**Sesiones vulnerables a secuestro (session hijacking)**

* **Tipo de riesgo:** Técnico / Seguridad
* **Categoría:** Autenticación / Gestión de sesiones / Protección de identidad

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Sesiones vulnerables a secuestro (session hijacking) |
| Categoría | Seguridad / Autenticación / Desarrollo |
| Causas probables | Cookies no protegidas (sin HttpOnly o Secure), sesiones sin expiración, tokens reutilizables, ausencia de rotación, uso de HTTP en vez de HTTPS. |
| Consecuencias | Robo de identidad, accesos maliciosos, suplantación de usuario, filtración de datos, daño reputacional y legal. |
| Fuente | Revisiones de seguridad, escaneo de cookies, análisis de tráfico, reportes de vulnerabilidades OWASP. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Alta (especialmente en aplicaciones web sin buenas prácticas de gestión de sesiones) |
| Impacto potencial | Alto (acceso directo a cuentas legítimas) |
| Nivel de riesgo | Muy alto |
| Indicadores de riesgo | Sesiones que no expiran, cookies visibles por JS, tokens predecibles o no cifrados, múltiples accesos simultáneos sin alertas. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Establecer cookies con flags HttpOnly, Secure y SameSite | Backend / DevOps | Express-session, middleware de seguridad |
| Implementar expiración de sesión por inactividad | Backend / Arquitectura | JWT con expiración, tokens firmados |
| Activar rotación periódica de tokens o sesiones | Backend / Seguridad | JWT refresh, mecanismo de revocación |
| Usar HTTPS en todas las comunicaciones | DevOps | Certificados TLS / Let's Encrypt |
| Monitorear sesiones activas por usuario | QA / Backend | Herramientas de tracking, logs |

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

| **Acción** | **Responsable** | **Herramientas / Recursos** |
| --- | --- | --- |
| Invalidar tokens o sesiones sospechosas automáticamente | Backend / QA | Blacklist de tokens, alerts |
| Cierre de sesión forzado y alerta al usuario | Soporte / Seguridad | Correo, notificación, logging |
| Revisión de IPs, agentes y patrones de uso | Seguridad TI | SIEM, ElasticSearch |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Auditoría completa de sesiones y trazabilidad | Seguridad / DevOps | Revisión de logs, SIEM |
| Implementar control de acceso contextual (ubicación, IP, hora) | Arquitecto / QA | IAM avanzado, MFA basado en contexto |
| Incluir control de sesión en pruebas automatizadas | QA / Dev | OWASP ZAP, test de integración |
| Capacitación del equipo en gestión segura de sesiones | Líder Técnico | Talleres OWASP, guías internas |

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

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Suplantación de usuarios con accesos privilegiados | Modificación o robo de información sensible | $30,000 MXN |
| Interrupción de sesiones legítimas | Pérdida de servicio y experiencia negativa del usuario | $10,000 MXN |
| Gestión de incidentes, soporte y recuperación | Trabajo operativo urgente | $8,000 MXN |
| Daño reputacional y pérdida de confianza | Baja de usuarios, quejas públicas | $20,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$68,000 MXN** |

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

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Configuración segura de cookies y tokens | $3,000 MXN |
| Establecimiento de expiración y rotación de sesión | $2,500 MXN |
| Activación universal de HTTPS | $1,500 MXN |
| Monitoreo y detección temprana | $2,000 MXN |
| Total medidas preventivas: | → $9,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Invalidación y cierre de sesiones | $1,500 MXN |
| Alertas a usuarios y contención inicial | $1,500 MXN |
| Análisis de comportamiento sospechoso | $2,000 MXN |
| Total medidas de mitigación: | → $5,000 MXN |

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

|  |  |
| --- | --- |
| Acción | Costo estimado (MXN) |
| Auditoría completa y ajustes de seguridad de sesión | $3,000 MXN |
| Implementación de MFA contextual o biométrica | $4,000 MXN |
| Capacitación del equipo en gestión segura de sesiones | $2,000 MXN |
| Total medidas correctivas: | → $9,000 MXN |

**📊 Resumen Económico del Plan de Contingencia**

| **Categoría** | **Costo estimado** |
| --- | --- |
| 🛡️ Prevención | $9,000 MXN |
| 🚨 Mitigación | $5,000 MXN |
| 🔄 Recuperación | $9,000 MXN |
| 💥 Costo de no hacer nada | $68,000 MXN |

**📈 Análisis Costo-Beneficio**

* **Costo total de implementar todas las estrategias:**  
  $9,000 + $5,000 + $9,000 = **$23,000 MXN**
* **Ahorro potencial si se previene o controla el riesgo:**  
  $68,000 – $23,000 = **$45,000 MXN**
* **Retorno estimado de la inversión en gestión del riesgo:**  
  ≈ **195% de ROI**