Logo

Description automatically generated with medium confidence

**Tarea 2**

**Seguridad del Software**

**Especialización en Ingeniería del Software**

**MAURICIO SIERRA DEL CHIARO**

1. Por qué es importante asegurar el software?

El objetivo principal es evitar que los hackers tomen control de nuestro sistema o acceso no autorizado a información del software. Además de evitar daños físicos en algunos casos.

Los software cada vez hacen parte de nuestra vida cotidiana y cada vez más conectados a internet y por consiguiente se tiene un riesgo latente de un ciberataque.

1. A que se refiere los estándares de codificación segura y cuáles son las principales dificultades y barreras para su implementación en las organizaciones?

Los estándares de codificación segura son un conjunto de mejores prácticas para desarrollar software para evitar vulnerabilidades en la aplicación.

Las principales barreras de implementación en las organizaciones son: Mínimas consideraciones de seguridad durante el desarrollo de la aplicación, no pensar como un atacante mientras se desarrolla el software, diseños y/o especificaciones malas, interacciones inesperadas con otros componentes o con un ambiente de ejecución diferente para el que fue diseñado o desarrollado.

1. ¿Cuáles son las mejores prácticas y herramientas recomendadas para la construcción de software seguro y cuáles cuando el software es adquirido y no construido directamente?

Las herramientas recomendadas es usar IDEs que nos ayudan a detectar errores de forma temprana y evitar excepciones en tiempo de ejecución. Además tienen ayudas para hacer despliegue de la aplicación, herramientas de entrenamiento y herramientas adicionales que nos ayudan a cumplir las necesidades de los proyectos. Como los analizadores estáticos de código que nos ayudan a identificar muchos problemas un ejemplo seria SCALe que nos ayuda a verificar código en C, C++, Java, PERL, Python basados en reglas predefinidas y extensibles por los equipos de desarrollo. Además hace análisis de manejo de hilos de forma segura, el flujo de los datos en aplicaciones Android y flujo de llamadas en los sistemas operativos.

En los casos que no seamos los desarrolladores del código se recomienda tener instaladas por lo menos los parches de seguridad. En caso de tener acceso al código fuente también se recomienda hacerle un análisis estático a ese código. Testear los binarios. Requerir los reportes de pruebas de seguridad. Aplicar la defensa en profundidad y solo habilitar los módulos que son requeridos. Hacer pruebas dinámicas o de penetración e instalar un sistema de monitoreo externo.