**Accesos no autorizados al backend**

* **Tipo de riesgo:** Técnico / Seguridad / Operativo
* **Categoría:** Control de accesos / Autenticación / Seguridad de infraestructura

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Accesos no autorizados al backend |
| Categoría | Seguridad / Control de accesos / Infraestructura |
| Causas probables | Credenciales débiles o filtradas, ausencia de autenticación multifactor, configuración errónea de permisos, falta de monitoreo, vulnerabilidades explotables. |
| Consecuencias | Robo o manipulación de datos, interrupción de servicios, escalamiento de privilegios, pérdida de confianza, sanciones legales. |
| Fuente | Registros de accesos, alertas de seguridad, auditorías de permisos, incidentes reportados. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta (alta en sistemas con controles deficientes) |
| Impacto potencial | Crítico (puede comprometer toda la infraestructura y datos) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Intentos fallidos repetidos, accesos desde IPs no reconocidas, cambios inesperados en configuraciones. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar autenticación multifactor (MFA) | Seguridad / Dev | Authenticator apps, hardware tokens |
| Aplicar políticas estrictas de contraseñas | Seguridad | Políticas IAM, reglas de complejidad |
| Segmentar la red y limitar accesos según roles | DevOps / Seguridad | Firewalls, VPN, Zero Trust |
| Monitorizar accesos y detectar anomalías | Seguridad / QA | SIEM, IDS/IPS, logs centralizados |
| Revisar y actualizar permisos periódicamente | Seguridad / QA | Auditorías internas, gestión IAM |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Bloquear accesos sospechosos y revisar sesiones activas | Seguridad / DevOps | Firewalls, bloqueo IP, terminación de sesiones |
| Revisar logs y realizar análisis forense | Seguridad | SIEM, herramientas de análisis |
| Reforzar autenticación temporalmente | Seguridad / Dev | MFA temporal, tokens de emergencia |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Realizar auditoría completa de accesos y permisos | Seguridad / QA | Informes, revisiones detalladas |
| Actualizar políticas y procedimientos de control de acceso | PM / Seguridad | Manuales, políticas internas |
| Capacitar al equipo en buenas prácticas de seguridad | Recursos Humanos | Talleres, cursos |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Acceso y manipulación no autorizada de datos | Robo, modificación o eliminación de información | $50,000 MXN |
| Interrupción de servicios críticos | Pérdida de disponibilidad y reputación | $30,000 MXN |
| Costos legales y multas | Sanciones por incumplimiento de normativas | $20,000 MXN |
| Esfuerzos de recuperación y fortalecimiento | Tiempo y recursos para remediar el incidente | $15,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$115,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Implementación de MFA | $4,000 MXN |
| Aplicación de políticas de contraseñas | $2,000 MXN |
| Segmentación y control de acceso | $3,000 MXN |
| Monitorización y alertas | $3,000 MXN |
| Auditorías periódicas | $2,000 MXN |
| Total medidas preventivas: | → $14,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Bloqueo y análisis de accesos sospechosos | $3,000 MXN |
| Refuerzo temporal de autenticación | $2,000 MXN |
| Investigación y análisis forense | $3,000 MXN |
| Total medidas de mitigación: | → $8,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Auditoría y revisión de controles | $3,500 MXN |
| Actualización de políticas y capacitación | $2,500 MXN |
| Total medidas correctivas: | → $6,000 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $14,000 MXN |
| 🚨 Mitigación | $8,000 MXN |
| 🔄 Recuperación | $6,000 MXN |
| 💥 Costo de no hacer nada | $115,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $14,000 + $8,000 + $6,000 = **$28,000 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $115,000 – $28,000 = **$87,000 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **311% de ROI**