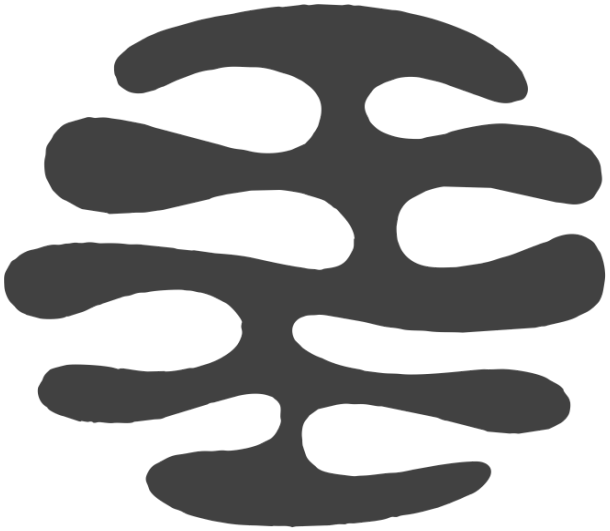

CARONTE

Análisis de riesgos

Devising a Project

Grupo 9

Borrego Angulo, Hugo

Chico Castellano, Álvaro

Duque Colete, Rafael

Galván Cancio, Daniel

García Carballo, Juan

García Escudero, Ángel

García Rivero, Andrés Francisco

Guillén Fernández, David

Herencia Solís, Lucas Manuel

Linares Barrera, Jaime

Muñoz Rodríguez, Jorge

Pérez Santiago, Alejandro

Rodríguez Reina, Javier

Solís Padilla, Isaac

Youssafi Benichikh, Karim

Índice

1. Introducción

Este documento presenta un Análisis de Riesgos detallado basado en el Registro de Riesgos previamente elaborado. En él, cada riesgo identificado se describe con un mayor nivel de detalle especificando su impacto potencial en el proyecto.

Además, se desarrollan planes de contingencia detallados, estableciendo estrategias concretas para mitigar, evitar, transferir o aceptar cada riesgo. Estas respuestas buscan minimizar el impacto negativo en el desarrollo del proyecto y fortalecer la confianza de los usuarios y partes interesadas.

La información contenida en este documento será revisada de forma continua por el equipo de proyecto para mantenerla actualizada a lo largo del desarrollo.

2. Identificación de riesgos

2.1 Internos

Brecha de seguridad (filtración de datos) [R1]. Al manejar datos sensibles de personas fallecidas y sus familiares, existe un alto riesgo de filtraciones o accesos no autorizados.

Opciones de personalización limitadas [R2]. La falta de opciones más flexibles para la creación de esquelas puede generar insatisfacción en los usuarios.

Fallo en las estimaciones por parte del equipo de desarrollo [R3]. Al tratarse de un nicho nuevo para la mayoría del equipo, es posible que las estimaciones no sean del todo precisas debido al desconocimiento del tema.

Falta de conocimientos tecnologías seleccionadas por parte del equipo de desarrollo [R4]. No todos los integrantes del equipo poseen el mismo nivel de conocimiento en las tecnologías utilizadas. Esto puede provocar que se asignen tareas a miembros que no dominan determinadas herramientas, afectando la eficiencia del desarrollo.

Fallo en la recopilación de requisitos [R5]. Dado que el nicho es desconocido para la mayoría del equipo, existe el riesgo de orientar el desarrollo del producto en una dirección que no satisfaga al cliente, lo que podría generar modificaciones posteriores en los requisitos o en la funcionalidad base de la aplicación.

Descenso de la productividad del equipo de desarrollo por causas externas [R6]. Pueden surgir situaciones fuera de nuestro control que afecten la productividad del equipo, como enfermedades, problemas familiares o la deserción de miembros del proyecto.

Deadlines agresivos [R7]. Existe el riesgo de que la funcionalidad de la aplicación no esté completamente desarrollada para la fecha de entrega debido a retrasos y problemas durante el proceso de desarrollo.

Aparición de errores en la etapa de testeo [R8]. Es posible que el proceso de testing no reciba la suficiente atención durante el desarrollo, lo que podría derivar en la aparición de errores graves en etapas avanzadas, comprometiendo la calidad del producto.

Falta de comunicación dentro del equipo de desarrollo [R9]. El gran número de personas involucradas en el proyecto podría generar deficiencias en la comunicación, formando microgrupos y provocando malentendidos. Esto podría dar lugar a visiones divergentes sobre el estado y el avance del proyecto.

Documentación insuficiente o deficiente [R10]. Existe el riesgo de que la documentación generada a lo largo del desarrollo no sea suficiente o no tenga la calidad necesaria para cumplir con sus objetivos, lo que podría ocasionar problemas y confusión.

Documentación de código insuficiente o deficiente [R11]. Dado que el código es desarrollado por múltiples personas con distintos estilos y hábitos de programación, es posible que resulte difícil de entender o modificar sin una documentación adecuada, lo que podría generar retrasos y complicaciones en el mantenimiento del proyecto.

2.2 Externos

Sensibilidad del mercado [R12]. Algunas personas pueden rechazar la digitalización del proceso por considerarlo impersonal o frío.

Dependencia de proveedores externos [R13]. La calidad y disponibilidad de ciertos productos dependen de proveedores externos, lo que puede afectar la experiencia del cliente.

Interrupción de servicios de API [R14]. Si los servicios de terceros sufren interrupciones o cambios en sus políticas, la plataforma podría verse afectada en funcionalidad o costos.

Competencia de servicios tradicionales [R15]. La preferencia por métodos tradicionales y la falta de familiaridad con soluciones digitales pueden dificultar la adopción del servicio y frenar su crecimiento.

3. Análisis de riesgos

A continuación, se presenta la tabla de impacto de los riesgos, en la que se analiza el efecto que cada riesgo identificado podría tener en el proyecto, resaltando los posibles aspectos negativos y sus implicaciones.

Riesgo	Impacto financiero/recursos
R1	Pérdida de confianza, posibles sanciones legales, costos de mitigación y reforzamiento de seguridad.
R2	Posible insatisfacción del usuario, menor retención y reducción de adopción del servicio.
R3	Sobrecarga de trabajo, necesidad de reasignar recursos y posibles retrasos en hitos clave.
R4	Retrasos en el desarrollo, necesidad de formación adicional y posibles errores técnicos.
R5	Costos adicionales por cambios en requisitos, retrabajo y posibles retrasos en entregas.
R6	Reducción del ritmo de desarrollo, impacto en las entregas y necesidad de redistribuir tareas.
R7	Posible incumplimiento de plazos, necesidad de overtime y riesgo de disminución en la calidad del producto.
R8	Mayor carga de trabajo para corrección, retrasos en entrega y posible insatisfacción del usuario.
R9	Descoordinación del equipo, malentendidos, errores en implementación y posible re-trabajo.
R10	Dificultad para escalar el producto, mayor tiempo en la incorporación de nuevos miembros y problemas en el mantenimiento.
R11	Mayor dificultad en mantenimiento y evolución del código, retrasos en nuevas implementaciones.
R12	Riesgo de rechazo del mercado, necesidad de estrategias de marketing y educación del usuario.
R13	Aumento de costos si se requiere un proveedor alternativo, posible afectación en la calidad del servicio.
R14	Costos adicionales en desarrollo, pérdida de funcionalidad y riesgo de

	interrupción del servicio.
R15	Dificultad para captar clientes, necesidad de invertir en diferenciación y marketing para posicionamiento.

4. Planes de contingencia

Riesgo 1

1. Contención inmediata:
    a. Aislar los sistemas o bases de datos afectados para detener la filtración.
    b. Revocar o suspender temporalmente los accesos comprometidos o sospechosos.
    c. Desconectar servicios críticos para evitar más accesos no autorizados.
2. Identificación del incidente:
    a. Analizar los registros de acceso (logs) para identificar el origen y el alcance de la filtración.
    b. Determinar si la brecha fue resultado de un ataque externo, fallo interno o vulnerabilidad técnica.
3. Mitigación de la vulnerabilidad:
    a. Implementar medidas correctivas de inmediato (reconfiguración de permisos, parches de seguridad, reforzamiento del cifrado de datos).
    b. Modificar contraseñas comprometidas y reforzar los mecanismos de autenticación (por ejemplo, implementando autenticación multifactor).
4. Si es requerido por normativas legales (como GDPR o leyes de privacidad locales), notificar a los usuarios afectados explicando el tipo de datos comprometidos y las medidas que se están tomando para proteger su información.
5. Evaluación del impacto:
    a. Determinar la cantidad de datos expuestos, el tipo de información comprometida y los posibles daños (legales, reputacionales, operativos).
    b. Elaborar un informe detallado del incidente y sus consecuencias.
6. Restauración de servicios:
    a. Asegurarse de que todos los sistemas afectados sean revisados y reforzados antes de su restauración.
7. Documentar las lecciones aprendidas y establecer procesos preventivos más robustos para futuros riesgos.

Riesgo 2

1. Expandir las opciones de personalización con más plantillas y elementos editables.
2. Recoger feedback de los clientes para adaptar las funcionalidades a sus necesidades.

Riesgo 3

1. Analizar qué tareas se vieron afectadas por la estimación incorrecta y determinar el nivel de retraso o recursos excedentes.
2. Repriorizar el backlog de tareas, enfocándose en los entregables más importantes o críticos para cumplir con los plazos.
3. Asignación de recursos:
    a. **En caso de sobreestimación:** Redirigir los recursos disponibles a tareas pendientes o no planificadas.
    b. **En caso de infraestimación:** Reasignar recursos adicionales a las tareas afectadas. Si no es posible, reducir el alcance del sprint o de la fase en curso.
4. Si el impacto es significativo, evaluar y negociar cambios en los plazos del proyecto o la entrega de versiones parciales priorizando funcionalidades esenciales.
5. Analizar las causas del fallo en la estimación (falta de información, complejidad no anticipada, etc.) y registrar el aprendizaje. Actualizar el proceso de estimación para mejorar en futuras iteraciones.

Riesgo 4

1. Reasignar las tareas críticas a los miembros más experimentados para evitar retrasos significativos.
2. Asignar a expertos internos para asistir de forma temporal a los desarrolladores menos experimentados en las tecnologías clave.
3. Realizar sesiones de formación para abordar las tecnologías o áreas que han generado los problemas.
4. Dividir tareas complejas en subtareas que puedan ser asumidas por desarrolladores con diferentes niveles de experiencia, de manera que el proyecto continúe avanzando.
5. Analizar cómo ha afectado la falta de conocimientos al cronograma y a los entregables del proyecto. Ajustar los plazos o el alcance según sea necesario.

6. Identificar las causas del problema y registrar medidas correctivas para evitar situaciones similares en el futuro, como mejorar el proceso de selección de tecnologías o asegurar formaciones previas.

Riesgo 5

1. Realizar una reunión con los stakeholders para identificar los requisitos que no se han cumplido o que están mal definidos. Recopilar información detallada sobre las correcciones necesarias.
2. Evaluar el impacto de los cambios en el desarrollo actual, identificando tareas que deben ser modificadas, reestructuradas o añadidas.
3. Repriorizar el backlog, asegurando que las funcionalidades críticas sean implementadas primero. Redefinir los requisitos de acuerdo con la información actualizada de los stakeholders.
4. Dividir los nuevos requisitos en entregables manejables y realizar iteraciones rápidas (sprints) para implementar los cambios de forma controlada. Validar los avances de manera constante con los stakeholders.
5. Reasignar recursos para acelerar la corrección de los requisitos. Si no es posible, renegociar el alcance o los plazos del proyecto para minimizar el impacto en la fecha de entrega.
6. Modificar la documentación del proyecto para reflejar los cambios en los requisitos. Asegurar que todos los miembros del equipo tengan acceso a la información actualizada.
7. Una vez implementados los cambios, realizar una retrospectiva para identificar por qué ocurrió el fallo en la recopilación de requisitos. Ajustar los procesos de definición y validación de requisitos para futuras fases del proyecto.

Riesgo 6

1. Evaluar cómo las situaciones externas están afectando la productividad. Determinar las tareas y entregables críticos que corren riesgo de retraso o incumplimiento.
2. Reasignar temporalmente las tareas a otros miembros disponibles del equipo. Enfocar los recursos en las áreas más críticas para mantener el avance en los entregables prioritarios.
3. Ajustar el backlog y el cronograma para centrarse en las funcionalidades esenciales. Posponer tareas de menor prioridad si es necesario.
4. Ofrecer opciones de trabajo flexible, como horarios ajustados o teletrabajo, para ayudar a los miembros del equipo afectados por problemas personales a seguir contribuyendo en la medida de sus posibilidades.

5. Mantener una vigilancia continua sobre la situación del equipo. Reunirse regularmente para evaluar el estado del proyecto y detectar posibles caídas adicionales en la productividad.
6. Una vez que la productividad se haya restablecido, realizar una retrospectiva para analizar las causas, la efectividad de las acciones tomadas y mejorar los planes de contingencia para futuros eventos similares.

Riesgo 7

1. Analizar el progreso actual del desarrollo, identificando las funcionalidades que ya están completas, las que presentan retrasos y aquellas que corren riesgo de no ser terminadas a tiempo.
2. Identificar las funcionalidades esenciales para el proyecto y priorizarlas. Posponer o eliminar aquellas que no sean críticas o que puedan ser implementadas en futuras versiones o fases.
3. Reasignar tareas a los desarrolladores más experimentados o disponibles para acelerar el desarrollo de las funcionalidades prioritarias.
4. Una vez cumplida la entrega, realizar una retrospectiva para analizar las causas de los retrasos, identificar mejoras en la gestión de plazos y ajustar el proceso de planificación para futuros proyectos.

Riesgo 8

1. Detectar los errores graves que han surgido durante la etapa de testeo y clasificarlos según su criticidad (bloqueantes, mayores o menores). Determinar qué funcionalidades están afectadas.
2. Priorizar la resolución de los errores críticos que afectan el funcionamiento del producto. Definir un plan claro para corregirlos, estableciendo plazos específicos para cada categoría de error.
3. Reasignar recursos del equipo de desarrollo para enfocarse en la resolución de los errores más importantes.
4. Analizar cómo se generaron los errores para identificar posibles fallos en los procesos de desarrollo y testing, como falta de pruebas unitarias, integración continua o pruebas automatizadas.
5. Realizar una ronda de pruebas exhaustivas (regresión, integración y aceptación) para garantizar que las correcciones no generen nuevos errores.
6. Documentar los errores detectados, su impacto y las soluciones aplicadas. Realizar una retrospectiva para ajustar el proceso de testing y prevenir fallos similares en futuros proyectos.

Riesgo 9

1. Detectar los puntos críticos donde se han producido malentendidos o falta de información. Identificar los microgrupos o personas que no están alineados con los objetivos y el avance del proyecto.
2. Convocar una reunión de todo el equipo para aclarar el estado actual del proyecto, los objetivos, los entregables y los roles de cada miembro. Establecer un plan para mejorar la coordinación.
3. Definición de reuniones periódicas:
    a. **Reuniones semanales:** Sesiones para revisar el estado general del proyecto, identificar riesgos, resolver dudas pendientes y coordinar las próximas tareas.
    b. **Revisiones de sprint:** Reuniones al final de cada sprint para evaluar el avance y definir los siguientes pasos.
    c. **Retrospectivas:** Sesiones periódicas para identificar mejoras en la colaboración y comunicación del equipo.
4. Asegurar que cada miembro del equipo tenga roles y responsabilidades bien definidos. Esto evita que surjan malentendidos sobre quién debe realizar ciertas tareas o tomar decisiones.
5. Asegurar que la información importante del proyecto (requisitos, decisiones, estado del proyecto) esté debidamente documentada y accesible para todos los miembros.
6. Una vez implementadas las medidas correctivas, realizar una retrospectiva para analizar los problemas de comunicación iniciales. Identificar áreas donde el proceso de comunicación pueda seguir mejorando y ajustar las prácticas del equipo en consecuencia.

Riesgo 10

1. Identificar las áreas del proyecto donde la documentación es insuficiente o confusa. Determinar los aspectos críticos que requieren una documentación urgente, como funcionalidades, procesos, API o integraciones clave.
2. Priorizar la creación o mejora de la documentación en las áreas más afectadas.
3. Asignar responsables para trabajar en la documentación priorizada, asegurando que cumpla con estándares mínimos de claridad, estructura y contenido necesario.
4. Una vez que se haya completado la mejora de la documentación, realizar una retrospectiva para analizar las causas del problema. Identificar oportunidades de mejora en los procesos de documentación y ajustar las prácticas para prevenir futuras deficiencias.

Riesgo 11

1. Identificar los módulos, componentes o partes del código que carecen de documentación o tienen una documentación confusa. Determinar cuáles son críticos para el mantenimiento y desarrollo continuo del proyecto.
2. Asignar a desarrolladores familiarizados con el código afectado para que redacten o actualicen la documentación necesaria.
3. Definir qué partes del código requieren documentación inmediata, como funciones complejas, clases críticas, servicios o APIs utilizados frecuentemente.
4. Generar documentación clara.
5. Una vez que se haya corregido la documentación deficiente, realizar una retrospectiva para analizar los motivos del problema. Ajustar procesos internos para prevenir futuros problemas relacionados con la documentación del código.

Riesgo 12

1. Mejorar la experiencia digital incorporando más elementos visuales amigables y mensajes cálidos que hagan la interacción con la plataforma más cercana y humanizada.
2. Comunicar los beneficios del servicio digital, destacando cómo puede facilitar y personalizar el proceso sin perder el toque humano.
3. Analizar el incidente para identificar lecciones aprendidas y reforzar la estrategia de comunicación y soporte en el futuro.

Riesgo 13

1. Determinar qué productos o servicios están afectados por el fallo del proveedor, identificando los clientes y entregables impactados.
2. Recurrir a proveedores de respaldo previamente identificados o buscar de forma urgente nuevos proveedores que puedan cubrir la necesidad temporalmente. Evaluar los costos asociados a esta solución alternativa para tomar decisiones informadas sobre la viabilidad económica.
3. Redirigir los recursos internos disponibles para producir o gestionar temporalmente los productos afectados, si es posible.
4. Informar de manera inmediata y transparente a los clientes sobre la situación, los productos afectados, las soluciones implementadas y cualquier posible cambio en precios o condiciones del servicio, en caso de que los costos adicionales impacten en la operación.

5. Documentar el incidente, identificar las causas y proponer mejoras en la gestión de proveedores para evitar futuras interrupciones.

Riesgo 14

1. Evaluar qué funcionalidades de la plataforma están afectadas por la interrupción o cambio en la API. Determinar la magnitud del impacto en los usuarios y en los procesos internos.
2. Activación de soluciones temporales:
    a. Implementar una versión limitada de las funcionalidades afectadas, desactivando temporalmente aquellas que dependan exclusivamente de la API.
    b. Enviar datos estáticos o de caché, si es posible, para mantener parte del servicio operativo.
    c. Adaptar los servicios afectados para continuar operando con cambios mínimos, siempre que sea posible, hasta que la API sea restablecida o se implementen alternativas.
3. Comunicarse de inmediato con el proveedor para obtener detalles sobre la causa de la interrupción o el cambio en sus políticas, así como el tiempo estimado de resolución.
4. Informar a los usuarios afectados sobre la situación, los servicios limitados y los pasos que se están tomando para restablecer la funcionalidad.
5. Si el cambio en la política del proveedor afecta los costos, evaluar rápidamente la posibilidad de reducir el uso de la API para minimizar el impacto financiero mientras se resuelve el problema.
6. Una vez que la API esté disponible nuevamente o los cambios sean aplicados, restaurar las funcionalidades completas y monitorear el rendimiento para asegurar la estabilidad.
7. Analizar el incidente, documentando las causas, los tiempos de respuesta y las soluciones implementadas. Establecer aprendizajes para mejorar la respuesta ante futuras interrupciones de servicios externos.

Riesgo 15

1. Evaluar el nivel de preferencia de los usuarios por los servicios tradicionales y cómo afecta la adopción de la plataforma digital. Identificar las principales barreras que impiden la transición a la solución digital, como la confianza, la falta de conocimiento o el valor percibido del servicio.
2. Diferenciación y mejora de la propuesta de valor:

    a. Destacar las ventajas del servicio digital frente a los métodos tradicionales, como comodidad, accesibilidad, rapidez y opciones de personalización.
    b. Implementar nuevas funcionalidades que refuercen el atractivo de la plataforma y generen un mayor valor agregado para el usuario.
    c. Explorar alianzas con funerarias y empresas del sector para integrarlas en el ecosistema digital y aumentar la legitimidad del servicio.
3. Estrategia de comunicación y marketing:
    a. Diseñar campañas informativas enfocadas en educar a los usuarios sobre los beneficios del servicio digital.
    b. Utilizar testimonios y casos de éxito para generar confianza y demostrar el impacto positivo de la digitalización.
    c. Ofrecer promociones o pruebas gratuitas para incentivar a los usuarios a probar la plataforma sin riesgo.
4. Monitoreo y adaptación del servicio:
    a. Analizar constantemente la reacción del mercado y la evolución de la competencia.
    b. Recoger feedback de los usuarios y ajustar la estrategia en función de sus necesidades y preocupaciones.
    c. Revisar y optimizar la plataforma para mantenerse competitivos y adaptarse a nuevas demandas.
5. Evaluación posterior:
    a. Analizar el impacto de las acciones implementadas y su efectividad en la adopción del servicio.
    b. Documentar aprendizajes clave y ajustar las estrategias para mejorar la competitividad a largo plazo.

5. Registro de riesgos

La gestión de riesgos es un pilar fundamental en la administración de proyectos según la guía PMBOK. Su propósito es identificar, evaluar y mitigar los riesgos que puedan comprometer el éxito del proyecto, garantizando un desarrollo más controlado y eficiente.

Para ello, los riesgos se han clasificado en dos grandes categorías: internos y externos. Posteriormente, han sido analizados y priorizados en función de su impacto y probabilidad, asignándoles un factor de riesgo que determina su nivel de criticidad. Finalmente, se han diseñado planes de contingencia específicos para cada riesgo, asegurando una respuesta rápida y efectiva ante cualquier eventualidad.

Este registro será revisado de forma continua por el equipo de proyecto para mantenerlo actualizado a lo largo del desarrollo.

5.1 Tabla de registro de riesgos

ID DEL RIESGO	CATEGORÍA	RIESGO	IMPACTO	PROBABILIDAD	FACTOR	PRIORIDAD	INTERESADOS	RESPONSABLES		PLAN DE CONTINGENCIA (RESPUESTA)
								SEGUIMIENTO	RESPUESTA	
R1	Riesgo Interno	Brecha de seguridad (filtración de datos)	10	6	60	***1***	Equipo de proyecto, Usuarios.	Equipo de proyecto.	Equipo de proyecto.	Detener la filtración, reforzar la seguridad y restaurar sistemas.
R2	Riesgo Interno	Opciones de personalización limitadas	4	7	28	***7***	Equipo de proyecto, Usuarios.	Equipo de proyecto.	Equipo de proyecto.	Mejorar opciones de personalización según el feedback.
R3	Riesgo Interno	Fallo en las estimaciones por parte del equipo de desarrollo	8	6	48	***2***	Equipo de proyecto.	Equipo de proyecto.	Equipo de proyecto.	Ajustar prioridades y reasignar recursos para evitar retrasos.

R4	Riesgo Interno	Falta de conocimientos tecnologías seleccionadas por parte del equipo de desarrollo	7	7	49	***2***	Equipo de proyecto.	Equipo de proyecto.	Equipo de proyecto.	Apoyar a los menos experimentados y reorganizar tareas.
R5	Riesgo Interno	Fallo en la recopilación de requisitos	10	4	40	***4***	Equipo de proyecto, Cliente.	Equipo de proyecto.	Equipo de proyecto.	Revisar requisitos, hacer ajustes y renegociar plazos o alcance si es necesario.
R6	Riesgo Interno	Descenso de la productividad del equipo de desarrollo por causas externas	6	6	36	***5***	Equipo de proyecto.	Equipo de proyecto.	Equipo de proyecto.	Redistribuir trabajo y ofrecer flexibilidad para mantener el ritmo.
R7	Riesgo Interno	Deadlines agresivos	8	4	24	***7***	Equipo de proyecto, Cliente.	Equipo de proyecto.	Equipo de proyecto.	Priorizar lo esencial y reasignar tareas para cumplir plazos.

R8	Riesgo Interno	Aparición de errores en la etapa de testeo	9	5	45	***3***	Equipo de proyecto.	Equipo de proyecto.	Equipo de proyecto.	Corregir errores críticos y reforzar pruebas antes de lanzar.
R9	Riesgo Interno	Falta de comunicación dentro del equipo de desarrollo	8	6	48	***2***	Equipo de proyecto.	Equipo de proyecto.	Equipo de proyecto.	Mejorar comunicación y reuniones para alinear al equipo.
R10	Riesgo Interno	Documentación insuficiente o deficiente	7	5	35	***5***	Equipo de proyecto.	Equipo de proyecto.	Equipo de proyecto.	Documentar lo esencial y estandarizar la información.
R11	Riesgo Interno	Documentación de código insuficiente o deficiente	7	6	42	***3***	Equipo de proyecto.	Equipo de proyecto.	Equipo de proyecto.	Completar documentación técnica para facilitar mantenimiento.
R12	Riesgo Externo	Sensibilidad del mercado	8	5	40	***4***	Equipo de proyecto.	Equipo de proyecto.	Equipo de proyecto.	Hacer la experiencia más humana y cercana al usuario.

R13	Riesgo Externo	Dependencia de proveedores externos	10	3	30	***6***	Equipo de proyecto, Usuarios.	Equipo de proyecto.	Equipo de proyecto.	Buscar proveedores alternativos y minimizar impacto en clientes.
R14	Riesgo Externo	Interrupción de servicios de API	10	3	30	***6***	Equipo de proyecto.	Equipo de proyecto.	Equipo de proyecto.	Aplicar soluciones temporales mientras se restablece el servicio.
R15	Riesgo Externo	Competencia de servicios tradicionales	9	7	63	***1***	Equipo de proyecto.	Equipo de proyecto.	Equipo de proyecto.	Diferenciar el servicio con beneficios claros y estrategias de marketing efectivas.

6. Plan de gestión de la calidad

6.1 Normas y procedimientos aplicables

La gestión de riesgos en el proyecto Caronte se llevará a cabo bajo las directrices del PMBOK, asegurando un enfoque estructurado y eficiente. Además, se implementarán los procedimientos internos de Caronte, incluyendo la creación y actualización regular de un Registro de Riesgos, en el que se documentará cada riesgo identificado junto con su probabilidad, impacto y estrategias de respuesta.

La identificación de riesgos se realizará en la fase de planificación a través de:

- Reuniones internas con el equipo de desarrollo.
- Análisis de proyectos similares y experiencias previas.
- Evaluación de riesgos específicos del sector funerario, como la aceptación del mercado y la dependencia de proveedores externos.

Los riesgos serán clasificados en internos y externos, abordando aspectos como seguridad de datos, disponibilidad de servicios de API, fallos en estimaciones de desarrollo y resistencia del mercado a la digitalización. Su priorización se realizará mediante una Matriz de Probabilidad e Impacto, permitiendo un enfoque efectivo en la mitigación de aquellos riesgos con mayor criticidad.

En caso de materialización de un riesgo, se ejecutarán los Planes de Contingencia previamente definidos, minimizando su impacto en el alcance, tiempo, costos y calidad del proyecto. Además, cualquier cambio significativo en la gestión de riesgos, así como las medidas correctivas o preventivas, serán documentados y comunicados a los interesados, garantizando transparencia y eficiencia en la gestión del proyecto.

6.2 Categorías de riesgos

En el proyecto Caronte, los riesgos se clasificarán en dos categorías principales: internos y externos. Esta clasificación permite un enfoque más eficiente en su identificación, análisis y mitigación, asegurando la continuidad y éxito del proyecto.

- **Riesgos Internos.** Estos riesgos surgen dentro del equipo de desarrollo y la gestión del proyecto. Pueden estar relacionados con la planificación, ejecución y mantenimiento de la plataforma, así como con la coordinación del equipo.
- **Riesgos Externos.** Estos riesgos provienen de factores ajenos al equipo de desarrollo, pero que pueden impactar significativamente el proyecto.

6.3 Metodología para la recogida de riesgos

La identificación de riesgos en el proyecto Caronte se llevará a cabo de manera continua y estructurada a lo largo de todo el ciclo de vida del proyecto. El objetivo de esta metodología es detectar proactivamente los riesgos potenciales, documentarlos y priorizarlos para su posterior análisis y tratamiento.

Las principales técnicas utilizadas para la identificación de riesgos son las siguientes:

- **Brainstorming con el equipo.** Se realizaron sesiones de lluvia de ideas con el equipo de desarrollo para listar posibles riesgos basados en experiencias previas y conocimientos técnicos. Esta técnica permite obtener una visión global de los desafíos que podrían afectar el proyecto, asegurando que se consideren tanto riesgos internos como externos.
- **Análisis de proyectos similares.** Se investigaron casos de proyectos con características y situaciones similares para identificar riesgos recurrentes.
- **Lecciones aprendidas de experiencias anteriores.** Se revisaron fallos comunes en proyectos previos realizados por los miembros del equipo para evitar repetir errores pasados.
- **Registro de riesgos continuo.** El Registro de Riesgos será actualizado de manera periódica a medida que se identifiquen nuevos riesgos o cambien las condiciones del proyecto. Esto garantizará que los riesgos se documenten inmediatamente y se clasifiquen según su impacto y probabilidad, permitiendo una gestión dinámica y eficiente.

Al aplicar estas técnicas, el proyecto Caronte asegura que la identificación de riesgos no será un proceso aislado de la fase de planificación, sino que se mantendrá activo en todas las etapas del proyecto. Esto permitirá que el equipo de desarrollo tome decisiones informadas y reaccione de manera rápida y eficaz ante la aparición de nuevos riesgos.

6.4 Metodología para análisis y priorización de riesgos

El análisis de riesgos en el proyecto Caronte se llevará a cabo de manera estructurada, evaluando cada riesgo identificado en función de su probabilidad de ocurrencia y su impacto potencial en el proyecto. Este análisis permitirá priorizar los riesgos y definir estrategias de respuesta adecuadas.

El análisis se realizará mediante la siguiente metodología:

1. **Análisis Cualitativo de Riesgos.** Este análisis tiene como objetivo evaluar subjetivamente los riesgos en función de su probabilidad de ocurrencia y su impacto en el proyecto. Esto permitirá clasificar los riesgos y determinar cuáles requieren una atención inmediata. Los pasos del análisis cualitativo son los siguientes:
    - **Evaluación de Probabilidad e Impacto.** Cada riesgo será evaluado en función de su probabilidad de ocurrencia y el impacto que podría tener en aspectos clave del proyecto como seguridad, desarrollo, plazos, costos y satisfacción del usuario. La evaluación se basará en la experiencia del equipo y en el análisis de proyectos similares.
    - **Uso de la Matriz de Probabilidad e Impacto.** Para clasificar los riesgos, se empleará una escala de 1 a 10 tanto para la probabilidad como para el impacto, multiplicando ambos valores para obtener un factor de riesgo. Según este factor, los riesgos se agruparán en tres categorías:
        - **Baja prioridad (1-9):** Impacto menor, no afecta objetivos críticos.
        - **Media prioridad (10-36):** Puede causar retrasos o costos adicionales.
        - **Alta prioridad (37-100):** Impacto crítico, compromete el éxito del proyecto.
    - **Priorización de Riesgos:** Los riesgos serán ordenados según su criticidad. Aquellos con alta probabilidad y alto impacto serán tratados con urgencia, mientras que los de menor impacto serán monitoreados y gestionados de forma pasiva.
2. **Análisis Cuantitativo de Riesgos:** Para los riesgos que requieran un análisis más detallado, se aplicará una evaluación cuantitativa. Este análisis busca cuantificar el impacto financiero, operativo y temporal que cada riesgo podría tener en el proyecto.
    - **Cálculo del Valor del Riesgo:** Para cada rieso identificado, se calculará un valor de exposición utilizando la fórmula:
        - **Valor del Riesgo = Probabilidad x Impacto**

    Este cálculo permitirá determinar la necesidad de establecer reservas de contingencia para mitigar el impacto en caso de materialización del riesgo.

3. **Revisión y Validación:** El análisis cualitativo y cuantitativo será revisado periódicamente con el equipo del proyecto y los interesados clave. Se actualizarán los riesgos según la evolución del proyecto y se definirán acciones correctivas o preventivas según sea necesario para minimizar su impacto.

6.5 Reservas de contingencia

En el proyecto Caronte, se establecerán reservas de contingencia para afrontar los impactos de los riesgos que puedan materializarse durante el desarrollo del proyecto, garantizando la disponibilidad de recursos suficientes para gestionar desviaciones sin comprometer los objetivos estratégicos.

1. **Determinación de las Reservas:** Las reservas de contingencia se definirán en función del análisis cuantitativo de los riesgos más críticos, considerando tanto los costos como el tiempo necesario para mitigarlos. La cantidad asignada dependerá de la evaluación del factor de riesgo (probabilidad x impacto), asegurando que haya margen suficiente para absorber posibles desviaciones en el presupuesto o en los plazos de entrega.
2. **Distribución de las Reservas:** Las reservas se asignarán a las áreas del proyecto con mayor exposición a riesgos, priorizando los riesgos técnicos, de seguridad y operativos. Estos fondos estarán específicamente destinados a cubrir imprevistos relacionados con los riesgos más importantes del proyecto. El uso de las reservas de contingencia deberá ser aprobado por el equipo de dirección del proyecto. Su uso se activará únicamente cuando un riesgo identificado se materialice, y cada uso será registrado y justificado en los informes de seguimiento.
3. **Revisión y Ajuste:** Las reservas serán revisadas de forma periódica, ajustándose según la evolución del proyecto. Si la probabilidad o el impacto de ciertos riesgos cambian, se redefinirán los valores de reserva para mantener una gestión eficiente y adaptada a las condiciones actuales del desarrollo.

6.6 Protocolo para contingencias

Para garantizar una respuesta rápida y efectiva ante la materialización de un riesgo en el proyecto Caronte, se implementarán protocolos de contingencia estructurados. Estos protocolos permitirán mitigar el impacto de los riesgos en el menor tiempo posible, asegurando la estabilidad del proyecto y minimizando desviaciones en el alcance, tiempo, costos y calidad.

Pasos para la Activación de Protocolos de Contingencia

1. **Detección del Riesgo:** Cuando un riesgo identificado se materializa, el equipo encargado de su monitoreo deberá alertar inmediatamente al responsable del proyecto y a los interesados clave.
2. **Evaluación del Impacto:** Una vez detectado el riesgo, se realizará una evaluación rápida para determinar su impacto en el proyecto, identificando el impacto financiero, los efectos en el cronograma y la afectación en la plataforma. Si el impacto es significativo, se procederá a activar el plan de contingencia correspondiente.
3. **Activación de la Contingencia:** El responsable del proyecto activará el plan de contingencia adecuado, según la naturaleza y el impacto del riesgo. Las acciones de contingencia podrán incluir:
    a. Refuerzo inmediato de medidas de seguridad en caso de brechas de datos.
    b. Reasignación de recursos en caso de problemas técnicos o de productividad.
    c. Modificación de cronogramas para ajustarse a nuevos plazos.
    d. Implementación de soluciones temporales ante fallos en servicios de API.

    En este paso, se hará uso de las reservas de contingencia asignadas previamente.

4. **Comunicación del Plan de Contingencia:** Se informará de inmediato a todos los miembros del equipo y a los interesados clave sobre la activación del protocolo de contingencia. Se utilizarán los canales de comunicación internos para garantizar que todos los involucrados estén al tanto de la situación, se comuniquen claramente las acciones a tomar y se establezcan los próximos pasos a seguir.
5. **Seguimiento y Monitoreo de la Contingencia:** Una vez activada la contingencia, se implementará un proceso de seguimiento continuo para evaluar la efectividad de las medidas implementadas. El equipo analizará si las acciones correctivas están mitigando el impacto del riesgo y si se requerirán ajustes adicionales para controlar la situación en el futuro.
6. **Documentación y Lecciones Aprendidas:** Tras la activación de un protocolo de contingencia, se documentarán los eventos y acciones tomadas en el Registro de Riesgos y en los informes de seguimiento.Además, se extraerán lecciones aprendidas para evitar la recurrencia del riesgo en el futuro y optimizar los tiempos de respuesta en situaciones similares.

6.7 Actividades de seguimiento de riesgos

El seguimiento de riesgos en el proyecto Caronte es un proceso continuo que garantiza la identificación, evaluación y control de los riesgos a lo largo del ciclo de vida del proyecto. Estas actividades permitirán mantener actualizada la información sobre los riesgos, evaluar la efectividad de las estrategias de mitigación y detectar nuevas amenazas a tiempo. Las actividades que se realizarán son:

- **Monitoreo de los riesgos identificados:** Todos los riesgos documentados en el Registro de Riesgos serán revisados periódicamente para evaluar si su probabilidad e impacto han cambiado a lo largo del proyecto. Esta revisión incluirá la evaluación de la efectividad de las estrategias de mitigación implementadas.
- **Detección de nuevos riesgos:** Durante la ejecución del proyecto, se realizarán revisiones regulares para identificar cualquier nuevo riesgo no previsto inicialmente. Estos riesgos serán evaluados y, si es necesario, se agregarán al Registro de Riesgos, definiendo estrategias de respuesta adecuadas.
- **Revisión del estado de los planes de mitigación y contingencia:** Los planes de mitigación y contingencia para los riesgos de mayor prioridad serán revisados en reuniones de seguimiento.
- **Reuniones de seguimiento de riesgos:** Se realizarán reuniones de seguimiento específicas para analizar el estado de los riesgos y las acciones correctivas implementadas. Se revisarán los riesgos críticos y se actualizarán las estrategias según sea necesario.

Estas actividades garantizarán que el proyecto Caronte mantenga un control continuo sobre los riesgos, asegurando la implementación de medidas correctivas oportunas y una gestión efectiva de los posibles impactos.

"Risks". Se ha utilizado la IA para mejorar la redacción de algunas secciones del documento, así como para corregir errores ortográficos que hubieran pasado desapercibidos. Toda la información generada por IA ha sido revisada por el equipo Caronte.