

# **Plan de Manejo de Riesgos**



**Equipo: Docsify  
Cristina Vázquez  
Juan Carlos Medina  
Susana Jaramillo  
Mariana Ávalos  
Marcelo Álvarez**

**Universidad Panamericana  
Clase: Gestión de riesgos  
Profesor: Ricardo Ramírez Herrmann**

## Contenido

<b>1. Antecedentes</b>	<b>3</b>
<b>2. Objetivos y entregables del proyecto</b>	<b>3</b>
<b>3. Plan de gestión de riesgos</b>	<b>4</b>
3.1. Descripción del Apetito por el riesgo de sus patrocinadores y partes interesadas.	4
3.2. Identificación de estrategias seleccionarán para los riesgos que identifiquen (aceptar, mitigar, transferir, evitar)	5
3.3. Indicación del marco de referencia de gestión de riesgo.	8
3.4. Tabla RACI (roles y responsabilidades) para su proyecto respecto a administración de riesgos	9
3.5. Listado de Recursos (financieros y humanos) disponibles para el proyecto. En caso de recursos financieros indicar recursos disponibles más fondo de reserva, en caso de recursos humanos indicar, rol, meses disponibles, horas diarias disponibles promedio diario y horas totales disponibles por persona (meses * horas disponibles por día * días al mes trabajando).	11
3.6. Cronograma de su proyecto (Gantt) con las actividades de administración de riesgos incluidas.	12
3.7. Risk Breakdown structure que usara su proyecto	13
3.8. Definiciones cualitativas de Matriz de probabilidad e impacto	14
<b>4. Análisis de aplicabilidad de herramientas de identificación de riesgos</b>	<b>17</b>
<b>5. Lista de riesgos identificados</b>	<b>18</b>
<b>6. Análisis Cualitativo de riesgos</b>	<b>23</b>
<b>7. Análisis Cuantitativo de los riesgos más relevantes</b>	<b>25</b>
7.1. Análisis Riesgo #11 - Simulación Montecarlo	25
7.2. Análisis Riesgo #10 - Árbol de decisiones	28
7.3. Análisis de riesgo #16 - Árbol de decisiones	30
7.4. Fondo de Contingencia para Riesgos	31
<b>9. Plan de Actividades con las acciones incluidas para la gestión de riesgos</b>	<b>33</b>
<b>10. Indicadores de riesgos KRI y sus límites de alerta</b>	<b>34</b>
<b>11. Aprendizajes del equipo respecto a la gestión de riesgos</b>	<b>37</b>
<b>Referencias</b>	<b>38</b>

# 1. Antecedentes

El sector de Salud Privada de México no posee un sistema digital de registros médicos que sea fácil de usar y confiable; los médicos necesitan un sistema que les automatice la búsqueda, el almacenamiento y la realización de los expedientes y registros. Por esta carencia, casi todos prefieren el uso del papel y un sistema de archivado tradicional.

En septiembre de 2022 realizamos una encuesta donde el 55% de los encuestados afirmó no tener un sistema digital para el manejo de registros médicos, y que le gustaría usar alguno. Los encuestados fueron principalmente médicos con más de 5 años de experiencia mínima y mexicanos.

Ante esta clara necesidad en un área de la sociedad mexicana tan importante, nosotros decidimos ser los creadores de ese sistema, en un formato de página web destinado a todos los médicos.

## 2. Objetivos y entregables del proyecto

El objetivo de nuestro proyecto es sacar al mercado en el tercer trimestre de 2023 un sistema web de manejo de registros médicos que sea accesible desde internet y atractivo para nuestros clientes (médicos del sector privado). Para esto, tenemos que hacer toda la planeación previa, incluyendo un correcto control de riesgos.

Nuestros entregables finales serán tres:

- El Acta Constitutiva del proyecto.
- La página web en su versión 1.0.
- Un plan de ejecución del proyecto.

### 3. Plan de gestión de riesgos

#### 3.1. Descripción del Apetito por el riesgo de sus patrocinadores y partes interesadas.

Hay dos grupos de interesados en el proyecto que vale la pena analizar en esta sección:

1. El equipo de la empresa, Docsify.
2. Los doctores, que son nuestros clientes.

Como empresa, Docsify está abierta al riesgo de nuevas tecnologías, en específico de mejores implementaciones para la facilidad de nuestros clientes. Para eso, estaremos en constante contacto con doctores selectos y les preguntaremos cómo mejorar la aplicación. También, no tenemos miedo a tomar mayores riesgos si hay una mayor recompensa al final del túnel. Por ejemplo, tener alianzas con médicos que no conocemos pero son sobresalientes en su área de especialidad para generar interés en nuestro producto.

En contraste, nuestros clientes -doctores en puestos medios y altos en consultorios, hospitales y clínicas- tienen una mínima hambre al riesgo, mayormente por la naturaleza de su estresante campo laboral. Es por esto que las entregas deben de ser claras, sencillas, y propuestas con mucha anterioridad; una sola actualización repentina podría alienar a varios de nuestros clientes. Aunque pueden correr un poco de riesgo relacionado con dinero, pues nuestros clientes meta tienen suficiente. Para ganarnos su confianza, debemos de transmitir la menor cantidad de riesgo posible.

### 3.2. Identificación de estrategias seleccionarán para los riesgos que identifiquen (aceptar, mitigar, transferir, evitar)

Los riesgos que se identificaron se enlistan a continuación con su estrategia correspondiente. Se realiza puntualmente una estrategia por riesgo ya que se considera que cada riesgo tiene su propia naturaleza y, debido a que el software relaciona disciplinas muy diferentes entre sí, cada solución depende de la causa de cada uno de los problemas potenciales.

ID	Riesgo	Estrategia	Descripción Estrategia
1	Actualización de buscador (browser) en máquinas de desarrollo o pruebas que modifican el comportamiento del software.	Aceptar	Los buscadores son software de empresas externas (Google, Microsoft) por lo que las actualizaciones no pueden evitarse. Estar preparados con tiempo de reserva por si falla el software web por la actualización del buscador.
2	Complicaciones técnicas para implementar funcionalidades clave.	Transferir	En caso de que algún miembro del equipo no pueda encontrar la solución a un problema, solicitar <i>Peer Programming</i> para que otro integrante le ayude.
3	Exceso de cambios en el producto por parte del cliente.	Evitar	Aclarar con el cliente la cantidad límite de cambios para evitar que se de el exceso de cambios en el feedback.
4	Pérdida de archivos de diseño (.psd, .ai, etc).	Mitigar	Para evitarlo por completo necesitaríamos PCs con un procesador muy costoso, por lo que lo mejor es estar preparado con copias de seguridad de archivos diarios.
5	Interrupción repentina del presupuesto por parte de inversionistas.	Mitigar	Reducir las probabilidades con el constante engagement del stakeholder.
6	Una aplicación similar sale al mercado antes que la nuestra.	Aceptar	Depende del mercado, lo único es estar preparado con features diferenciadoras para lanzarse durante diferentes etapas, no todas al mismo tiempo.

7	Nuevas leyes de privacidad en el uso de los datos clínicos.	Aceptar	Depende del entorno socio-económico, y lo único es estar informado del estado actual de legislaciones de privacidad de datos.
8	Pérdida de datos durante testing o desarrollo.	Evitar	Se deben evitar las condiciones que generan este riesgo, por lo que se deberá trabajar con una copia de seguridad de la BD realizada cada semana, además de tener 2 versiones principales: desarrollo y producción.
9	Demandas por parte del equipo de trabajo.	Mitigar	Es imposible mantener a todos los empleados complacidos, pero se puede mantener constante comunicación para que una renuncia o conflicto no nos tome por sorpresa.
10	Sistema resultante (iterado o final) es demasiado lento (execution time).	Mitigar	Tratar de reducir su probabilidad mediante las constantes pruebas de calidad donde pedazos de código que sean muy lento o tengan complejidad computacional de $O(n^3)$ sean rechazados, a menos que sea indispensable esa complejidad.
11	Almacenamiento en la nube excedido repentinamente.	Evitar	Se puede desaparecer el riesgo si se configuran logs y se designa a alguien encargado de checar las estadísticas del host de datos.
12	Renuncias por parte del equipo del proyecto.	Mitigar	No se puede obligar a nadie a continuar, pero se puede mantener una baja rotación de personal con un Management consciente de su condición humana y emocional.
13	Despidos por parte del equipo del proyecto.	Aceptar	Es siempre una posibilidad, y de ser necesario, sólo nos toca convivir con ello.

14	Falta de personal debido a exceso de trabajo.	Mitigar	Se tiene un número de integrantes limitado, y el exceso de trabajo se puede sólo reducir, con un Scrum Master y calendario de trabajo constantemente abierto al feedback de los integrantes.
15	Falta de presupuesto.	Mitigar	Se puede llegar a ese punto pero se puede tratar de aplazar lo más posible a través de un control de costos y gastos que cubra todos los departamentos.
16	Ataque cibernético	Evitar	Se busca que todas las fuentes de riesgo de seguridad desaparezcan, a través de control en los accesos a la BD y la configuración de acceso con VPN e IP estática privada.

### 3.3. Indicación del marco de referencia de gestión de riesgo.

1. **Identificación de riesgos:** En esta etapa, se identifican todos los posibles riesgos que podrían afectar el proyecto. Para la creación del software de registro del historial clínico, algunos de los riesgos que podrían identificarse son: falta de cumplimiento de las regulaciones de privacidad de datos, fallos en la seguridad del software, falta de integración con los sistemas existentes en el hospital, etc.
2. **Evaluación de riesgos:** Una vez que se han identificado los riesgos, se debe evaluar la probabilidad de que ocurran y el impacto que tendrían en el proyecto. Por ejemplo, la falta de cumplimiento de las regulaciones de privacidad de datos podría tener un impacto significativo en la reputación del hospital y el software.
3. **Priorización de riesgos:** En esta etapa, se clasifican los riesgos según su probabilidad e impacto, y se priorizan para su tratamiento. Por ejemplo, los riesgos con alta probabilidad e impacto deberían recibir más atención que los riesgos con baja probabilidad e impacto.
4. **Planificación de la respuesta al riesgo:** En esta etapa, se desarrollan planes para manejar los riesgos prioritarios identificados. Esto podría incluir la implementación de medidas de seguridad adicionales para proteger la privacidad de los datos del paciente, el diseño de pruebas rigurosas para garantizar la calidad del software y la realización de pruebas de integración exhaustivas.
5. **Implementación de la respuesta al riesgo:** Una vez que se han desarrollado los planes de respuesta al riesgo, se implementan para reducir la probabilidad o el impacto de los riesgos identificados. Por ejemplo, si se ha identificado un riesgo de seguridad, se podría implementar una función de autenticación de dos factores para aumentar la seguridad del software.
6. **Monitoreo y control de los riesgos:** En esta etapa, se supervisan continuamente los riesgos y se toman medidas para mitigarlos si es necesario. Es importante establecer un proceso de seguimiento continuo para garantizar que los riesgos se estén manejando adecuadamente.

Algunos elementos extra que se pudieran implementar en la gestión de riesgos de Docsify, se encuentran:

- **Involucrar a los stakeholders clave:** Involucrar a los stakeholders clave, como los médicos, administradores del hospital y el equipo de IT. Esto ayudará a identificar riesgos adicionales y asegurar que las respuestas al riesgo sean adecuadas.
- **Establecer un equipo de gestión de riesgos:** Forma un equipo dedicado a la gestión de riesgos, que esté encargado de identificar y mitigar los riesgos del proyecto. Este equipo deberá estar compuesto por miembros del equipo de proyecto y stakeholders clave.
- **Realizar una evaluación de seguridad:** Asegúrate de realizar una evaluación de seguridad completa del software antes de su lanzamiento. Esto puede incluir pruebas de penetración y análisis de vulnerabilidades para identificar posibles vulnerabilidades de seguridad.



- **Establecer protocolos de respaldo:** Establecer protocolos de respaldo para garantizar que los datos del paciente se puedan recuperar en caso de una falla del sistema o alguna amenaza externa como un desastre natural. Esto puede incluir copias de seguridad regulares y almacenamiento de datos críticos de manera cíclica.
- **Capacitar al personal médico:** Asegurarnos de que el personal médico esté capacitado en el uso del software y en la protección de los datos del paciente. Esto puede incluir la capacitación en buenas prácticas de seguridad y privacidad de datos.
- **Realizar revisiones de seguridad periódicas:** Realizar revisiones de seguridad periódicas del software para identificar y mitigar posibles vulnerabilidades de seguridad. Esto puede incluir pruebas de penetración y análisis de vulnerabilidades regulares.
- **Mantenerse actualizado con las regulaciones de privacidad de datos:** Mantener al equipo actualizado con las regulaciones de privacidad de datos y ajustar el software en consecuencia. Esto puede incluir la implementación de medidas adicionales de seguridad para cumplir con los estándares de privacidad de datos actuales.

### 3.4. Tabla RACI (roles y responsabilidades) para su proyecto respecto a administración de riesgos

A continuación se muestra la Tabla RACI de los responsables respecto a las actividades principales del proceso de administración de riesgos. Cabe resaltar que el Socio Fundador es un integrante fuera del equipo de trabajo en la Universidad Panamericana, aunque por sus años de experiencia en el sector salud, se considera en muchas de las actividades. Por último, las acotaciones: R = responsable, A = accountable, C = consultado, I = informado.

Project tasks	PM/CTO	Lead designer	Director ingeniería y calidad	Director de logística	Director Desarrollo y programación	Socio fundador
Planeación del manejo de riesgos						
Definir estrategia y framework	A	I	I	R	I	C
Definir elementos de matriz de probabilidad e impacto	A	I	R	I	I	I
Definir apetito por el riesgo	A	I	C	R	I	C
Identificación de riesgos						
Selección de técnicas de identificación a utilizar	A, R	C	C	R	C	I
Planeación de la(s) técnicas presenciales: brainstorming y AMEF	A	C	C	C	C	I
Planeación de la(s) técnicas no presenciales: checklists	A	C	C	C	C	I
Sesión de brainstorming	A	R	R	R	R	C
Sesión de AMEF	A, R	R	R	R	R	I
Responder a Checklist	R	I	C	A	I	C
Documentación de los riesgos finales	A	C	C	R	C	I
Análisis cualitativo						
Categorización de riesgos y matriz de probabilidad e impacto	A	C	R	C	C	I
Análisis cuantitativo						
Análisis de árbol de decisión para riesgos priorizados	A	I	R	C	I	I
Planeación de la respuesta al riesgo						
Seleccionar acciones a realizar para riesgos priorizados	A, R	R	R	R	R	I
Definir formatos de reporte de riesgos	C	I	R	A	C	I
Implementación de respuesta al riesgo						
Mantener el reportaje de riesgos	I	I	R	A	C	I
Administración de recursos de reservas para riesgos	A	I	R	R	I	C
Monitoreo de riesgos						
Analizar reportes de riesgos cada sprint	R	I	C	A	I	C
Evaluación de plan de respuesta si se materializa un riesgo	R	I	R	A	C	I

3.5. Listado de Recursos (financieros y humanos) disponibles para el proyecto. En caso de recursos financieros indicar recursos disponibles más fondo de reserva, en caso de recursos humanos indicar, rol, meses disponibles, horas diarias disponibles promedio diario y horas totales disponibles por persona (meses \* horas disponibles por día \* días al mes trabajando).

### Página web

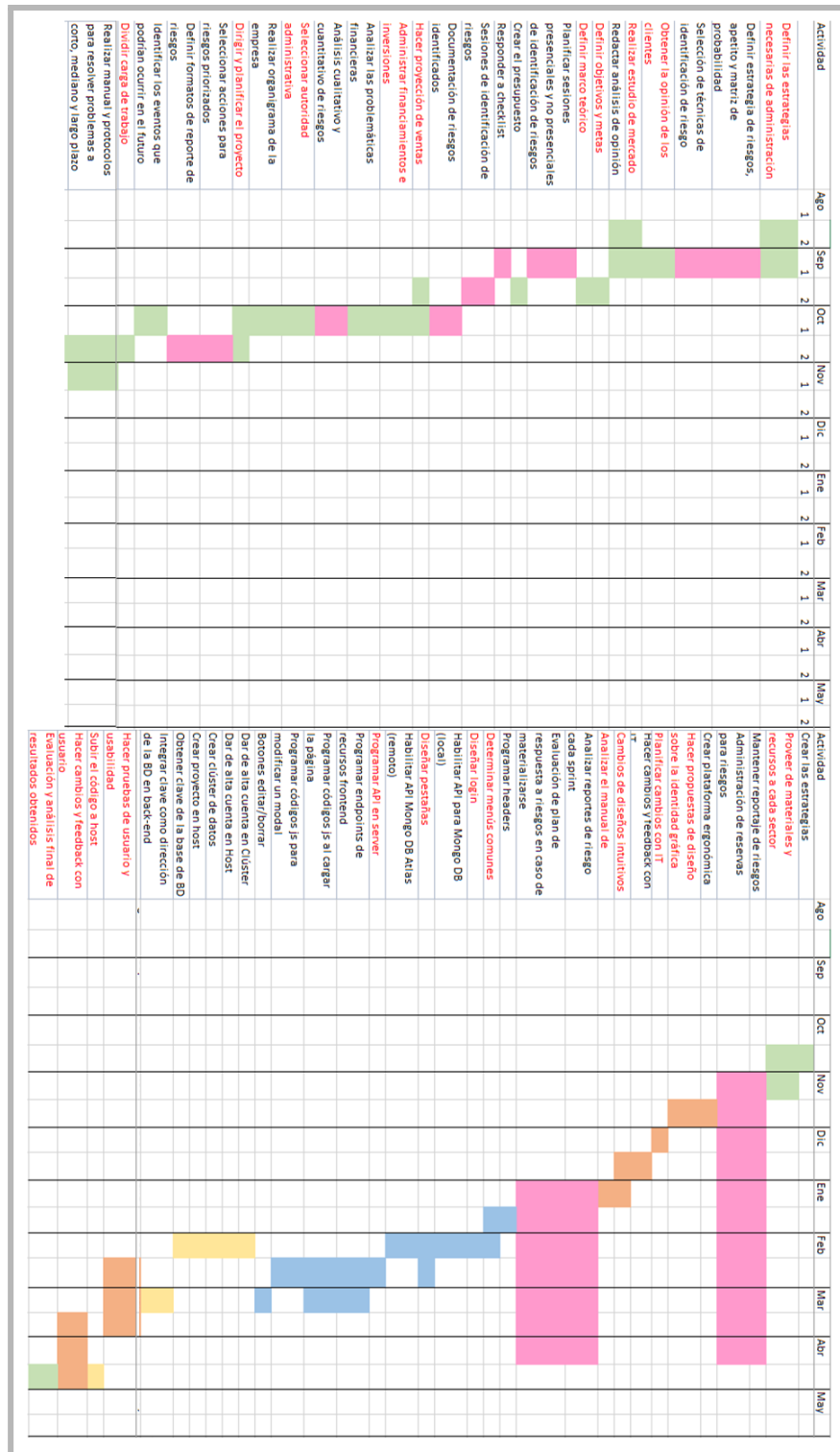
#### Determinación del Costos

			COSTO POR UNIDAD	
PRODUCTO	Pagina web		COSTO FIJO	\$ 132,315.67
CANTIDAD	1		COSTO VARIABLE	\$ 8,935.78
			COSTO TOTAL	\$ 141,251.45
			FONDO DE RESERVA	\$ 28,250.29
Liste los costos asociados a la producción			RECURSOS DISPONIBLES TOTALES	\$ 169,501.74
CANTIDAD	MEDIDA	DETALLE	COSTO FIJO	COSTO VARIABLE
1	Mensual	Servicio de cloud	\$ 1,666.67	\$ 83.33
3	Unidad	Computadoras	\$ 24,000.00	\$ 1,200.00
1	Mensual	Servicio de Internet	\$ 649.00	\$ 32.45
1	Mensual	Seguro contra ataque cibernetico	\$ 6,000.00	\$ 120.00
1	Unidad	Licencias de software	\$ 50,000.00	\$ 7,500.00
1	Unitario	Recursos Humanos	\$ 50,000.00	
Total			\$ 132,315.67	\$ 8,935.78

<b>Total de Horas</b>		64		
Areas	Horas diarias	Minutos	Dias	Meses
Recursos Humanos	64	3840	2.666666667	0.088888889
Area	Tareas	Horas Promedio Diarias	Minutos asignados	
Recursos Humanos	Reclutamiento y selección	8	3840	
Recursos Humanos	Capacitación y Desarrollo	8	3840	
Recursos Humanos	Administración de sueldos y beneficios	8	3840	
Recursos Humanos	Gestión del desempeño	8	3840	
Recursos Humanos	Salud y seguridad ocupacional	8	3840	
Recursos Humanos	Gestión del clima laboral	8	3840	
Recursos Humanos	Relaciones laborales	8	3840	
Recursos Humanos	Responsabilidad social	8	3840	

### 3.6. Cronograma de su proyecto (Gantt) con las actividades de administración de riesgos incluidas.

A continuación se presenta el cronograma del proyecto en forma de un diagrama de Gantt, donde están programadas las actividades del proyecto en su totalidad. Las actividades en rojo forman parte de la ruta crítica del proyecto, mientras que las actividades cuya señalización en el tiempo tiene un color rosa, son las actividades relacionadas al manejo de riesgos, mismas que coinciden con las actividades de la Tabla RACI.



### 3.7. Risk Breakdown structure que usara su proyecto

El RBS de los 15 riesgos que se identificaron en específico para este proyecto está dividido según la fuente que genera el riesgo: riesgos técnicos, de gestión, comerciales o de mercado, y externos.

RBS Nivel 0	RBS Nivel 1	Riesgo (ID)
Fuentes de Riesgo	1. Riesgos Técnicos	#1 Buscador
		#2 Complicaciones en implementación
		#4 Pérdida de archivos de diseño
		#8 Pérdida de datos
		#10 Sistema lento
		#16 Ataque cibernético
	2. Riesgos de Gestión	#3 Exceso de cambios
		#11 Almacenamiento excedido
		#13 Despidos
		#14 Falta de personal
	3. Riesgos Comerciales	#5 Interrupción de presupuesto
		#6 Aplicación similar surge en el mercado
		#15 Falta de presupuesto
	4. Riesgos Externos	#7 Nuevas leyes de privacidad
		#9 Demandas por parte del equipo
		#12 Renuncias por parte del equipo

### 3.8. Definiciones cualitativas de Matriz de probabilidad e impacto

Con el fin de facilitar la administración de riesgos durante el proyecto, se hará uso del software Project Risk Manager. En esta herramienta se define una matriz de probabilidad e impacto que será la que se utilice para el presente proyecto:

**Risk Matrix**

<b>PROBABILITY</b>	Probable (4)	4 Moderate	8 Major	12 Severe	16 Severe
	Possible (3)	3 Minor	6 Moderate	9 Major	12 Severe
	Unlikely (2)	2 Minor	4 Moderate	6 Moderate	8 Major
	Rare (1)	1 Minor	2 Minor	3 Minor	4 Moderate
		Low (1)	Medium (2)	High (3)	Very High (4)
<b>IMPACT</b>					



Como se observa, el resultado de multiplicar el valor de la probabilidad por el valor del impacto, define si un riesgo es parte de 4 categorías: Minor, Moderate, Major y Severe. El proyecto también hará uso de las definiciones que el software proporciona para estas categorías:

**Risk Ranking Definitions**

RANKING	DEFINITION
SEVERE	Risk that has a severe negative effect on objectives that cannot be endured. Urgent management attention required to reduce probability and impact. If the risk cannot be mitigated then it may invalidate the relevant objective or venture.
MAJOR	Risk that has major negative effect on objectives. Management attention required to reduce probability and impact. If the risk cannot be mitigated then it may have serious implications in relation to the objectives.
MODERATE	Risk that has a moderate negative effect on objectives that can be managed. Management attention should be applied to reduce the probability and impact. However, for those risks with a "Very High Impact", "Rare Probability" rating, a robust fall-back/contingency plan may suffice, plus early warning mechanisms to detect any increase in likelihood so that appropriate management action can be taken.
MINOR	Risk that has a minor negative effect on objectives. Risks with a "Low Impact", "Possible Probability" rating may require some mitigation to reduce probability, if this can be done cost effectively, to minimise the chance of risk occurrence and, hence, of any impact occurring. Likewise, risks with a "High Impact", "Rare Probability" rating may require some mitigation to reduce impact, but also only if this can be done cost effectively.

Las configuraciones del proyecto dentro de esta herramienta son esenciales para administrarlo consistentemente, por lo que a continuación se mostrarán dichas configuraciones que el proyecto tiene hasta el día de hoy, como producto de la etapa de planeación del manejo de riesgos.

Se define el proyecto dentro de la herramienta de la siguiente manera:

Contractor Logo:		Client Logo:	
Project Name:	<input type="text" value="Docsify"/>	Client Name:	<input type="text"/>
Project Manager:	<input type="text" value="Avalos Arce, Mariana"/>	Risk Manager:	<input type="text" value="Avalos Arce, Mariana"/>
Planned Start Date:	<input type="text" value="8/19/2023"/>	Planned End Date:	<input type="text" value="5/15/2024"/>
Commercial Budget:	<input type="text" value="407,820"/> <input type="text" value="USD"/>	Max. Cost Exposure:	<input type="text" value="100,000"/> <input type="text" value="USD"/>
Man-hour Budget:	<input type="text" value="364"/>	Max. Schedule Exposure:	<input type="text" value="4"/> <input type="text" value="Weeks"/>
Project Type:	<input type="text" value="Onshore - Brown Field"/>	Industry Sector:	<input type="text" value="Information Technology"/>
Region/Country:	<input type="text" value="Global"/>		

Debido a que el proyecto trata de desarrollar un software para la digitalización de registros médicos, no está dirigido a ningún cliente en particular, sino que se trata del primer producto de la startup Docsify, y por lo tanto, no se llenaron los campos de Client Logo y Client Name.

Otra aclaración importante es que, en los campos de Commercial Budget y Max Cost Exposure se establecen cantidades en la moneda USD. Sin embargo, los números en temas monetarios dentro del software siempre denotan cantidades en MXN, sólo que a falta de este tipo de cambio dentro del software, se utiliza USD.

Partiendo de que el proyecto tiene un apetito por el riesgo que podría catalogarse como Pareto Risk, los umbrales de riesgo que definen si un riesgo de Costo, Tiempo o Producción se considera como *Low*, *Medium*, *High* o *Very High* se establecen de la siguiente manera:

Rating	Cost as % of project budget	Schedule as % of project baseline	Production Loss (Weeks)	Reputation
4 Very High	61 - < 100%	77 - < 100%	More than 26 weeks	Severe Damage
3 High	33 - < 61%	51 - < 77%	8 - < 26 weeks	Long Term Damage
2 Medium	15 - < 33%	23 - < 51%	4 - < 8 weeks	Medium Term Damage
1 Low	0 - < 15%	0 - < 23%	0 - < 4 weeks	Short Term Damage

Dichos umbrales muestran que, para riesgos de costo se tiene menor tolerancia y una mayor cantidad de riesgos se consideran como Very High dentro del plan de mitigación de ser materializados, mientras que en riesgos de alcance (project baseline) se tendría más tolerancia e incluso la mayor proporción de los riesgos cae en la categoría de Medium, ya que al ser un proyecto con secciones de gestión bajo metodologías ágiles, presentan una gran tolerancia a cambios en alcance. Sin embargo, uno de los aspectos que el proyecto reconoce como waterfall es la restricción moderada o alta en cuestiones de tiempo de producción, por lo que la mayoría de riesgos de Production Loss se consideran High Priority, generando menor tolerancia a partir de 8 semanas.



## 4. Análisis de aplicabilidad de herramientas de identificación de riesgos

Herramienta	Aplicabilidad	Razonamiento	Selección: S/N	Actividades a incluir en el plan del proyecto relacionadas con la identificación de riesgos (seleccionadas)	Fecha de inicio y de fin de aplicación de herramienta
Delphi	4	Bastante aplicable porque el proyecto es orientado a la industria del software/seguridad donde el expertis ayuda, pero demasiado tiempo en las iteraciones.	No	No aplica	
Brainstorming	5	Es un equipo numeroso, que conoce del tema. Necesitamos recolectar todas las ideas posibles.	Sí	1. Sesión de brainstorming con todos los integrantes (etapa de planeación)	Inicio: 01/03/23 19:30 Fin: 01/03/23 20:30
Checklist	5	La industria del software tiene dentro de sus subramas riesgos ya conocidos. Se haría con otras técnicas.	Sí	1. Selección de checklist (PM, durante la planeación) 2. Responder al checklist (Equipo, durante planeación)	Inicio: 02/03/23 18:30 Fin: 02/03/23 19:30
Entrevistas	3	El equipo conoce del tema, por lo que hacer entrevistas con externos de temas amplios resultaría redundante, muy tardado.	No	No aplica	
RCA	2	Los riesgos en materia del software son claros, por lo que analizar a fondo un riesgo no nos ayuda a cubrir muchas áreas. Mucho tiempo.	No	No aplica	
FODA	1	Demasiado amplio y orientado a las características de una empresa. Lo que se necesita es mayor detalle que FODA.	No	No aplica	
AMEF	5	La priorización en temas de software es necesaria para decidir en cuál enfocarnos.	Sí	1. Selección de riesgos de las otras 2 técnicas 2. AMEF con NPR para los riesgos 3. Ordenamiento de riesgos según NPR	Inicio: 08/03/23 19:30 Fin: 08/03/23 22:00

## 5. Lista de riesgos identificados

A continuación se presenta el Registro de Riesgos con los resultados de las sesiones de identificación de riesgos. Estas sesiones involucraron las técnicas de Checklists y Brainstorming, donde se identificaron riesgos en la industria que pudieran ocurrir para el presente proyecto, mismo que tiene como alcance la producción y desarrollo de un sistema para mantener registros médicos digitales, sin incluir etapas de lanzamiento, marketing y/o mantenimiento del software. Los campos comunes a todos los riesgos son un ID único, Riesgo (overview), Descripción del riesgo, Causas del riesgo, Estrategia, Descripción de la estrategia y el Risk Owner, que en este caso es el departamento(s) responsable del seguimiento a dicho riesgo.

ID	Riesgo	Descripción de riesgo	Causas	Estrategia	Descripción de Estrategia	Risk Owner (responsable)
1	Actualización de buscador (browser) en máquinas de desarrollo o pruebas que modifican el comportamiento del software.	El browser es el principal cliente de una aplicación web, por lo que una actualización mayor del buscador en máquinas de desarrolladores y/o de pruebas de usuario podría significar funciones deprecadas, sin soporte o inválidas que en otras versiones del browser son válidas. Esto provocaría fallos e inconsistencias del sistema dependiendo de la versión de buscador que se use.	Falta de monitoreo en documentación y anuncios de Google Chrome y Firefox, Falta de registro de versión en lista de Cls.	Aceptar	Los buscadores son software de empresas externas (Google, Microsoft) por lo que las actualizaciones no pueden evitarse. Estar preparados con tiempo de reserva por si falla el software web por la actualización del buscador.	Depto. IT
2	Complicaciones técnicas para implementar funcionalidades clave.	Durante el desarrollo de un sistema, siempre existe la incertidumbre de que algún feature sea demasiado complejo de implementar, por lo que se complica dicho feature o tarda más en lograrse.	Dificultad del proceso, estimaciones equivocadas de tiempo, requerimientos fuera del alcance computacional del proyecto, falta de experiencia por parte del equipo de desarrollo.	Transferir	En caso de que algún miembro del equipo no pueda encontrar la solución a un problema, solicitar Peer Programming para que otro integrante le ayude.	Depto. IT
3	Exceso de	El cliente, durante	Descontento por	Evitar	Aclarar con el cliente	Depto.

	cambios en el producto por parte del cliente.	Sprint Review o en Pruebas de Usuario, presenta demasiadas solicitudes de cambio o nuevas implementaciones al producto iterado. Pone en riesgo la calidad y/o el tiempo de entrega.	parte del cliente con lo que se desarrolló, poca comunicación del Project Manager con el cliente sobre lo que se está implementando o cambiando, el cliente no está bien informado sobre el alcance del proyecto.		la cantidad límite de cambios para evitar que se de el exceso de cambios en el feedback.	IT, Project Manager
4	Pérdida de archivos de diseño (.psd, .ai, etc).	El software que el equipo de Diseño utiliza es propenso a "congelarse" y provocar la interrupción del sistema operativo de la máquina donde se trabaja, lo que resulta comúnmente en el repentino reinicio de la computadora sin guardado de cambios en los archivos.	Exceso de procesos en la RAM, poco monitoreo del estado de la RAM, saturación de llamadas al CPU (clicks), falta de versiones guardadas como respaldo.	Mitigar	Para evitarlo por completo necesitaríamos PCs con un procesador muy costoso, por lo que lo mejor es estar preparado con copias de seguridad de archivos diarios.	Depto. Diseño
5	Interrupción repentina del presupuesto por parte de inversionistas.	En cualquier momento durante el desarrollo del sistema se puede presentar un corte repentino del presupuesto planeado, ya sea por causas internas o externas al equipo del proyecto.	Descontento de inversionistas, falta de comunicación, problemas económicos por parte de inversionistas (recortes, inflación, despidos).	Mitigar	Reducir las probabilidades con el constante engagement del stakeholder.	Project Manager, Depto. de logística
6	Una aplicación similar sale al mercado antes que la nuestra.	Existe el riesgo latente en la industria tecnológica de que una aplicación similar exista en el mercado antes de que el proyecto sea liberado al mercado, lo que puede representar un cambio radical en los ingresos planeados,	Naturaleza de cambio rápido y constante en la industria tecnológica, violaciones al acuerdo de privacidad por parte de algún miembro del	Aceptar	Depende del mercado, lo único es estar preparado con features diferenciadoras para lanzarse durante diferentes etapas, no todas al mismo tiempo.	Depto. de Calidad

		precio de venta y respuesta del mercado.	equipo, falta de planeación de la respuesta ante tal contingencia.			
7	Nuevas leyes de privacidad en el uso de los datos clínicos.	Existe la posibilidad que durante el transcurso del proyecto, nuevas leyes sean aprobadas acerca del uso y manejo de datos clínicos de pacientes y/o doctores, por lo que funcionalidades de la aplicación podrían pasar de legales a ilegales.	Aprobación de nuevas leyes en el ámbito estatal o Federal, poco monitoreo de iniciativas en Cámara de Diputados.	Aceptar	Depende del entorno socio-económico, y lo único es estar informado del estado actual de legislaciones de privacidad de datos.	Depto. Logística
8	Pérdida de datos durante testing o desarrollo.	Durante el proceso de desarrollo del sistema y base de datos, este riesgo se refiere al caso donde por algún error o caso de prueba no previsto, se realice alguna modificación irremediable en la base de datos que resulte en la pérdida de datos o modelos importantes en la base de datos.	Falta de respaldos en la base de datos, ignorar la regla de utilización de versión local de la base de datos, Unit Tests de los controllers no previstos.	Evitar	Se deben evitar las condiciones que generan este riesgo, por lo que se deberá trabajar con una copia de seguridad de la BD realizada cada semana, además de tener 2 versiones principales: desarrollo y producción.	Depto. IT, Depto. Calidad
9	Demandas por parte del equipo de trabajo.	Algún miembro o ex-miembro del equipo presenta una demanda legal al equipo del proyecto.	Despidos injustificados, descontentos o maltratos no controlados, falta de atención legal en los procesos de renuncia y despidos.	Mitigar	Es imposible mantener a todos los empleados complacidos, pero se puede mantener constante comunicación para que una renuncia o conflicto no nos tome por sorpresa.	Depto. Logística
10	Sistema resultante (iterado o final) es demasiado lento (execution time).	El sistema entregado al final de un Sprint o del proyecto, al unirse con las demás iteraciones, presenta un tiempo de respuesta demasiado lento en las máquinas de pruebas.	Fallos en análisis de métricas de mantenimiento de software, complejidad computacional del prototipo es de $O(n^3)$ o mayor, modularidad del	Mitigar	Tratar de reducir su probabilidad mediante las constantes pruebas de calidad donde pedazos de código que sean muy lento o tengan complejidad computacional de $O(n^3)$ sean	Depto. Calidad

			código no supervisada por las métricas actuales.		rechazados, a menos que sea indispensable esa complejidad.	
11	Almacenamiento en la nube excedido repentinamente.	Este riesgo se refiere al caso donde la capacidad de almacenamiento contratado hasta el momento no sea suficiente para continuar con el cronograma o sea rebasado antes de lo previsto, resultando en cobros por exceso de almacenamiento.	Falta de monitoreo en los logs del clúster de datos y/o mensajes por parte de la empresa de almacenamiento, ejecuciones en la base de datos que por error saturan el almacenamiento.	Evitar	Se puede desaparecer el riesgo si se configuran logs y se designa a alguien encargado de checar las estadísticas del host de datos.	Depto. IT
12	Renuncias por parte del equipo del proyecto.	Durante el transcurso del proyecto, siempre existe la posibilidad de que un miembro del equipo ya no forme parte del mismo, sin algún aviso o con poco tiempo de anticipación, provocando reorganización o retrasos en el cronograma.	Algún miembro del equipo presenta problemas personales y renuncia por lo mismo, o renuncias por situaciones que se suscitan en el proyecto, descontentos o quejas no resueltas.	Mitigar	No se puede obligar a nadie a continuar, pero se puede mantener una baja rotación de personal con un Management consciente de su condición humana y emocional.	Project Manager, Depto. de Logística
13	Despidos por parte del equipo del proyecto.	Durante el transcurso del proyecto, siempre existe la posibilidad de que un miembro del equipo sea despedido.	Falta de compromiso por parte del agraviado, rendimiento deficiente, falta de motivación, comportamientos que no reflejan la filosofía del equipo.	Aceptar	Es siempre una posibilidad, y de ser necesario, sólo nos toca convivir con ello.	Project Manager, Depto. de Logística
14	Falta de personal debido a exceso de trabajo.	Existe la posibilidad de que, durante el desarrollo del proyecto, los recursos humanos	Estimaciones de carga de trabajo y tiempo poco realistas, exceso	Mitigar	Se tiene un número de integrantes limitado, y el exceso de trabajo se puede sólo reducir,	Project Manager, Depto. de

		sean insuficientes para cumplir con el cronograma, lo que resultaría en retrasos y/o nuevas contrataciones.	de bugs o implementaciones no previstas, procesos complejos no previstos en el cronograma.		con un Scrum Master y calendario de trabajo constantemente abierto al feedback de los integrantes.	Logística
15	Falta de presupuesto.	Puede ocurrir que, durante la realización de las actividades del proyecto, se requiera de inversiones nuevas no previstas.	Actividades no previstas en el cronograma, gastos repentinos no contemplados, complejidad de actividades rebasa las estimaciones.	Mitigar	Se puede llegar a ese punto pero se puede tratar de aplazar lo más posible a través de un control de costos y gastos que cubra todos los departamentos.	Project Manager, Depto. de Logística
16	Ataque cibernético	Existe el riesgo de que durante el desarrollo y pruebas de seguridad seamos objeto de un ataque cibernético (secuestro de BD, virus).	Vulnerabilidades en la encriptación de la información en la BD, falta de configuración de permisos para los usuarios con acceso y falta de controles de seguridad en la conexión VPN otorgada a terceros.	Evitar	Se busca que todas las fuentes de riesgo de seguridad desaparezcan, a través de control en los accesos a la BD y la configuración de acceso con VPN e IP estática privada.	Depto. IT

## 6. Análisis Cualitativo de riesgos

El nivel de apetito por el riesgo de este proyecto se clasifica como Pareto Risk, ya que estamos dispuestos a aceptar riesgos con una alta razón recompensa-riesgo, donde de ser necesario, se tomarán riesgos al contemplar su recompensa. Este nivel de riesgo hace que **la matriz de probabilidad e impacto** tenga un número equitativo de celdas en cada color verde, amarillo, naranja y rojo. Si clasificamos los riesgos identificados en el Risk Registry (16), podemos visualizar su severidad (multiplicación de probabilidad x impacto) en el siguiente diagrama, que muestra los riesgos con su ID (identificación de riesgos describe cada ID).

Probability	Riesgo			
Probable (4)	Moderate (4)	Major (8)	Severe (12) #11	Severe (16) #16
Possible (3)	Minor (3) #2 #3	Moderate (6)	Major (9) #6	Severe (12) #10
Unlikely (2)	Minor (2) #1	Moderate (4) #15 #8	Moderate (6)	Major (8)
Rare (1)	Minor (1) #4	Minor (2) #9	Minor(3) #13 #14 #5 #12	Moderate (4) #7
Impact	Low (1)	Medium (2)	High (3)	Very high (4)

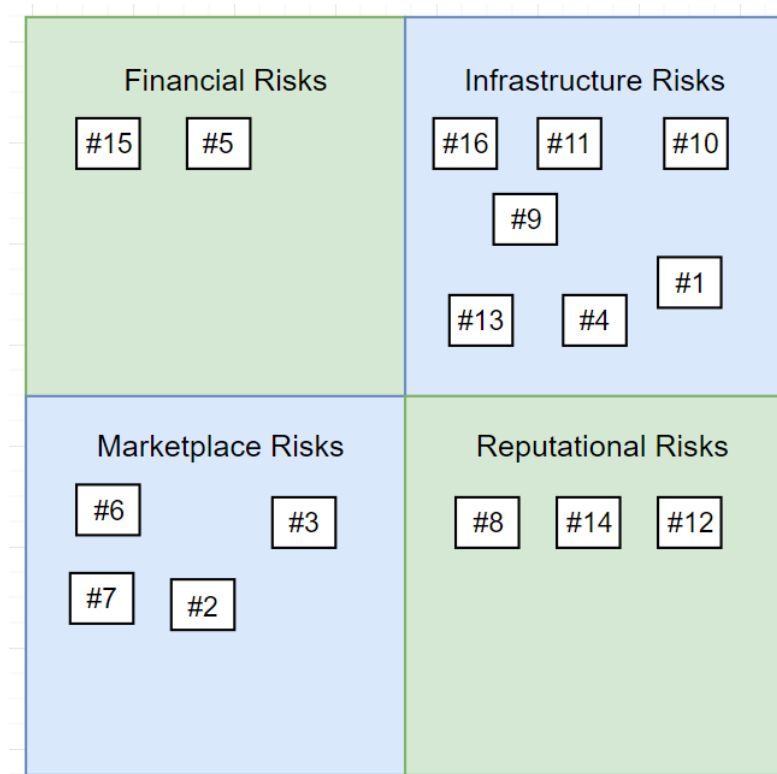
De esta manera, se identifican 3 riesgos con alta razón de riesgo-recompensa: riesgos con ID #11, #16 y #10. Si recordamos a qué riesgos corresponden dichos IDs sabemos que son:

- Riesgo #11: Almacenamiento excedido en el clúster de datos
- Riesgo #16: Ataque cibernético debido a vulnerabilidad en clúster de datos
- Riesgo #10: Sistema resultante se ejecuta demasiado lento por falta de optimización de algoritmos

Por lo tanto, **dichos riesgos serán el objeto de análisis cuantitativo** en las siguientes secciones, ya que según el apetito por el riesgo, al tratarse de riesgos con alto nivel de recompensa estamos comprometidos a atajarlos debidamente y a enfocarnos en ellos por encima de los restantes al ser los de alto impacto y probabilidad. Asimismo, los **tres**

**riesgos más importantes** o severos del proyecto se clasifican como riesgos de **infraestructura** siguiendo el modelo FIRM del Risk Management Institute. Se utiliza este modelo para tener una identificación y preparación al riesgo lo más completa posible. Se busca que lo estratégico, táctico y operativo sea involucrado en cada uno de los tres riesgos que se analizan a continuación de forma cuantitativa. Al ser riesgos de infraestructura, y según el PMI, de tecnología interna, su análisis es meramente cuantitativo, a excepción de la clasificación utilizando la matriz de probabilidad e impacto y FIRM.

Siguiendo con el análisis cualitativo de los riesgos, se presenta la clasificación de los riesgos (con su ID, donde la sección de identificación de riesgos describe cada ID) por su naturaleza según el modelo FIRM del IRM, para asegurar una identificación completa de riesgos.





## 7. Análisis Cuantitativo de los riesgos más relevantes

### 7.1. Análisis Riesgo #11 - Simulación Montecarlo

El riesgo #11 de **almacenamiento excedido** en el clúster de datos se daría debido a una **estimación errónea** acerca de la cantidad de memoria en la nube que un usuario promedio tendría en el sistema. Por ello, es preciso realizar una simulación de Montecarlo para modelar la probabilidad de que los usuarios se excedan en la cantidad de memoria destinada para ellos. Para ello, lo primero que hay que estimar es cuál es la cantidad promedio que usaría una persona en un servicio cloud, lo cual se obtiene después de simular, con una distribución de probabilidad, la cantidad que N usuarios utilizarían del servicio.

La cantidad de almacenamiento digital requerido por una persona no parece seguir una distribución normal, ya que hay muchos factores que pueden influenciar las necesidades de almacenamiento y las preferencias de éste. Por ejemplo, pueden existir usuarios que utilizan almacenamiento en la nube de forma básica, mientras que otros usuarios dependen más de grandes archivos. Además, el uso de cloud está influenciado por muchos factores externos como avance tecnológico, cambios en los formatos de almacenamiento, y procesamiento.

Por lo tanto, la distribución de probabilidad del almacenamiento digital estará muy probablemente sesgada y será no-normal, con una cola larga a la derecha. Esto por la suposición de que la gran mayoría de la población sólo necesitará una porción de almacenamiento pequeña, mientras que el subconjunto más pequeño de individuos con necesidades especializadas o intensamente enfocadas en archivos pesados podrá requerir de cantidades más grandes de almacenamiento.

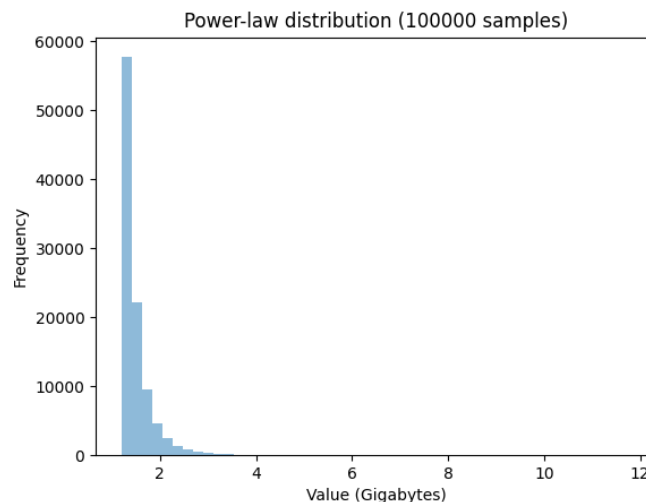
Esta distribución se conoce como power law distribution, donde los casos extremos, que en este caso son los usuarios con grandes necesidades de almacenamiento, tienen un impacto considerable en la distribución. Esta distribución coincide con otro fenómeno del ámbito, que es el tráfico de redes de internet. Un estudio publicado en Journal of Information Science en 2011, titulado A power law distribution for file sizes in a large network of personal computers (Lehman et al., 2011), analiza la distribución de los tamaños de los archivos a través de una red local inalámbrica con 250 000 archivos, y encuentra que el almacenamiento requerido sigue una distribución power law. De forma similar, un artículo publicado en Proceedings of the International Conference on Management of Emergent Digital EcoSystems también en 2011 titulado Modeling User Demand for Cloud Storage: An Empirical Study (Jiang et al., 2011), examina la distribución de almacenamiento en un grupo de usuarios y encontró que también seguía una power law distribution.

La distribución power law sigue la siguiente función:

$$f(x) = (\alpha - 1) * (x / x_{min})^{-(\alpha)},$$

donde  $x$  es la variable aleatoria que representa el almacenamiento requerido de un usuario de un servicio en la nube,  $\alpha$  es el parámetro de escala y  $x_{\min}$  es el valor mínimo (Sarasola, 2023).

En el estudio de Jiang, se estima que estos parámetros son:  $\alpha = 1.19$  GB y  $x_{\min} 6.16$  GB (Jiang et al., 2011). Cabe resaltar que este tamaño en GB no es del tamaño de los archivos, sino de los datos en dichos archivos, medidos por bytes. Entonces, si utilizamos la herramienta de Python para crear 100,000 muestras de valores que siguen esta distribución, se obtiene el siguiente histograma de frecuencia:



Adicionalmente, se obtienen las siguientes medidas de tendencia central:

- Promedio: 1.475 GB por usuario
- Desviación estándar: 0.3648 GB de la media
- IQR: 0.298 GB de la media

A pesar de que la distribución no es normal, la desviación estándar nos habla de la variación de los datos con respecto de la media aritmética. En distribuciones no-normales, la desviación estándar resulta una medida demasiado sensible a outliers, que en caso de *powerlaw*, son muy relevantes. Por lo mismo, se puede calcular el IQR o rango intercuartil para saber la variación de los datos más concretamente. Para resolver la cuestión de qué probabilidad existe de que un usuario sobrepase el almacenamiento que el proyecto estima, primero tenemos que recordar el supuesto de que en el proyecto el usuario tendrá como máximo 1.5 GB de espacio aproximadamente. Por lo tanto, si en la simulación calculamos el número de datos que sobrepasan el valor de 1.5 y dividimos esta cuenta entre 100,000:

$$P(x > 1.5 \text{ GB}) = \text{casos donde } x > 1.5 / 100,000 = 3,206 / 100,000 = 0.03206$$

Así, sabemos ahora que **existe una probabilidad del 3.21% de que un usuario sobrepase el espacio estimado en el servicio de la nube**. Si tomamos en cuenta que estos datos son de 2011, y tomamos el crecimiento anual promedio de almacenamiento en cloud computing de 4.5% (New York Times, 2021), obtenemos que el promedio es 2.55 GB

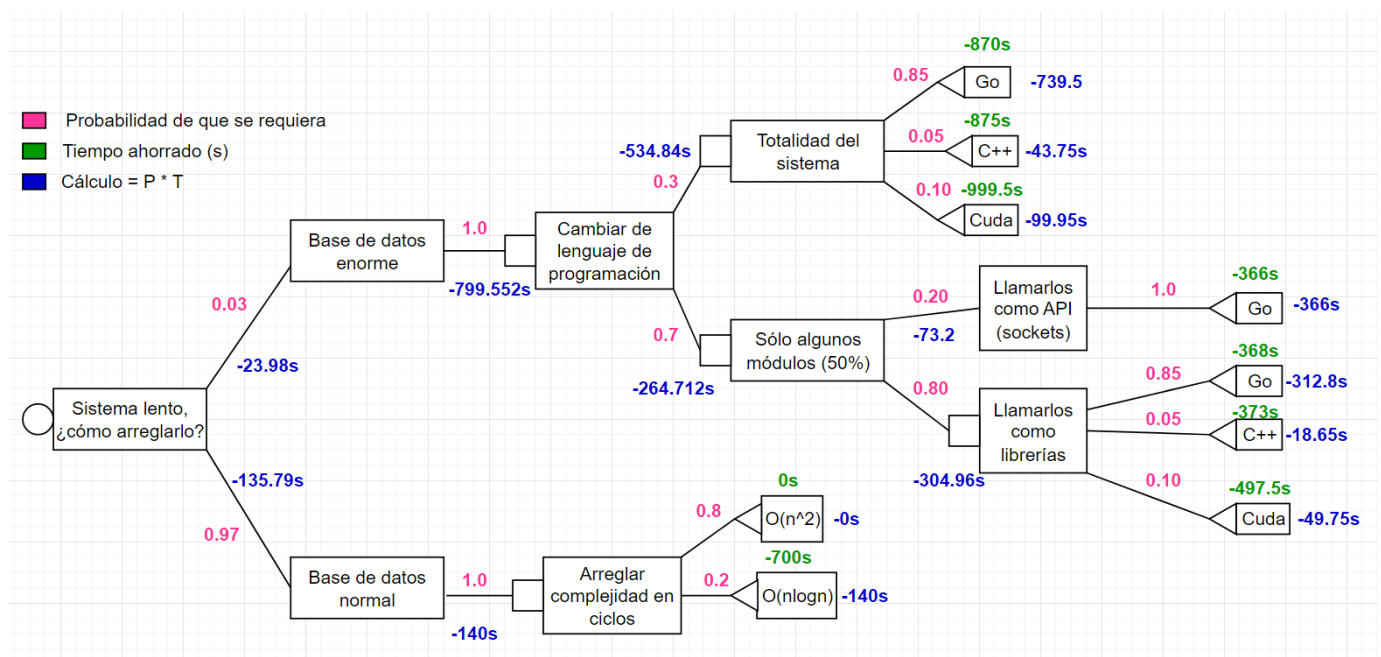
y que existe una probabilidad del 3.21% de que se exceda. El código que se usó para este apartado se encuentra en el repositorio de la documentación del proyecto: <https://github.com/the-other-mariana/pm/blob/master/PM2/risks/week6/montecarlo.py>

## 7.2. Análisis Riesgo #10 - Árbol de decisiones

El riesgo #10 se refiere a aquel caso donde **el sistema resultante** de algún sprint termine siendo **demasiado lento** para el usuario. Este riesgo depende del feedback y de la definición nominal de “demasiado” lento. Si esto sucede, se debe analizar cuál es el camino a tomar, ya que existe una gran variedad de caminos a seguir cuando un sistema se percibe como “lento”.

Se realiza el siguiente análisis de árbol de decisión: suponiendo, para simpleza de cálculos, que el sistema realiza 1 operación en 1 segundo (s), y que un usuario requiere, en un momento dado t, 1000 operaciones, entonces el siguiente análisis muestra como “impacto” los segundos que se ahorraría en la ejecución del sistema si se compara con un sistema actual “lento” que tarda 1000s por 1000 operaciones. Es decir, cada rama muestra cada decisión y los segundos que se reducirían del sistema que tarda 1000s. Para el cálculo de tiempos en opciones paralelas en CPU (Go / C++), se asumen sistemas de 8 cores o núcleos; para opciones paralelas con GPU (CUDA), se asumen sistemas de 2000 núcleos. El “EMV” en lugar de ser de valor monetario esperado, será de valor de tiempo a reducir esperado por cada opción. Es una especie de árbol de decisión con base en los segundos ahorrados respecto al sistema “actual” de 1000s.

En el diagrama de abajo, se denota la probabilidad de que una opción se requiera en la implementación del sistema, el tiempo ahorrado con dicha opción en segundos y el cálculo del “EMV” de tiempo ahorrado probable.



Así, aunque resulte atractivo utilizar GPUs o paralelismo hoy en día, la opción que reduce con mayor probabilidad la ejecución del sistema en situaciones “normales” sería la alternativa de **Arreglar complejidad en ciclos**, y buscar la opción de métodos con **complejidad  $O(n\log n)$** . Sin embargo, como se vio en el análisis de Montecarlo, existe un 3.21% de probabilidad de que la base de datos requiere almacenamiento fuera de lo estimado. Si se presenta este caso, la opción que mejoraría los tiempos de ejecución sería cambiar el lenguaje de la **totalidad** del sistema, ya que cambiar algunas partes a otros

lenguajes requiere de comunicación por internet (sockets) o tiempo de espera en ejecuciones de librerías externas.

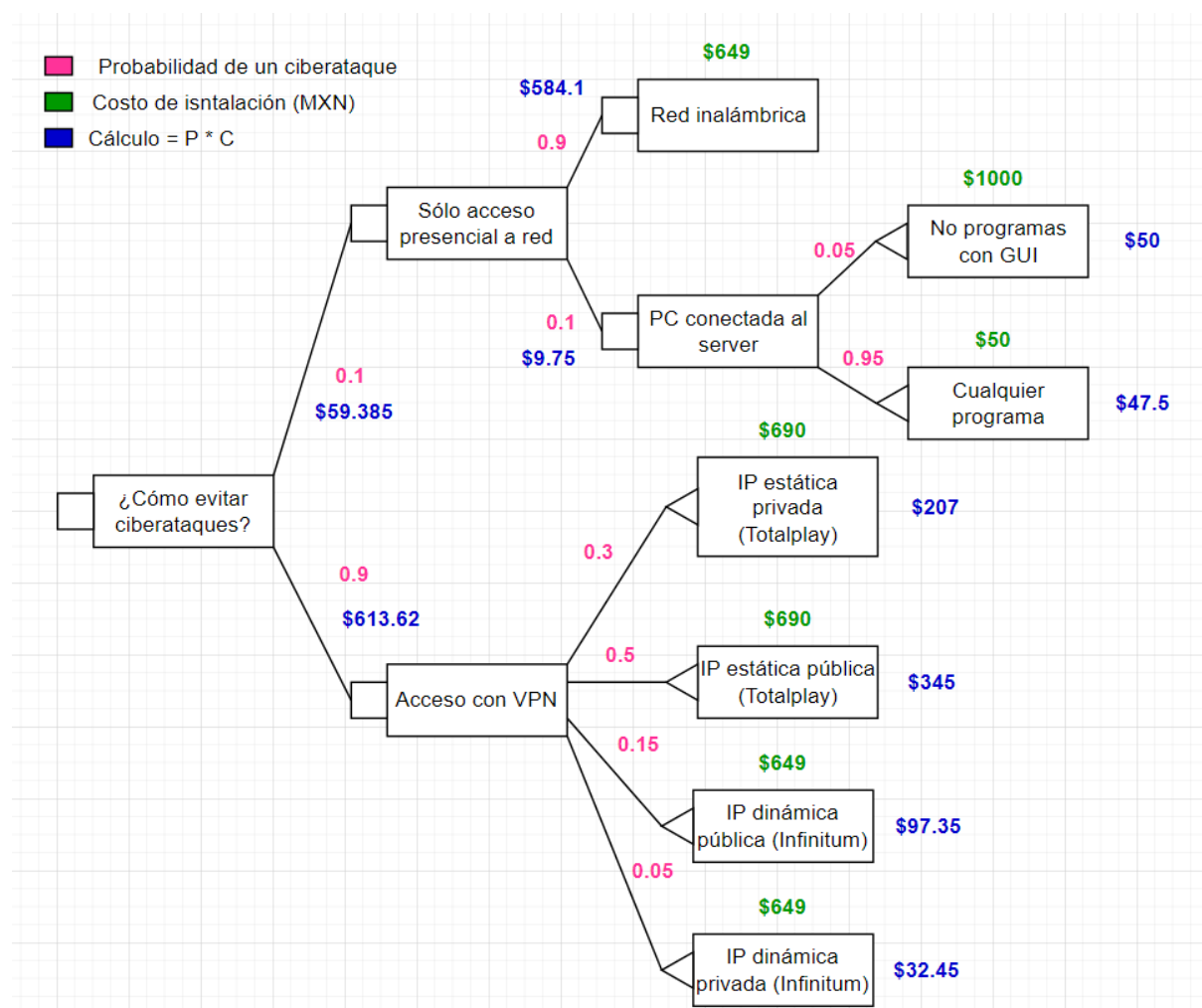
Sin embargo, se sugiere un análisis previo de tiempos para desarrollar dichas alternativas, ya que cambiar el lenguaje del sistema podría alargar la fecha de entrega, mientras que cambiar sólo unas partes resulta en la reducción del 50% de la reducción que ofrece el cambio de lenguaje en su totalidad.

Este análisis también sirve de guía no sólo en contingencia o reducción de impacto del riesgo #10, sino también para saber cuál alternativa tomar para la reducción de tiempo de ejecución **antes de desarrollar el sistema**, es decir, mitigación de probabilidad de que el riesgo #10 se presente. Con esto, sabemos de antemano que debemos buscar orientar las pruebas de calidad para mantener una complejidad del sistema no mayor a  $O(n \log n)$  para asegurar que el sistema no resulte "lento".

### 7.3. Análisis de riesgo #16 - Árbol de decisiones

El riesgo #16 se refiere a la **posibilidad de sufrir un ataque cibernético**, por lo que se realizará un árbol de decisiones para identificar el camino que se debe seguir para prevenir (reducción de probabilidad) un ataque cibernético por vulnerabilidades del sistema.

Se establece en cada rama la probabilidad o vulnerabilidad a un ciberataque dada dicha opción, y en cada nodo adicionalmente se establece el costo de dicha opción. De esta manera, al tener una opción costosa pero que reduce la probabilidad de un ataque a un porcentaje pequeño, entonces se “reduce” su costo al multiplicarse. Así, la opción a seguir será la de menor costo ponderado.



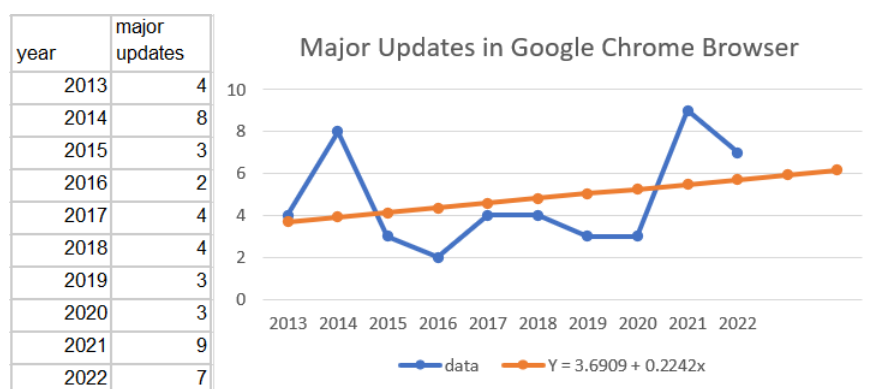
Podemos concluir que la opción que presenta menor “costo” ponderado es la de permitir acceso a la Base de datos solamente a través de acceso presencial, y únicamente a través de una PC que está conectada permanentemente al servidor, y que restringe cualquier instalación de programa que utilice una GUI (Graphical User Interface), ya que con esto obliga a realizar cualquier actividad a través de la terminal únicamente. Esta alternativa reduce el costo y la probabilidad de un ciberataque. Por lo tanto, resulta ser el camino más conveniente para evitar un ciberataque por vulnerabilidades de red, es decir, reducir la probabilidad del riesgo.

## 7.4. Fondo de Contingencia para Riesgos

Con la información obtenida en el análisis cuantitativo y cualitativo expuesto anteriormente, además de cálculos posteriores, se establece la siguiente tabla que contiene el EMV de cada riesgo identificado y el total al sumar todos los EMV's, es decir, el Presupuesto o Fondo de Contingencia para Riesgos:

EMVs				
Área en RBS	ID	Riesgo	Probabilidad	Impacto
Riesgos técnicos	#1	Actualización en buscador durante el desarrollo	1.64%	\$ 1,800.00
	#2	Complicaciones en la implementación	63%	\$ 57,487.50
	#4	Pérdida de archivos de diseño	1%	\$ 2,400.00
	#8	Pérdida de datos durante testing/desarrollo	10%	\$ 600.00
	#10	Sistema resultante demasiado lento	70%	\$ 76,650.00
	#16	Ataque cibernético	80%	\$ 175,200.00
Riesgos de gestión	#3	Exceso de solicitudes de cambio del cliente	70%	\$ 102,200.00
	#11	Almacenamiento excedido	3.21%	\$ 878.74
	#13	Despidos	10%	\$ 1,825.00
	#14	Falta de personal	10%	\$ 43,800.00
Riesgos comerciales	#5	Interrupción del presupuesto	7%	\$ 2,555.00
	#6	Aplicación similar surge antes en el mercado	65%	\$ 71,175.00
	#15	Falta de presupuesto	40%	\$ 14,600.00
Riesgos externos	#7	Nuevas leyes de privacidad	1%	\$ 300.00
	#9	Demandas por parte de miembros del equipo	9%	\$ 19,710.00
	#12	Renuncias por parte del equipo	12%	\$ 1,095.00
TOTAL				\$ 572,276.24

Los EMV de cada riesgo se calcularon con su probabilidad e impacto. La probabilidad se estimó con cálculos de regresión lineal (riesgos #1, #7), simulación montecarlo (riesgo #11) y juicio de expertos como abogados e ingenieros de software y telecomunicaciones. Se sugiere continuar estos métodos de estimación durante el proyecto para obtener datos consistentes. A manera de ejemplo, se muestra el cálculo de la regresión lineal para determinar la probabilidad del riesgo #1:



Así, se obtiene que habrá 6 actualizaciones mayores en Google Chrome, por lo que si estimamos que cada actualización es un día de trabajo y el proyecto dura un año (365 días), entonces la probabilidad de que el riesgo #1 afecte el día a día del proyecto es 1.64%.

Para el cálculo del impacto de cada riesgo se utilizó una tabla con estimaciones de horas de trabajo y personal involucrado en dado caso que se presentara cada riesgo, además del costo por hora de estos involucrados (internos o externos al proyecto).

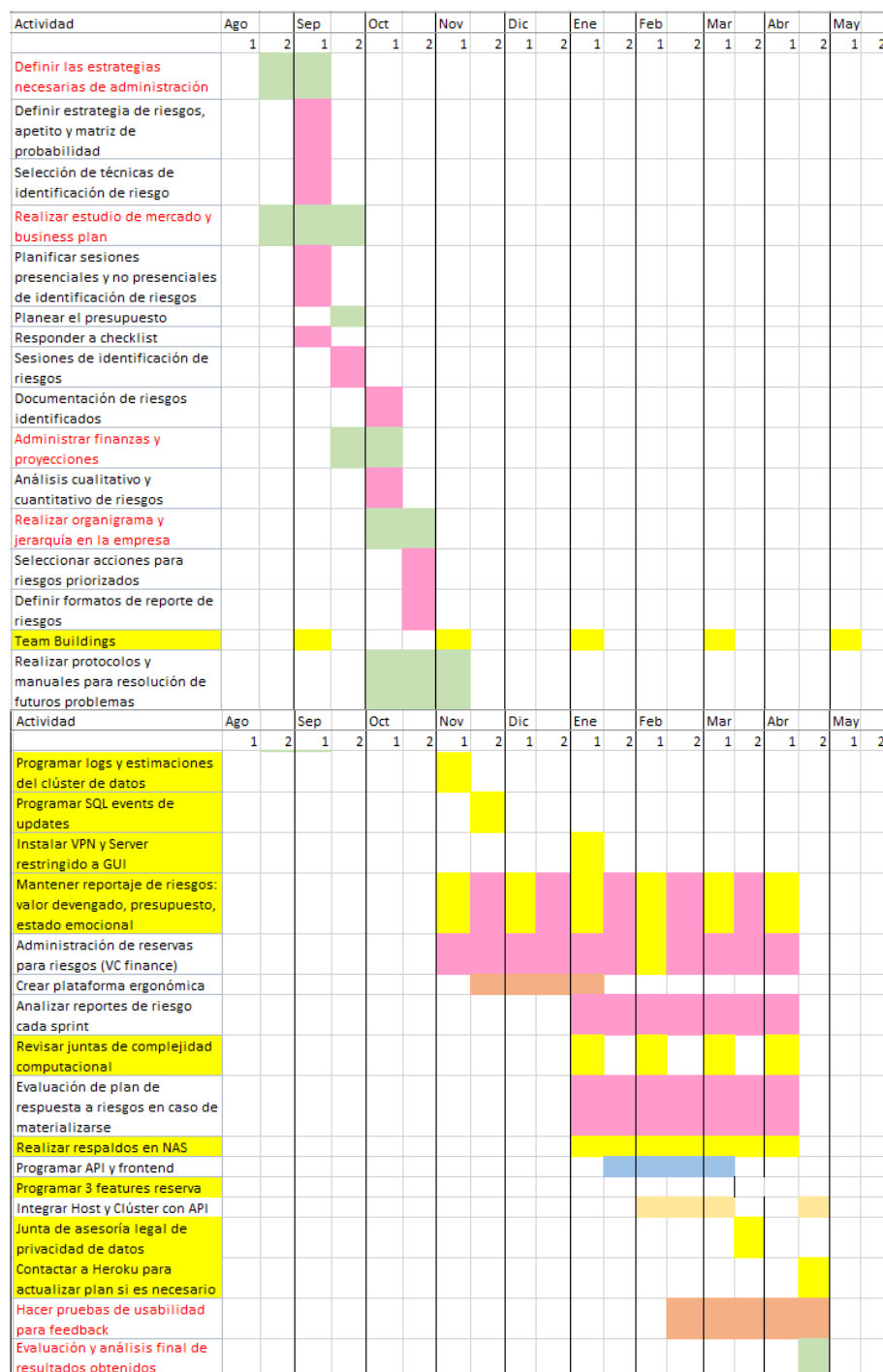
Calculo de Impacto				
Horas implicadas	Frecuencia/año	Personas	Precio/hora	Precio total
2	6	1	150 \$	1,800.00
2	229.95	1	125 \$	57,487.50
8	2	1	150 \$	2,400.00
4	1	1	150 \$	600.00
1	255.5	2	150 \$	76,650.00
2	292	1	300 \$	175,200.00
2	255.5	2	100 \$	102,200.00
0.5	11.7165	1	150 \$	878.74
0.5	36.5	1	100 \$	1,825.00
8	36.5	1	150 \$	43,800.00
1	25.55	1	100 \$	2,555.00
2	237.25	1	150 \$	71,175.00
1	146	1	100 \$	14,600.00
1	2	1	150 \$	300.00
2	32.85	1	300 \$	19,710.00
0.25	43.8	1	100 \$	1,095.00
			TOTAL	\$ 572,276.24

De esta forma, la suma de los EMV de cada riesgo forma el Presupuesto de Contingencia de Riesgos para este proyecto.



## 9. Plan de Actividades con las acciones incluidas para la gestión de riesgos

Anteriormente se presentó un cronograma con las actividades incluidas de administración de riesgos. Ahora, se presenta dicho cronograma aumentado con las actividades de la gestión de los riesgos más representativos del proyecto: riesgos #16, #11, #10, #6, #7, #15, #8 y #12. El cronograma muestra las actividades de administración de riesgos en color rosa y las de gestión de riesgos en color amarillo primario. Las demás actividades se resumieron en comparación con el anterior cronograma, para efectos de espacio y entendimiento del mismo.



## 10. Indicadores de riesgos KRI y sus límites de alerta

### 1. Número de conexiones con estado "TIME\_WAIT" por segundo

Es posible que un **ataque cibernético** explote vulnerabilidades del tamaño de buffer TCP del sistema donde un servidor está alojado. Si el atacante manda continuamente datos que exceden el tamaño máximo del buffer del socket donde el servidor está escuchando, puede causar el ataque Denial of Service (DDoS), uno de los ataques cibernéticos más comunes.

Los servidores de la aplicación utilizan el sistema operativo Linux Ubuntu 20.04 LTS, donde su tamaño de buffer para sockets de lectura es de 6291456 bytes. Por ello, si se utiliza el comando:

```
Unset  
netstat -antp | grep <server_port>
```

Donde `<server_port>` es el socket que el servidor escucha, se podrá obtener el número de conexiones a ese socket y el tamaño de estos requests. Si existe una conexión con el tamaño de buffer al límite, mostrará el estado TIME\_WAIT o algún número cercano a 6291456. Si esto ocurre de forma repetida, se corre peligro de un ataque DDoS. Así, se propone que el  $KRI_1$  sea:

$$KRI_1 = \frac{\text{conexiones con status TIME WAIT}}{\text{segundo}} + \frac{\text{conexiones con } 6291456 - \epsilon < \text{size} < 6291456}{\text{segundo}}$$

Si se observa que el  $KRI_1$  tiene valores arriba de 128 (límite en Linux de conexiones simultáneas a internet para un usuario) o  $KRI_1 > 128$ , entonces se encuentra en alerta de un posible ciberataque.

### 2. Promedio de Profundidad de Identación por Módulo (PIM) cada 1000 LoC

El propósito de este KRI es ayudar a la mitigación de la probabilidad del **riesgo #10 Sistema resultante demasiado lento**, donde se propone medir el número de indentación por módulo en el código fuente, donde indentación se conoce como la cantidad de tabulaciones de espacios dentro de un bloque de código. El cálculo de este KRI sería el siguiente

$$KRI_2 = \frac{\frac{1}{n} \sum_{i=1}^n \text{ord}(9)}{1K \text{ LoC}}$$

donde  $n$  es igual al número de módulos en cada 1000 LoC (Lines of Code) y  $\text{ord}(9)$  significa las indentaciones en dicho módulo, por su valor ascii de 9. Así, se calcula el promedio de

identación en los módulos de cada 1000 líneas de código y si  $KRI_2 > 4$ , entonces se tiene una alerta y se corre el riesgo de que el sistema utiliza demasiados recursos y puede llegar a ser más lento.

### 3. Backlog Management Index (BMI)

El propósito de este KRI es atacar el **riesgo #3 Exceso de cambios** y el **riesgo #14 Falta de personal**, por medio del cálculo del Backlog Management Index (BMI), ya que este índice nos sirve para conocer el estado del backlog y tareas por hacer en relación al total de tareas. Se propone calcular de la siguiente manera:

$$KRI_3 = BMI = \frac{\text{No. de bugs cerrados en 1 semana}}{\text{No. de bugs detectados en 1 semana}} \times 100 (\%)$$

Al ser una métrica conocida en la industria del software, se proponen los siguientes límites para su análisis:

Fitness Function	Significado	Seguimiento
BMI > 100	El backlog está siendo reducido y se llegará a cero.	No
BMI = 100	El backlog de mantenimiento siempre es constante. Cada nueva semana hay que arreglar el mismo número de problemas.	No
BMI < 100	El backlog está aumentando y el mantenimiento sólo incrementará.	Sí, zona de alerta.

La zona de alerta ( $KRI_3 < 100$ ) será una forma de saber si la cantidad de trabajo sólo va en aumento, por lo que se considera buen indicador numérico para saber si el cliente está excediendo los cambios a su producto o bien, si se necesita contratar más personal, ya que el actual no es suficiente. Se experimentará mejoría conforme el índice se acerque a 100 o menos.

### 4. Número de usuarios con uso mayor a 1.5 GB mensuales

El propósito de este KRI será atajar el riesgo #11 Almacenamiento excedido, por medio del monitoreo del número de usuarios con uso en el clúster de datos que exceden los 1.5 GB en el mes pasado. Se propone que el KRI esté definido como:

$$KRI_4 = \frac{\text{GB por usuario} > 1.5}{1 \text{ mes}}$$

Donde 1.5 representa el promedio estimado por el análisis con el método Montecarlo presentado anteriormente. De este mismo análisis se obtiene el límite de alerta: si  $KRI_4 > 3$ , el proyecto se encuentra en riesgo de que el almacenamiento se exceda en el próximo mes y se tenga que pagar una penalización, por lo que en estos casos es urgente contactar al servicio de clúster de datos (MongoDB Atlas) para que se extienda el plan actual.

#### 5. Porcentaje del Presupuesto de Contingencia utilizado cada mes

El propósito de este KRI es el monitoreo financiero de la gestión de riesgos del proyecto en general, a través del cálculo del porcentaje consumido del Fondo de Contingencia para riesgos, definido como:

$$KRI_5 = \frac{KRI_5 \text{ anterior} + \text{gasto del mes}}{\text{Total del Fondo de Contingencia}} \times 100 (\%)$$

Para la definición de la zona de alerta de este KRI se deberá calcular el porcentaje del fondo consumido de los meses anteriores para obtener la desviación estándar del mismo o  $\sigma$ , y si  $KRI_5 > \sigma$ , entonces el proyecto está en zona de alerta respecto al porcentaje de fondo o presupuesto utilizado y corre el riesgo de terminar prematuramente.

## 11. Aprendizajes del equipo respecto a la gestión de riesgos

Gracias a la clase de Gestión de Riesgos y la elaboración de este Plan de Riesgos, hemos aprendido varias cosas. Este último apartado sirve como conclusión general de todo el equipo acerca de los nuevos conocimientos adquiridos.

Lo primero que aprendimos fue la importancia de agregar las medidas que tomaremos contra los riesgos analizados en el cronograma del proyecto. Antes pensábamos que con tener las actividades por hacer bastaba, pero hace mucho sentido incluirlas en el cronograma para actuar lo antes posible y de manera concreta contra esos riesgos.

En segundo lugar, aprendimos a usar el árbol de decisiones y lo útil que es para generar un presupuesto de riesgos. Cuando nos preguntaban antes cuánto dinero apartar para los riesgos, simplemente lanzábamos un número al aire, pero con este método probabilístico es mucho más real la estimación y más convincente para aquel que haya pedido el presupuesto.

Por último, fue revelador conocer todas las herramientas que existen para analizar, agrupar y gestionar los riesgos. En vez de dar soluciones genéricas a cada posible amenaza u oportunidad, ahora sabemos cómo separarlos en categorías, darles su debida importancia y peso, cuáles son los que debemos atacar con mayor urgencia, etc. Esto nos ayudó mucho a conocer mejor nuestras debilidades en el proyecto y tomar medidas al respecto.

En general, fue muy fructífero para la rentabilidad de nuestro proyecto el hacer un plan de riesgos serio, y nos ayudó a ampliar nuestros horizontes hacia lo que podría pasar, no solo el presente. Ahora estamos mejor parados en nuestra planeación.

## Referencias