuándo podría ocurrir este riesgo.

*2.14.5 Estrategias de Mitigación*

Para mitigar este caso se procede a siempre tener respaldo de todo lo que sea importante en una nube en la red, de modo que independientemente quién lo necesite pueda acceder a él, mientras se soluciona el problema. Además, de realizar constante mantenimiento a los UPS operativos.

*2.14.6 Plan de Contingencia*

En caso de materializarse este riesgo, se recurriría a utilizar el código guardado de manera local en alguna de las computadoras de los miembros del equipo y en cuánto se encuentren operativos los servidores se actualizarían los datos.

**2.15 Inexperiencia en labores de desarrollo de software en equipo**

*2.15.1 Magnitud del riesgo: Media.*

*2.15.2 Descripción*

Para alguno de los equipos es la primera vez que trabajan en un grupo tan numeroso. Siendo principiantes, existe la posibilidad que la comunicación entre los miembros del equipo no sea óptima.

*2.15.3 Impactos*

La falta de experiencia generar problemas serios de comunicación y roce entre los integrantes del grupo, lo que dificulta el trabajo en equipo.

*2.15.4 Indicadores*

Altercados frecuentes entre los integrantes del equipo. Avance lento en el desarrollo del sistema o desorientación por parte de los miembros en cuanto a sus tareas.

*2.15.5 Estrategias de Mitigación*

Para evitar incurrir en errores de falta experiencia en trabajo en equipo, se puede crear un grupo vía email (a través de de Google) o mediante mensajería instantánea. Esto a modo de comunicación. Adicionalmente, hay que asegurarse que cada integrante posea la información de contacto (correo electrónico, número de celular, etc.) de los otros integrantes y acordar reuniones grupales semanales para aclarar dudas.

*2.15.6 Plan de Contingencia*

De llegar a un extremo de alta abrumación por trabajar en un equipo tan numeroso se recurre a solicitar apoyo del gerente del proyecto, el profesor de teoría o preparadores de la asignatura.

**2.16 Ignorar Riesgos**

*2.16.1 Magnitud del riesgo: Media.*

*2.16.2 Descripción*

Sucede si los miembros del equipo deciden hacer caso omiso a algunos o todos los riesgos listados en este documento.

*2.16.3 Impactos*

La peor consecuencia que podría tener la materialización de este riesgo es que se concreten otros riesgos mencionados en el documento.

*2.16.4 Indicadores*

El principal indicador de este riesgo es que durante la elaboración del sistema se estén ignorando las diferentes estrategias de mitigación de los demás riesgos indicados en este documento.

*2.16.5 Estrategias de Mitigación*

Este riesgo puede ser evitado fácilmente si durante la elaboración del sistema se consulta, cuidadosamente, y se toma en cuenta el contenido desarrollado en este documento. Además, se deberá tener mucha cautela en la toma de decisiones con la finalidad de evitar la materialización de algunos de los riesgos mencionados.

*2.16.6 Plan de Contingencia*

En caso de concretarse este riesgo, y que aunado a ell se materialicen otros riesgos mencionados en el documento, se proseguirá a atacar cada riesgo mediante la ejecución de su plan de contingencia correspondiente.

2.17 **Entradas malformadas en la base de datos**

2.17.1 Magnitud de Riesgo: Media

2.17.2 Descripción

Existe la posibilidad de que los usuarios llenen formularios de manera incorrecta, o que diferentes usuarios se refieran a un mismo elemento de maneras distintas. Es responsabilidad del sistema unificar o corregir dichas inconsistencias donde sea posible, y rechazar entradas incorrectas.

2.17.3 Impactos

Al filtrar datos provenientes de la información almacenada por los usuarios (a través de formularios) en la base de datos puede traer problemas en cuanto a agrupación de nombres en común. Como consecuencia le traería más trabajo a la persona que trabaja con esta información.

2.17.4 Indicadores

Datos almacenados en distintos formatos. Por ejemplo, distintos formatos para una fecha dada (dd/mm/yy, mm/dd/yy, dd-mm-yy, mm-dd-yy, mezcla de números y letras, etc.), correos incompletos, entre otros.

2.17.5 Estrategia de mitigación

Filtros en los campos de formularios, reemplazo de campos claves por menús emergentes con opciones discretas.

2.17.6 Plan de Contingencia

Reformular expresiones regulares en los modelos de la base de datos, crear indicadores para que los usuarios utilicen un único formato en los campos requeridos.

**2.18 Desuso**

*2.18.1 Magnitud del riesgo: Baja.*

*2.18.2 Descripción*

Cuando el sistema, ya sea porque no es práctico usarlo, no se adecua al cambio, no cumple las expectativas de los usuarios finales o por alguna otra razón, no está siendo utilizado por la CCT y los trabajadores emplean el Sistema Beta o métodos manuales para llevar a cabo las tareas.

*2.18.3 Impactos*

Las consecuencias de incurrir en este riesgo serían: desempeño de actividades lento e ineficiente, debido al uso de sistema anterior o el posible uso de métodos manuales y desánimo de nuevos estudiantes de ingeniería de computación para implementar nuevos sistemas de información para la CCT.

*2.18.4 Indicadores*

La manera principal de identificar que el riesgo de desuso está por ocurrir es el desagrado de la CCT ante el sistema. Si la CCT continúa realizando sus labores diarias de la misma manera en la que lo habían estado haciendo hasta ahora, a través del Sistema Beta, puede darse por seguro que el sistema implementado está en desuso.

*2.18.5 Estrategias de Mitigación*

Dado que ya existe un sistema en uso (Sistema Beta) se ha decidido prevenir este riesgo manteniendo un constante contacto con los *stakeholders* de la CCT para que el sistema que se está implementando se ajuste a lo que ellos requieren, intentando cumplir con el mayor número de requerimientos propuestos. Adicionalmente, se propone implementar la interfaz de usuario muy similar a la del Sistema Beta.

*2.18.6 Plan de Contingencia*

Si se llegase a concretar el riesgo, al ya haberse hecho la entrega final del sistema, y el sistema final no ha de ser del agrado del cliente, entonces Hexacode ofrecería sus más sinceras disculpas al cliente de la CCT por no haber cumplido sus expectativas (si estas habían estado especificadas por escrito). Adicionalmente, se ofrecería una nueva implementación de los módulos que tengan problemas o de la totalidad del sistemas (de ser posible), corriendo esto por cuenta de Hexacode. En el peor de los casos, si existe sólo rechazo del sistema y habiendo cumplido con todas las funcionalidades exigidas, entonces se concretarían talleres de preparación al personal de la CCT para motivar y explicar el manejo del nuevo sistema por parte de Hexacode.

**2.19 Ausencia de servidores**

*2.19.1 Magnitud del riesgo: Baja.*

*2.19.2 Descripción*

Existe la necesidad de contar con servidores en los que se puedan alojar el sistema de información en desarrollo y así poder brindar un correcto funcionamiento. La no disponibilidad de servidores o el fallo de estos afectan directamente al proyecto.

*2.19.3 Impactos*

No poder brindar el servicio funcional a la CCT por no poseer una plataforma en la USB que sirva al sistema en desarrollo.

*2.19.4 Indicadores*

Ausencia en la asignación de equipos capacitados para alojar el sistema en desarrollo, trayendo con esto una ausencia total o parcial del servicio que busca ofrecer el software implementado.

*2.19.5 Estrategias de Mitigación*

La manera de mitigar este riesgo es a través de conversaciones con los administradores de los servidores en los cuales ha de alojarse el sistema, haciéndole saber del software que estamos desarrollando para adquirir servidores que se ajusten al desempeño requerido. Adicionalmente se deberían planear simulacros de entradas masivas de usuarios al sistema para observar la reacción del sistema al estar utilizando dichos servidores.

*2.19.6 Plan de Contingencia*

De ocurrir errores en cuanto a las fallas que pueden existir por hardware o en la adquisición incorrecta se recomendaría la búsqueda de nuevos servidores, que se adapten a las características del sistema que se está desarrollando, para brindar un buen servicio de búsqueda y actualizaciones a los actuales.

**2.20 Mala comunicación o requerimientos mal definidos por parte de los desarrolladores o analistas**

*2.20.1 Magnitud del riesgo: Baja.*

*2.20.2 Descripción*

Implica no tener claras las ideas respecto al producto que quiere el cliente o dueño del sistema. Es importante destacar que el cliente ya tiene un sistema actual en funcionamiento el cual será reemplazado por SAGP.

*2.20.3 Impactos*

El sistema podría verse afectado de las siguientes maneras: pérdida de la visión del proyecto, que conlleva a que no realice el objetivo deseado y no sea factible completar su desarrollo. Pérdida de tiempo para el cliente, puesto que el levantamiento de información implica una nueva reunión o reuniones para aclarar los requisitos. Atraso considerable en las actividades del proyecto.

*2.20.4 Indicadores*

La principal manera de poder identificar si este riesgo está por ocurrir es observar las primeras impresiones de los clientes-usuarios durante las presentaciones de los prototipos del sistema. Si se aprecia una actitud de rechazo por parte del cliente/usuario y se evidencian muchas objeciones con lo implementado se comprueba que los requerimientos no estaban del todo claros.

*2.20.5 Estrategias de Mitigación*

La forma mas efectiva de contrarrestar los efectos de este riesgo durante el desarrollo del sistema , es enfocarse en mantener contacto con el cliente siempre que sea necesario y mostrar nuevas funcionalidades a medida que se van implementando. Esto con el fin de recibir impresiones sobre lo que se ha realizado.

*2.20.6 Plan de Contingencia*

En caso de materializarse el riesgo, el plan de trabajo es realizar una reunión con el cliente para aclarar ideas, y que éste pueda manifestar cuáles son los aspectos o características del prototipo que no se corresponden con sus necesidades.