**RIESGO 2: Incompatibilidad con el entorno de producción**

* **Tipo de riesgo:** Técnico / Infraestructura
* **Categoría:** Configuración / Integración / Entrega
* **Descripción:** Este riesgo ocurre cuando el software que ha sido probado y validado en ambientes de desarrollo o staging no se comporta de manera consistente en el entorno de producción, debido a diferencias de configuración, versiones de dependencias, variables de entorno o infraestructura.

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Incompatibilidad con el entorno de producción |
| Categoría | Infraestructura / Entrega / DevOps |
| Causas probables | Ambientes inconsistentes, configuración manual, dependencias desalineadas, infraestructura no replicable. |
| Consecuencias | Fallos en ejecución de la aplicación, errores en tiempo de ejecución, tiempos de recuperación prolongados, interrupciones del servicio. |
| Fuente | Entornos de staging distintos al productivo, gestión deficiente de variables y versiones, pruebas poco realistas. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Alta |
| Impacto potencial | Alto (puede provocar fallas críticas no previstas en staging) |
| Nivel de riesgo | Alto |
| Indicadores de riesgo | Fallos que no ocurren en QA pero sí en producción, errores de configuración en deploys, diferencias en sistema operativo o librerías. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Estandarizar ambientes con infraestructura como código. | DevOps | Docker, Terraform, Ansible |
| Validar imágenes y configuraciones con staging idéntico a producción. | QA / DevOps | Docker Compose, Kubernetes, entornos espejo |
| Gestionar versiones de dependencias y variables de entorno por ambiente. | Desarrolladores | .env, Helm Charts, archivos de configuración |
| Establecer procesos de validación cruzada de entorno antes del deploy. | QA / Líder Técnico | Scripts de validación, checklist de entorno |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Activar mecanismos de rollback o reintento controlado. | DevOps | Backups, versiones previas, snapshots |
| Identificar y aislar módulos o servicios con fallos. | QA / Dev | Logs, monitoreo, observabilidad |
| Cambiar configuración en caliente si la plataforma lo permite. | DevOps | Feature flags, gestores de configuración |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Documentar causas y ajustar los entornos de preproducción. | QA / Líder Técnico | Postmortem, revisión de infraestructura |
| Ajustar versiones, librerías o configuraciones detectadas. | Dev / DevOps | ConfigMaps, control de dependencias |
| Implementar pruebas automatizadas que validen entorno y dependencias. | QA / Dev | Test de integración, test de ambiente |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Fallo de servicios por incompatibilidad en producción | Soporte de emergencia, pérdida de funcionalidad | $40,000 MXN |
| Reversión y reprocesamiento de datos | Tiempos operativos adicionales, horas hombre | $25,000 MXN |
| Afectación a usuarios y reputación | Soporte adicional, pérdida de confianza | $15,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$80,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Estándar de ambientes y uso de Docker/Kubernetes | $6,500 MXN |
| Validación cruzada de staging y producción | $4,000 MXN |
| Gestión de versiones y configuración automática | $3,000 MXN |
| 🛡️ Total medidas preventivas: | **$13,500 MXN** |

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Rollback o redirección de tráfico | $3,500 MXN |
| Diagnóstico de entorno y ajustes live | $2,000 MXN |
| 🚨 Total medidas de mitigación: | **$5,500 MXN** |

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Análisis de causas y ajuste de ambientes | $3,000 MXN |
| Refactor de configuración y dependencias | $4,000 MXN |
| 🔄 Total medidas correctivas: | **$7,000 MXN** |

**Resumen Económico del Plan de Contingencia**

|  |  |
| --- | --- |
| Categoría | Costo estimado |
| 🛡️ Prevención | $13,500 MXN |
| 🚨 Mitigación | $5,500 MXN |
| 🔄 Recuperación | $7,000 MXN |
| 💥 Costo de no hacer nada | $80,000 MXN |

**📈 Análisis Costo-Beneficio**

**Costo total de implementar todas las estrategias:**  
$13,500 + $5,500 + $7,000 = **$26,000 MXN**

**Ahorro potencial si se previene o controla el riesgo:**  
$80,000 – $26,000 = **$54,000 MXN**

**(≈ 208% de retorno sobre inversión en homologación de entornos y pruebas previas)**