**Exposición de claves en repositorios públicos**

* **Tipo de riesgo:** Técnico / Seguridad / Desarrollo
* **Categoría:** Gestión de secretos / Seguridad de código / Cumplimiento

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Exposición de claves en repositorios públicos |
| Categoría | Seguridad / Gestión de secretos / Desarrollo |
| Causas probables | Subida accidental de archivos con claves, falta de controles de revisión, ausencia de herramientas de detección, prácticas inseguras en manejo de secretos. |
| Consecuencias | Accesos no autorizados, compromiso de sistemas, robo de datos, daño reputacional, multas por incumplimiento. |
| Fuente | Auditorías de código, escaneo de repositorios, reportes de seguridad, historial de incidentes. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta (frecuente en equipos sin controles estrictos) |
| Impacto potencial | Crítico (puede comprometer múltiples sistemas y datos) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Presencia de secretos en repositorios públicos, alertas de herramientas como git-secrets o truffleHog, reportes de exposición. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar herramientas automáticas para detección de secretos antes de commit | Dev / QA | git-secrets, truffleHog, pre-commit hooks |
| Capacitar al equipo en buenas prácticas de gestión de secretos | Recursos Humanos | Talleres, guías internas |
| Usar gestores de secretos seguros (Vault, AWS Secrets Manager) | Dev / Infra | HashiCorp Vault, AWS Secrets Manager |
| Configurar reglas estrictas en repositorios (branch protection, revisiones) | DevOps | GitHub/GitLab policies |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Revocar claves expuestas inmediatamente | Seguridad / Dev | Consolas de gestión de claves |
| Reemplazar y rotar secretos comprometidos | Seguridad / Dev | Gestión de secretos automatizada |
| Monitorizar accesos anómalos tras exposición | Seguridad | SIEM, logs de acceso |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Auditoría y revisión de repositorios | QA / Seguridad | Escáneres, informes automáticos |
| Actualizar políticas y procedimientos de manejo de secretos | PM / Seguridad | Manuales, checklists |
| Implementar escaneo continuo en pipelines de CI/CD | DevOps / QA | Integración git-secrets, scans automáticos |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Acceso no autorizado a sistemas críticos | Robo o manipulación de datos | $45,000 MXN |
| Tiempo de respuesta y remediación | Horas-hombre y recursos adicionales | $20,000 MXN |
| Daño reputacional y pérdida de clientes | Desconfianza y fuga de usuarios | $20,000 MXN |
| Multas y sanciones legales por incumplimiento | Costos legales y regulatorios | $15,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$100,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Implementación de herramientas automáticas de detección | $3,500 MXN |
| Capacitación y concientización del equipo | $2,000 MXN |
| Uso de gestores de secretos seguros | $3,000 MXN |
| Configuración de políticas de repositorio | $1,500 MXN |
| Total medidas preventivas: | → $10,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Revocación y rotación de claves comprometidas | $4,000 MXN |
| Monitoreo intensivo post-exposición | $2,000 MXN |
| Total medidas de mitigación: | → $6,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Auditoría y revisión de seguridad en repositorios | $3,000 MXN |
| Actualización de políticas y escaneo continuo | $2,500 MXN |
| Total medidas correctivas: | → $5,500 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $10,000 MXN |
| 🚨 Mitigación | $6,000 MXN |
| 🔄 Recuperación | $5,500 MXN |
| 💥 Costo de no hacer nada | $100,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $10,000 + $6,000 + $5,500 = **$21,500 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $100,000 – $21,500 = **$78,500 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **365% de ROI**