**Fallos de seguridad en almacenamiento en la nube**

* **Tipo de riesgo:** Técnico / Seguridad / Infraestructura
* **Categoría:** Almacenamiento / Configuración en la nube / Protección de activos digitale

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Fallos de seguridad en almacenamiento en la nube |
| Categoría | Infraestructura / Seguridad / DevOps |
| Causas probables | Configuraciones públicas por defecto, permisos excesivos en buckets, ausencia de cifrado, falta de monitoreo de acceso, ignorancia de buenas prácticas cloud. |
| Consecuencias | Acceso no autorizado a información sensible, modificación o eliminación de archivos, fuga de datos personales o empresariales, sanciones legales. |
| Fuente | Auditorías cloud, escaneo de buckets (ej. S3, GCS), pruebas de penetración, herramientas CSPM (Cloud Security Posture Management). |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta (muy frecuente si no se usan políticas cloud estrictas) |
| Impacto potencial | Crítico (exposición total de archivos, datos confidenciales y configuraciones internas) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Buckets públicos, archivos no cifrados, accesos sin autenticación, logs inactivos, alertas no configuradas. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Configurar el almacenamiento para acceso privado por defecto | DevOps / Seguridad | AWS S3 IAM, GCS Bucket Policies, Azure Blob Config |
| Aplicar cifrado en reposo y en tránsito | DevOps | AES-256, TLS 1.2+, SSE-KMS |
| Establecer políticas de acceso granular (principio de mínimo privilegio) | Seguridad / QA | IAM roles, políticas JSON, auditorías de permisos |
| Habilitar registro de accesos (auditoría) | DevOps | AWS CloudTrail, GCP Audit Logs, Azure Monitor |
| Revisar permisos de buckets periódicamente | DevOps / QA | Checklists internos, herramientas de escaneo |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Cambiar permisos a privado de forma inmediata | DevOps / Seguridad | Consolas cloud, CLI |
| Revocar accesos no autorizados | DevOps | IAM Policies, herramientas de acceso |
| Revisar logs de acceso y detectar descargas o alteraciones | QA / Seguridad | ELK, CloudTrail, SIEM |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar revisión de configuración cloud como parte del CI/CD | DevOps / QA | Terraform con Sentinel, AWS Config, Checkov |
| Realizar postmortem del incidente y documentación de vulnerabilidad | PM / Seguridad | Informes internos, plan de acción |
| Capacitar al equipo en mejores prácticas de seguridad en la nube | Recursos Humanos | Talleres cloud, guías AWS / GCP |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Fuga de datos confidenciales desde un bucket expuesto | Acceso no autorizado a archivos sensibles | $45,000 MXN |
| Pérdida o alteración de documentos alojados | Afectación operativa e integridad de datos | $20,000 MXN |
| Trabajo de contención y mitigación urgente | Tiempo DevOps y Seguridad | $12,000 MXN |
| Posibles sanciones legales por datos expuestos | Multas o revisión externa | $18,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$95,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Configuración privada de almacenamiento | $2,500 MXN |
| Cifrado en reposo y tránsito | $2,000 MXN |
| Revisión y ajuste de políticas IAM | $2,500 MXN |
| Activación de logging y control de acceso | $2,000 MXN |
| Total medidas preventivas: | → $9,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Cambiar configuraciones inseguras | $2,000 MXN |
| Monitoreo y análisis de accesos anómalos | $2,000 MXN |
| Revocación y rotación de accesos vulnerables | $1,500 MXN |
| Total medidas de mitigación: | → $5,500 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Integración de revisión cloud en pipelines CI/CD | $3,000 MXN |
| Postmortem, documentación y ajustes operativos | $2,500 MXN |
| Capacitación del equipo en prácticas seguras cloud | $3,000 MXN |
| Total medidas correctivas: | → $8,500 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $9,000 MXN |
| 🚨 Mitigación | $5,500 MXN |
| 🔄 Recuperación | $8,500 MXN |
| 💥 Costo de no hacer nada | $95,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $9,000 + $5,500 + $8,500 = **$23,000 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $95,000 – $23,000 = **$72,000 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **313% de ROI**