**APIs expuestas sin autenticación**

* **Tipo de riesgo:** Técnico / Seguridad / Acceso no autorizado
* **Categoría:** Integración / Desarrollo / Gestión de identidades

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | APIs expuestas sin autenticación |
| Categoría | Seguridad / Desarrollo / API Management |
| Causas probables | Pruebas sin autenticación activada, endpoints públicos mal configurados, falta de control de versiones, desconocimiento del principio de “zero trust”. |
| Consecuencias | Acceso no autorizado a datos o funcionalidades, fuga de información, acciones maliciosas por usuarios externos, corrupción o pérdida de datos. |
| Fuente | Análisis de seguridad, pruebas de penetración, escaneo de APIs públicas, revisiones de arquitectura. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Alta (especialmente en desarrollos ágiles o pruebas rápidas) |
| Impacto potencial | Crítico (puede otorgar acceso completo a funcionalidades sensibles) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | APIs accesibles sin autenticación, endpoints sin tokens, falta de control de permisos, ausencia de trazabilidad de accesos. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar autenticación obligatoria en todas las APIs | Backend / Arquitecto | JWT, OAuth 2.0, Auth0, Firebase Auth |
| Validar permisos y roles por endpoint (autorización granular) | Backend / QA | RBAC, pruebas unitarias, mocks |
| Asegurar APIs con gateway y control de acceso | DevOps / Backend | API Gateway, Kong, AWS API Gateway |
| Limitar acceso según IP o red segura | DevOps | Firewalls, whitelisting, restricciones por entorno |
| Documentar y revisar los endpoints expuestos | QA / Arquitectura | Swagger, Postman, revisión técnica |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Deshabilitar endpoints inseguros temporalmente | DevOps / Backend | Configuración del servidor / gateway |
| Revisar accesos registrados en logs | Seguridad / QA | SIEM, Cloud Logging, ELK Stack |
| Implementar reglas de control dinámico en el gateway | DevOps | Reglas condicionales, límites |
| Comunicar y coordinar plan de acción con stakeholders | Líder Técnico / PM | Canales internos, incident report |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Refactorizar APIs para incluir autenticación y autorización | Backend / Arquitecto | JWT, OAuth, pruebas unitarias |
| Validar exposición de APIs con escáneres de seguridad | QA / DevSecOps | OWASP API Security Top 10, ZAP |
| Establecer políticas de revisión obligatoria de endpoints | PMO / QA | Checklist de despliegue seguro |
| Documentar incidente y capacitar al equipo | Líder Técnico | Postmortem, talleres de seguridad |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Acceso no autorizado a funcionalidades críticas | Explotación de servicios internos por usuarios externos | $35,000 MXN |
| Robo o modificación de datos por falta de autenticación | Pérdida de integridad y privacidad | $25,000 MXN |
| Tiempo de recuperación y cierre de brechas | Refactorización urgente de múltiples endpoints | $12,000 MXN |
| Costos legales y de notificación | Informe a autoridades, asesoría legal | $8,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$80,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Configuración de autenticación (JWT, OAuth2, etc.) | $3,500 MXN |
| Desarrollo de roles y permisos por endpoint | $2,500 MXN |
| Integración con API Gateway y configuración de seguridad | $2,000 MXN |
| Documentación y revisión técnica de APIs | $2,000 MXN |
| Total medidas preventivas: | → $10,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Desactivación temporal de endpoints inseguros | $1,500 MXN |
| Revisión de accesos en logs y análisis rápido | $2,000 MXN |
| Implementación temporal de filtros en gateway | $1,500 MXN |
| Total medidas de mitigación: | → $5,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Refactorización de APIs y pruebas de autenticación | $4,000 MXN |
| Escaneo y auditoría de exposición de endpoints | $3,000 MXN |
| Taller de concientización para el equipo | $2,000 MXN |
| Total medidas correctivas: | → $9,000 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $10,000 MXN |
| 🚨 Mitigación | $5,000 MXN |
| 🔄 Recuperación | $9,000 MXN |
| 💥 Costo de no hacer nada | $80,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $10,000 + $5,000 + $9,000 = **$24,000 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $80,000 – $24,000 = **$56,000 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **233% de ROI**