**RIESGO 6: Errores de permisos en servidores o servicios**

* **Tipo de riesgo:** Técnico / Seguridad / Infraestructura
* **Categoría:** Accesos / Configuración / Gobernanza
* **Descripción:** Este riesgo se presenta cuando existen configuraciones incorrectas de permisos en servidores o servicios (por ejemplo, bases de datos, APIs, archivos, carpetas o procesos), lo que puede dar lugar a accesos no autorizados, fallos operativos o restricciones indebidas que interrumpen el funcionamiento normal del sistema.

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Errores de permisos en servidores o servicios |
| Categoría | Infraestructura / Seguridad / Operaciones |
| Causas probables | Asignación manual de permisos, desconocimiento de políticas de seguridad, falta de revisión de roles. |
| Consecuencias | Exposición de datos sensibles, fallos en ejecución de procesos, caídas de servicio, violaciones de acceso. |
| Fuente | Gestión de roles deficiente, ausencia de auditoría, procesos de configuración no estandarizados. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta |
| Impacto potencial | Alto (puede generar fallos críticos o incidentes de seguridad) |
| Nivel de riesgo | Alto |
| Indicadores de riesgo | Accesos fallidos, usuarios con privilegios innecesarios, bloqueos o vulnerabilidades reportadas. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar control de accesos basado en roles (RBAC). | DevOps / Seguridad | IAM, Active Directory, políticas RBAC |
| Revisar y auditar permisos regularmente en todos los entornos. | Seguridad / DevOps | Auditorías automatizadas, scripts de revisión |
| Documentar y versionar configuraciones de permisos. | Líder Técnico | Git, Ansible, Terraform, repos privados |
| Integrar validaciones de permisos en el pipeline de despliegue. | DevOps | CI/CD + linters, escáneres de políticas |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Aislar el servicio afectado y bloquear accesos indebidos. | DevOps | Firewalls, grupos de seguridad, ACLs |
| Reasignar temporalmente permisos mínimos funcionales. | DevOps / QA | Herramientas de gestión de usuarios |
| Escalar a seguridad si se detecta exposición de información. | PM / CISO | Protocolos de incidente, Bitácora |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Revisar configuraciones afectadas y corregir los permisos. | DevOps / QA | Scripts de validación, documentación |
| Fortalecer políticas de acceso y autenticación. | Seguridad / DevOps | MFA, OAuth, políticas de contraseñas |
| Capacitar al equipo en buenas prácticas de seguridad. | RRHH / Seguridad | Cursos de hardening, sesiones internas |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Pérdida de acceso a servicios por bloqueo | Interrupción de operaciones internas y externas | $30,000 MXN |
| Exposición de información sensible | Notificación legal, respuesta a incidentes, pérdida de confianza | $50,000 MXN |
| Tiempo invertido en diagnóstico y solución | Costos operativos, impacto en despliegues | $20,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$100,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Implementación de RBAC + auditorías | $6,000 MXN |
| Validación automática en pipelines | $3,500 MXN |
| Documentación y versionamiento de accesos | $3,000 MXN |
| 🛡️ Total medidas preventivas: | **$12,500 MXN** |

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Aislamiento y reasignación segura | $3,000 MXN |
| Gestión de crisis con seguridad | $2,000 MXN |
| 🚨 Total medidas de mitigación: | **$5,000 MXN** |

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Corrección y endurecimiento de configuraciones | $3,000 MXN |
| Capacitación de equipo técnico en accesos seguros | $4,000 MXN |
| 🔄 Total medidas correctivas: | **$7,000 MXN** |

**Resumen Económico del Plan de Contingencia**

|  |  |
| --- | --- |
| Categoría | Costo estimado |
| 🛡️ Prevención | $12,500 MXN |
| 🚨 Mitigación | $5,000 MXN |
| 🔄 Recuperación | $7,000 MXN |
| 💥 Costo de no hacer nada | $100,000 MXN |

**📈 Análisis Costo-Beneficio**

**Costo total de implementar todas las estrategias:**  
$12,500 + $5,000 + $7,000 = **$24,500 MXN**

**Ahorro potencial si se previene o controla el riesgo:**  
$100,000 – $24,500 = **$75,500 MXN**

**(≈ 308% de retorno sobre inversión en gestión segura de permisos)**