**Características de un modelado de amenaza eficaz**

El **modelado de amenazas** es el proceso de identificación de activos, sus vulnerabilidades y cómo cada uno de ellos está expuesto a las amenazas. Es un enfoque estratégico que combina diversas actividades de seguridad, como la gestión de vulnerabilidades, el análisis de amenazas y la respuesta a incidentes. Los equipos de seguridad suelen realizar estos ejercicios para garantizar que sus sistemas estén adecuadamente protegidos. El modelado de amenazas se usa además para encontrar proactivamente formas de reducir los riesgos para cualquier sistema o proceso comercial.

Tradicionalmente, el modelado de amenazas se asocia con el campo del desarrollo de aplicaciones. En esta lectura, aprenderás sobre las metodologías comunes de modelado de amenazas que se utilizan para diseñar software capaz de resistir ataques. También te informarás acerca de la creciente necesidad de seguridad de las aplicaciones y las formas en que puedes participar.

**Por qué es importante la seguridad de las aplicaciones**

Las aplicaciones se han convertido en una parte esencial del éxito de muchas organizaciones. Por ejemplo, las aplicaciones basadas en la web permiten a los clientes de cualquier parte del mundo conectarse con empresas, sus socios y otros clientes.

Las aplicaciones móviles también cambiaron la forma en que las personas acceden al mundo digital. Los smartphones suelen ser la principal forma en que se intercambian datos entre los usuarios y una empresa. El volumen de datos que procesan las aplicaciones hace que asegurarlas sea clave para reducir el riesgo para las personas que se conectan a ellas.

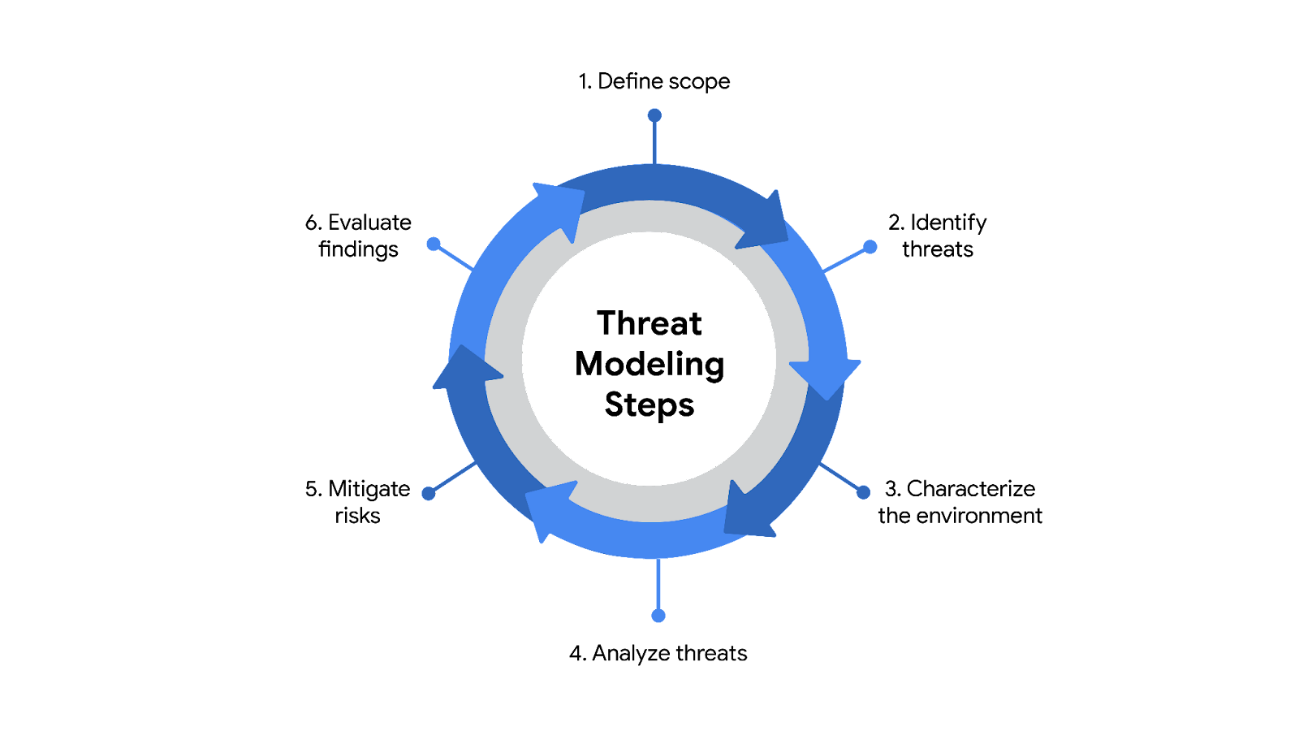
Por ejemplo, supongamos que una aplicación utiliza bibliotecas de registro basadas en Java con la vulnerabilidad Log4Shell ([CVE-2021-44228](https://nvd.nist.gov/vuln/detail/CVE-2021-44228) ). Si esta no se parchea, puede permitir la ejecución remota de código que un atacante puede usar para obtener acceso completo a tu sistema, desde cualquier parte del mundo. Si se explota, una vulnerabilidad crítica como esta puede afectar a millones de dispositivos.

**Defensa de la capa de aplicación**

La defensa de la capa de aplicación requiere de pruebas adecuadas para descubrir debilidades que pueden conducir a un riesgo. El modelado de amenazas es una de las principales formas de garantizar que una aplicación cumpla con los requisitos de seguridad. Estos análisis suelen ser realizados por un equipo de DevSecOps (desarrollo, seguridad y operaciones).

Un proceso típico de modelado de amenazas se realiza en un ciclo:

* Definir el alcance
* Identificar amenazas
* Caracterizar el entorno
* Analizar amenazas
* Mitigar riesgos
* Evaluar los hallazgos



Lo ideal es que el modelado de amenazas se realice antes, durante y después del desarrollo de una aplicación. Sin embargo, realizar un análisis exhaustivo del software consume tiempo y recursos. Se debe evaluar todo: desde la arquitectura de la aplicación hasta sus fines comerciales. Como resultado, a lo largo de los años se desarrolló una serie de metodologías de modelado de amenazas para hacer que el proceso sea más sencillo.

**Nota:** El modelado de amenazas debe incorporarse en cada etapa del ciclo de vida del desarrollo de software (SDLC).

**Marcos comunes**

Al realizar un modelado de amenazas, hay varios métodos que se pueden utilizar, como los siguientes:

* STRIDE
* PASTA
* Trike
* VAST

Las organizaciones pueden usar cualquiera de estas metodologías para recopilar información y tomar decisiones que les permitan mejorar su postura de seguridad. Básicamente, el modelo “correcto” depende de la situación y los tipos de riesgos a los que una aplicación podría enfrentarse.

**STRIDE**

STRIDE es una metodología de modelado de amenazas desarrollada por Microsoft. Se utiliza comúnmente para identificar vulnerabilidades en seis vectores de ataque específicos. El acrónimo en inglés representa cada uno de estos vectores: suplantación, manipulación, repudio, divulgación de información, denegación de servicio y elevación de privilegios.

**PASTA**

El **proceso de simulación de ataques y análisis de amenazas** (PASTA, por sus siglas en inglés) es un proceso de modelado de amenazas centrado en el riesgo desarrollado por dos líderes de OWASP y respaldado por una empresa de ciberseguridad llamada VerSprite. Su enfoque principal es descubrir evidencia de amenazas viables y representar esta información como un modelo. El diseño basado en la evidencia de la metodología PASTA puede aplicarse al modelado de amenazas de una aplicación o el entorno que da soporte a esa aplicación. Su proceso de siete etapas consta de varias actividades que incorporan artefactos de seguridad relevantes del entorno, como informes de evaluación de vulnerabilidades.

**Trike**

Trike es una metodología y herramienta de código abierto que adopta un enfoque centrado en la seguridad para el modelado de amenazas. Se usa comúnmente para enfocarse en permisos de seguridad, casos de uso de aplicaciones, modelos de privilegios y otros elementos que propician un entorno seguro.

**VAST**

La metodología de modelado de amenazas visual, ágil y simple (VAST, por sus siglas en inglés) forma parte de una plataforma automatizada de modelado de amenazas llamada ThreatModeler®. Muchos equipos de seguridad optan por utilizar VAST como una forma de automatizar y optimizar sus evaluaciones de modelado de amenazas.

**Cómo participar en el modelado de amenazas**

El modelado de amenazas suele ser llevado a cabo por profesionales de la seguridad experimentados, pero casi nunca de forma independiente. Esto sucede sobre todo cuando se trata de asegurar aplicaciones. Los programas son sistemas complejos responsables de manejar una gran cantidad de datos y procesar una gran variedad de comandos de usuarios y otros sistemas.

Una de las claves para el modelado de amenazas es plantear las preguntas correctas:

* ¿En qué estamos trabajando?
* ¿Qué es lo que puede salir mal?
* ¿Qué estamos haciendo al respecto?
* ¿Nos hemos ocupado de todo?
* ¿Hicimos un buen trabajo?

Se necesita tiempo y práctica para aprender a trabajar con elementos como diagramas de flujo de datos y árboles de ataque. Sin embargo, todas las personas pueden aprender a realizar un modelado de amenazas efectivo. Independientemente de tu nivel de experiencia, participar en uno de estos ejercicios siempre comienza con el simple hecho de plantearse las preguntas correctas.

**Conclusiones clave**

Muchas personas utilizan aplicaciones de software para llevar adelante sus vidas cotidianas. En la actualidad, asegurar las aplicaciones es más importante que nunca. El modelado de amenazas es una de las principales formas de determinar si existen controles de seguridad para proteger la privacidad de los datos. Desarrollar las habilidades necesarias para liderar una actividad de modelado de amenazas es cuestión de práctica. Sin embargo, incluso un analista de seguridad con poca experiencia puede aportar una contribución valiosa al proceso. Todo comienza por adoptar la mentalidad de atacante y pensar críticamente sobre cómo se manejan los datos.