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. • *¿La aplicación procesará transacciones?* • *¿Se requerirá de un intenso procesamiento back-end?* • *¿Existen regulaciones de la industria que deban considerarse?* La aplicacion debera de poder contactar compradores con vendedores, existe una pasarela de pagos donde el cliente dejara sus datos para procesar el pago, guardar y asegurar los datos para que el cliente se sienta seguro, la aplicacion debera ser facil de usar, dependiendo de la region debera poder cumplir ciertas regulaciones legales.
II. Definición del alcance técnico	Lista de tecnologías utilizadas por la aplicación: • *API* • *PKI* • *AES* • *SHA-256* • *SQL* El uso de la API se haria para conectar con difentes funcionalidades como la pasarela de pago, que fluya mejor el back-end con front-end haciendo que la experiencia de usuario sea mejor, los PKI servirian para garantizar la autneticidad entre el comprador y vendedor tambien asegura que la informacion que se intercambie entre usuario y servidor sea cifrada, AES nos ayudara a cifrar los datos que el cliente envie, esto incluye los datos de la tarjeta bancaria tanto almacenados como en transito, es decir que mantiene cifrada cuando se envia la informacion y cuando se almacena en la BBDD, SHA-256 se utilizara en el caso que un cliente quiera acceder a su cuenta, al ingresar sus credenciales de usuario comprobara el HASH con el que esta almacenado de esta manera se comprueba que no haya una alteracion en la informacion del usuario y el uso de SQL nos ayuda a almacenar los datos que el cliente proporcione o informacion que sera necesario almacenar como crear un historial de compras, devoluciones, etc. Escribe **2 o 3 oraciones** (entre 40 y 60 palabras) que describan por qué eliges priorizar esa tecnología sobre las demás.
III. Descomposición de la aplicación	Ejemplo de diagrama de flujo de datos Usuario se registra, se guardan su informacion en la BBDD. Usuario inicia sesion, se comprueba sus credenciales con la base de

	datos, en caso de que sus credenciales coincidan le da acceso a la aplicacion caso contrario no le da acceso. Usuario busca un producto, se realiza un proceso de busqueda en la base de datos, se muestra al usuario todas las coincidencias Usuario quiere comprar un producto, le envian a rellenar su informacion, pasarela y metodo de pago, se ve la entrega o recogida del producto.
IV. Análisis de amenazas	En la hoja de trabajo PASTA, enumera **2 tipos de amenazas** que sean riesgos para la información que la aplicación maneja. • *¿Cuáles son las amenazas internas?* • *¿Cuáles son las amenazas externas?* Amenazas internas: Informacion no cifrada, falta de certificados PKI, base de datos vulnerable a inyeccion SQL. Amanezas Externas: Que empleados tengan acceso a todo (principio de minimo privilegio), ataque de intermediario (Man in the middle).
V. Análisis de vulnerabilidades	En la hoja de trabajo de PASTA, enumera **2 vulnerabilidades** que podrían explotarse. • *¿Podría existir algún problema con la base de código?* • *¿Es posible que haya debilidades en la base de datos?* • *¿Es posible que existan fallas en la red?* La pasalera de pagos, problemas en como se encripta la informacion. Registro de usuarios, contraseña con pocas medidas de seguridad, falta de normas minimas para una contraseña.
VI. Modelado de ataques	Utiliza el diagrama PASTA para crear un árbol de ataque. Amenaza -> ataque de intermediario vulnerabilidad -> datos con cifrados en transmision Amenaza -> Ataque de fuerza bruta por parte de un tercero Vulnerabilidad -> falta de MFA Amenaza -> Personal con acceso a toda la informacion vulnerabilidad -> Falta de principio de minimo privilegios.
VII. Análisis de riesgos e impacto	Enumera **4 controles de seguridad** sobre los que hayas aprendido que puedan reducir el riesgo. - Marntener el software y la dependencias actualizadas - MFA, para poder comprobar la identidad del usuario - Principio de minimos privilegios para saber que personal deberia poder acceder a la informacion de usuarios con datos confidenciales. - Certificados PKI para la autetificacion de cliente o serividor y que pueda fluir la informacion de manera segura.