Camyo

Grupo 5

Análisis de Riesgos

Devising a Project (#DP)

Miembros del grupo:

- José Ramón Baños Botón
- Isabel X. Cantero Corchero
- Sheng Chen
- Carlos García Martínez
- Carlos García Ortiz
- Raúl Heras Pérez
- Pedro Jiménez Guerrero
- Claudia Meana Iturri
- Rubén Pérez Garrido
- Lucía Pérez Gutiérrez
- Francisco Pérez Manzano
- Diego José Pérez Vargas
- María C. Rodríguez Millán
- Sonia María Rus Morales
- Adriana Vento Conesa
- Jun Yao

Ingeniería del Software y Práctica Profesional • Curso 2024-25

Índice

Introducción

Este documento presenta un análisis de riesgos para la plataforma digital de matchmaking diseñada cuyo propósito es enlazar a profesionales del sector transporte (autónomos y empleados) con empresas que buscan cubrir vacantes. El objetivo primordial es identificar y evaluar los principales riesgos que podrían afectar el correcto funcionamiento, la seguridad y la reputación de la plataforma, así como proponer medidas de mitigación y planes de contingencia para asegurar su fiabilidad y continuidad.

Identificación de Riesgos

A continuación, se detallan los riesgos encontrados, cada uno agrupado en categorías que abarcan distintos ámbitos críticos: aspectos técnicos, legales, operativos, financieros, reputacionales, de seguridad de la información, estratégicos, de calidad, de estimación, de requisitos, organizativos, internos y externos.

1. **Riesgos Técnicos**
    - Fallas del servidor o caídas del sistema.
    - Vulnerabilidades de ciberseguridad (ataques, robo de datos, ransomware, etc.).
    - Integraciones con terceros (APIs) no seguras.
    - Caídas de servicios externos (APIs).
    - Sobrecarga de servidores ante crecimiento de usuarios.
2. **Riesgos Legales y de Cumplimiento**
    - Incumplimiento de la normativa de protección de datos (RGPD u otras legislaciones locales).
    - Incumplimiento de leyes laborales o de contratación.
    - Uso indebido de los datos de los usuarios.
3. **Riesgos Operativos**
    - Falta de personal técnico o de soporte para la gestión de la plataforma.
    - Procesos de registro y validación de usuarios ineficientes.
    - Dependencia de proveedores externos (hosting, pasarelas de pago, etc.).
4. **Riesgos Económico-Financieros**
    - Fluctuaciones en el mercado del transporte que disminuyan la demanda de la plataforma.
    - Problemas de liquidez (si se depende de comisiones o suscripciones).
    - Retrasos en la obtención de ingresos o falta de inversión.
    - Dependencia de herramientas de pago o con licencia gratuita expirada.
5. **Riesgos de Reputación**
    - Mala experiencia de usuario (baja calidad de las ofertas o transportistas no confiables).
    - Comentarios o reseñas negativas en redes sociales y foros.
    - Casos de fraude o estafa dentro de la plataforma.
6. **Riesgos de Seguridad de la Información**
    - Pérdida o robo de datos sensibles de empresas y transportistas.
    - Acceso no autorizado a sistemas internos.
    - Phishing o ingeniería social dirigida a usuarios.

7. **Riesgos Estratégicos**
    - Entrada de competidores con mejores propuestas o mayor inversión.
    - Cambios en la legislación que afecten la intermediación de empleo.
    - Excesiva dependencia de un solo segmento de mercado o tipo de cliente.
8. **Riesgos de Calidad**
    - Grandes errores en el código.
    - Interfaz no intuitiva que insatisface las expectativas y necesidades de los clientes y usuarios.
    - Falta de testing.
    - Testing poco exhaustivo, dejando errores sin detectar.
    - Falta de pruebas piloto antes del lanzamiento de la aplicación.
    - Falta de pruebas de rendimiento y carga.
    - No considerar opciones de accesibilidad.
9. **Riesgos de Estimación**
    - Subestimar y/o sobreestimar el esfuerzo requerido para las actividades.
    - Planificaciones muy optimistas.
10. **Riesgos de Requisitos**
    - Requisitos ambiguos o contradictorios.
    - Cambios en el alcance.
11. **Riesgos Organizativos**
    - Falta de roles y responsabilidades definidos en el equipo.
    - Escasa comunicación entre miembros y subgrupos del equipo.
    - Dificultad con el uso de la tecnología escogida.
12. **Riesgos Internos**
    - Conflictos internos entre los miembros del equipo.
    - Factor autobús.
    - Baja productividad.
13. **Riesgos Externos**
    - Cambios en la legislación que afecten al modelo de negocio.
    - Aparición de competidores similares que cuenten con mayores recursos.

Evaluación de Riesgos

La evaluación de los riesgos se realiza en base a dos criterios principales: la **probabilidad** de que el riesgo ocurra y el **impacto** que tendría en caso de que sucediera. A continuación, se presentan las tablas por categorías de riesgo, en las que se incluye información sobre el ID del riesgo, su probabilidad, su impacto, el factor de riesgo, su prioridad y las medidas de mitigación propuestas para dicho riesgo.

1. Riesgos Técnicos

ID	Riesgo	Probabilidad	Impacto	Factor	Prioridad	Medidas de mitigación
R1	Falla del servidor o caídas del sistema	2	10	20	10	Monitoreo proactivo.
R2	Vulnerabilidades de ciberseguridad	4	9	36	9	Mantenimiento de sistemas y librerías actualizadas.
R3	Integraciones con terceros (APIs) no seguras.	2	8	16	6	Utilización de protocolos seguros (HTTPS) y SLAs con terceros.
R4	Caídas de servicios externos (APIs).	1	8	8	7	Monitoreo de la disponibilidad de los servicios de terceros.
R5	Sobrecarga de servidores ante crecimiento de usuarios.	4	8	32	7	Monitorización del rendimiento y capacidad.

2. Riesgos Legales y de Cumplimiento

ID	Riesgo	Probabilidad	Impacto	Factor	Prioridad	Medidas de mitigación

R6	Incumplimiento de la normativa de protección de datos (RGPD u otras legislaciones locales).	2	9	18	8	Designación de un responsable de Protección de Datos.
R7	Incumplimiento de leyes laborales o de contratación.	2	8	16	6	Documentar todos los procesos de reclutamiento y pagos.
R8	Uso indebido de los datos de los usuarios.	1	9	9	7	Aseguramiento de buenas prácticas en el equipo.

3. Riesgos Operativos

ID	Riesgo	Probabilidad	Impacto	Factor	Prioridad	Medidas de mitigación
R9	Falta de personal técnico o de soporte para la gestión de la plataforma.	4	7	28	6	Manuales y documentación para el personal.
R10	Procesos de registro y validación de usuarios ineficientes.	3	6	18	5	Simplificación de formularios.
R11	Dependencia de proveedores externos (hosting, pasarelas de pago, etc.).	5	8	40	8	Revisión del plan de contingencia.

4. Riesgos Económico-Financieros

ID	Riesgo	Probabilidad	Impacto	Factor	Prioridad	Medidas de mitigación
R12	Fluctuaciones en el mercado del transporte que disminuyan la demanda de la plataforma.	4	7	28	7	Ajuste de planes de precios.
R13	Problemas de liquidez (si se depende de comisiones o suscripciones).	4	8	32	8	Revisión y optimización de costos fijos y modelos de ingresos.
R14	Retrasos en la obtención de ingresos o falta de inversión.	5	8	40	9	Revisión del plan de contingencia.
R15	Dependencia de herramientas de pago o con licencia gratuita expirada.	2	5	10	4	Evaluación de alternativas.

5. Riesgos de Reputación

ID	Riesgo	Probabilidad	Impacto	Factor	Prioridad	Medidas de mitigación
R16	Mala experiencia de usuario (baja calidad de las ofertas o transportistas no confiables).	4	8	32	7	Aseguramiento de la calidad y encuestas de satisfacción.

R17	Comentarios o reseñas negativas en redes sociales y foros.	3	6	18	6	Monitorización de redes sociales para responder con rapidez.
R18	Casos de fraude o estafa dentro de la plataforma.	3	8	24	7	Revisión del plan de contingencia.

6. Riesgos de Seguridad de la Información

ID	Riesgo	Probabilidad	Impacto	Factor	Prioridad	Medidas de mitigación
R19	Pérdida o robo de datos sensibles de empresas y transportistas.	4	9	36	8	Formación sobre buenas prácticas de seguridad para el equipo.
R20	Acceso no autorizado a sistemas internos.	3	8	24	7	Inspección de código manual/automático.
R21	Phishing o ingeniería social dirigida a usuarios.	5	7	35	6	Formación sobre buenas prácticas de seguridad para el equipo.

7. Riesgos Estratégicos

ID	Riesgo	Probabilidad	Impacto	Factor	Prioridad	Medidas de mitigación
R22	Entrada de competidores con mejores propuestas o	4	8	32	8	Análisis constante de nuevos

	mayor inversión.					competidores.
R23	Cambios en la legislación que afecten la intermediación de empleo.	2	8	16	6	Monitorear cambios en regulaciones, contratar asesoría legal.
R24	Excesiva dependencia de un solo segmento de mercado o tipo de cliente.	4	7	28	7	Realización de estudios de mercado para identificar oportunidades de expansión.

8. Riesgos de Calidad

ID	Riesgo	Probabilidad	Impacto	Factor	Prioridad	Medidas de mitigación
R25	Grandes errores en el código.	4	8	32	3	Inspección de código manual/automático y testing.
R26	Interfaz no intuitiva.	3	7	21	5	Pruebas piloto y aseguramiento de calidad.
R27	Falta de testing.	2	9	18	2	Planificación y revisión constante del plan de testing.
R28	Testing poco exhaustivo.	4	8	32	3	Aseguramiento de calidad y revisión del testing.
R29	Falta de pruebas piloto.	5	6	30	6	Gestión adecuada del plan de usuarios piloto.
R30	Falta de pruebas de	4	8	32	4	Aseguramiento de calidad y revisión del testing.

	rendimiento y carga.					
R31	No considerar opciones de accesibilidad.	5	4	20	5	Aseguramiento de la calidad.

9. Riesgos de Estimación

ID	Riesgo	Probabilidad	Impacto	Factor	Prioridad	Medidas de mitigación
R32	Subestimar/sobreestimar el esfuerzo requerido.	3	8	24	9	Revisión de la planificación, estimación mediante técnicas.
R33	Planificaciones muy optimistas.	3	8	24	9	Revisión de la planificación, estimación mediante técnicas.

10. Riesgos de Requisitos

ID	Riesgo	Probabilidad	Impacto	Factor	Prioridad	Medidas de mitigación
R34	Requisitos ambiguos o contradictorios.	5	7	35	2	Revisión del documento de requisitos.
R35	Cambios en el alcance.	3	9	27	1	Revisión de la declaración

						del alcance.

11. Riesgos Organizativos

ID	Riesgo	Probabilidad	Impacto	Factor	Prioridad	Medidas de mitigación
R36	Falta de roles y responsabilidades definidos en el equipo.	1	5	5	8	Reunión para la división de responsabilidades y documentación detallada y acorde.
R37	Escasa comunicación entre miembros y subgrupos.	5	7	35	4	Fomentar las habilidades interpersonales y el trabajo en equipo.
R38	Dificultad con el uso de la tecnología escogida.	3	8	24	6	Formación previa al inicio de las fases de desarrollo.

12. Riesgos Internos

ID	Riesgo	Probabilidad	Impacto	Factor	Prioridad	Medidas de mitigación
R39	Conflictos internos entre los miembros del equipo.	3	8	24	6	Fomentar las habilidades interpersonales y la comunicación efectiva entre miembros del equipo.
R40	Factor autobús.	3	9	27	5	Formación uniforme entre los miembros del equipo, reparto

						equitativo de tareas.
R41	Baja productividad.	6	6	36	3	Gestión eficiente del rendimiento del equipo.

13. Riesgos Externos

ID	Riesgo	Probabilida	Impacto	Factor	Prioridad	Medidas de mitigación
R42	Cambios en la legislación que afecten al modelo de negocio.	2	7	14	8	Monitorear cambios en regulaciones, contratar asesoría legal.
R43	Aparición de competidores similares que cuenten con mayores recursos.	6	9	54	1	Análisis constante de nuevos competidores.

Plan de Contingencia

Para cada riesgo identificado, se definen estrategias de respuesta considerando el tiempo limitado del proyecto:

Riesgos Técnicos

- **Fallas del servidor:** Migración a un servidor de respaldo automático en la segunda mitad del proyecto.
- **Ciberseguridad:** Implementar backup en tiempo real y respuestas rápidas ante incidentes dentro del primer mes.
- **Integraciones con terceros (API) no seguras:** Implementar autenticación y autorización segura y forzar el uso de HTTPS para evitar accesos no autorizados.
- **Caídas de servicios externos (APIs):** Implementar mecanismos de reintento, además de monitoreo constante y cambiar a servicios alternativos si es necesario.

Riesgos Legales y de Cumplimiento

- **Incumplimiento de la normativa de protección de datos (RGPD):** Implementar medidas de seguridad y procesos de control para garantizar el cumplimiento del RGPD, incluyendo control de acceso a la información sensible.
- **Incumplimiento de leyes laborales o de contratación:** Establecer procesos de verificación de las normativas, asegurándose de que todos los contractos y las condiciones laborales cumplan con la normativa vigente.
- **Uso indebido de los datos de los usuarios:** Aplicar políticas de privacidad y acceso a los datos, junto con el cifrado de la información sensible.

Riesgos Operativos

- **Falta de personal técnico o de soporte para la gestión de la plataforma:** Crear un plan de emergencia con personal de backup, o utilizar un servicio de soporte gestionado externo. Además, capacitar al personal existente en aspectos técnicos esenciales.
- **Procesos de registro y validación de usuarios ineficientes:** Reducir el número de campos requeridos para simplificar el proceso de registro, y utilizar la validación en tiempo real para recibir un feedback inmediato.

- **Dependencia de proveedores externos (hosting, pasarelas de pago, etc.):** Implementar soluciones alternativas y añadir proveedores de backup para garantizar la continuidad operativa en caso de problemas con proveedores externos. Además, potenciar las competencias del personal interno para gestionar de manera autónoma las funciones críticas.

Riesgos Económico-Financieros

- **Fluctuaciones en el mercado del transporte que disminuyan la demanda de la plataforma:** Diversificar los servicios ofrecidos y adaptar estrategias de marketing para atraer nuevos clientes.
- **Problemas de liquidez (si se depende de comisiones o suscripciones):** Ampliar las fuentes de ingreso para reducir la dependencia de un solo modelo de ganancia, y crear un fondo de emergencia.
- **Retrasos en la obtención de ingresos o falta de inversión:** Diversificar las fuentes de ingresos u optimizar la monetización actual, además se pueden buscar fuentes alternativas de financiamiento.
- **Dependencia de herramientas de pago o con licencia gratuita expirada:** Valorar alternativas de código abierto o negociar mejores condiciones con los proveedores para garantizar la continuidad operativa.

Riesgos de Reputación

- **Mala experiencia de usuario (baja calidad de las ofertas o transportistas no confiables):** Implementar un sistema de evaluación y verificación para los transportistas, garantizando mayor fiabilidad en las ofertas
- **Comentarios o reseñas negativas en redes sociales y foros:** Monitorear las opiniones de los usuarios y responder de manera oportuna y transparente a las críticas, mejorar el servicio en base a los comentarios recibidos.
- **Casos de fraude o estafa dentro de la plataforma:** Reforzar los sistemas de seguridad con autenticación avanzada y verificaciones de identidad, monitorear las transacciones para prevenir actividades fraudulentas.

Riesgos de Seguridad de la Información

- **Pérdida o robo de datos sensibles de empresas y transportistas:** Implementar copias de seguridad regulares con acceso limitado solo a los usuarios

autorizados, e implementar cifrado end-to-end para la protección de los datos sensibles

- **Acceso no autorizado a sistemas internos:** Adoptar autenticación de múltiples factores y monitorear constantemente los intentos de acceso sospechosos.
- **Phishing o ingeniería social dirigida a usuarios:** Implementar filtros avanzados para detectar y bloquear intentos de phishing, y doble verificación para solicitudes sensibles

Riesgos Estratégicos

- **Entrada de competidores con mejores propuestas o mayor inversión:** Diferenciarse a través de una oferta innovadora, mejorando la calidad del servicio, personalizar los servicios y fidelizar a los clientes.
- **Cambios en la legislación que afecten la intermediación de empleo:** Monitorear constantemente las normativas, colaborar con expertos legales para garantizar la conformidad con la legislación.
- **Excesiva dependencia de un solo segmento de mercado o tipo de cliente:** Diversificar el tipo de servicios ofrecidos o los modelos de negocio, adaptar la oferta a más categorías de usuarios, para reducir el riesgo de concentración.

Riesgos de Calidad

- **Grandes errores en el código:** Revisar el código periódicamente e implementar herramientas de análisis estático para identificar bugs críticos.
- **Interfaz no intuitiva:** Realizar investigaciones sobre los usuarios objetivo para comprender sus necesidades y hábitos, y desarrollar prototipos interactivos para probar con usuarios reales. Aplicar principios de diseño UX para mejorar la experiencia.
- **Falta de testing:** Definir una estrategia de testing que incluya test automáticos, manuales y funcionales. Asegurarse de que el proceso de desarrollo integre testing continuos para reducir el riesgo de fallos.
- **Testing poco exhaustivo:** Ampliar la cobertura de las pruebas incluyendo escenarios relistas y casos limite considerando varios dispositivos, sistemas operativos y condiciones de red.

- **Falta de pruebas piloto:** Lanzar versiones beta del software incluyendo un grupo seleccionado de usuarios finales para recopilar feedbacks e identificar problemas antes del lanzamiento.
- **Falta de pruebas de rendimiento y carga:** Simular escenarios de uso intensivo utilizando herramientas de pruebas de estrés para garantizar la escalabilidad y estabilidad del software. Implementar sistemas de monitoreo en tiempo real para prever y prevenir ralentizaciones.

Riesgos de Estimación

- **Subestimar/sobreestimar el esfuerzo requerido:** Basarse en datos históricos de proyectos similares, incluir siempre un margen de seguridad en los cálculos e incluir a varios miembros del equipo en la evaluación del compromiso requerido. Además, monitorear constantemente el avance y adaptar las previsiones.
- **Planificaciones muy optimistas:** Incluir márgenes de seguridad en los tiempos, adoptar metodologías agiles y recoger feedback continuo para mantener expectativas realistas.

Riesgos de Requisitos

- **Requisitos ambiguos o contradictorios:** Adoptar un proceso de recopilación y gestión estructurado, aclarar objetivos y expectativas, utilizar herramientas de gestión y validación de requisitos.
- **Cambios en el alcance:** Adoptar metodologías de desarrollo agiles para integrar cambios de manera gradual sin comprometer todo el proyecto. Establecer un proceso de gestión de cambios con evaluación del impacto en tiempos y costos.

Riesgos Organizativos

- **Falta de roles y responsabilidades definidos:** definir las responsabilidades de manera detallada para cada miembro del equipo, dividir las actividades según las competencias. Organizar reuniones periódicas y proporcionar feedback constante.

- **Escasa comunicación entre miembros y subgrupos:** Utilizar herramientas de colaboración, establecer reuniones periódicas y definir tareas claras para casa miembro del grupo.
- **Dificultad con el uso de la tecnología escogida:** Proporcionar formación continua, documentación detallada y soporte técnico constante. Si es necesario, evaluar el uso de herramientas más intuitiva o personalizar las soluciones para adoptar a las necesidades.

Riesgos Internos

- **Conflictos internos entre miembros del equipo:** Crear un ambiente de trabajo transparente y promover la comunicación abierta. Adoptar estrategias de gestión de conflictos como un mediator interno. Definir claramente los objetivos del equipo y las expectativas.
- **Factor autobús:** Organizar sesiones para mejorar la motivación y reducir el impacto de dinámicas personales, proporcionar feedback positiva y fomentar el crecimiento personal
- **Baja productividad:** Monitorear constantemente la carga de trabajo, distribuir las actividades de manera equilibrada y proporcionar incentivos para el logro de los objetivos.

Riesgos Externos

- **Cambios en la legislación que afecten al modelo de negocio:** Crear un equipo dedicado que se encargue de monitorear los cambios en la legislación o colaborar con consultores externos especializados. Diversificar el modelo de negocio reduciendo la dependencia de normativas específicas.
- **Aparición de competidores similares que cuenten con mayores recursos:** Diferenciar el producto o servicio ofrecido, invertir en la innovación. Analizar constantemente el mercado para fidelizar el cliente.

Presupuesto de contingencia para los riesgos

La elaboración de un presupuesto de contingencia permite disponer de recursos financieros para hacer frente a riesgos que puedan materializarse y que no estén contemplados en el presupuesto operativo habitual.

Categoría de Riesgo	Descripción	Monto Estimado	Justificación
Técnicos	- Contratación de servicios adicionales de seguridad - Infraestructura en la nube con escalabilidad y alta disponibilidad.	2.000 € – 3.000 €	Cubre el coste de contratar herramientas para prevenir ataques y brechas de datos. Garantiza la adquisición o ampliación de servicios de hosting para reducir el tiempo de inactividad.
Legales / Cumplimiento	- Ajustes de contratos o uso de datos. - Formación del personal.	1.000 € – 3.000 €	Permite costear posibles revisiones y auditorías legales, así como honorarios de abogados y formación interna para evitar denuncias o sanciones.
Operativos	- Contratos alternativos con otros proveedores (hosting, pasarelas de pago).	1.000 € – 2.500 €	Cubre el pago inicial o la implementación de proveedores y servicios secundarios para suplir a los principales en caso de fallos, asegurando la continuidad operativa.
Económico-Financieros	- Optimización de estructuras de costes.	1.000 € – 2.000 €	Asegura un colchón financiero para afrontar situaciones en las que la plataforma genere menos ingresos o haya retrasos en los pagos, evitando comprometer la operación del proyecto.

Reputación	- Departamento de refuerzo en UX/UI. - Gestión de crisis y comunicación con usuarios.	500 € – 2.000 €	Permite mejorar la atención y la imagen de la plataforma, cubriendo costos de rediseño y comunicación ante grandes volúmenes de usuarios.
Seguridad de la Información	- Pérdida o robo de datos sensibles de empresas y transportistas. - Acceso no autorizado a sistemas internos. - Phishing o ingeniería social dirigida a usuarios.	1.000 € – 2.000 €	Inversión en cifrado de datos, autenticación multifactorial, monitorización de accesos y herramientas de filtrado contra ataques de phishing.
Estratégicos	- Entrada de competidores con mayores propuestas o mayor inversión. - Cambios en la legislación que afecten la intermediación de empleo.	1.000 € – 2.500 €	Investigación de mercado para mantenerse competitivos y asesoría legal para atender cambios normativos.
Calidad	- Grandes errores en el código. - Interfaz no intuitiva. - Falta de testing o testing poco exhaustivo. - Falta de pruebas piloto.	1.000 € – 2.000 €	Cubriría las revisiones periódicas de código, la adopción de metodologías de testing continuo, la realización de prototipos y pruebas piloto con usuarios reales, y la implementación de herramientas de análisis estático y pruebas de rendimiento.
Estimación	- Subestimar / sobreestimar el esfuerzo requerido. - Planificaciones muy optimistas.	1.000 € – 2.000 €	Un mayor rigor en la estimación de tiempos y costos minimiza retrasos y sobrecostes imprevistos.
Requisitos	- Requisitos ambiguos o contradictorios.	500 € – 2.000 €	Formación y seguimiento para asegurar claridad y

			coherencia en lo que se desarrolla.
Organizativos	- Falta de roles y responsabilidades definidos. - Escasa comunicación entre miembros y subgrupos. - Dificultad con la tecnología escogida.	500 € – 2.000 €	Definición de un organigrama y funciones claras, y posible consultoría organizativa para optimizar flujos de trabajo
Internos	- Conflictos internos entre miembros del equipo. - Baja productividad general.	1.000 € – 2.000 €	Incluye incentivos o dinámicas para elevar la motivación y productividad.
Externos	- Cambios en la legislación que afecten el modelo de negocio. - Aparición de competidores similares que cuenten con mayores recursos.	1.000 € – 2.500 €	Permite afrontar modificaciones de la ley, cubrir la redacción de nuevos términos y proporcionar formación al equipo para que cumpla con las regulaciones actualizadas sin interrumpir el servicio. Se requiere vigilancia constante de las tendencias.

Total Aproximado del Fondo de Contingencia: 13.500 € – 29.500 €

Recomendación de Reserva General

Se sugiere destinar entre un **10% y un 20%** del presupuesto total del proyecto como **fondo de contingencia**. Esta reserva sirve para cubrir gastos imprevistos más allá de los estimados en cada partida y brinda flexibilidad para reaccionar rápidamente a incidentes que requieran inversión adicional inmediata.

Justificación del Presupuesto de Contingencia

- **Variabilidad de los costes**: El coste real de las medidas puede fluctuar en función de la severidad del incidente y la urgencia de la respuesta.
- **Protección de la continuidad del negocio**: Contar con recursos financieros asignados específicamente a la gestión de crisis minimiza el riesgo de que un incidente afecte gravemente la operación o la reputación de la plataforma.
- **Agilidad y rapidez de actuación**: Un fondo de contingencia bien dimensionado permite la contratación inmediata de expertos, la adquisición de herramientas de seguridad o la migración a proveedores alternativos sin dilaciones que puedan agravar el problema.

Este presupuesto debe revisarse de forma periódica (mensualmente durante el proyecto y posteriormente cada semestre) para ajustarlo a cambios en los riesgos, a la evolución del mercado y a las experiencias reales de la operación.

Conclusiones

Del análisis anterior se desprende que la plataforma digital de matchmaking para el sector transporte enfrenta una amplia gama de riesgos con distintos niveles de probabilidad e impacto. En particular, los riesgos críticos se centran en el ámbito de la ciberseguridad, protección de datos y reputación, que pueden afectar tanto la confianza de los usuarios como la estabilidad del servicio.

El análisis de probabilidad e impacto ha permitido priorizar las áreas que requieren acciones de mitigación inmediatas y planes de contingencia sólidos. Se recomienda la implementación de medidas de seguridad avanzadas, auditorías periódicas y la optimización continua de la experiencia de usuario. Asimismo, el seguimiento del mercado y de la normativa vigente es clave para minimizar los riesgos operativos y estratégicos.

Dado que el proyecto tiene una duración de solo 3 meses, es fundamental garantizar que las estrategias de mitigación y contingencia sean ejecutadas dentro de este período. La correcta planificación financiera y operativa, junto con la adaptación a cambios regulatorios y tecnológicos, resultará esencial para asegurar el éxito del proyecto y la sostenibilidad de la plataforma en el corto plazo.

Con este análisis detallado, la plataforma estará mejor preparada para gestionar los riesgos identificados y garantizar un funcionamiento eficiente y seguro dentro del tiempo de ejecución del proyecto.

Referencias

https://stafiz.com/es/como-realizar-un-analisis-de-riesgos-en-la-gestion-de-proyectos

https://www.startechup.com/es/blog/10-common-software-development-risks/

https://asana.com/es/resources/risk-matrix-template

https://asana.com/es/resources/contingency-plan

https://www.tarlogic.com/es/blog/owasp-top-10-riesgos-aplicaciones-moviles/

https://www.nedigital.com/es/blog/software-de-ciberseguridad

https://www.globalsuitesolutions.com/es/que-es-un-software-de-cumplimiento-legal/