

Desarrollo de Software Seguro

Código: DSS-001

Propuesta de Valor: DESARROLLO - PROGRAMACIÓN - METODOLOGÍAS

Duración: 20 Horas



El tema de mejorar la seguridad del software lleva años tratando de solucionarse. Cada fabricante ha establecido sus propias metodologías con el objetivo de garantizar que las aplicaciones son creadas con criterios de seguridad desde el diseño, para evitar en la medida de lo posible la aparición de vulnerabilidades. Y no es sólo un tema de hacer las cosas bien desde el principio. Es un tema de costes. Siempre solucionar los problemas a posteriori es más caro que a priori, en el diseño. En el mundo del software vale más diseñar y pensar bien las cosas antes de lanzarlas al mercado que una vez que las aplicaciones ya se han comercializado como se verá en este curso.



AUDIENCIA

- Este curso está dirigido a: Líderes de Proyecto de desarrollo, Desarrolladores, Analistas de Calidad, Analistas Funcionales, Oficiales de Seguridad Informática, Auditores.



PRE REQUISITOS

- No tiene prerequisites previos



OBJETIVOS

- Introducción
- Ciclo de Vida Orientado a la Seguridad
- Educación y Conciencia
- Verificación Automatizada



CERTIFICACIÓN DISPONIBLE

- Certificación emitida por COGNOS.



CONTENIDO

1. INTRODUCCIÓN

- 1.1. ¿QUÉ SIGNIFICA DESARROLLO SEGURO?
- 1.2. ¿POR QUÉ ES IMPORTANTE DESARROLLAR DE FORMA SEGURA?

2. CICLO DE VIDA ORIENTADO A LA SEGURIDAD

- 2.1. EDUCACIÓN Y CONCIENCIA
- 2.2. ORIGEN DEL PROYECTO (INCEPTION)
- 2.3. DEFINIR LAS MEJORES PRÁCTICAS A SEGUIR
- 2.4. VALORACIÓN Y ANÁLISIS DEL RIESGO DEL PRODUCTO
- 2.5. CASOS DE ABUSO
- 2.6. POLÍTICAS DE CODIFICACIÓN SEGURA
- 2.7. POLÍTICAS DE PRUEBAS SEGURAS
- 2.8. EMPUJANDO LA CALIDAD: ENTRENAMIENTO, REVISIÓN DE PARES, ACTUALIZACIÓN DE MODELOS, PRUEBA
- 2.9. REVISIONES FINALES DE SEGURIDAD
- 2.10. LIBERACIÓN DEL PRODUCTO
- 2.11. EJECUTANDO LA RESPUESTA A LA SEGURIDAD

3. NIVELES DE VERIFICACIÓN DE SEGURIDAD

- 3.1. VERIFICACIÓN AUTOMATIZADA
- 3.2. VERIFICACIÓN MANUAL
- 3.3. VERIFICACIÓN DE DISEÑO
- 3.4. VERIFICACIÓN INTERNA

4. REQUERIMIENTOS A VERIFICAR

- 4.1. REQUERIMIENTOS DE SEGURIDAD DE ARQUITECTURA
- 4.2. REQUERIMIENTOS DE AUTENTICACIÓN Y CONTROL DE ACCESO
- 4.3. REQUERIMIENTOS DE MANEJO DE SESIÓN
- 4.4. REQUERIMIENTOS DE VALIDACIÓN DE ENTRADA DE DATOS
- 4.5. REQUERIMIENTOS DE CRIPTOGRAFÍA
- 4.6. REQUERIMIENTOS DE MANEJO DE ERROR
- 4.7. REQUERIMIENTOS DE PROTECCIÓN DE DATOS
- 4.8. REQUERIMIENTOS DE SEGURIDAD DE COMUNICACIÓN
- 4.9. REQUERIMIENTOS DE SEGURIDAD EN HTTP
- 4.10. REQUERIMIENTOS DE CONFIGURACIÓN DE SEGURIDAD
- 4.11. REQUERIMIENTOS DE BÚSQUEDA DE CÓDIGO MALICIOSO
- 4.12. REQUERIMIENTOS DE SEGURIDAD INTERNA



BENEFICIOS

- Al finalizar el curso el estudiante podrá garantizar que las aplicaciones son creadas con criterios de seguridad desde el diseño, para evitar en la medida de lo posible la aparición de vulnerabilidades.