**Resumen de la actividad**

En esta actividad, practicarás el uso del marco del modelo de amenazas del Proceso de Simulación de Ataques y Análisis de Amenazas (PASTA). Determinarás si es seguro lanzar una nueva aplicación de compras.

El modelado de amenazas es una parte importante del desarrollo de software seguro. Los equipos de seguridad suelen realizar modelos de amenazas para identificar vulnerabilidades antes de que lo hagan los actores maliciosos. PASTA es un marco de uso común para evaluar el perfil de riesgo de las nuevas aplicaciones.

**Escenario**

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.

Formas parte del creciente equipo de seguridad de una empresa para entusiastas y coleccionistas de zapatos. La empresa se está preparando para lanzar una aplicación móvil que facilite a sus clientes la compra y venta de zapatos.

Estás realizando un modelo de amenazas de la aplicación utilizando el marco PASTA. Pasarás por cada una de las siete etapas del marco para identificar los requisitos de seguridad de la nueva aplicación de la empresa de zapatos.

**Instrucciones paso a paso**

Sigue las instrucciones y responde a las preguntas incluidas para completar la actividad.

**Parte 1 - Accede a los recursos**

Paso 1: Accede a la plantilla

Para usar la plantilla para este elemento del curso, haz clic en el enlace de abajo y selecciona “*Use Template”* (Usar plantilla).

Enlace a la plantilla: [Hoja de trabajo de PASTA](https://docs.google.com/document/d/1u3aU6ZnWfcjzwZt79OdIwJ27dcyCZYDtmEEMivey3Os/template/preview?resourcekey=0-TAMA_2t0BCj5-BL9wG23Ng)

O BIEN

Si no tienes una cuenta de Google, puedes descargar la plantilla directamente desde el siguiente archivo adjunto.

[Activity Apply the PASTA threat model framework\_PASTA-worksheet](https://d3c33hcgiwev3.cloudfront.net/Y8hSBfvQR22yGveMgthPKQ_2293eb1ec93e4f68976b6d78220e64f1_Activity-Apply-the-PASTA-threat-model-framework_PASTA-worksheet.docx?Expires=1706313600&Signature=dR10KhItYsjy~v7KIsz2ErQEXrFkP2LzSszU9TjMUig~wxuBWU-LYr32f6il3hmuar4NqgnnVbTWeeahnEKESUR8QA4~voXyWNbfO-VmxTNqJ1G9DyOem6hVOuL9RXHhNi8y0rFdJGJ8Ws9vFd2yPHqLEQiRPyBzzpUFN3CTVEw_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/Y8hSBfvQR22yGveMgthPKQ_2293eb1ec93e4f68976b6d78220e64f1_Activity-Apply-the-PASTA-threat-model-framework_PASTA-worksheet.docx?Expires=1706313600&Signature=dR10KhItYsjy~v7KIsz2ErQEXrFkP2LzSszU9TjMUig~wxuBWU-LYr32f6il3hmuar4NqgnnVbTWeeahnEKESUR8QA4~voXyWNbfO-VmxTNqJ1G9DyOem6hVOuL9RXHhNi8y0rFdJGJ8Ws9vFd2yPHqLEQiRPyBzzpUFN3CTVEw_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

Paso 2: Accede a los materiales de apoyo

Los siguientes materiales de apoyo te ayudarán a completar esta actividad. Mantenlos abiertos a medida que avances en los siguientes pasos.

Para usar los materiales de apoyo para este elemento del curso, haz clic en el siguiente enlace y selecciona “*Use Template”* (Usar plantilla).

Enlace a los materiales de apoyo:

* [Diagrama de flujo de datos de PASTA](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g)
* [Árbol de ataque de PASTA](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?resourcekey=0-zYPY7AhPJdcClXamlAfOag#slide=id.p)

O BIEN

Si no tienes una cuenta de Google, puedes descargar los materiales de apoyo directamente desde el archivo adjunto a continuación.

[Activity Apply the PASTA threat model framework\_PASTA-data-flow-diagram](https://d3c33hcgiwev3.cloudfront.net/EI8B6OzSTJWQp2uo9uzJGg_37709d25075249eaa903fac9091b06f1_Activity-Apply-the-PASTA-threat-model-framework_PASTA-data-flow-diagram.pptx?Expires=1706313600&Signature=VcgAHuNE6Ikr-Ge7vuQ0GnlhvXhFly2QT37voE6rXlupQ-HJxrPz2UVRNFyfLXZb~KbLD7GzoL8YkAOSunicMUiAE2gzjySpSKrffKIa4i4lcfJZE1TdrXWCi4ZiVXeinScuN6yM8eR1OQpJftAC0QRk0X2I28uAvw794P~hB~k_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[PPTX File](https://d3c33hcgiwev3.cloudfront.net/EI8B6OzSTJWQp2uo9uzJGg_37709d25075249eaa903fac9091b06f1_Activity-Apply-the-PASTA-threat-model-framework_PASTA-data-flow-diagram.pptx?Expires=1706313600&Signature=VcgAHuNE6Ikr-Ge7vuQ0GnlhvXhFly2QT37voE6rXlupQ-HJxrPz2UVRNFyfLXZb~KbLD7GzoL8YkAOSunicMUiAE2gzjySpSKrffKIa4i4lcfJZE1TdrXWCi4ZiVXeinScuN6yM8eR1OQpJftAC0QRk0X2I28uAvw794P~hB~k_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[Activity Apply the PASTA threat model framework\_PASTA-attack-tree-diagram](https://d3c33hcgiwev3.cloudfront.net/PpqdVzEbSIisYPRLFbSKbw_a523590b1b114d9b832d5ca7957e28f1_Activity-Apply-the-PASTA-threat-model-framework_PASTA-attack-tree-diagram.pptx?Expires=1706313600&Signature=aY9uvgolN7Ee4kYJq77NnR3fMnsHmXu7sG3ozDu98aGWrI06l90ht~W73-LYSqtB~uWMfShWCf3nvGeYmRDiVwt-7L~EpcWfBAsz7e0KtR4vPnlusEBzCDZdyofjWXhKpTe8IjB-QtFL5x3-gDwB1Cnd2VWKC1xIvMKqTAAyQbw_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[PPTX File](https://d3c33hcgiwev3.cloudfront.net/PpqdVzEbSIisYPRLFbSKbw_a523590b1b114d9b832d5ca7957e28f1_Activity-Apply-the-PASTA-threat-model-framework_PASTA-attack-tree-diagram.pptx?Expires=1706313600&Signature=aY9uvgolN7Ee4kYJq77NnR3fMnsHmXu7sG3ozDu98aGWrI06l90ht~W73-LYSqtB~uWMfShWCf3nvGeYmRDiVwt-7L~EpcWfBAsz7e0KtR4vPnlusEBzCDZdyofjWXhKpTe8IjB-QtFL5x3-gDwB1Cnd2VWKC1xIvMKqTAAyQbw_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

**Parte 2 - Completa las etapas de PASTA**

Paso 1: Identifica los objetivos empresariales de la aplicación móvil

El objetivo principal de la Etapa I del marco PASTA es comprender por qué se desarrolló la aplicación y qué se espera de ella.

***Nota:*** *La Etapa I suele requerir la recopilación de información de muchas personas de una empresa.*

Primero, revisa la siguiente descripción de por qué la empresa de zapatos decidió desarrollar esta nueva aplicación:

**Descripción:** Nuestra aplicación debe conectar a la perfección a vendedores y compradores. Debe ser fácil para los usuarios registrarse, iniciar sesión y administrar sus cuentas. La privacidad de los datos es una gran preocupación para nosotros. Queremos que los usuarios se sientan seguros de que somos responsables con su información.

Los compradores deben poder plantear sus dudas directamente a los vendedores. También deberían poder puntuar a los vendedores para fomentar un buen servicio. Las ventas deben ser claras y rápidas de procesar. Los usuarios deben disponer de varias opciones de pago para facilitar el proceso de compra. El manejo adecuado de los pagos es muy importante para evitar problemas legales.

En la fila de la **Etapa 1** de la **hoja de trabajo de PASTA,** anota de **2 a 3** objetivoscomerciales que hayas identificado a partir de la descripción.

Paso 2: Evalúa los componentes de la aplicación

En la Etapa II se define el alcance tecnológico del proyecto. Normalmente, el equipo de desarrollo de aplicaciones participa en esta etapa porque es el que tiene más conocimientos sobre la base de código y la lógica de la aplicación. Tu responsabilidad como profesional de la seguridad sería evaluar la arquitectura de la aplicación para detectar riesgos de seguridad.

Por ejemplo, la aplicación intercambiará y almacenará una gran cantidad de datos de los usuarios. Estas son algunas de las tecnologías que utilizará:

* Interfaces de programación de aplicaciones (API).
* Infraestructura de claves públicas (PKI).
* Sistema de cifrado avanzado (AES).
* SHA-256.
* SQL.

Considera lo que aprendiste sobre estas tecnologías:

* *¿Cuál de estas tecnologías evaluarías primero? ¿Qué riesgos presentan desde el punto de vista de la seguridad?*

En la fila de la **Etapa II** de la **hoja de trabajo de PASTA**, escribe **2-3 frases** (40-60 palabras) que describan por qué eliges priorizar esa tecnología sobre las demás.

Paso 3: Revisa un diagrama de flujo de datos

Durante la Etapa III de PASTA, el objetivo es analizar cómo la aplicación está manejando la información. Aquí se desglosa cada proceso.

Por ejemplo, uno de los procesos de la aplicación podría ser permitir a los compradores buscar en la base de datos los zapatos que están a la venta.

Abre el recurso de **diagrama de flujo de datos de PASTA**. Revisa el diagrama y considera cómo las tecnologías que evaluaste se relacionan con la protección de los datos del usuario en este proceso.

***Nota:*** *Los desarrolladores de software suelen disponer de diagramas de flujo de datos detallados disponibles para que los equipos de seguridad los usen y verifiquen que la información se procesa de forma segura.*

Paso 4: Utiliza la mentalidad de un atacante para analizar las amenazas potenciales

La Etapa IV consiste en identificar las amenazas potenciales para la aplicación. Esto incluye las amenazas a las tecnologías que enumeraste en la Etapa II. También afecta a los procesos del diagrama de flujo de datos de la Etapa III.

Por ejemplo, el sistema de autenticación de la aplicación podría ser atacado por un virus. La autenticación también podría ser atacada si un agente de amenaza realiza ingeniería social a un empleado.

En la fila de la **Etapa IV** de la hoja de trabajo de PASTA, enumera **2 tipos** de amenazas que supongan un riesgo para la información que maneja la aplicación de la empresa de zapatos.

***Consejo profesional:*** *Los registros internos del sistema que usarás como analista de seguridad son una buena fuente de inteligencia sobre amenazas.*

Paso 5: Enumera las vulnerabilidades que pueden ser aprovechadas por esas amenazas

La etapa V de PASTA es el análisis de vulnerabilidades. Aquí, debes considerar la superficie de ataque de las tecnologías enumeradas en la Etapa II.

Por ejemplo, la aplicación utilizará un sistema de pago. El formulario utilizado para recopilar la información de la tarjeta de crédito puede ser vulnerable si no encripta los datos.

En la **Etapa V** de la **hoja de trabajo de PASTA**, enumera **2 tipos** de vulnerabilidades que podrían aprovecharse.

***Consejo profesional:*** *Recursos como la*  [*lista CVE®*](https://cve.mitre.org/cve/search_cve_list.html) *y*  [*OWASP*](https://owasp.org/www-community/vulnerabilities/) *son útiles para encontrar vulnerabilidades de software comunes.*

Paso 6: Asigna activos, amenazas y vulnerabilidades a un árbol de ataques

En la Etapa VI de PASTA, la información recopilada en los dos pasos anteriores se utiliza para construir un árbol de ataque.

Abre el recurso de **árbol de ataque de PASTA**. Revisa el diagrama y considera cómo los agentes de amenaza pueden aprovechar potencialmente estos vectores de ataque.

**Nota:** Las aplicaciones como esta suelen tener árboles de ataque grandes y complejos con muchas ramas.

Paso 7: Identifica nuevos controles de seguridad que puedan reducir el riesgo

El modelado de amenazas PASTA se usa comúnmente para reducir la probabilidad de los riesgos de seguridad. En la Etapa VII, el objetivo final es implementar defensas y salvaguardas que mitiguen las amenazas.

En la **Etapa VII** de la **hoja de trabajo de PASTA**, enumera **4 controles de seguridad** que hayas aprendido y que puedan reducir las posibilidades de un incidente de seguridad, como una filtración de datos.

**Qué debes incluir en tu respuesta**

Asegúrate de incluir los siguientes elementos en la actividad terminada:

* **2-3** objetivos comerciales.
* **2-3** requisitos tecnológicos.
* **2** amenazas potenciales.
* **2** vulnerabilidades del sistema.
* **4** defensas que limitan el riesgo.