**API sin límites de acceso por IP o usuario**

* **Tipo de riesgo:** Técnico / Seguridad / Operativo
* **Categoría:** Seguridad de APIs / Control de acceso / Protección contra abuso

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | API sin límites de acceso por IP o usuario |
| Categoría | Seguridad / Control de acceso / APIs |
| Causas probables | Falta de implementación de rate limiting, ausencia de API Gateway, configuración incorrecta, falta de monitoreo. |
| Consecuencias | Ataques de denegación de servicio, sobrecarga de servidores, abuso de recursos, afectación del rendimiento y disponibilidad. |
| Fuente | Logs de servidor, monitoreo de tráfico, reportes de incidentes. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta (común en APIs mal configuradas o sin control) |
| Impacto potencial | Alto (puede causar interrupciones y pérdida de servicio) |
| Nivel de riesgo | Alto |
| Indicadores de riesgo | Picos inusuales de tráfico, respuestas lentas, errores 503, saturación del sistema. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar rate limiting y cuotas por IP/usuario | Desarrollo | API Gateway, proxies, herramientas de throttling |
| Configurar API Gateway con políticas de acceso | DevOps / Seguridad | AWS API Gateway, Azure API Management |
| Monitorear y alertar sobre patrones de tráfico inusuales | Seguridad | SIEM, sistemas de monitoreo |
| Capacitar al equipo en mejores prácticas de seguridad API | Recursos Humanos | Cursos y talleres |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Aplicar bloqueos temporales a IP o usuarios sospechosos | Seguridad | Firewalls, WAF |
| Escalar infraestructura temporalmente | DevOps | Autoscaling en nube |
| Notificar a usuarios y equipos afectados | Comunicación / Soporte | Canales de atención |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Revisar y fortalecer políticas de control de acceso | Seguridad / PM | Documentación y auditorías |
| Mejorar sistemas de monitoreo y alertas | Seguridad / DevOps | SIEM y herramientas de análisis |
| Capacitación continua y simulacros | Recursos Humanos | Cursos y simulacros |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Interrupción del servicio | Pérdida de disponibilidad y usuarios afectados | $45,000 MXN |
| Daño a la reputación | Pérdida de confianza de clientes | $35,000 MXN |
| Costos operativos por recuperación | Escalado y soporte para restaurar servicio | $25,000 MXN |
| Multas regulatorias por falta de control | Penalizaciones por incumplimiento | $20,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$125,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Implementación de rate limiting y API Gateway | $5,000 MXN |
| Monitoreo y alertas | $3,000 MXN |
| Capacitación del personal | $2,500 MXN |
| Total medidas preventivas: | → $10,500 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Bloqueo y mitigación temporal | $3,500 MXN |
| Escalado de infraestructura | $4,000 MXN |
| Comunicación y soporte | $2,500 MXN |
| Total medidas de mitigación: | → $10,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Revisión y mejora de políticas | $3,000 MXN |
| Mejoras en monitoreo y capacitación | $2,500 MXN |
| Total medidas correctivas: | → $5,500 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $10,500 MXN |
| 🚨 Mitigación | $10,000 MXN |
| 🔄 Recuperación | $5,500 MXN |
| 💥 Costo de no hacer nada | $125,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $10,500 + $10,000 + $5,500 = **$26,000 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $125,000 – $26,000 = **$99,000 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **380% de ROI**