**RIESGO 13: Vulnerabilidades introducidas en última versión**

* **Tipo de riesgo:** Seguridad / Técnico / Calidad
* **Categoría:** Desarrollo / Control de Calidad / Seguridad Informática
* **Descripción:** Este riesgo ocurre cuando la última versión del software incluye vulnerabilidades de seguridad no detectadas durante el ciclo de desarrollo, exponiendo al sistema a ataques, pérdida de datos o accesos no autorizados.

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Vulnerabilidades introducidas en última versión |
| Categoría | Seguridad / Desarrollo / Control de Calidad |
| Causas probables | Falta de pruebas de seguridad, integración de código inseguro, presión por entregas rápidas. |
| Consecuencias | Exposición a ataques, pérdida de información, daño a la reputación y cumplimiento normativo. |
| Fuente | Procesos deficientes de revisión y testing de seguridad, falta de herramientas de análisis. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta |
| Impacto potencial | Crítico (compromete confidencialidad, integridad y disponibilidad) |
| Nivel de riesgo | Alto |
| Indicadores de riesgo | Reportes de vulnerabilidades post-lanzamiento, incidentes de seguridad. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Integrar análisis estático y dinámico de seguridad en CI/CD. | DevOps / Seguridad | SonarQube, OWASP ZAP, Snyk, Fortify |
| Capacitar a desarrolladores en prácticas de codificación segura. | RRHH / Seguridad | Talleres, guías, bootcamps |
| Revisiones de código enfocadas en seguridad. | Líder Técnico / QA | Pull Requests con checklist de seguridad |
| Realizar pruebas de penetración periódicas. | Seguridad / QA | Herramientas pentesting, servicios especializados |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Aplicar parches y hotfixes de seguridad urgentes. | Dev / Seguridad | Herramientas de despliegue rápido |
| Monitorizar actividad anómala y alertas de seguridad. | Seguridad / DevOps | SIEM, IDS/IPS, sistemas de monitoreo |
| Notificar a usuarios y equipos sobre riesgos y acciones. | PM / Comunicación | Canales internos y externos de comunicación |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Investigar causa raíz y reforzar controles de seguridad. | Seguridad / Líder Técnico | Informes, auditorías |
| Actualizar políticas y procedimientos de seguridad. | Seguridad / PM | Documentación, capacitaciones |
| Implementar mejoras en automatización de pruebas de seguridad. | QA / DevOps | Pipelines CI/CD, herramientas de escaneo |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Brechas de seguridad y ataques exitosos | Robo o pérdida de datos, interrupción de servicio | $80,000 MXN |
| Sanciones legales y cumplimiento normativo | Multas y costos legales | $40,000 MXN |
| Daño reputacional y pérdida de confianza | Impacto negativo en clientes y mercado | $50,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$170,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Integración de análisis de seguridad en CI/CD | $8,000 MXN |
| Capacitación en codificación segura | $4,000 MXN |
| Pruebas de penetración y revisiones | $5,000 MXN |
| 🛡️ Total medidas preventivas: | **$17,000 MXN** |

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Parches rápidos y monitoreo continuo | $6,000 MXN |
| Comunicación y gestión de incidentes | $3,000 MXN |
| 🚨 Total medidas de mitigación: | **$9,000 MXN** |

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Investigación y actualización de políticas | $5,000 MXN |
| Automatización y refuerzo de pruebas de seguridad | $4,000 MXN |
| 🔄 Total medidas correctivas: | **$9,000 MXN** |

**Resumen Económico del Plan de Contingencia**

|  |  |
| --- | --- |
| Categoría | Costo estimado |
| 🛡️ Prevención | $17,000 MXN |
| 🚨 Mitigación | $9,000 MXN |
| 🔄 Recuperación | $9,000 MXN |
| 💥 Costo de no hacer nada | $170,000 MXN |

**📈 Análisis Costo-Beneficio**

**Costo total de implementar todas las estrategias:**  
$17,000 + $9,000 + $9,000 = **$35,000 MXN**

**Ahorro potencial si se previene o controla el riesgo:**  
$170,000 – $35,000 = **$135,000 MXN**

**(≈ 386% de retorno sobre inversión en seguridad y control de calidad)**