UTT
UNIVERSIDAD TECNOLÓGICA DE TIJUANA
GOBIERNO DE BAJA CALIFORNIA

TEMA:

Secure Coding Principles Specification.

PRESENTADO POR:

Medina Palacios Fernando

GRUPO:

10° B

MATERIA:

Desarrollo móvil integral

CARRERA:

TI. Desarrollo de software multiplataforma

Docente:

Ray Brunett Parra Galaviz

Tijuana, Baja California, 15 de enero del 2025

Los principios de codificación segura son directrices fundamentales que buscan garantizar la creación de software robusto y protegido contra vulnerabilidades y amenazas. A continuación, se presentan los principios más destacados:

- **Seguridad por defecto:** El sistema debe configurarse con parámetros de seguridad preestablecidos desde su inicio. Por ejemplo, al crear una cuenta de usuario, se debería asignar una contraseña generada automáticamente con caracteres aleatorios y exigir al usuario cambiarla en su primer acceso, siguiendo políticas de seguridad establecidas.
- **Fallar de manera segura:** Los errores deben manejarse de forma que no comprometan la seguridad del sistema. Si ocurre un fallo, el sistema debería revertir cualquier acción parcial y notificar al usuario sin revelar detalles internos que puedan ser explotados.
- **Minimizar la superficie de ataque:** Se debe reducir al máximo las áreas del sistema susceptibles a ataques. Cada funcionalidad adicional puede introducir nuevos riesgos; por ello, es esencial limitar las funciones a lo estrictamente necesario y restringir su acceso según el rol del usuario.
- **Defensa en profundidad:** Implementar múltiples capas de seguridad para proteger el sistema, de modo que, si una capa falla, otras continúen brindando protección.
- **Principio del mínimo privilegio:** Otorgar a cada usuario o proceso únicamente los permisos necesarios para realizar sus funciones, evitando accesos innecesarios que puedan ser explotados maliciosamente.
- **Validación y sanitización de entradas:** Verificar y limpiar todos los datos ingresados por los usuarios para prevenir ataques como inyecciones SQL o scripts entre sitios (XSS).
- **Control de acceso y autenticación segura:** Implementar mecanismos robustos de autenticación, como la autenticación multifactorial, y gestionar adecuadamente las sesiones para proteger el acceso a los datos y funcionalidades del sistema.
- **Protección de datos personales:** Respetar los derechos de los usuarios sobre sus datos, obteniendo su consentimiento explícito para la recopilación y procesamiento, y asegurando la minimización de datos, es decir, recolectar solo la información estrictamente necesaria.

La aplicación rigurosa de estos principios durante el ciclo de desarrollo de software es esencial para construir aplicaciones seguras y resilientes frente a posibles amenazas y ataques.