**No cumplir con regulaciones (ej. LFPDPPP, GDPR)**

* **Tipo de riesgo:** Legal / Técnico / Estratégico
* **Categoría:** Cumplimiento normativo / Protección de datos / Gobernanza

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | No cumplir con regulaciones (LFPDPPP, GDPR, etc.) |
| Categoría | Legal / Seguridad / Gestión de datos personales |
| Causas probables | Desconocimiento normativo, falta de asesoría legal, omisión de políticas de privacidad, almacenamiento indebido de datos, ausencia de consentimiento. |
| Consecuencias | Multas económicas, sanciones legales, bloqueo de operaciones, daño reputacional, pérdida de confianza del usuario. |
| Fuente | Auditorías externas, quejas de usuarios, revisiones regulatorias, escaneos de cumplimiento, pruebas legales. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta (especialmente en empresas pequeñas o startups sin asesoría legal continua) |
| Impacto potencial | Crítico (implica responsabilidad jurídica y sanciones económicas graves) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Falta de política de privacidad, datos personales sin consentimiento explícito, ausencia de mecanismos de revocación de consentimiento, retención indefinida de datos. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Contratar asesoría legal especializada en protección de datos | Dirección / Legal | Despacho jurídico, consultores externos |
| Desarrollar y publicar política de privacidad clara y accesible | Legal / PM | Página web, documentos legales |
| Solicitar consentimiento explícito para el tratamiento de datos | Desarrollo / Legal | Formularios digitales, registros de consentimiento |
| Clasificar y documentar los datos personales tratados | Seguridad / QA | Inventario de datos, herramientas DLP |
| Establecer tiempo máximo de retención y mecanismos de eliminación segura | Arquitectura / Legal | Cron jobs, scripts de limpieza, políticas internas |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Suspender temporalmente operaciones de tratamiento de datos | Dirección / QA | Modo mantenimiento, control legal |
| Corregir flujos de recopilación sin consentimiento | Dev / Legal | Scripts, revisión de formularios |
| Notificar de forma proactiva a usuarios y autoridades | Comunicación / Legal | Plantillas de aviso, correo certificado |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Presentar respuesta formal ante autoridades | Legal | Documentación jurídica, asesores |
| Revisar y reforzar políticas internas de cumplimiento normativo | QA / PMO | Auditorías legales, checklist de cumplimiento |
| Incluir cumplimiento legal como criterio obligatorio de desarrollo | PM / QA | Checklists, nuevas políticas |
| Capacitar al equipo en manejo legal de datos personales | Recursos Humanos | Talleres, webinars, guía interna |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Multas por incumplimiento de LFPDPPP / GDPR | Sanciones legales y económicas | $80,000 MXN |
| Suspensión temporal de operaciones por orden judicial | Inactividad y pérdida de ingresos | $25,000 MXN |
| Costo de regularización legal y actualización de políticas | Consultoría, redacción de documentos | $12,000 MXN |
| Pérdida de confianza y usuarios por reputación afectada | Deserción de clientes / usuarios | $20,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$137,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Asesoría legal externa y redacción de política de privacidad | $6,000 MXN |
| Diseño e implementación de formulario de consentimiento | $2,000 MXN |
| Clasificación y documentación de datos tratados | $2,500 MXN |
| Implementación de eliminación segura de datos | $2,000 MXN |
| Total medidas preventivas: | → $12,500 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Suspensión y reconfiguración de flujos ilegales | $3,000 MXN |
| Notificación oficial a usuarios y autoridades | $2,000 MXN |
| Soporte y ajuste legal en medio de incidente | $2,500 MXN |
| Total medidas de mitigación: | → $7,500 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Atención jurídica del incidente | $5,000 MXN |
| Revisión y refuerzo de cumplimiento normativo | $3,000 MXN |
| Capacitación interna sobre protección de datos personales | $2,500 MXN |
| Total medidas correctivas: | → $10,500 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $12,500 MXN |
| 🚨 Mitigación | $7,500 MXN |
| 🔄 Recuperación | $10,500 MXN |
| 💥 Costo de no hacer nada | $137,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $12,500 + $7,500 + $10,500 = **$30,500 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $137,000 – $30,500 = **$106,500 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **349% de ROI**