**Fallos en la gestión de permisos por roles**

* **Tipo de riesgo:** Técnico / Seguridad / Operativo
* **Categoría:** Gestión de accesos / Control de autorizaciones / Seguridad de aplicaciones

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Fallos en la gestión de permisos por roles |
| Categoría | Seguridad / Control de accesos / Desarrollo |
| Causas probables | Configuración incorrecta de roles, ausencia de revisiones periódicas, errores en asignación de permisos, falta de pruebas de autorización. |
| Consecuencias | Accesos indebidos, escalamiento de privilegios, vulneración de datos sensibles, incumplimiento normativo. |
| Fuente | Auditorías de seguridad, revisiones de código, reportes de accesos no autorizados. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta (frecuente en sistemas complejos sin controles rigurosos) |
| Impacto potencial | Alto (afecta la confidencialidad y la integridad del sistema) |
| Nivel de riesgo | Alto |
| Indicadores de riesgo | Excesos en permisos, accesos fuera de rol, falta de segregación de funciones. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Definir y documentar claramente roles y permisos | Seguridad / Desarrollo | Políticas IAM, manuales |
| Implementar control RBAC (Role-Based Access Control) | Dev / Seguridad | Frameworks de autorización, herramientas IAM |
| Realizar pruebas y validaciones de autorización | QA / Seguridad | Tests automatizados, pentesting |
| Auditar permisos periódicamente | Seguridad / QA | Informes, revisiones manuales |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Detectar y corregir accesos indebidos | Seguridad / Dev | Monitoreo, alertas de seguridad |
| Revocar permisos erróneos | Seguridad | Consolas IAM, herramientas de administración |
| Revisar logs de accesos sospechosos | Seguridad / QA | SIEM, herramientas de análisis |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Revisar y actualizar políticas de permisos | PM / Seguridad | Manuales, políticas internas |
| Capacitar al equipo en gestión correcta de accesos | Recursos Humanos | Talleres, cursos |
| Implementar mejoras en la herramienta de control de acceso | DevOps / Seguridad | Actualizaciones de software, parches |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Accesos no autorizados y manipulación de datos | Robo, alteración o divulgación de información | $40,000 MXN |
| Pérdida de integridad del sistema | Fallos operativos y errores | $25,000 MXN |
| Costos legales y sanciones | Multas por incumplimiento normativo | $15,000 MXN |
| Recursos para remediación y auditoría | Horas-hombre y consultoría | $15,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$95,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Definición y documentación de roles | $3,000 MXN |
| Implementación de RBAC | $4,000 MXN |
| Pruebas y validaciones de permisos | $2,500 MXN |
| Auditorías periódicas | $2,000 MXN |
| Total medidas preventivas: | → $11,500 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Corrección de accesos indebidos | $3,000 MXN |
| Revocación de permisos | $2,000 MXN |
| Revisión de logs | $1,500 MXN |
| Total medidas de mitigación: | → $6,500 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Actualización de políticas y capacitación | $3,000 MXN |
| Implementación de mejoras técnicas | $3,000 MXN |
| Total medidas correctivas: | → $6,000 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $11,500 MXN |
| 🚨 Mitigación | $6,500 MXN |
| 🔄 Recuperación | $6,000 MXN |
| 💥 Costo de no hacer nada | $95,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $11,500 + $6,500 + $6,000 = **$24,000 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $95,000 – $24,000 = **$71,000 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **296% de ROI**