**Fugas de datos personales de usuarios**

* **Tipo de riesgo:** Técnico / Legal / Reputacional
* **Categoría:** Seguridad de la información / Cumplimiento normativo / Infraestructura

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Fugas de datos personales de usuarios |
| Categoría | Seguridad / Legal / Protección de Datos |
| Causas probables | Falta de cifrado en tránsito o en reposo, errores en configuración de base de datos, accesos no controlados, exposición accidental de logs, errores humanos. |
| Consecuencias | Sanciones legales, pérdida de confianza del usuario, demandas, impacto reputacional, fuga de información crítica. |
| Fuente | Auditorías internas, análisis de cumplimiento (LFPDPPP, GDPR), hallazgos de pentesting, reportes de usuarios o de incidentes. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Alta (por malas prácticas comunes y amenazas externas frecuentes) |
| Impacto potencial | Crítico (puede implicar demandas legales y pérdida masiva de usuarios) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Datos personales sin cifrado, ausencia de control de acceso, bases de datos sin protección, accesos no monitoreados, archivos de respaldo expuestos |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar cifrado en tránsito y reposo (TLS, AES-256) | DevSecOps / Backend | OpenSSL, TLS 1.3, AWS KMS, Azure Key Vault |
| Establecer controles de acceso por roles (RBAC) | Arquitecto / DevOps | IAM, Firebase Auth, Auth0 |
| Auditar almacenamiento y transmisión de datos personales | QA / Auditoría TI | Checklists, herramientas de escaneo de seguridad |
| Aplicar hashing irreversible a datos sensibles no requeridos en claro | Backend | SHA-256, bcrypt, salting |
| Sensibilizar al equipo sobre la protección de datos | Líder de proyecto | Talleres, políticas internas, capacitaciones |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Activar planes de respuesta a incidentes | Seguridad TI | Plan IR, comunicación legal |
| Revocar accesos comprometidos y rotar claves | DevOps / Seguridad | Gestión IAM, Bitwarden, HashiCorp |
| Monitorear logs y alertar accesos anómalos | DevOps / QA | SIEM, Datadog, AWS CloudTrail |
| Contactar a usuarios afectados y ofrecer contención inmediata | Comunicación / Legal | Protocolos de privacidad y notificación |

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

| **Acción** | **Responsable** | **Herramientas / Recursos** |
| --- | --- | --- |
| Realizar investigación forense y documentar el incidente | Seguridad TI | Herramientas forenses, reportes |
| Ajustar políticas y prácticas de seguridad | CTO / PMO | Normativas internas, auditorías |
| Informar a autoridades competentes y cumplir obligaciones legales | Legal / Dirección | CNPD, INAI, regulaciones LFPDPPP |
| Refactorizar el almacenamiento inseguro de datos | Dev / Arquitecto | DB Encryption, acceso segmentado |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Fuga de base de datos con información personal | Multas por violación a LFPDPPP / GDPR | $50,000 MXN |
| Afectación reputacional y pérdida de usuarios | Cancelaciones, abandono, mala reputación online | $25,000 MXN |
| Soporte post-incidente y atención a usuarios afectados | Personal de soporte, horas extra | $10,000 MXN |
| Refactorización de almacenamiento y arquitectura | Reingeniería urgente, revisión técnica | $20,000 MXN |
| Notificación y cumplimiento legal | Honorarios legales, comunicaciones | $8,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$113,000 MXN** |

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

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

|  |  |
| --- | --- |
|  | Costo estimado (MXN) |
| Implementación de cifrado en tránsito y en reposo | $4,000 MXN |
| Configuración de control de accesos y roles | $2,500 MXN |
| Auditoría inicial de seguridad y almacenamiento | $3,000 MXN |
| Capacitación del equipo en manejo seguro de datos | $2,000 MXN |
| Total medidas preventivas: | → $11,500 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Activación de plan de respuesta a incidentes | $2,000 MXN |
| Revocación de accesos y rotación de claves | $1,500 MXN |
| Supervisión y monitoreo de accesos | $2,500 MXN |
| Comunicación con usuarios | $1,000 MXN |
| Total medidas de mitigación: | → $7,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Investigación y reporte técnico del incidente | $3,000 MXN |
| Refactorización técnica y segmentación de datos | $5,000 MXN |
| Cumplimiento con regulación y asesoría legal | $4,000 MXN |
| Total medidas correctivas: | → $12,000 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $11,500 MXN |
| 🚨 Mitigación | $7,000 MXN |
| 🔄 Recuperación | $12,000 MXN |
| 💥 Costo de no hacer nada | $113,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $11,500 + $7,000 + $12,000 = **$30,500 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $113,000 – $30,500 = **$82,500 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **270% de ROI**