| **ANÁLISIS DE RIESGOS** |
| --- |

| **N°** | **Riesgo identificado** | **Categoría PESTEL** | **Impacto (1-5)** | **Probabilidad (1-5)** | **Nivel de riesgo  (I x P)** |
| --- | --- | --- | --- | --- | --- |
| R1 | Fallas en el servidor de producción | Tecnológica | 5 | 3 | 15 |
| R2 | Cambios en las leyes de protección de datos | Legal | 4 | 2 | 8 |
| R3 | Dificultad para integrar los microservicios | Tecnológica | 4 | 4 | 16 |
| R4 | Baja adopción por parte de usuarios docentes | Social | 3 | 3 | 9 |
| R5 | Aumento en el costo de servicios en la nube | Económica | 3 | 4 | 12 |
| R6 | Pérdida de datos críticos por errores en el proceso de backup | Tecnológica | 5 | 2 | 10 |
| R7 | Errores en el manejo de pagos y facturación | Legal/Económica | 4 | 3 | 12 |
| R8 | Ataques de seguridad: SQL Injection o Cross Site Scripting (XSS) | Tecnológica | 5 | 4 | 20 |
| R9 | Caída del servicio por alta carga de usuarios concurrentes | Tecnológica | 4 | 3 | 12 |
| R10 | Retrasos en la entrega de módulos clave por parte del equipo de desarrollo | Organizacional | 4 | 4 | 16 |

| PROBABILIDAD | Constante (5) |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Moderado (4) |  |  |  |  |  |
| Ocasional (3) |  |  |  |  |  |
| Posible (2) |  |  |  |  |  |
| Improbable (1) |  |  |  |  |  |
|  |  | Insignificante (1) | Menor (2) | Crítico (3) | Mayor (4) | Catastrófico (5) |
|  |  | IMPACTO | | | | |

**Estrategias para afrontar cada uno de los riesgos:**

| **N°** | **Tipo (Alto / Medio / Bajo)** | **Riesgo identificado** | **Nivel de riesgo (I x P)** | **Estrategia de mitigación** |
| --- | --- | --- | --- | --- |
| R1 | Alto | Fallas en el servidor de producción | 15 | Implementar backups automáticos y redundancia en la arquitectura (clústeres y balanceo). |
| R2 | Medio | Cambios en las leyes de protección de datos | 8 | Revisar normativas actuales (como GDPR/Ley chilena) y ajustar políticas de privacidad. |
| R3 | Alto | Dificultad para integrar los microservicios | 16 | Usar API Gateway, Swagger y pruebas automatizadas para detectar errores de integración. |
| R4 | Medio | Baja adopción por parte de usuarios docentes | 9 | Realizar capacitaciones, tutoriales y pruebas piloto con retroalimentación. |
| R5 | Alto | Incremento en costos de nube | 12 | Optimizar el uso de recursos, usar instancias escalables y revisar presupuesto mensual. |
| R6 | Medio | Pérdida de datos por errores de backup | 10 | Programar backups diarios y pruebas de recuperación de datos periódicas. |
| R7 | Alto | Errores en el proceso de pagos | 12 | Validar las integraciones de pasarelas de pago, realizar pruebas de extremo a extremo. |
| R8 | Alto | Vulnerabilidades de seguridad | 20 | Realizar pruebas de penetración, implementar filtros de seguridad y validación de entradas. |
| R9 | Alto | Caída por sobrecarga de usuarios | 12 | Realizar pruebas de carga y aplicar escalado automático. |
| R10 | Alto | Retrasos en la entrega de módulos | 16 | Realizar seguimiento diario, implementar Scrum y tener revisiones semanales de avance. |