**Faltas en el cifrado de tokens o cookies**

* **Tipo de riesgo:** Técnico / Seguridad / Criptografía
* **Categoría:** Seguridad de comunicaciones / Protección de datos / Autenticación

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Faltas en el cifrado de tokens o cookies |
| Categoría | Seguridad / Criptografía / Desarrollo |
| Causas probables | Uso de algoritmos débiles o no recomendados, configuración incorrecta, transmisión en texto plano, falta de TLS, almacenamiento inseguro. |
| Consecuencias | Robo o manipulación de tokens, secuestro de sesión, exposición de datos sensibles, ataques de replay o CSRF. |
| Fuente | Auditorías de seguridad, análisis de vulnerabilidades, reportes de incidentes. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media (por falta de conocimientos o configuraciones incorrectas) |
| Impacto potencial | Alto (puede comprometer la integridad de sesiones y datos) |
| Nivel de riesgo | Alto |
| Indicadores de riesgo | Tokens sin cifrado, cookies sin atributos seguros, tráfico no cifrado. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Implementar cifrado fuerte para tokens y cookies (AES-256, HMAC) | Desarrollo / Seguridad | Bibliotecas criptográficas seguras |
| Usar siempre TLS 1.2 o superior para transmisión | Infraestructura / DevOps | Certificados SSL, configuración HTTPS |
| Configurar cookies con atributos Secure, HttpOnly y SameSite | Desarrollo | Configuración de servidor y framework |
| Realizar revisiones y auditorías de seguridad criptográfica | Seguridad / QA | Escáneres y revisiones manuales |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Detectar tokens expuestos o comprometidos | Seguridad | Monitoreo y alertas |
| Revocar tokens y renovar claves criptográficas | Desarrollo / Seguridad | Gestión de claves y autenticación |
| Aplicar parches y actualizaciones urgentes | DevOps | Herramientas de gestión de parches |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Auditoría completa de mecanismos criptográficos | Seguridad / QA | Informes y análisis |
| Actualización de políticas y estándares criptográficos | PM / Seguridad | Manuales y políticas internas |
| Capacitación continua en criptografía y seguridad | Recursos Humanos | Cursos y talleres |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Robo o manipulación de sesiones | Secuestro de cuentas y acceso indebido | $45,000 MXN |
| Exposición de datos sensibles | Daño a la privacidad y cumplimiento normativo | $35,000 MXN |
| Costos legales y multas | Multas por incumplimiento y asesoría legal | $25,000 MXN |
| Pérdida de reputación y confianza | Daño a la imagen corporativa | $20,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$125,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Implementación de cifrado fuerte y configuración TLS | $4,500 MXN |
| Configuración segura de cookies | $2,500 MXN |
| Revisiones y auditorías criptográficas | $3,000 MXN |
| Capacitación en criptografía y seguridad | $2,000 MXN |
| Total medidas preventivas: | → $12,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Detección y respuesta a incidentes | $3,500 MXN |
| Revocación y renovación de claves | $2,500 MXN |
| Aplicación de parches | $2,000 MXN |
| Total medidas de mitigación: | → $8,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Auditoría y actualización de políticas | $3,000 MXN |
| Capacitación continua | $2,500 MXN |
| Total medidas correctivas: | → $5,500 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $12,000 MXN |
| 🚨 Mitigación | $8,000 MXN |
| 🔄 Recuperación | $5,500 MXN |
| 💥 Costo de no hacer nada | $125,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $12,000 + $8,000 + $5,500 = **$25,500 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $125,000 – $25,500 = **$99,500 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **390% de ROI**