ANÁLISIS DE RIESGOS

Sistema de Gestión Documental Universitaria TESCHI

CARÁTULA

INSTITUCIÓN: Tecnológico de Estudios Superiores de Chimalhuacán (TESCHI)
PROYECTO: Sistema de Gestión Documental Universitaria
MATERIA: Ingeniería de Software
DOCENTE: Modesto Castro Yolanda
SEMESTRE: 7ISC23

INTEGRANTES DEL EQUIPO:

1. **Gálvez Romero Irvin Osvaldo** - Administrador de Base de Datos / Desarrollador Full-Stack
2. **Cruz Contreras Ángel Valentín** - Desarrollador Frontend / UI/UX
3. **Sánchez Vargas Kevin Antonio** - Analista de Sistemas / Desarrollador Backend
4. **Juárez Vargas Alberto** - Líder de Proyecto / DevOps

FECHA: [Fecha actual]
VERSIÓN: 1.0

1. INTRODUCCIÓN

1.1 Propósito del Documento

Este documento presenta un análisis completo de riesgos para el Sistema de Gestión Documental Universitaria TESCHI, incluyendo identificación, evaluación, mitigación y monitoreo de riesgos que pueden afectar el éxito del proyecto.

1.2 Alcance

El análisis cubre todos los aspectos del proyecto incluyendo:

- Riesgos técnicos
- Riesgos de recursos humanos
- Riesgos de cronograma
- Riesgos de calidad
- Riesgos de seguridad
- Riesgos de negocio

1.3 Metodología

- **Identificación:** Brainstorming, análisis de experiencia, revisión de literatura
- **Evaluación:** Matriz de probabilidad e impacto
- **Mitigación:** Estrategias de prevención y contingencia

- **Monitoreo:** Seguimiento continuo y actualización

---

2. IDENTIFICACIÓN DE RIESGOS

2.1 Riesgos Técnicos

R-001: Problemas de Integración Frontend-Backend

Descripción: Dificultades en la integración entre el frontend React y el backend Node.js que pueden causar retrasos o funcionalidades incompletas.

Causas Potenciales:

- Incompatibilidad de versiones de APIs
- Diferencias en el manejo de datos
- Problemas de autenticación entre capas
- Errores en la comunicación HTTP

Indicadores:

- Errores 404/500 en llamadas API
- Datos no sincronizados entre frontend y backend
- Problemas de autenticación
- Funcionalidades que no responden

R-002: Problemas de Rendimiento con Archivos Grandes

Descripción: El sistema puede experimentar problemas de rendimiento al manejar archivos grandes o múltiples usuarios subiendo documentos simultáneamente.

Causas Potenciales:

- Limitaciones de memoria del servidor
- Ancho de banda insuficiente
- Algoritmos de procesamiento ineficientes
- Falta de optimización de consultas

Indicadores:

- Tiempo de respuesta > 10 segundos
- Errores de timeout
- Alto uso de CPU/memoria
- Quejas de usuarios sobre lentitud

R-003: Vulnerabilidades de Seguridad

Descripción: El sistema puede ser vulnerable a ataques de seguridad que comprometan la integridad de los datos o la privacidad de los usuarios.

Causas Potenciales:

- Implementación insegura de autenticación
- Falta de validación de entrada
- Exposición de datos sensibles
- Configuración insegura del servidor

Indicadores:

- Intentos de acceso no autorizado
- Datos expuestos en logs
- Errores de validación
- Alertas de seguridad

R-004: Problemas de Base de Datos

Descripción: La base de datos puede experimentar problemas de rendimiento, corrupción o pérdida de datos.

Causas Potenciales:

- Consultas mal optimizadas
- Falta de respaldos regulares
- Corrupción de datos
- Problemas de concurrencia

Indicadores:

- Consultas lentas (> 1 segundo)
- Errores de conexión a BD
- Datos inconsistentes
- Fallos en respaldos

2.2 Riesgos de Recursos Humanos

R-005: Disponibilidad Limitada del Equipo

Descripción: Los miembros del equipo pueden no estar disponibles debido a compromisos académicos, personales o de salud.

Causas Potenciales:

- Exámenes y proyectos académicos
- Enfermedades o emergencias personales
- Conflictos de horarios
- Sobrecarga de trabajo

Indicadores:

- Ausencias frecuentes a reuniones
- Retrasos en entregas
- Comunicación limitada
- Estrés del equipo

R-006: Falta de Conocimiento Técnico Específico

Descripción: El equipo puede carecer de conocimiento específico en tecnologías o metodologías requeridas para el proyecto.

Causas Potenciales:

- Tecnologías nuevas o poco conocidas
- Falta de experiencia en el dominio
- Cambios en requerimientos técnicos
- Curva de aprendizaje empinada

Indicadores:

- Tiempo excesivo en tareas simples
- Errores técnicos frecuentes
- Búsqueda constante de documentación
- Frustración del equipo

R-007: Conflictos Interpersonales

Descripción: Desacuerdos o tensiones entre miembros del equipo pueden afectar la productividad y el ambiente de trabajo.

Causas Potenciales:

- Diferencias en enfoques técnicos
- Personalidades incompatibles
- Comunicación inefectiva
- Distribución desigual de trabajo

Indicadores:

- Reuniones tensas
- Comunicación hostil
- Evitación de colaboración
- Baja moral del equipo

2.3 Riesgos de Cronograma

R-008: Retrasos en Entregas

Descripción: Las entregas del proyecto pueden retrasarse debido a estimaciones incorrectas o problemas imprevistos.

Causas Potenciales:

- Estimaciones optimistas
- Cambios de requerimientos
- Problemas técnicos no anticipados
- Dependencias externas

Indicadores:

- Tareas que toman más tiempo del estimado
- Acumulación de trabajo pendiente
- Presión por cumplir fechas límite
- Calidad comprometida por prisa

R-009: Cambios de Requerimientos

Descripción: Los requerimientos del proyecto pueden cambiar durante el desarrollo, causando retrasos y trabajo adicional.

Causas Potenciales:

- Feedback tardío de stakeholders
- Cambios en necesidades del negocio
- Mejores ideas durante el desarrollo
- Falta de claridad inicial

Indicadores:

- Solicitudes de cambio frecuentes
- Revisión constante de especificaciones
- Trabajo rehacer
- Confusión sobre funcionalidades

R-010: Dependencias Externas

Descripción: El proyecto puede depender de servicios, herramientas o recursos externos que no estén disponibles o funcionen correctamente.

Causas Potenciales:

- Servicios de terceros no disponibles
- Herramientas de desarrollo con problemas
- Recursos de infraestructura limitados
- Cambios en APIs externas

Indicadores:

- Servicios externos caídos
- Herramientas no funcionando
- Limitaciones de recursos
- Cambios en APIs sin aviso

2.4 Riesgos de Calidad

R-011: Bugs Críticos en Producción

Descripción: El sistema puede tener bugs críticos que afecten la funcionalidad principal o la experiencia del usuario.

Causas Potenciales:

- Pruebas insuficientes
- Código complejo sin documentación
- Integración no probada adecuadamente
- Presión por entregar rápido

Indicadores:

- Funcionalidades que no funcionan
- Errores frecuentes en producción
- Quejas de usuarios
- Pérdida de datos

R-012: Problemas de Usabilidad

Descripción: El sistema puede ser difícil de usar o no cumplir con las expectativas de usabilidad de los usuarios.

Causas Potenciales:

- Falta de pruebas con usuarios reales
- Diseño no intuitivo
- Falta de feedback de usuarios
- Cambios de último minuto

Indicadores:

- Usuarios confundidos
- Tiempo excesivo para completar tareas
- Abandono de funcionalidades
- Quejas sobre interfaz

R-013: Problemas de Rendimiento

Descripción: El sistema puede no cumplir con los requisitos de rendimiento especificados.

Causas Potenciales:

- Código no optimizado
- Consultas de base de datos lentas
- Falta de caché
- Arquitectura no escalable

Indicadores:

- Tiempo de respuesta lento
- Alto uso de recursos
- Timeouts frecuentes
- Usuarios frustrados

2.5 Riesgos de Seguridad

R-014: Ataques de Seguridad

Descripción: El sistema puede ser objetivo de ataques maliciosos que comprometan la seguridad de los datos.

Causas Potenciales:

- Vulnerabilidades no parcheadas
- Configuración insegura
- Falta de monitoreo de seguridad
- Ataques dirigidos

Indicadores:

- Intentos de acceso no autorizado
- Tráfico sospechoso
- Alertas de seguridad
- Datos comprometidos

R-015: Pérdida de Datos

Descripción: Los datos del sistema pueden perderse debido a fallos de hardware, software o errores humanos.

Causas Potenciales:

- Fallos de hardware
- Errores en respaldos
- Corrupción de base de datos
- Errores de operación

Indicadores:

- Datos no accesibles
- Respaldos fallidos
- Errores de base de datos
- Pérdida de archivos

2.6 Riesgos de Negocio

R-016: Falta de Adopción por Usuarios

Descripción: Los usuarios pueden no adoptar el sistema o usarlo de manera limitada.

Causas Potenciales:

- Falta de capacitación
- Resistencia al cambio
- Sistema no intuitivo

- Falta de valor percibido

Indicadores:

- Bajo uso del sistema
- Quejas de usuarios
- Resistencia a usar
- Retorno a procesos antiguos

R-017: Cambios en Requerimientos del Negocio

Descripción: Los requerimientos del negocio pueden cambiar significativamente durante el desarrollo.

Causas Potenciales:

- Cambios en la organización
- Nuevas regulaciones
- Cambios en procesos
- Feedback de usuarios

Indicadores:

- Solicitudes de cambio frecuentes
- Confusión sobre objetivos
- Trabajo rehacer
- Retrasos en el proyecto

---

3. EVALUACIÓN DE RIESGOS

3.1 Matriz de Probabilidad e Impacto

ID	Riesgo	Probabilidad	Impacto	Nivel	Prioridad
R-001	Problemas de Integración Frontend-Backend	Media	Alto	Alto	1
R-002	Problemas de Rendimiento con Archivos Grandes	Media	Medio	Medio	2
R-003	Vulnerabilidades de Seguridad	Baja	Crítico	Alto	1
R-004	Problemas de Base de Datos	Baja	Alto	Medio	2
R-005	Disponibilidad Limitada del Equipo	Alta	Medio	Alto	1
R-006	Falta de Conocimiento Técnico Específico	Media	Medio	Medio	3

ID	Riesgo	Probabilidad	Impacto	Nivel	Prioridad
R-007	Conflictos Interpersonales	Baja	Medio	Bajo	4
R-008	Retrasos en Entregas	Alta	Alto	Crítico	1
R-009	Cambios de Requerimientos	Media	Alto	Alto	1
R-010	Dependencias Externas	Baja	Medio	Bajo	4
R-011	Bugs Críticos en Producción	Media	Crítico	Alto	1
R-012	Problemas de Usabilidad	Media	Medio	Medio	3
R-013	Problemas de Rendimiento	Media	Medio	Medio	3
R-014	Ataques de Seguridad	Baja	Crítico	Alto	1
R-015	Pérdida de Datos	Baja	Crítico	Alto	1
R-016	Falta de Adopción por Usuarios	Media	Alto	Alto	1
R-017	Cambios en Requerimientos del Negocio	Media	Alto	Alto	1

3.2 Escalas de Evaluación

3.2.1 Probabilidad

- **Muy Baja (1):** < 10% de probabilidad
- **Baja (2):** 10-30% de probabilidad
- **Media (3):** 30-60% de probabilidad
- **Alta (4):** 60-80% de probabilidad
- **Muy Alta (5):** > 80% de probabilidad

3.2.2 Impacto

- **Muy Bajo (1):** Impacto mínimo en el proyecto
- **Bajo (2):** Impacto menor, fácil de manejar
- **Medio (3):** Impacto moderado, requiere atención
- **Alto (4):** Impacto significativo, puede afectar objetivos
- **Crítico (5):** Impacto severo, puede causar falla del proyecto

3.2.3 Nivel de Riesgo

- **Muy Bajo (1-2):** Riesgo aceptable
- **Bajo (3-4):** Riesgo bajo, monitorear
- **Medio (5-6):** Riesgo medio, mitigar
- **Alto (7-8):** Riesgo alto, mitigar activamente
- **Crítico (9-10):** Riesgo crítico, mitigar inmediatamente

---

4. ESTRATEGIAS DE MITIGACIÓN

4.1 Riesgos Críticos (Nivel 9-10)

R-008: Retrasos en Entregas

Estrategia de Mitigación:

- **Prevención:**
    - Estimaciones realistas con buffer del 20%
    - Revisión semanal del cronograma
    - Identificación temprana de problemas
    - Comunicación proactiva con stakeholders
- **Contingencia:**
    - Priorización de funcionalidades críticas
    - Redistribución de recursos
    - Extensión de cronograma si es necesario
    - Comunicación transparente de retrasos

Responsable: Irvin Osvaldo
Fecha de Implementación: Inmediata
Costo Estimado: $0 (recursos internos)

4.2 Riesgos Altos (Nivel 7-8)

R-001: Problemas de Integración Frontend-Backend

Estrategia de Mitigación:

- **Prevención:**
    - Definición clara de APIs desde el inicio
    - Desarrollo de mocks para testing
    - Integración continua con pruebas automatizadas
    - Documentación detallada de APIs
- **Contingencia:**
    - Sesiones de debugging en parejas

    - Consulta con expertos externos
    - Refactoring de código si es necesario
    - Implementación de fallbacks

Responsable: Ángel Valentín, Kevin Antonio
Fecha de Implementación: Semana 2
Costo Estimado: $200 (herramientas de testing)

R-003: Vulnerabilidades de Seguridad

Estrategia de Mitigación:

- **Prevención:**
    - Auditoría de seguridad regular
    - Implementación de mejores prácticas
    - Validación de entrada en todos los campos
    - Encriptación de datos sensibles
- **Contingencia:**
    - Parcheo inmediato de vulnerabilidades
    - Consulta con expertos en seguridad
    - Implementación de medidas adicionales
    - Notificación a usuarios si es necesario

Responsable: Alberto, Irvin Osvaldo
Fecha de Implementación: Semana 1
Costo Estimado: $300 (herramientas de seguridad)

R-005: Disponibilidad Limitada del Equipo

Estrategia de Mitigación:

- **Prevención:**
    - Planificación flexible de horarios
    - Documentación detallada del trabajo
    - Distribución equilibrada de responsabilidades
    - Comunicación proactiva sobre disponibilidad
- **Contingencia:**
    - Redistribución de tareas
    - Extensión de cronograma si es necesario
    - Búsqueda de recursos adicionales
    - Priorización de tareas críticas

Responsable: Irvin Osvaldo
Fecha de Implementación: Inmediata
Costo Estimado: $0 (recursos internos)

R-009: Cambios de Requerimientos

Estrategia de Mitigación:

- **Prevención:**
    - Análisis detallado de requerimientos iniciales
    - Comunicación regular con stakeholders
    - Prototipos tempranos para validación
    - Proceso formal de control de cambios
- **Contingencia:**
    - Evaluación de impacto de cambios
    - Ajuste de cronograma y recursos
    - Comunicación transparente de impactos
    - Priorización de cambios críticos

Responsable: Irvin Osvaldo, Ángel Valentín
Fecha de Implementación: Semana 1
Costo Estimado: $0 (recursos internos)

R-011: Bugs Críticos en Producción

Estrategia de Mitigación:

- **Prevención:**
    - Pruebas exhaustivas en todos los niveles
    - Code review obligatorio
    - Pruebas de regresión automatizadas
    - Ambiente de staging idéntico a producción
- **Contingencia:**
    - Plan de rollback rápido
    - Equipo de respuesta 24/7
    - Comunicación inmediata a usuarios
    - Corrección prioritaria de bugs críticos

Responsable: Todo el equipo
Fecha de Implementación: Semana 3
Costo Estimado: $500 (herramientas de testing)

R-014: Ataques de Seguridad

Estrategia de Mitigación:

- **Prevención:**
    - Implementación de medidas de seguridad robustas

    - Monitoreo continuo de seguridad
    - Actualizaciones regulares de seguridad
    - Capacitación del equipo en seguridad

- **Contingencia:**

    - Plan de respuesta a incidentes
    - Aislamiento inmediato de sistemas afectados
    - Notificación a autoridades si es necesario
    - Restauración de servicios seguros

Responsable: Alberto, Irvin Osvaldo
Fecha de Implementación: Semana 1
Costo Estimado: $400 (herramientas de monitoreo)

R-015: Pérdida de Datos

Estrategia de Mitigación:

- **Prevención:**

    - Respaldos automáticos diarios
    - Almacenamiento en múltiples ubicaciones
    - Pruebas regulares de restauración
    - Monitoreo de integridad de datos

- **Contingencia:**

    - Plan de recuperación de desastres
    - Restauración inmediata desde respaldos
    - Comunicación a usuarios afectados
    - Análisis de causa raíz

Responsable: Alberto
Fecha de Implementación: Semana 2
Costo Estimado: $200 (servicios de respaldo)

R-016: Falta de Adopción por Usuarios

Estrategia de Mitigación:

- **Prevención:**

    - Involucrar usuarios en el diseño
    - Capacitación adecuada
    - Interfaz intuitiva y fácil de usar
    - Comunicación clara de beneficios

- **Contingencia:**

    - Programas de capacitación adicionales

    - Mejoras basadas en feedback
    - Incentivos para uso del sistema
    - Soporte personalizado

Responsable: Kevin Antonio, Irvin Osvaldo
Fecha de Implementación: Semana 4
Costo Estimado: $300 (capacitación y materiales)

R-017: Cambios en Requerimientos del Negocio

Estrategia de Mitigación:

- **Prevención:**
    - Análisis detallado de necesidades del negocio
    - Comunicación regular con stakeholders
    - Prototipos para validación temprana
    - Arquitectura flexible
- **Contingencia:**
    - Proceso ágil de adaptación
    - Revisión de prioridades
    - Ajuste de cronograma y recursos
    - Comunicación transparente de impactos

Responsable: Irvin Osvaldo, Ángel Valentín
Fecha de Implementación: Semana 1
Costo Estimado: $0 (recursos internos)

4.3 Riesgos Medios (Nivel 5-6)

R-002: Problemas de Rendimiento con Archivos Grandes

Estrategia de Mitigación:

- **Prevención:**
    - Optimización de algoritmos de procesamiento
    - Implementación de compresión de archivos
    - Límites de tamaño de archivo
    - Procesamiento asíncrono
- **Contingencia:**
    - Escalado horizontal de servidores
    - Implementación de CDN
    - Optimización adicional de código
    - Monitoreo de rendimiento

Responsable: Ángel Valentín, Alberto
Fecha de Implementación: Semana 6
Costo Estimado: $150 (herramientas de optimización)

R-004: Problemas de Base de Datos

Estrategia de Mitigación:

- **Prevención:**
    - Optimización de consultas
    - Implementación de índices apropiados
    - Monitoreo de rendimiento
    - Respaldos regulares
- **Contingencia:**
    - Optimización de consultas problemáticas
    - Escalado de base de datos
    - Restauración desde respaldos
    - Consulta con expertos

Responsable: Alberto, Ángel Valentín
Fecha de Implementación: Semana 4
Costo Estimado: $100 (herramientas de monitoreo)

R-012: Problemas de Usabilidad

Estrategia de Mitigación:

- **Prevención:**
    - Pruebas de usabilidad con usuarios reales
    - Diseño centrado en el usuario
    - Prototipos iterativos
    - Feedback continuo
- **Contingencia:**
    - Mejoras basadas en feedback
    - Rediseño de interfaces problemáticas
    - Capacitación adicional de usuarios
    - Documentación mejorada

Responsable: Kevin Antonio
Fecha de Implementación: Semana 8
Costo Estimado: $200 (herramientas de testing de usabilidad)

R-013: Problemas de Rendimiento

Estrategia de Mitigación:

- **Prevención:**
    - Optimización de código
    - Implementación de caché
    - Monitoreo de rendimiento
    - Pruebas de carga
- **Contingencia:**
    - Optimización adicional
    - Escalado de infraestructura
    - Implementación de CDN
    - Consulta con expertos

Responsable: Todo el equipo
Fecha de Implementación: Semana 6
Costo Estimado: $250 (herramientas de monitoreo)

4.4 Riesgos Bajos (Nivel 3-4)

R-006: Falta de Conocimiento Técnico Específico

Estrategia de Mitigación:

- **Prevención:**
    - Capacitación del equipo
    - Consulta con expertos
    - Documentación detallada
    - Práctica con tecnologías
- **Contingencia:**
    - Capacitación adicional
    - Consulta con expertos externos
    - Cambio de tecnologías si es necesario
    - Extensión de cronograma

Responsable: Todo el equipo
Fecha de Implementación: Semana 2
Costo Estimado: $400 (cursos y consultoría)

R-007: Conflictos Interpersonales

Estrategia de Mitigación:

- **Prevención:**
    - Comunicación clara y regular
    - Definición clara de roles
    - Actividades de team building

    - Resolución proactiva de conflictos

- **Contingencia:**

    - Mediación de conflictos
    - Reorganización del equipo
    - Capacitación en comunicación
    - Consulta con recursos humanos

Responsable: Irvin Osvaldo
Fecha de Implementación: Inmediata
Costo Estimado: $100 (actividades de team building)

R-010: Dependencias Externas

Estrategia de Mitigación:

- **Prevención:**

    - Evaluación de proveedores
    - Contratos con SLA claros
    - Planes de contingencia
    - Monitoreo de servicios

- **Contingencia:**

    - Cambio de proveedores
    - Implementación de alternativas
    - Desarrollo de soluciones internas
    - Negociación de SLA

Responsable: Alberto, Irvin Osvaldo
Fecha de Implementación: Semana 3
Costo Estimado: $300 (servicios alternativos)

---

5. PLAN DE MONITOREO

5.1 Frecuencia de Monitoreo

5.1.1 Monitoreo Diario

Riesgos Monitoreados:

- R-005: Disponibilidad del equipo
- R-008: Retrasos en entregas
- R-011: Bugs críticos en producción
- R-014: Ataques de seguridad
- R-015: Pérdida de datos

Actividades:

- Revisión de métricas de rendimiento
- Verificación de disponibilidad del equipo
- Monitoreo de logs de seguridad
- Verificación de respaldos

5.1.2 Monitoreo Semanal

Riesgos Monitoreados:

- R-001: Problemas de integración
- R-002: Problemas de rendimiento
- R-004: Problemas de base de datos
- R-009: Cambios de requerimientos
- R-012: Problemas de usabilidad

Actividades:

- Revisión de progreso del proyecto
- Análisis de métricas de calidad
- Evaluación de satisfacción del usuario
- Revisión de cronograma

5.1.3 Monitoreo Mensual

Riesgos Monitoreados:

- R-003: Vulnerabilidades de seguridad
- R-006: Falta de conocimiento técnico
- R-007: Conflictos interpersonales
- R-010: Dependencias externas
- R-016: Falta de adopción por usuarios
- R-017: Cambios en requerimientos del negocio

Actividades:

- Auditoría de seguridad
- Evaluación del equipo
- Análisis de satisfacción del usuario
- Revisión de estrategias de mitigación

5.2 Herramientas de Monitoreo

5.2.1 Monitoreo Técnico

- **GitHub:** Control de versiones y colaboración
- **SonarQube:** Análisis de calidad de código
- **New Relic:** Monitoreo de aplicaciones
- **Sentry:** Monitoreo de errores
- **Lighthouse:** Métricas de rendimiento web

5.2.2 Monitoreo de Proyecto

- **Jira/Trello:** Gestión de tareas y cronograma
- **Slack/Teams:** Comunicación del equipo
- **Google Analytics:** Métricas de uso
- **SurveyMonkey:** Encuestas de satisfacción

5.2.3 Monitoreo de Seguridad

- **OWASP ZAP:** Pruebas de seguridad
- **Nmap:** Escaneo de puertos
- **Wireshark:** Análisis de tráfico de red
- **Logwatch:** Análisis de logs del sistema

5.3 Reportes de Riesgos

5.3.1 Reporte Diario

Contenido:

- Estado de riesgos críticos
- Métricas de rendimiento
- Alertas de seguridad
- Disponibilidad del equipo

Audiencia: Líder de proyecto **Formato:** Email/chat **Duración:** 5 minutos

5.3.2 Reporte Semanal

Contenido:

- Estado de todos los riesgos
- Progreso de mitigaciones
- Nuevos riesgos identificados
- Recomendaciones

Audiencia: Todo el equipo **Formato:** Reunión + documento **Duración:** 30 minutos

5.3.3 Reporte Mensual

Contenido:

- Análisis de tendencias
- Efectividad de mitigaciones
- Nuevas estrategias
- Actualización de matriz de riesgos

Audiencia: Stakeholders **Formato:** Presentación + documento **Duración:** 1 hora

---

6. COSTOS DE MITIGACIÓN

6.1 Resumen de Costos

Categoría	Costo Estimado	Justificación
Herramientas de Testing	$500	Pruebas automatizadas y de calidad
Herramientas de Seguridad	$700	Auditoría y monitoreo de seguridad
Herramientas de Monitoreo	$350	Monitoreo de rendimiento y errores
Capacitación del Equipo	$400	Cursos y consultoría técnica
Servicios de Respaldo	$200	Respaldos automáticos y recuperación
Herramientas de Usabilidad	$200	Testing de usabilidad y UX
Team Building	$100	Actividades de integración del equipo
Servicios Alternativos	$300	Dependencias externas de respaldo
TOTAL	**$2,750**	**Mitigación completa de riesgos**

6.2 Análisis Costo-Beneficio

6.2.1 Beneficios de la Mitigación

- **Reducción de retrasos:** $5,000 (valor del tiempo ahorrado)
- **Prevención de pérdida de datos:** $10,000 (valor de los datos)
- **Mejora de seguridad:** $3,000 (prevención de ataques)
- **Mejora de calidad:** $2,000 (reducción de bugs)
- **Mejora de productividad:** $4,000 (eficiencia del equipo)

Total de Beneficios: $24,000

6.2.2 ROI de la Mitigación

- **Inversión:** $2,750
- **Beneficios:** $24,000
- **ROI:** 773%
- **Período de Recuperación:** 1.4 meses

---

7. CONCLUSIONES Y RECOMENDACIONES

7.1 Conclusiones Principales

1. **Riesgos Críticos Identificados:** Se identificaron 9 riesgos críticos que requieren atención inmediata
2. **Mitigación Efectiva:** Las estrategias propuestas pueden reducir significativamente el impacto de los riesgos
3. **ROI Positivo:** La inversión en mitigación tiene un ROI del 773%
4. **Monitoreo Continuo:** Es esencial mantener un monitoreo constante de los riesgos

7.2 Recomendaciones

7.2.1 Implementación Inmediata

- Implementar medidas de seguridad básicas
- Establecer proceso de control de cambios
- Configurar monitoreo de riesgos críticos
- Iniciar capacitación del equipo

7.2.2 Implementación a Corto Plazo (1-2 semanas)

- Implementar herramientas de testing
- Configurar respaldos automáticos
- Establecer monitoreo de rendimiento
- Iniciar pruebas de usabilidad

7.2.3 Implementación a Mediano Plazo (1-2 meses)

- Implementar herramientas de seguridad avanzadas
- Completar capacitación del equipo
- Establecer monitoreo completo
- Implementar mejoras de rendimiento

7.3 Próximos Pasos

1. **Aprobación del Plan:** Obtener aprobación de stakeholders
2. **Asignación de Recursos:** Asignar responsables y presupuesto
3. **Implementación:** Ejecutar estrategias de mitigación
4. **Monitoreo:** Iniciar monitoreo continuo
5. **Revisión:** Revisar y actualizar el plan regularmente

---

8. ANEXOS

Anexo A: Matriz de Riesgos Detallada

ID	Riesgo	Prob	Imp	Nivel	Estrategia	Responsable	Costo	Fecha
R-001	Integración Frontend-Backend	3	4	7	Prevención + Contingencia	Ángel, Kevin	$200	Sem 2
R-002	Rendimiento Archivos Grandes	3	3	6	Prevención + Contingencia	Ángel, Alberto	$150	Sem 6
R-003	Vulnerabilidades Seguridad	2	5	7	Prevención + Contingencia	Alberto, Irvin	$300	Sem 1
R-004	Problemas Base de Datos	2	4	6	Prevención + Contingencia	Alberto, Ángel	$100	Sem 4

ID	Riesgo	Prob	Imp	Nivel	Estrategia	Responsable	Costo	Fecha
R-005	Disponibilidad Equipo	4	3	7	Prevención + Contingencia	Irvin	$0	Inmediata
R-006	Falta Conocimiento Técnico	3	3	6	Prevención + Contingencia	Todo equipo	$400	Sem 2
R-007	Conflictos Interpersonales	2	3	5	Prevención + Contingencia	Irvin	$100	Inmediata
R-008	Retrasos Entregas	4	4	8	Prevención + Contingencia	Irvin	$0	Inmediata
R-009	Cambios Requerimientos	3	4	7	Prevención + Contingencia	Irvin, Ángel	$0	Sem 1
R-010	Dependencias Externas	2	3	5	Prevención + Contingencia	Alberto, Irvin	$300	Sem 3
R-011	Bugs Críticos Producción	3	5	8	Prevención + Contingencia	Todo equipo	$500	Sem 3
R-012	Problemas Usabilidad	3	3	6	Prevención + Contingencia	Kevin	$200	Sem 8
R-013	Problemas Rendimiento	3	3	6	Prevención + Contingencia	Todo equipo	$250	Sem 6
R-014	Ataques Seguridad	2	5	7	Prevención + Contingencia	Alberto, Irvin	$400	Sem 1
R-015	Pérdida Datos	2	5	7	Prevención + Contingencia	Alberto	$200	Sem 2
R-016	Falta Adopción Usuarios	3	4	7	Prevención + Contingencia	Kevin, Irvin	$300	Sem 4
R-017	Cambios Requerimientos Negocio	3	4	7	Prevención + Contingencia	Irvin, Ángel	$0	Sem 1

Anexo B: Cronograma de Implementación

Semana	Actividades	Responsable	Costo
1	Seguridad básica, Control de cambios	Alberto, Irvin	$700
2	Integración, Conocimiento técnico	Ángel, Kevin, Todo	$600
3	Testing, Dependencias externas	Todo equipo, Alberto	$800
4	Base de datos, Adopción usuarios	Alberto, Kevin	$500

Semana	Actividades	Responsable	Costo
6	Rendimiento, Optimización	Ángel, Alberto, Todo	$400
8	Usabilidad, Mejoras UX	Kevin	$200

Anexo C: Referencias

- PMBOK Guide - Project Management Institute
- ISO 31000:2018 - Risk Management
- NIST SP 800-30 - Risk Assessment Guide
- OWASP Risk Rating Methodology

Documento elaborado por: Equipo de Desarrollo TESCHI
Fecha de creación: [Fecha actual]
Última actualización: [Fecha actual]
Próxima revisión: [Fecha + 1 mes]