**RIESGO 14: Librerías de terceros sin mantenimiento**

* **Tipo de riesgo:** Técnico / Dependencias externas
* **Categoría:** Seguridad / Actualización / Confiabilidad
* **Descripción:** Este riesgo ocurre cuando se integran al proyecto librerías de terceros (NPM, PyPI, Maven, etc.) que han sido abandonadas, no tienen actualizaciones, presentan vulnerabilidades sin parches, o son incompatibles con nuevas versiones del entorno. Esto puede comprometer la seguridad, funcionalidad y estabilidad del sistema.

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Librerías de terceros sin mantenimiento |
| Categoría | Dependencias / Seguridad / Soporte |
| Causas probables | Selección sin validación de mantenibilidad, librerías open source sin comunidad activa. |
| Consecuencias | Incompatibilidad futura, vulnerabilidades, problemas de compilación, fallas silenciosas. |
| Fuente | Dependencias en package.json, requirements.txt, módulos externos, plugins y SDKs abandonados. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Alta |
| Impacto potencial | Alto (afecta seguridad, rendimiento, soporte técnico y continuidad del desarrollo) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Dependencias con más de 1 año sin actualizaciones, issues no resueltos, sin actividad en GitHub. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Verificar actividad y mantenimiento de cada librería antes de integrarla. | Dev / QA | npm trends, GitHub insights, libraries.io |
| Establecer una política de validación de dependencias externas. | Líder Técnico | Checklist interno, procesos de revisión |
| Priorizar librerías con comunidad activa y alternativas bien soportadas. | Dev / PM | StackShare, Openbase, DevRank |
| Mantener inventario actualizado de dependencias por proyecto. | DevOps / QA | OWASP Dependency-Track, SBOM (CycloneDX) |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Detectar librerías obsoletas con escaneo automático. | QA / DevOps | npm audit, Snyk, Sonatype, OWASP tools |
| Evaluar impacto de actualización o sustitución. | Dev | Tests de regresión, changelogs |
| Crear wrappers para facilitar sustitución futura de librerías no críticas. | Dev | Patrones Adapter, Facade |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Sustituir las librerías descontinuadas por alternativas seguras. | Dev / QA | React-dropzone → FilePond, etc. |
| Aislar y refactorizar las partes del sistema que dependían de estas. | Dev Backend | Interfaces, componentes reutilizables |
| Documentar decisiones y cambios en el stack tecnológico. | PM / Líder Técnico | Confluence, READMEs, changelogs |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Vulnerabilidad explotada por librería | Brecha de seguridad, daño reputacional | $50,000 MXN |
| Retrabajo por incompatibilidad grave | Refactorización y urgencia en producción | $25,000 MXN |
| Caídas por falta de soporte | Interrupción del servicio, soporte no disponible | $20,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$95,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Investigación y validación de cada librería | $3,500 MXN |
| Política de dependencias y revisión semestral | $2,500 MXN |
| Capacitación en gestión de dependencias externas | $3,000 MXN |
| 🛡️ Total medidas preventivas: | **$9,000 MXN** |

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Implementación de escaneo continuo | $3,000 MXN |
| Evaluación de impacto y ajustes | $2,500 MXN |
| 🚨 Total medidas de mitigación: | **$5,500 MXN** |

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Sustitución de librerías y refactor | $4,000 MXN |
| Actualización de documentación técnica | $2,000 MXN |
| Pruebas y validación de estabilidad post-cambio | $2,500 MXN |
| 🔄 Total medidas correctivas: | **$8,500 MXN** |

**Resumen Económico del Plan de Contingencia**

|  |  |
| --- | --- |
| Categoría | Costo estimado |
| 🛡️ Prevención | $9,000 MXN |
| 🚨 Mitigación | $5,500 MXN |
| 🔄 Recuperación | $8,500 MXN |
| 💥 Costo de no hacer nada | $95,000 MXN |

**📈 Análisis Costo-Beneficio**

**Costo total de implementar todas las estrategias:**  
$9,000 + $5,500 + $8,500 = **$23,000 MXN**

**Ahorro potencial si se previene o controla el riesgo:**  
$95,000 – $23,000 = **$72,000 MXN**

**(≈ 313% de retorno sobre inversión en manejo de dependencias)**