**Vulnerabilidades por librerías desactualizadas**

* **Tipo de riesgo:** Técnico / Seguridad / Desarrollo
* **Categoría:** Dependencias / Mantenimiento / Seguridad de software

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Vulnerabilidades por librerías desactualizadas |
| Categoría | Desarrollo / Seguridad / Mantenimiento |
| Causas probables | Uso de librerías con fallos conocidos, falta de actualización continua, dependencia de versiones no soportadas, falta de monitoreo de vulnerabilidades. |
| Consecuencias | Exposición a ataques conocidos, fallos de seguridad explotables, pérdida de integridad y confidencialidad, incumplimiento normativo. |
| Fuente | Análisis de dependencias, alertas de seguridad (CVE), auditorías de código, reportes de vulnerabilidades. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta (muy común en proyectos sin mantenimiento constante) |
| Impacto potencial | Alto (puede facilitar accesos no autorizados o fallos críticos) |
| Nivel de riesgo | Alto |
| Indicadores de riesgo | Alertas CVE sin atender, versiones antiguas, falta de parches, bibliotecas no compatibles. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar escaneo automático de dependencias | Dev / QA | OWASP Dependency-Check, Snyk, WhiteSource |
| Establecer políticas de actualización periódica | PM / Dev | Roadmaps, calendarios de mantenimiento |
| Revisar y evaluar nuevas versiones antes de integración | QA / Dev | Testing automatizado, entornos staging |
| Capacitar al equipo en gestión de vulnerabilidades | Recursos Humanos | Cursos, talleres de seguridad |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Aplicar parches o actualizaciones urgentes | DevOps / Dev | Gestión de versiones, CI/CD pipelines |
| Revertir versiones problemáticas | DevOps / QA | Control de versiones, rollback |
| Aislar componentes vulnerables temporalmente | Arquitecto / Dev | Contenedores, microservicios |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Auditoría completa de todas las dependencias | QA / Seguridad | Escáneres de seguridad, informes CVE |
| Refactorización para eliminar dependencias obsoletas | Dev / Arquitecto | Revisión de código, planificación |
| Integrar escaneo continuo como parte del ciclo de vida | DevOps / QA | Integración en pipelines CI/CD |

**4. ESTIMACIÓN DE PÉRDIDAS ECONÓMICAS POR RIESGO NO CONTROLADO**

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Explotación de vulnerabilidad para acceso no autorizado | Robo o modificación de datos | $35,000 MXN |
| Tiempo de respuesta a incidentes y remediación | Horas-hombre, parches de emergencia | $20,000 MXN |
| Daño reputacional y pérdida de confianza | Usuarios insatisfechos y abandono | $15,000 MXN |
| Costos legales por incumplimiento | Multas y asesoría legal | $10,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$80,000 MXN** |

**5. COSTO DE IMPLEMENTACIÓN DE ESTRATEGIAS DE CONTROL**

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Implementación de escaneo automático | $3,000 MXN |
| Políticas y calendarios de actualización | $1,500 MXN |
| Pruebas y validación en entornos controlados | $2,000 MXN |
| Capacitación en gestión de dependencias | $2,000 MXN |
| Total medidas preventivas: | → $8,500 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Aplicación urgente de parches | $3,000 MXN |
| Rollback de versiones problemáticas | $2,000 MXN |
| Aislamiento temporal de módulos vulnerables | $1,500 MXN |
| Total medidas de mitigación: | → $6,500 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Auditoría exhaustiva de dependencias | $3,000 MXN |
| Refactorización para actualización y eliminación | $4,000 MXN |
| Integración de escaneo continuo en CI/CD | $2,500 MXN |
| Total medidas correctivas: | → $9,500 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $8,500 MXN |
| 🚨 Mitigación | $6,500 MXN |
| 🔄 Recuperación | $9,500 MXN |
| 💥 Costo de no hacer nada | $80,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $8,500 + $6,500 + $9,500 = **$24,500 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $80,000 – $24,500 = **$55,500 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **226% de ROI**