Plan de Gestión de Proyecto
Anexo de Administración del Tratamiento de Riesgos

Proyecto: UnaGauchada
Revisión 0

Ficha del documento

Fecha	Revisión	Autor	Cambio	Verificado dep. calidad.
09/05/2017	0	WeDevelop		

Documento validado por las partes en fecha:

Por el cliente	Por la empresa suministradora
Fdo. Sr./ Sra	Fdo. Sr./Sra

Contenido

1 Tabla de Administración de Tratamiento de Riesgos

Id Riesgo	Nombre	Probabilidad	Impacto	Responsable	Estado
1	Se subestima el tiempo requerido para el desarrollo	70%	2	Pierobón M., Matía	No ocurrido
2	Fallo en la elicitación de requerimientos	70%	2	Castro, Federico	No ocurrido
3	Detección de característica no deseada	70%	4	Castro, Federico	No ocurrido
4	Falta de formación en herramientas	60%	3	Rios, Gastón	Ocurrido
5	Ocurren cambios en los requerimientos	50%	2	Rios, Gastón	Ocurrido
6	Se genera software ineficiente	50%	4	Pierobón M., Matía	No ocurrido
7	Pérdida de información en el servidor de db	40%	1	Pierobón M. Matías	No ocurrido
8	Ataque exitoso de seguridad	40%	3	Pierobón M. Matías	No ocurrido
9	Baja del servicio de pagos	30%	2	Rios, Gastón	No ocurrido
10	Miss-read en test de autodeploy	30%	3	Pierobón M. Matías	
11	Sobrecarga de tráfico en el servidor estático	20%	2	Rios, Gastón	
12	Falla en la tarea de renovación de certificado	10%	1	Rios, Gastón	
13	Pérdida de credenciales de mantenimiento	10%	4	Castro, Federico	
14	Baja del servidor de repositorio	10%	2	Pierobón M., Matía	
15	Pérdida de información en el deployment	10%	4	Rios, Gastón	
16	Presupuesto insuficiente	10%	1	Rios, Gastón	
17	Problema de salud de un empleado.	10%	3	Castro, Federico	
18	Baja del servicio estático	10%	1	Pierobón M., Matías	

2 Plan de administración de riesgos

Id Riesgo 1	**Nombre :**Se subestima el tiempo requerido para el desarrollo **Fecha : 09/05/2017**	
	Descripción : Se realizó una mala estimación del tiempo requerido para finalizar el sistema y este no es suficiente.	
Probabilidad: 70%		
Impacto: 2		
Responsable: *Rios, Gastón*		**Clase: Estimacion**
Estrategia de Mitigación (Anulación/Minimización): Se consultó el tiempo de la programación con personas experimentadas y se pautó una entrega con un poco de tiempo restante en caso de posibles problemas.		
Plan de Contingencia : Se pedirá posponer la entrega al cliente indicando las causas precisas de este problema, y en caso de no ser posible posponer la entrega se entregará el producto con su versión previa y se irán agregando las funcionalidades que no hayan sido finalizadas.		

Id Riesgo 2	**Nombre :** Falló en la elicitación de requerimientos **Fecha : 09/05/2017**	
	Descripción : Se generaron fallas en la elicitación de requerimientos, lo que generó requerimientos inconsistentes, erróneos o imprecisos.	
Probabilidad: 70%		
Impacto: 2		
Responsable: *Rios, Gastón*		**Clase: Requerimientos**
Estrategia de Mitigación (Anulación/Minimización): Se dedicó suficiente tiempo a esta tarea para intentar resolver problemas de elicitación en discusiones con el cliente. También los analistas de sistemas destinados a esta operación superaron el curso de ingeniería de software I en el que fueron capacitados para realizar esta tarea.		
Plan de Contingencia : Se utilizará la metodología ágil Scrum en la cual el cliente es parte del equipo desarrollador y puede detectar estos fallos y corregir el requerimiento en caso de encontrarlos.		

Id Riesgo 3	**Nombre :** Detección de característica no deseada **Fecha : 09/05/2017**	
	Descripción : Se encuentra una falla en el sistema (o bug) sobre un comportamiento no esperado del mismo	
Probabilidad: 70%		
Impacto: 4		
Responsable: *Castro, Federico*		**Clase: Tecnológico**
Estrategia de Mitigación (Anulación/Minimización): Se realizan test (automigratorios como estáticos) sobre las funcionalidades del sistema y se maneja cada funcionalidad de forma aislada del resto.		
Plan de Contingencia : Se genera un branch aparte para tratar el defecto, y una vez solucionado pasa a una rama de testeo, luego de pasar todos los test runner se realiza el merge a desarrollo y se corren test pre-production para luego ser combinada con la rama de producción la cual se etiqueta con una nueva versión minor.		

Id Riesgo 4	**Nombre :** Falta de formación en herramientas **Fecha : 09/05/2017**
	Descripción : Los empleados no tienen la formación necesaria para hacer un uso correcto de las herramientas necesarias.
Probabilidad: 60%	
Impacto: 3	
Responsable: *Pierobón Marcos, Matías*	**Clase: Personal**
Estrategia de Mitigación (Anulación/Minimización): Se buscará empleados que sepan utilizar las herramientas al contratarlos. Aquellos empleados que no tengan formación en las herramientas necesarias se les instruirá su uso previo al comienzo del proceso.	
Plan de Contingencia : Se realizarán cursos sobre las herramientas en las cuales estén incapacitados los empleados, caso contrario reemplazados por empleados mejor calificados mientras son reasignados.	

Id Riesgo 5	**Nombre :** Ocurren cambios en los requerimientos **Fecha : 09/05/2017**
	Descripción : Se produce un cambio en un requerimiento previamente elicitado, se agregan restricciones o se agregan nuevos requerimientos.
Probabilidad: 50%	
Impacto: 2	
Responsable: *Rios, Gaston*	**Clase: Requerimientos**
Estrategia de Mitigación (Anulación/Minimización): Se busco realizar la elicitación de requerimientos lo más precisa y abarcativa posible para evitar pasar de alto algún requerimiento o realizar una mala elicitación. También se buscará crear un código adaptable que responda bien a cambios mediante un aproach orientado a objetos.	
Plan de Contingencia : Se documentará el cambio de requerimientos, luego este agregue, quite o modifique características. En caso de remover o modificar caracteristicas existentes, este cambio será realizado mediante un hotfix del sistema. En caso de agregar nuevas características, estos cambios serán evaluados para ser aplicados según su prioridad.	

Id Riesgo 6	**Nombre :** Se genera software ineficiente **Fecha : 09/05/2017**
	Descripción : El sistema no cumple con los requisitos de eficiencia esperados.
Probabilidad: 50%	
Impacto: 4	
Responsable: *Pierobón Marcos, Matías*	**Clase: Tecnológico**
Estrategia de Mitigación (Anulación/Minimización): El servidor escogido para hostear al sistema en un principio es capaz de soportar más de 150 transacciones diarias, este valor estando dentro de las expectativas de taza de usos del sistema. Se evalúa la eficiencia del código generado durante la etapa de testing.	
Plan de Contingencia : El sistema es capaz de ser movido a un servidor de mayores prestaciones para soportar una tasa de uso superior a la esperada.	

Id Riesgo 7	**Nombre :** Pérdida de información en el servidor de db **Fecha : 09/05/2017**
	Descripción : El servidor de bases de dato sufre una pérdida de información persistente relevante al sistema
Probabilidad: 40%	
Impacto: 1	
Responsable: *Pierobón Marcos, Matías*	**Clase: Tecnológico**
Estrategia de Mitigación (Anulación/Minimización): Se elige el servidor de datos de Google-Inc Firebase por su alta garantía en seguridad y estrategias de duplicación y paridad. Como también sus continuos reportes sobre el estado del mismo. Se realizan backups con una cierta periodicidad de la información.	
Plan de Contingencia : Se inicia un pedido formal al equipo de soporte de Firebase como el intento de recuperación de paridad del mismo. Se prepara la restauración de backup .	

Id Riesgo 8	**Nombre :** Ataque exitoso de seguridad **Fecha : 09/05/2017**
	Descripción : La seguridad del sistema es vulnerada y terceros obtienen acceso a la información contenida.
Probabilidad: 40%	
Impacto: 3	
Responsable: *Pierobón Marcos, Matías*	**Clase: Tecnológico**
Estrategia de Mitigación (Anulación/Minimización): La información de contraseñas de usuarios es cifrada por protocolos bycript con un salt autogenerado durante la asignación de la misma, y el tráfico entre clientes y el servidor es cifrado por medio de un certificado SSL. Todos los datos pertinentes a las transacciones de créditos no son almacenados en el servidor.	
Plan de Contingencia : El acceso al servicio es temporalmente deshabilitado mientras se analiza el ataque y se corrigen las vulnerabilidades utilizadas. Se actualizan los certificados de seguridad de todos los involucrados con el sistema. Se informa a los usuarios y se les recomienda que re-autentifiquen su cuenta de correo, y que cambien su contraseña.	

Id Riesgo 9	**Nombre :** Baja del servicio de pagos **Fecha : 09/05/2017**
	Descripción : Fallo en la comunicación con el proveedor de pagos
Probabilidad: 30%	
Impacto: 2	
Responsable: *Pierobón Marcos, Matías*	**Clase: De Organización**
Estrategia de Mitigación (Anulación/Minimización): Se eligen servidores oficiales con oficinas de soporte especializadas y librerías no comunitarias. Se mantienen certificados SSL al dia de ambas partes.	
Plan de Contingencia : Se inicia un pedido formal al equipo del servicio junto a otros mecanismos legales.	