**Ataques por inyección SQL**

* **Tipo de riesgo:** Técnico / Seguridad
* **Categoría:** Desarrollo inseguro / Integridad de datos / Acceso no autorizado

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Ataques por inyección SQL |
| Categoría | Seguridad / Desarrollo / Base de datos |
| Causas probables | Falta de validación de entradas, concatenación de queries SQL, uso de librerías obsoletas, ausencia de prácticas seguras de codificación. |
| Consecuencias | Acceso no autorizado, modificación o eliminación de datos, fuga de información, corrupción de base de datos, impacto legal y reputacional. |
| Fuente | Análisis de código fuente, auditorías de seguridad, pruebas de penetración, informes de incidentes. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Alta (frecuente en sistemas sin validación robusta) |
| Impacto potencial | Crítico (puede implicar control total sobre la base de datos) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Consultas SQL dinámicas con entradas directas, errores en logs de BD, comportamientos anómalos en consultas, historial de ataques similares. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Uso de ORM (Object-Relational Mapping) para evitar consultas directas | Backend / Dev | Sequelize, Hibernate, Prisma |
| Validación estricta de entradas del usuario | Dev / QA | Joi, Yup, Express-validator |
| Uso de queries parametrizadas y stored procedures | Backend | PostgreSQL, MySQL, SQL Server |
| Implementación de escáneres automáticos de vulnerabilidades | DevSecOps | Snyk, SonarQube, OWASP Dependency Check |
| Capacitación en prácticas seguras de codificación | Líder Técnico | OWASP Top 10, guías internas, talleres |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Aislar el sistema afectado y detener temporalmente accesos a BD | DevOps / Seguridad TI | Copia de respaldo, firewall |
| Revisar logs para identificar vectores de entrada | QA / Auditoría | Log central, ElasticSearch |
| Aplicar hotfix para cerrar el punto de inyección | Backend | Refactorización de código |
| Notificar al equipo de seguridad y responsables legales | Coordinación | Canal interno, protocolo IR |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Revisión completa de código fuente para evitar nuevas inyecciones | QA / Dev | Code review, SonarQube |
| Pruebas de penetración para validar protección | Seguridad TI | OWASP ZAP, Burp Suite |
| Implementar política de codificación segura obligatoria | PMO / CTO | Checklists, guía de desarrollo |
| Documentar el incidente y reforzar puntos críticos | QA / PM | Informe postmortem, RCA |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Inyección SQL permite manipular o eliminar datos | Pérdida de integridad y confiabilidad del sistema | $40,000 MXN |
| Fuga de datos sensibles | Pérdida reputacional y posible sanción legal | $25,000 MXN |
| Interrupción del servicio y recuperación | Detención operativa y restauración de respaldos | $15,000 MXN |
| Atención a clientes afectados y soporte | Gestión de crisis y contención de daños | $8,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$88,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Implementación de ORM y validación de entradas | $3,500 MXN |
| Capacitación del equipo sobre OWASP y buenas prácticas | $2,000 MXN |
| Auditoría inicial de código | $2,500 MXN |
| Herramientas automáticas de análisis de seguridad | $3,000 MXN |
| Total medidas preventivas: | → $11,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Aislamiento del sistema y análisis | $2,500 MXN |
| Aplicación de hotfix | $2,000 MXN |
| Comunicación con equipo de seguridad | $1,000 MXN |
| Total medidas de mitigación: | → $5,500 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Revisión y refactorización del código | $4,000 MXN |
| Pruebas de seguridad posteriores | $3,000 MXN |
| Redacción y aplicación de nueva política interna | $2,000 MXN |
| Total medidas correctivas: | → $9,000 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $11,000 MXN |
| 🚨 Mitigación | $5,500 MXN |
| 🔄 Recuperación | $9,000 MXN |
| 💥 Costo de no hacer nada | $88,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $11,000 + $5,500 + $9,000 = **$25,500 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $88,000 – $25,500 = **$62,500 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **245% de ROI**