**RIESGO 20: Pérdida de sesiones o tokens de usuarios**

* **Tipo de riesgo:** Técnico / Seguridad / Autenticación
* **Categoría:** Gestión de sesiones / Seguridad / Backend
* **Descripción:** Este riesgo se produce cuando las sesiones o tokens de autenticación de los usuarios se pierden, expiran prematuramente o son invalidados indebidamente, lo que puede provocar que los usuarios sean desconectados inesperadamente, afectando la experiencia, seguridad y continuidad del servicio.

**1. IDENTIFICACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Elemento | Detalle |
| Nombre del riesgo | Pérdida de sesiones o tokens de usuarios |
| Categoría | Seguridad / Autenticación / Gestión de sesiones |
| Causas probables | Expiración mal configurada, almacenamiento inconsistente, errores en renovación de tokens. |
| Consecuencias | Usuarios desconectados, frustración, pérdida de datos de sesión, riesgo de accesos no autorizados. |
| Fuente | Bugs en backend, problemas con cookies, tokens JWT mal gestionados, fallos en servidores. |

**2. EVALUACIÓN DEL RIESGO**

|  |  |
| --- | --- |
| Criterio | Valoración |
| Probabilidad de ocurrencia | Media - Alta |
| Impacto potencial | Alto (afecta experiencia, seguridad y uso del sistema) |
| Nivel de riesgo | Alto |
| Indicadores de riesgo | Quejas de usuarios, reportes de logout inesperados, errores de autenticación frecuentes. |

**3. DEFINICIÓN DE MEDIDAS DE CONTROL**

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Configurar adecuadamente tiempos de expiración y renovación de tokens/sesiones. | Backend / Seguridad | Frameworks auth, JWT libraries, Redis/session store |
| Implementar almacenamiento robusto y redundante para sesiones y tokens. | Infraestructura | Bases de datos, Redis, Memcached |
| Usar HTTPS y proteger cookies con flags Secure, HttpOnly y SameSite. | Seguridad | Políticas de seguridad, configuración servidor |
| Capacitar al equipo en manejo seguro de sesiones y tokens. | RRHH / Líder | Talleres, documentación |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Detectar rápidamente fallos en autenticación y sesiones. | DevOps / QA | Logs, sistemas de monitoreo y alertas |
| Aplicar reconexión automática o mensajes claros para el usuario. | Frontend / UX | Alertas UI, retry logics |
| Restablecer sesiones o emitir nuevos tokens con validación. | Backend | APIs seguras, mecanismos de refresh tokens |

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

|  |  |  |
| --- | --- | --- |
| Acción | Responsable | Herramientas / Recursos |
| Revisar código y configuración para corregir errores identificados. | Dev / QA | Revisión de código, auditorías |
| Mejorar documentación y guías para gestión de sesiones y tokens. | Líder Técnico | Wiki, manuales internos |
| Realizar capacitación adicional sobre seguridad y autenticación. | RRHH / Seguridad | Talleres especializados |

**1. Estimación de Pérdidas Económicas por Riesgo No Controlado**

|  |  |  |
| --- | --- | --- |
| Escenario de materialización | Impacto directo | Costo estimado (MXN) |
| Pérdida de usuarios y frustración | Soporte y pérdida de fidelidad | $30,000 MXN |
| Incremento de fallos y riesgos de seguridad | Posibles accesos no autorizados o vulnerabilidades | $25,000 MXN |
| Retrasos en desarrollo para corrección | Horas hombre para resolver y testear | $15,000 MXN |
| Total estimado de pérdidas económicas: |  | → **$70,000 MXN** |

**2. Costo de Implementación de Estrategias de Control**

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Configuración y pruebas robustas de manejo de sesiones | $3,500 MXN |
| Implementación de almacenamiento seguro y redundante | $4,000 MXN |
| Capacitación en seguridad y gestión de sesiones | $3,000 MXN |
| 🛡️ Total medidas preventivas: | **$10,500 MXN** |

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Monitorización y detección rápida de fallos | $3,000 MXN |
| Implementación de mecanismos de reconexión o alertas | $2,000 MXN |
| 🚨 Total medidas de mitigación: | **$5,000 MXN** |

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

|  |  |
| --- | --- |
| Acción | Costo estimado |
| Corrección de código y revisión de configuraciones | $3,500 MXN |
| Actualización de documentación y capacitación adicional | $3,000 MXN |
| 🔄 Total medidas correctivas: | **$6,500 MXN** |

**Resumen Económico del Plan de Contingencia**

|  |  |
| --- | --- |
| Categoría | Costo estimado |
| 🛡️ Prevención | $10,500 MXN |
| 🚨 Mitigación | $5,000 MXN |
| 🔄 Recuperación | $6,500 MXN |
| 💥 Costo de no hacer nada | $70,000 MXN |

**📈 Análisis Costo-Beneficio**

**Costo total de implementar todas las estrategias:**  
$10,500 + $5,000 + $6,500 = **$22,000 MXN**

**Ahorro potencial si se previene o controla el riesgo:**  
$70,000 – $22,000 = **$48,000 MXN**

**(≈ 218% de retorno sobre inversión en gestión de sesiones y seguridad)**