REGISTRO DE RIESGOS

DOSSIER DE INGENIERÍA

Código: DOC-RSK-001
Estado: VIGENTE
Clasificación: INTERNO

Ambato – Ecuador
28/01/2026

CONTROL DE DOCUMENTO

PROPIEDAD	**DETALLE**
Código	DOC-RSK-001
Proyecto	_____
Versión	1.0
Estado	VIGENTE
Clasificación	INTERNO
Última Revisión	_____
Responsable	Project Manager

HISTORIAL DE VERSIONES

Versión	**Fecha**	**Autor**	**Descripción del Cambio**	**Revisado por**
1.0	_____	_____	Creación inicial del registro de riesgos	_____

APROBACIÓN

Rol	**Nombre**	**Firma**
Project Manager	_____	_____
Tech Lead	_____	_____
QA Lead	_____	_____

Contenido

1. PROPÓSITO 4
2. METODOLOGÍA DE EVALUACIÓN 4
2.1 Escala de Probabilidad 4
2.2 Escala de Impacto 4
2.3 Cálculo de Severidad 4
3. ESTRATEGIAS DE RESPUESTA 5
4. MATRIZ DE RIESGOS 5
5. REGLAS DE GOBIERNO 6
6. INTEGRACIÓN CON OTROS DOCUMENTOS 6

1. PROPÓSITO

Este documento identifica, evalúa y controla los riesgos del proyecto con el objetivo de reducir su impacto sobre:

- Alcance
- Tiempo
- Costo
- Calidad
- Seguridad

Este registro es un documento vivo y debe revisarse al menos una vez por semana.

2. METODOLOGÍA DE EVALUACIÓN

2.1 ESCALA DE PROBABILIDAD

Valor	Descripción
1	Muy baja
2	Baja
3	Media
4	Alta
5	Muy alta

2.2 ESCALA DE IMPACTO

Valor	Descripción
1	Impacto mínimo
2	Bajo
3	Medio
4	Alto
5	Crítico

2.3 CÁLCULO DE SEVERIDAD

Severidad = Probabilidad × Impacto

Rango	Nivel
1 – 5	Bajo

6 – 10	Medio
11 – 14	Alto
15 – 25	Crítico

3. ESTRATEGIAS DE RESPUESTA

- **Mitigar:** Reducir probabilidad o impacto.
- **Evitar:** Eliminar la causa.
- **Transferir:** Terceros, seguros, outsourcing.
- **Aceptar:** Asumir riesgo conscientemente.

4. MATRIZ DE RIESGOS

ID	Descripción del Riesgo	Prob	Imp	Severidad	Estrategia	Plan de Acción / Mitigación	Responsable	Estado
R-01	Retraso en entrega de API por tercero	4	5	20 (Crítico)	Mitigar	Crear mocks de API. Establecer contrato de fechas con proveedor.	Tech Lead	Abierto
R-02	Pérdida de datos durante migración	2	5	10 (Alto)	Evitar	Simulacros de migración. Backups completos.	DevOps	Abierto
R-03	Requisitos incompletos o ambiguos	3	4	12 (Alto)	Mitigar	Revisión cruzada del SRS. Firma cliente.	Analista	Abierto
R-04	Fuga de información sensible	2	5	10 (Alto)	Mitigar	Encriptación, RBAC, auditorías de seguridad.	Tech Lead	Abierto
R-05	Bajo rendimiento del sistema	3	4	12 (Alto)	Mitigar	Pruebas de carga tempranas. Cacheo.	QA Lead	Abierto
R-06	Rotación de personal	2	4	8 (Medio)	Mitigar	Documentación obligatoria. Code reviews.	PM	Abierto

R-07	Retraso por deuda técnica acumulada	3	3	9 (Medio)	Mitigar	Sprints de refactorización.	Tech Lead	Abierto
R-08	Fallas en pipeline CI/CD	2	3	6 (Medio)	Mitigar	Monitoreo pipeline. Rollback automático.	DevOps	Abierto
R-09	Incumplimiento de RNF de Seguridad	2	5	10	Mitigar	Análisis estático de código y pentesting temprano.	Tech Lead	Abierto
R-10	Degradación de Performance en carga	3	4	12	Mitigar	Pruebas de estrés y optimización de caché.	QA Lead	Abierto

5. REGLAS DE GOBIERNO

- Todo riesgo debe tener responsable.
- Todo riesgo debe tener plan de acción.
- Riesgos críticos se revisan semanalmente.
- Riesgos cerrados no se eliminan; se marcan como “cerrado”.

6. INTEGRACIÓN CON OTROS DOCUMENTOS

Este registro se vincula bidireccionalmente con:

- **DOC-PM-001 (Plan de Proyecto):** Referencia obligatoria para el control de hitos.
- **DOC-TRZ-001 (Matriz de Trazabilidad):** Los riesgos técnicos críticos deben estar vinculados a Requisitos No Funcionales (RNF).
- **DOC-TEST-002 (Casos de Prueba):** Los riesgos de alta severidad deben generar casos de prueba específicos para validar su mitigación.