**RIESGO 23: Exposición de claves API en el código**

* **Tipo de riesgo:** Técnico / Seguridad
* **Categoría:** Ciberseguridad / Desarrollo / Integraciones
* **Descripción:** Este riesgo ocurre cuando claves API, tokens secretos u otras credenciales sensibles se incluyen directamente en el código fuente o repositorios, exponiéndolas a terceros. Esto puede permitir accesos no autorizados, filtración de datos o uso indebido de servicios externos.

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Exposición de claves API en el código |
| Categoría | Seguridad / Gestión de secretos |
| Causas probables | Falta de buenas prácticas, ignorar archivos .env, commits accidentales, desconocimiento técnico. |
| Consecuencias | Accesos no autorizados, filtración de datos, costos por abuso de servicios, reputación afectada. |
| Fuente | Repositorios públicos, archivos de configuración mal gestionados, push accidentales. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Alta |
| Impacto potencial | Crítico (acceso a recursos sensibles, pérdida de datos, sanciones legales o financieras) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Claves visibles en código, uso inusual de servicios, alertas del proveedor o de seguridad. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar variables de entorno y separar credenciales del código. | Dev / Infraestructura | .env, .gitignore, Docker Secrets, Vault |
| Utilizar gestores de secretos para producción. | DevOps / Seguridad | HashiCorp Vault, AWS Secrets Manager, Azure Vault |
| Configurar reglas de detección de secretos en commits. | Dev / Líder Técnico | Git hooks, truffleHog, GitGuardian, pre-commit hooks |
| Capacitar al equipo sobre manejo seguro de claves. | RRHH / Seguridad | Talleres, cursos internos, políticas de seguridad |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Escanear repositorios en busca de claves expuestas. | Seguridad / QA | TruffleHog, Gitleaks, GitGuardian |
| Revocar inmediatamente las claves expuestas. | Dev / DevOps | Consolas de APIs, rotación de claves |
| Notificar a proveedores de servicios si hubo acceso indebido. | Seguridad | Canales de soporte, respuesta a incidentes |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Auditoría completa del código y control de acceso. | QA / Seguridad | SonarQube, GitHub Audit Log, permisos |
| Implementación de un pipeline de seguridad en CI/CD. | DevOps | GitHub Actions, GitLab CI, Snyk, CodeQL |
| Actualización de políticas y formación obligatoria. | RRHH / PMO | Manuales, políticas internas, sesiones de revisión |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Abuso de servicios con claves expuestas | Cargos inesperados por uso no autorizado | $40,000 MXN |
| Pérdida o robo de datos | Afectación legal y reputacional | $35,000 MXN |
| Tiempo del equipo en mitigación | Revocación, comunicación y control de daños | $15,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$90,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Implementación de variables de entorno | $3,000 MXN |
| Configuración de gestores de secretos | $4,000 MXN |
| Capacitación del equipo en seguridad de claves | $3,000 MXN |
| 🛡️ Total medidas preventivas: | **$10,000 MXN** |

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Escaneo automatizado de secretos en repositorios | $2,500 MXN |
| Revocación y regeneración de claves expuestas | $2,500 MXN |
| 🚨 Total medidas de mitigación: | **$5,000 MXN** |

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Auditoría, CI/CD seguro y actualización de políticas | $6,000 MXN |
| Formación obligatoria y refuerzo institucional | $3,500 MXN |
| 🔄 Total medidas correctivas: | **$9,500 MXN** |

**Resumen Económico del Plan de Contingencia**

|  |  |
| --- | --- |
| Categoría | Costo estimado |
| 🛡️ Prevención | $10,000 MXN |
| 🚨 Mitigación | $5,000 MXN |
| 🔄 Recuperación | $9,500 MXN |
| 💥 Costo de no hacer nada | $90,000 MXN |

**📈 Análisis Costo-Beneficio**

**Costo total de implementar todas las estrategias:**  
$10,000 + $5,000 + $9,500 = **$24,500 MXN**

**Ahorro potencial si se previene o controla el riesgo:**  
$90,000 – $24,500 = **$65,500 MXN**

**(≈ 267% de retorno sobre inversión en protección de claves API)**