**No validar archivos subidos por el usuario**

* **Tipo de riesgo:** Técnico / Seguridad / Operativo
* **Categoría:** Validación de entradas / Seguridad de aplicaciones / Prevención de ataques

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | No validar archivos subidos por el usuario |
| Categoría | Seguridad / Validación / Desarrollo |
| Causas probables | Falta de validaciones adecuadas, ausencia de filtros en el servidor, omisión de restricciones de tipo y tamaño, desconocimiento de ataques comunes (e.g., malware, scripts maliciosos). |
| Consecuencias | Inyección de malware, ejecución de código malicioso, corrupción de datos, compromiso del sistema, ataques de denegación de servicio (DoS). |
| Fuente | Registros de incidentes, pruebas de seguridad, auditorías de código. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta (común en aplicaciones con cargas de archivos sin restricciones) |
| Impacto potencial | Crítico (puede comprometer la integridad y disponibilidad del sistema) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Archivos sospechosos en servidor, fallos en antivirus, reportes de incidentes relacionados con archivos maliciosos. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar validación estricta de tipo y tamaño de archivo | Desarrollo | Validadores en backend, listas blancas |
| Escaneo antivirus y antimalware en archivos subidos | Seguridad | ClamAV, antivirus en servidor |
| Limitar permisos y ejecución sobre archivos subidos | DevOps | Configuración de sistema de archivos |
| Educar al equipo sobre riesgos de carga de archivos | Recursos Humanos | Talleres y guías |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Detectar y aislar archivos sospechosos | Seguridad / Dev | Sistemas de monitoreo, cuarentena |
| Revisar logs y alertas relacionadas | Seguridad | SIEM, análisis de logs |
| Aplicar parches y actualizaciones rápidas | DevOps | Herramientas de gestión de parches |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Auditoría y revisión de mecanismos de validación | QA / Seguridad | Informes de auditoría, pruebas |
| Actualización de políticas y procedimientos | PM / Seguridad | Manuales, checklist |
| Capacitación continua del equipo | Recursos Humanos | Cursos y talleres |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Infección del sistema por malware | Daños operativos, recuperación y restauración | $50,000 MXN |
| Robo o corrupción de datos | Pérdida de información y confianza | $30,000 MXN |
| Interrupción de servicio | Pérdidas económicas por downtime | $20,000 MXN |
| Costos legales y reputacionales | Multas y pérdida de clientes | $15,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$115,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Validación de archivos en backend | $4,000 MXN |
| Implementación de escaneo antivirus | $3,000 MXN |
| Configuración de permisos y seguridad | $2,000 MXN |
| Capacitación del equipo | $2,000 MXN |
| Total medidas preventivas: | → $11,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Detección y aislamiento de archivos maliciosos | $3,000 MXN |
| Análisis y respuesta a incidentes | $2,000 MXN |
| Aplicación de parches | $1,500 MXN |
| Total medidas de mitigación: | → $6,500 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Auditoría y revisión de validación | $3,000 MXN |
| Actualización de políticas y capacitación | $2,500 MXN |
| Total medidas correctivas: | → $5,500 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $11,000 MXN |
| 🚨 Mitigación | $6,500 MXN |
| 🔄 Recuperación | $5,500 MXN |
| 💥 Costo de no hacer nada | $115,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $11,000 + $6,500 + $5,500 = **$23,000 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $115,000 – $23,000 = **$92,000 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **400% de ROI**