Plan de Riesgos - Proyecto Webinnova

1. Identificación de Riesgos

1.1 Riesgos Técnicos

Fallas en el sistema: Los errores en el código o problemas de configuración pueden causar caídas del sistema o un mal
funcionamiento de la aplicación. Esto no solo afecta la experiencia del usuario, sino que también puede generar pérdida
de datos o interrupciones en el servicio.
Problemas de seguridad: La vulnerabilidad a ataques cibernéticos, como inyecciones SQL, ataques DDoS y accesos no autorizados,
puede comprometer la integridad de la información y la privacidad de los usuarios. La falta de medidas de seguridad adecuadas
puede llevar a la exposición de datos sensibles.
Obsolescencia tecnológica: Si se utilizan herramientas o tecnologías que no se actualizan, esto puede afectar la capacidad
de la aplicación para integrarse con nuevas funcionalidades o sistemas. Esto puede resultar en una experiencia de usuario
deficiente y una mayor dificultad para mantener la aplicación.
Integración con terceros: La dependencia de APIs o servicios de terceros para funciones críticas puede ser arriesgada, ya que
la inestabilidad de estos servicios puede afectar el rendimiento de la aplicación. Es esencial evaluar regularmente la fiabilidad
de estos servicios.

1.2 Riesgos de Recursos

Falta de personal capacitado: La escasez de desarrolladores, diseñadores o expertos en tecnología con las habilidades necesarias
puede comprometer la calidad del producto final. Esto puede llevar a un retraso en la implementación de funcionalidades clave.
Rotación de personal: La alta rotación en el equipo de trabajo puede provocar pérdidas de conocimiento crítico y dificultad en la
continuidad del proyecto. Esto puede generar tiempo adicional para que los nuevos integrantes se adapten y comprendan el estado
del proyecto.
Disponibilidad de recursos: La falta de recursos, como hardware y software, puede causar retrasos en el desarrollo. Es vital asegurarse

de que todos los recursos necesarios estén disponibles desde el inicio del proyecto.

1.3 Riesgos de Cronograma

Retrasos en la entrega: La incapacidad para cumplir con los plazos establecidos puede deberse a problemas técnicos, cambios en los
requerimientos o falta de recursos. Esto afectará la satisfacción del cliente y la reputación del equipo de trabajo.
Cambios en los requerimientos: Modificaciones en las especificaciones, ya sea por parte del cliente o debido a cambios en el mercado,
pueden llevar a re-trabajos y la necesidad de ajustar el cronograma del proyecto.
Estimaciones inexactas: Si las estimaciones iniciales de tiempo y recursos son incorrectas, se puede producir una falta de planificación
adecuada, resultando en retrasos y sobrecarga para el equipo de trabajo.

1.4 Riesgos Financieros

Aumento de costos: Gastos inesperados, como la adquisición de nuevas herramientas o la contratación de personal adicional, pueden
superar el presupuesto originalmente asignado. Esto puede comprometer el financiamiento general del proyecto.
Falta de financiamiento: La incapacidad para asegurar fondos necesarios para completar el proyecto puede poner en riesgo su finalización.
La búsqueda de inversores o financiación adicional debe estar en el plan desde el principio.
Dependencia de ingresos futuros: Si el proyecto depende de ingresos o financiamiento que aún no se han asegurado, cualquier retraso en la
obtención de estos fondos puede afectar significativamente el avance del proyecto.

1.5 Riesgos de Mercado

Competencia: La aparición de nuevas aplicaciones que ofrecen características similares o innovadoras puede afectar la cuota de mercado
de Webinnova, impactando las proyecciones de ingresos. Es fundamental hacer análisis de competencia constantes.
Cambios en la demanda: Las variaciones en las preferencias del consumidor o en las condiciones del mercado pueden hacer que el producto
sea menos relevante. Esto requiere un monitoreo continuo de las tendencias del mercado.
Regulaciones cambiantes: Nuevas leyes o regulaciones pueden afectar cómo se opera el proyecto, requiriendo ajustes que pueden consumir
tiempo y recursos. La vigilancia sobre los cambios regulatorios es crucial para la adaptación.

2. Análisis de Riesgos

Se debe realizar un análisis exhaustivo de cada riesgo, clasificándolos en función de su probabilidad de ocurrencia
y su impacto en el proyecto:

Riesgo	Probabilidad	Impacto	Priorización
Fallas en el sistema	Alta	Alto	Crítico
Problemas de seguridad	Medio	Alto	Alto
Obsolescencia tecnológica	Baja	Alto	Medio
Integración con terceros	Medio	Alto	Alto
Falta de personal capacitado	Alta	Medio	Alto
Rotación de personal	Medio	Medio	Medio
Disponibilidad de recursos	Alta	Alto	Crítico
Retrasos en la entrega	Alta	Alto	Crítico
Cambios en los requerimientos	Medio	Alto	Alto
Estimaciones inexactas	Medio	Alto	Alto
Aumento de costos	Medio	Medio	Medio
Falta de financiamiento	Baja	Alto	Alto
Dependencia de ingresos futuros	Medio	Alto	Alto
Competencia	Medio	Alto	Alto
Cambios en la	Medio	Medio	Medio

demanda			
Regulaciones cambiantes	Baja	Alto	Alto

3. Planificación de Respuestas a Riesgos

3.1 Estrategias Generales

Evitar: Modificar el plan del proyecto para eludir los riesgos más críticos, ajustando el enfoque y las prioridades según sea necesario.
Mitigar: Implementar acciones concretas para reducir la probabilidad o impacto de los riesgos identificados, utilizando tecnologías
avanzadas y mejores prácticas.
Aceptar: Reconocer la existencia de ciertos riesgos y preparar un plan de contingencia para situaciones inevitables, asegurando que haya
recursos asignados para estos casos.
Transferir: Pasar el riesgo a un tercero, como aseguradoras o proveedores, de manera que minimice el impacto directo en el proyecto.

3.2 Respuestas Específicas a Riesgos

Fallas en el sistema: Implementar un riguroso proceso de pruebas y monitoreo continuo del sistema, con un equipo dedicado a resolver
problemas técnicos rápidamente.
Problemas de seguridad: Realizar auditorías de seguridad periódicas, mantener el software actualizado y entrenar al personal sobre mejores
prácticas de seguridad.
Obsolescencia tecnológica: Establecer un calendario de revisión y actualización de tecnologías utilizadas, asegurando la adopción de
nuevas soluciones cuando sea necesario.
Integración con terceros: Evaluar regularmente la estabilidad y rendimiento de las APIs o servicios de terceros utilizados, teniendo
planes de respaldo si estos servicios fallan.
Falta de personal capacitado: Desarrollar un plan de capacitación continua y buscar talento externo para completar el equipo, ofreciendo
incentivos para la retención.
Rotación de personal: Crear un entorno de trabajo atractivo mediante beneficios y oportunidades de desarrollo, así como establecer procesos
de documentación para retener conocimiento crítico.
Disponibilidad de recursos: Realizar un inventario regular de los recursos necesarios y

establecer contactos con proveedores alternativos
para asegurar disponibilidad continua.
Retrasos en la entrega: Implementar metodologías ágiles que permitan ajustar el cronograma a la realidad del proyecto, permitiendo
replanificaciones periódicas.
Cambios en los requerimientos: Establecer un proceso formal de gestión de cambios para evaluar y aprobar modificaciones, minimizando el
impacto en el cronograma y el presupuesto.
Estimaciones inexactas: Utilizar herramientas de planificación más sofisticadas y técnicas de estimación, como PERT y CPM, para mejorar
la precisión de las proyecciones.
Aumento de costos: Monitorear y ajustar el presupuesto de manera proactiva, asegurando que haya un fondo de contingencia disponible para
gastos inesperados.
Falta de financiamiento: Buscar activamente inversores o subvenciones adicionales para asegurar el financiamiento necesario y evitar
interrupciones en el proyecto.
Dependencia de ingresos futuros: Desarrollar un plan de contingencia que incluya alternativas de financiamiento y una gestión prudente de
los recursos.
Competencia: Realizar análisis de mercado continuos para adaptar la propuesta de valor y garantizar que el producto se mantenga competitivo.
Cambios en la demanda: Estar en contacto constante con los usuarios para ajustar la oferta a sus necesidades y preferencias cambiantes.
Regulaciones cambiantes: Mantenerse informado sobre los cambios regulatorios que puedan afectar el proyecto y realizar ajustes necesarios
de manera oportuna.

4. Monitoreo y Revisión de Riesgos

Revisiones Periódicas: Realizar reuniones mensuales para evaluar el estado de los riesgos y la efectividad de las respuestas implementadas,
adaptando el plan de riesgos según sea necesario.
Actualización del Registro de Riesgos: Mantener un registro actualizado de los riesgos, incluyendo nuevos riesgos que puedan surgir y
cambios en los existentes. Esto debe ser un documento vivo que evolucione con el proyecto.
Comunicación con Stakeholders: Mantener a todos los interesados informados sobre el estado de los riesgos y las acciones que se están
tomando para abordarlos, asegurando transparencia y colaboración.