**Inyección de scripts maliciosos (XSS)**

* **Tipo de riesgo:** Técnico / Seguridad / Desarrollo
* **Categoría:** Seguridad de aplicaciones / Validación de entrada / Protección contra ataques

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Inyección de scripts maliciosos (XSS) |
| Categoría | Seguridad / Desarrollo / Validación de datos |
| Causas probables | Falta de validación o sanitización de entradas, uso incorrecto de funciones de escape, falta de Content Security Policy (CSP). |
| Consecuencias | Robo de sesiones, redirección a sitios maliciosos, modificación de contenido, pérdida de confianza de usuarios. |
| Fuente | Auditorías de seguridad, reportes de vulnerabilidades, análisis de código. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media-Alta (frecuente en aplicaciones web con entradas dinámicas) |
| Impacto potencial | Alto (puede comprometer la seguridad del usuario y la integridad de la aplicación) |
| Nivel de riesgo | Alto |
| Indicadores de riesgo | Presencia de entradas sin sanitizar, alertas de escaneo de seguridad, reportes de incidentes XSS. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Validar y sanitizar todas las entradas de usuario | Desarrollo | Librerías de sanitización, validadores |
| Implementar políticas Content Security Policy (CSP) | Desarrollo / Seguridad | Configuración de servidores y navegadores |
| Capacitar al equipo en técnicas seguras de desarrollo | Recursos Humanos | Cursos y talleres |
| Realizar revisiones y análisis de seguridad de código | Seguridad / QA | Herramientas de escaneo estático |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Detectar y bloquear ataques XSS en tiempo real | Seguridad | WAF (Web Application Firewall) |
| Aplicar parches rápidos para corregir vulnerabilidades | Desarrollo | Gestión de versiones y despliegues |
| Notificar y mitigar el impacto en usuarios afectados | Gestión / Comunicación | Protocolos de atención y comunicación |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Auditoría y refactorización del código afectado | Desarrollo / Seguridad | Revisiones manuales y automáticas |
| Actualización continua de políticas y controles | Seguridad / PM | Documentación interna |
| Capacitación continua y simulacros de ataques | Recursos Humanos | Cursos, simulaciones |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Robo de datos o sesiones | Pérdida de información y accesos indebidos | $50,000 MXN |
| Daño a la reputación | Pérdida de confianza de usuarios | $35,000 MXN |
| Costos legales y sanciones | Multas, auditorías y defensa legal | $30,000 MXN |
| Respuesta y remediación de incidentes | Tiempo de desarrollo y soporte | $25,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$140,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Validación y sanitización de entradas | $4,000 MXN |
| Implementación de CSP | $3,000 MXN |
| Capacitación en desarrollo seguro | $3,500 MXN |
| Análisis y revisión de seguridad del código | $4,000 MXN |
| Total medidas preventivas: | → $14,500 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Implementación y gestión de WAF | $5,000 MXN |
| Aplicación de parches y correcciones rápidas | $3,500 MXN |
| Comunicación y mitigación a usuarios | $2,500 MXN |
| Total medidas de mitigación: | → $11,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Auditoría y refactorización del código | $4,000 MXN |
| Actualización de políticas y capacitación continua | $3,000 MXN |
| Total medidas correctivas: | → $7,000 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $14,500 MXN |
| 🚨 Mitigación | $11,000 MXN |
| 🔄 Recuperación | $7,000 MXN |
| 💥 Costo de no hacer nada | $140,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $14,500 + $11,000 + $7,000 = **$32,500 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $140,000 – $32,500 = **$107,500 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **330% de ROI**