UTT
UNIVERSIDAD TECNOLÓGICA DE TIJUANA
GOBIERNO DE BAJA CALIFORNIA

TEMA:

Especificaciones de principios de código seguro

PRESENTADO POR:

Pliego Cortes Giovanni

GRUPO:

9° B

MATERIA:

Desarrollo móvil integral

CARRERA:

TI. Desarrollo de software multiplataforma

Docente:

Ray Brunett Parra Galaviz

Tijuana, Baja California, 15 de enero del 2024

Los principios de codificación segura representan un pilar fundamental en el desarrollo de software robusto y protegido contra vulnerabilidades. A través de diversas fuentes especializadas, se han establecido lineamientos claros y prácticas recomendadas que buscan minimizar los riesgos asociados con ataques cibernéticos. Este enfoque es relevante en un contexto donde la creciente digitalización hace que la seguridad sea un factor crítico para la integridad y confianza de los sistemas.

Uno de los principales referentes en este ámbito es OWASP (Open Web Application Security Project), una organización reconocida globalmente por sus esfuerzos en promover la seguridad en el desarrollo de software. OWASP proporciona guías como el *Secure Coding Practices Quick Reference Guide*, que enfatiza aspectos como la validación de entradas, el manejo seguro de datos y la protección contra vulnerabilidades comunes, tales como inyecciones o exposiciones accidentales de información sensible.

Por otro lado, instituciones como NIST (National Institute of Standards and Technology) han publicado estándares como el *Secure Software Development Framework (SSDF)*, que se enfoca en incorporar prácticas de seguridad desde las primeras etapas del ciclo de vida del software. Este marco subraya la importancia de la revisión de código, pruebas de penetración y monitoreo continuo para identificar y mitigar riesgos.

Además, el estándar ISO/IEC 27034 aborda la seguridad en las aplicaciones desde una perspectiva organizacional, estableciendo controles y procesos que deben implementarse para garantizar la protección de los sistemas frente a amenazas internas y externas.

En el ámbito empresarial, muchas compañías han adoptado herramientas de análisis estático y dinámico para automatizar la identificación de vulnerabilidades, lo cual complementa los principios de codificación segura y asegura la aplicación de estos estándares en proyectos reales.

En conclusión, los principios de codificación segura no solo son guías teóricas, sino que también se traducen en prácticas concretas respaldadas por organizaciones y estándares internacionales. Estas directrices permiten a los desarrolladores construir aplicaciones más seguras y resilientes, protegiendo así tanto los datos de los usuarios como la reputación de las organizaciones que dependen de la tecnología.