



UTT

UNIVERSIDAD TECNOLÓGICA DE TIJUANA

GOBIERNO DE BAJA CALIFORNIA

TEMA: Codificación Segura

PRESENTADO POR: Toledo Pérez Cristian Alejandro

GRUPO: 7B

MATERIA: Seguridad en el Desarrollo de Proyectos

PROFESOR: Resffa Elizabeth Fierro Garcia

Tijuana, Baja California, 17 de mayo del 2023

1.- ¿Que es la codificación segura?

La codificación, o la programación, es la práctica de diseñar programas ejecutables en un lenguaje que puede ser interpretado por nuestro ordenador. Cuando un desarrollador de software escribe su código fuente, debe tener en cuenta muchas cosas, como:

- La arquitectura y los requerimientos de diseño de la aplicación
- Optimización y eficiencia del código
- Seguridad del código

2.- ¿Por qué es importante?

En el proceso de desarrollo del software es fundamental tener en cuenta los posibles incidentes de ciberseguridad, para poder evitar la consiguiente filtración de datos sensibles e información personal. La codificación segura facilita a los programadores poder eliminar las vulnerabilidades más comunes en el software aplicando buenas prácticas denominadas estándares de codificación segura que ayudan a prevenir ciberataques.

3.- ¿Cómo programar de forma de segura?

Hay abundante literatura sobre las mejores prácticas en codificación segura. Por ejemplo, The Open Web Application Security Project (OWASP) ha creado un conjunto de directrices que ayudan a los desarrolladores a mitigar habituales vulnerabilidades de seguridad. De forma parecida, los estándares de codificación segura SEI CERT se apoyan en diez buenas prácticas de codificación segura que los programadores pueden incorporar para maximizar la seguridad de la aplicación.

4.- Recursos

Recurso	Descripción
OWASP Developer Guide	Una útil piedra angular para ayudar a los desarrolladores a evitar errores de programación de software. También puedes echar un vistazo a su herramienta de búsqueda de dependencias y que revela públicamente vulnerabilidades que podrían afectar a tu proyecto.
Microsoft's Bible on Secure Coding	Al igual que OWASP y SEI CERT, Microsoft también ha hecho una guía sobre prácticas de codificación segura para

	desarrolladores que estén creando software para sus productos. La guía cubre cada etapa del ciclo de vida del desarrollo del software y es muy completa.
OWASP Security Knowledge Framework	El OWASP SKF es una aplicación web de código abierto que explica prácticas de codificación segura en distintos lenguajes de programación. Es una forma fantástica de acelerar a ti y a tu equipo en el aprendizaje de lo básico en codificación segura sin importar el lenguaje que estés usando.
CheckMarx y CAST Software	CheckMarx y CAST son ejemplos de empresas que analizarán y estudiarán tu código para identificar potenciales vulnerabilidades de seguridad. Si tienes poca o nula experiencia con la codificación segura, puede ser una buena idea usar sus servicios para asegurar la seguridad y robustez de tu código fuente.
Tutoriales de Red Hat	Estos tutoriales son una forma muy buena para conseguir que tu equipo empiece a usar las prácticas de codificación segura. Red Hat ofrece tutoriales que cubren lo básico en validación de entrada, autorización y otras prácticas de codificación segura.