## Hoja de trabajo PASTA

| **Etapas** | **Empresa de zapatillas** |
| --- | --- |
| **I. Definición de objetivos comerciales y de seguridad** | Haz 2 o 3 anotaciones sobre requisitos comerciales específicos que se analizarán.   * *Los usuarios pueden crear perfiles de miembro a nivel interno o conectando cuentas externas.* * *La aplicación debe procesar transacciones financieras.* * *La aplicación debe cumplir con el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago, PCI-DSS.* |
| **II. Definición del alcance técnico** | Lista detecnologías utilizadas por la aplicación:   * *Interfaces de programación de aplicaciones (API)* * *Infraestructura de claves públicas (PKI)* * *Sistema de cifrado avanzado (AES)* * *SHA-256* * *SQL*   *Las API facilitan el intercambio de datos entre clientes, socios y empleados, por lo que deben priorizarse. Manejan una gran cantidad de datos sensibles al conectar a varios usuarios y sistemas. Antes de priorizar una tecnología sobre otra, deben considerarse detalles como cuáles son las API que se están utilizando porque, al aumentar la superficie de ataque, pueden ser más propensas a vulnerabilidades de seguridad.* |
| **III. Descomposición de la aplicación** | [Ejemplo de diagrama de flujo de datos](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview) |
| **IV. Análisis de amenazas** | En la hoja de trabajo PASTA, enumera **2 tipos de amenazas** que sean riesgos para la información que maneja la aplicación.   * *Inyección* * *Secuestro de sesión* |
| **V. Análisis de vulnerabilidades** | En la hoja de trabajo de PASTA, enumera **2 vulnerabilidades** que podrían explotarse.   * *Falta de sentencias preparadas* * *Token de API roto* |
| **VI. Modelado de ataques** | [Ejemplo de diagrama de árbol de ataque](https://docs.google.com/presentation/d/1o06tUwRsf7HWnZRXnRZ1GgHeMXAfNJbtGlhlH1bOKhA/template/preview?resourcekey=0-sNwWdxodv2yn-G70NyIpFg) |
| **VII. Análisis de riesgos e impacto** | Enumera **4 controles de seguridad** que puedan reducir el riesgo.  *SHA-256, procedimientos de respuesta a incidentes, política de contraseñas, principio de mínimo privilegio* |