**RIESGO 12: Infraestructura mal dimensionada**

* **Tipo de riesgo:** Cuantitativo y técnico
* **Categoría:** Tecnología / Arquitectura de sistemas / Rendimiento
* **Descripción:** Este riesgo surge cuando la infraestructura técnica (servidores, redes, bases de datos, almacenamiento, servicios en la nube, etc.) no está dimensionada adecuadamente respecto a las necesidades reales del sistema, ya sea por exceso (sobrecostos) o por defecto (caídas, lentitud, interrupciones, pérdida de datos).

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Infraestructura mal dimensionada |
| Categoría | Tecnología / Rendimiento / Costos |
| Causas probables | Falta de pruebas de carga, mala estimación de usuarios concurrentes, errores en predicción de escalabilidad, decisiones sin datos históricos, ausencia de arquitecto de infraestructura. |
| Consecuencias | Caídas del sistema, lentitud, experiencia de usuario negativa, pérdida de datos, altos costos en servicios no utilizados, afectación reputacional. |
| Fuente | Fase de planeación técnica, despliegue en entornos productivos, pruebas insuficientes. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta (común en proyectos sin arquitecturas elásticas o escalables) |
| Impacto potencial | Crítico (puede interrumpir el servicio y/o incrementar drásticamente los costos) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Saturación de servidores, sobreuso o infrautilización de recursos, errores en tiempo real, respuesta lenta o inestable del sistema. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

**A. Medidas Preventivas (Antes del riesgo)**

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Realizar pruebas de carga y rendimiento antes del despliegue en producción. | QA / DevOps | JMeter, k6, Locust, Lighthouse |
| Diseñar una arquitectura escalable y elástica (autoscaling, contenedores). | Arquitecto / DevOps | AWS, Azure, Docker, Kubernetes |
| Estimar usuarios concurrentes y requerimientos de tráfico futuro. | PM / Cliente / UX | Analytics históricos, benchmarking |
| Validar infraestructura con pruebas piloto o MVPs controlados. | Dev / QA | Entorno staging, sandbox |
| Establecer métricas de uso y alertas antes del lanzamiento. | DevOps / QA | Grafana, Prometheus, New Relic |

**B. Medidas de Mitigación (Durante el riesgo)**

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Monitorear en tiempo real el consumo de recursos y ajustar según demanda. | DevOps | AWS CloudWatch, Azure Monitor, GCP Stackdriver |
| Activar mecanismos de autoescalado o instancias de respaldo. | DevOps / CTO | Load balancer, horizontal scaling |
| Implementar cachés y CDN para reducir carga directa. | Backend / DevOps | Redis, Varnish, Cloudflare, Amazon CloudFront |
| Priorizar funcionalidades críticas en caso de limitaciones. | PO / Dev | Modo degradado, feature flags |

**C. Medidas Correctivas (Después del riesgo)**

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Documentar el error de dimensionamiento y su origen. | QA / DevOps | RCA, informes de monitoreo |
| Redimensionar infraestructura según uso real. | DevOps / CTO | Ajuste de instancias, refactor de arquitectura |
| Establecer revisión periódica del dimensionamiento. | PMO / Arquitecto | Auditoría técnica, KPIs |
| Planificar migración a una arquitectura más eficiente o flexible. | Dirección / CTO | Infraestructura como código, serverless |

**1. Estimación de Pérdidas Económicas por Riesgo No Controlado**

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Caídas del sistema por falta de capacidad | Pérdida de ventas / interrupciones críticas | $30,000 MXN |
| Contratación urgente de recursos o servidores adicionales | Costos sobreestimados de emergencia | $12,000 MXN |
| Reputación y atención al cliente por fallos | Daño comercial y tiempo de soporte | $8,000 MXN |
| Refactorización posterior para escalar correctamente | 2 semanas de trabajo técnico | $24,000 MXN (2 devs × $6,000 × 2 semanas) |
| Total estimado de pérdidas económicas: |  | → **$74,000 MXN** |

**2. Costo de Implementación de Estrategias de Control**

**A. Costos de Medidas Preventivas (Antes del riesgo)**

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Pruebas de carga y estimación técnica | $3,000 MXN |
| Arquitectura escalable y entornos de prueba | $5,000 MXN |
| Estimaciones de tráfico y usuarios | $2,000 MXN |
| Configuración de alertas y dashboards de monitoreo | $3,000 MXN |
| 🟦 Total medidas preventivas: | **$13,000 MXN** |

**B. Costos de Medidas de Mitigación (Durante el riesgo)**

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Autoescalado y balanceo de carga | $4,000 MXN |
| Activación de instancias de emergencia | $3,000 MXN |
| Implementación de caché y CDN | $2,500 MXN |
| Monitoreo en tiempo real | $2,000 MXN |
| Total medidas de mitigación: | **$11,500 MXN** |

**C. Costos de Medidas Correctivas (Después del riesgo)**

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Análisis posterior y documentación del fallo | $1,500 MXN |
| Refactorización y redimensionamiento | $6,000 MXN |
| Revisión periódica y migración futura (planificación técnica) | $3,000 MXN |
| Total medidas correctivas: | **$10,500 MXN** |

**Resumen Económico del Plan de Contingencia**

|  |  |
| --- | --- |
| Categoría | Costo estimado |
| 🛡️ Prevención | $13,000 MXN |
| 🚨 Mitigación | $11,500 MXN |
| 🔄 Recuperación | $10,500 MXN |
| 💥 Costo de no hacer nada | $74,000 MXN |

**📈 Análisis Costo-Beneficio**

**Costo total de implementar todas las estrategias:**  
$13,000 + $11,500 + $10,500 = **$35,000 MXN**

**Ahorro potencial si se previene o controla el riesgo:**  
$74,000 – $35,000 = **$39,000 MXN**

**(≈ 52.7% de retorno sobre la inversión en mitigación)**