# Modelo de Madurez de Aseguramiento de Software

# *Software Assurance Maturity Model (OWASP SAMM)*

Mitsiu Alejandro Carreño Sarabia
Desarrollo de Software
Designa
Aguascalientes, México
mitsiu.carreno@alumnos.ucags.edu.mx

Yesica Díaz Gutierrez
Departamento de Planeación Geodésica
INEGI
Aguascalientes, México
yesica.diaz@alumnos.ucags.edu.mx

***Resumen* — En este documento se presenta el modelo propuesto por Open Worldwide Application Security Project - Software Assurance Maturity Model (OWASP SAMM) el cuál tiene como principal objetivo ofrecer un marco de trabajo que ayuda/orienta a las organizaciones a evaluar, formular e implementar estrategias enfocadas en seguridad de software.**

***Palabras Clave - Modelo de Madurez, Seguridad, Software, OWASP, Ciclo de desarrollo.***

## I. Introducción

Este modelo se centra en asegurar la seguridad en el software así como su contexto. Desarrollado por OWASP con la finalidad de ayudar a las organizaciones a evaluar, formular e implementar estrategias enfocadas en seguridad de software desde una perspectiva del Software Development Lifecycle (SDLC) existente. OWASP SAMM está planeada para poderse implementar en diversos contextos, con diversos niveles de interacción con software (desarrollo, outsourcing o adquisición de software). El modelo SAMM se compone de 15 prácticas de seguridad agrupadas en funciones comerciales. Cada práctica de seguridad a su vez cuenta con dos flujos de actividades, las cuales están estructuradas en tres niveles de maduración.

## II. Definición

SAMM significa Software Assurance Maturity Model (Modelo de madurez de aseguramiento de software) [1].

Es un enfoque altamente prescriptivo y de fácil uso diseñado para ayudar a las organizaciones a mejorar su postura de seguridad del software. SAMM es accesible y medible, lo que lo hace adecuado incluso para aquellos que no son expertos en seguridad.

## III. Características

El establecimiento y organización del modelo SAMM dentro de una organización implica cierta estructura y configuración como soporte.

- Análisis del estado actual en términos de seguridad, identificar vulnerabilidades y debilidades, y medir su nivel de madurez en seguridad del software.
- Establecimiento de metas claras y alineadas con los objetivos generales de la empresa en cuanto a seguridad del software. Estas metas deben ser específicas y alcanzables.
- Creación de un plan estratégico que describe cómo la organización alcanzará sus metas de seguridad del software, identificando pasos intermedios, actividades, recursos y plazos necesarios para la implementación.
- Orientación específica sobre cómo llevar a cabo acciones concretas para mejorar la seguridad del software. El modelo proporciona directrices detalladas sobre qué prácticas de seguridad implementar, cómo hacerlo y cómo medir el progreso.

SAMM se compone de 15 prácticas de seguridad organizadas en 5 funciones comerciales. Cada práctica incluye actividades divididas en 3 niveles de madurez. Los niveles inferiores son menos formales y más fáciles de implementar

que los superiores. Por lo tanto, el modelo no requiere que todas las organizaciones alcancen el máximo nivel de madurez en todas las categorías; permite la adaptación según las necesidades específicas de cada organización.

### *A. Áreas Críticas de Negocios en SAMM*

- **Governance (Gobernanza):** Se centra en la gestión de actividades de desarrollo de software desde una perspectiva de gobierno. Incluye políticas de seguridad, gestión de riesgos y supervisión de actividades de desarrollo.
- **Design (Diseño):** Trata cómo se planifican y diseñan sistemas de software desde el principio, incluyendo la especificación de requisitos de seguridad y arquitecturas de alto nivel.
- **Implementation (Implementación):** Aborda la construcción y despliegue de software, incluyendo la implementación de medidas de seguridad, la gestión de dependencias de terceros y la gestión de defectos de seguridad.
- **Verification (Verificación):** Se enfoca en verificar la seguridad del software a través de pruebas, revisiones de código y evaluaciones de seguridad.
- **Operations (Operaciones):** Se refiere a la gestión y el mantenimiento de la seguridad del software una vez que está en producción, incluyendo la gestión de incidentes de seguridad y la protección de datos en producción.

### *B. Prácticas de Seguridad en SAMM*

Cada una de las cinco áreas críticas de negocios mencionadas anteriormente se desglosa en tres prácticas de seguridad específicas. En total, hay quince prácticas de seguridad diferentes en SAMM “Fig. 1 Estructura OWASP SAMM”.

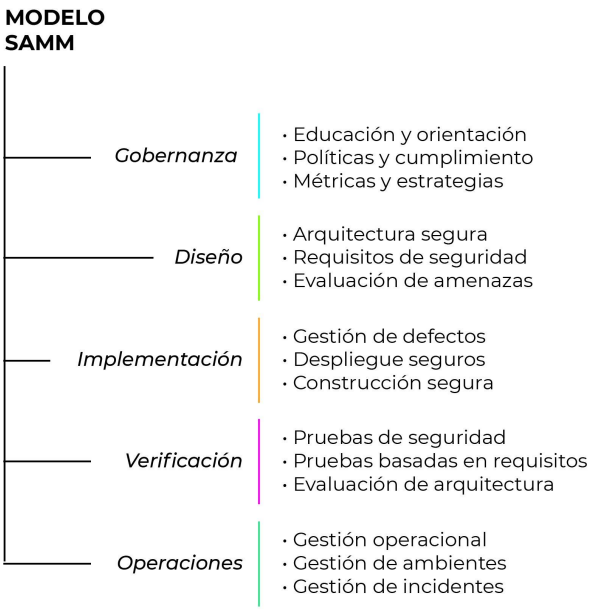


Figure 1. Estructura OWASP SAMM

### *C. Niveles de Madurez en SAMM*

Cada práctica de seguridad tiene tres niveles de madurez que representan diferentes etapas de mejora:

- **Inicial:** En este nivel, la organización está en las primeras etapas de establecer prácticas de seguridad en esa área. Se realizan actividades básicas de seguridad.
- **Definido:** En este nivel, se han establecido prácticas más sólidas y se han definido objetivos de seguridad específicos. La organización tiene un enfoque más estructurado en esa área.
- **Optimizado:** En el nivel más alto de madurez, la organización ha optimizado sus prácticas de seguridad en esa área y ha alcanzado objetivos avanzados. Se siguen prácticas de seguridad de vanguardia y se busca la mejora continua.

## IV. Aplicaciones

El OWASP SAMM es un marco que se puede aplicar a una amplia variedad de aplicaciones y proyectos de desarrollo de software en diversas industrias. A continuación, se presentan ejemplos de aplicaciones y escenarios donde puede ser útil:

- Las aplicaciones Web pueden ser complejas cuando interactúan con múltiples sistemas, y para la mayoría de las organizaciones la tarea de producir una

aplicación segura o corregir una ya existente puede ser difícil [2].

- Las aplicaciones para dispositivos móviles son un vector de vulnerabilidad, por lo que asegurar los procesos de producción, despliegue y mantenimiento es fundamental para proteger datos, infraestructura, y propiedad intelectual.
- Desarrollo de software para la gestión de cursos en línea implementado por las instituciones educativas.
- El gobierno desarrolla software para gestión de registros o la seguridad nacional.

Por lo que SAMM ayuda a garantizar que estas aplicaciones sean seguras desde el inicio y cumplan con los estándares de seguridad

## V. Conclusiones

El modelo OWASP SAMM cubre uno de los aspectos más subestimados de la industria, la seguridad, dada su adaptabilidad, permite que organizaciones de diversas índoles, metodologías, capacidades técnicas y tamaños puedan implementar el modelo. Dada esta flexibilidad, cada organización puede establecer los objetivos que mejor se adapten a sus necesidades. Dadas estas características, el modelo OWASP SAMM es pionero en el enfoque que da priorizando la seguridad en el flujo de madurez natural del software.

## Referências Bibliográfica


[1] D. Sebastien and W. Bart, "OWASP SAMM V2.0," https://drive.google.com/file/d/1cI3Qzfrly_X89z7StLWI5p_Jfqs0-OZv/view

[2] https://www.magazcitum.com.mx/index.php/archivos/1416