Security Chapters - Desarrollo Seguro

1. Finalidad

La finalidad de "Security Chapters" es proporcionar a los alumnos unos conocimientos, habilidades y herramientas que puedan implementar en su día a día para incrementar la seguridad en sus ámbitos de acción y responsabilidad buscando la certificación de habilidades.

En el caso del itinerario de "Desarrollo Seguro" se persigue proporcionar a los asistentes los conocimientos y capacidades fundamentales necesarias para planificar, desarrollar e implementar soluciones software seguras desde las fases más tempranas de su desarrollo.

2. Créditos / Horas del plan de estudios

La distribución de las 16 horas de la fase síncrona del curso (1,6 créditos) es la siguiente:

- Teoría: 0,7 créditos / 7 horas
- Práctica: 0,9 créditos / 9 horas

El itinerario formativo de Desarrollo Seguro se distribuye de la siguiente manera:

- Chapter Level 0: 0,2 créditos / 2 horas - 1 sesión
- Chapter Level 1: 0,2 créditos / 2 horas - 1 sesión
- Chapter Level 2: 0,4 créditos / 4 horas - 2 sesiones
- Chapter Level 3: 0,4 créditos / 4 horas - 2 sesiones
- Chapter Level 4: 0,4 créditos / 4 horas - 2 sesiones

3. Normas y Certificado de superación.

La fase síncrona se desarrollará en modalidad en línea por lo que los participantes deberán conectarse a la emisión de las clases en directo durante todas las sesiones programadas, así como realizar una serie de prácticas que permitirán valorar si han obtenido los conocimientos adecuados para superar el curso y ser considerados como "APTOS". En caso de no superar el mínimo exigido, el alumno será considerado "NO APTO" suponiendo la baja en el curso.

Será obligatoria la asistencia a todas sesiones para avanzar al siguiente nivel, siendo condición imprescindible para acceder a los niveles 2, 3 y 4 superar una prueba que evalúe los conocimientos adquiridos en los niveles anteriores.

Cualquier modificación de lo anterior, por circunstancias que así lo exijan, quedará reflejada en el Acta de finalización del curso.

4. Destinatarios

Podrá solicitar el curso el personal al servicio de las Administraciones Públicas de los grupos A1, A2, B y C1, y el personal laboral equivalente, que tenga responsabilidades, a nivel técnico, en la planificación, creación, gestión, administración o mantenimiento de desarrollos en las tecnologías de la información y comunicaciones, o con la seguridad de los mismos.

Se supondrá, por parte de los asistentes, un conocimiento mínimo en lenguajes de programación y seguridad. Un aprovechamiento óptimo de la formación se conseguirá si se cuenta además con conocimientos o experiencia previa en el área de desarrollo de software y conocimientos técnicos en JAVA.

5. Materias y asignaturas

A continuación, se detallan las materias y asignaturas en las que se distribuye el curso con expresión de contenidos.

Itinerario	Chapter	CRÉDITOS			Contenido
		TOT	TEO	PRA	
Desarrollo seguro	Concienciación en Ciberseguridad	0,2	0,2	0	En este chapter, se tratará sobre varias formas en que se pueden mantener los datos propios y los de su organización a salvo de los ciberdelincuentes.
	El ciclo sin fin	0,2	0,2	0	En este chapter, se dará un repaso a este ciclo sin fin en las organizaciones y cómo se puede implementar la seguridad, ya que debe tenerse en cuenta en todas las etapas del proceso de desarrollo, desde el diseño hasta la implementación. La seguridad es la parte más importante del ciclo de vida del software, ya que es esencial que el software sea seguro y confiable.
	Re-Diseño In-Seguro	0,4	0,1	0,3	En este chapter, se podrá repasar consideraciones importantes que abordan la seguridad del diseño del software. Al diseñar una aplicación segura, es importante considerar todos los posibles ataques contra el sistema y asegurarse de que no sean posibles de explotar. Esto incluye tanto ataques externos como internos.
	Valida la puerta de entrada	0,4	0,1	0,3	En este chapter, se realizará un análisis sobre las diferentes estrategias de la validación de parámetros de entrada. Los desarrolladores deben validar los parámetros de entrada en las aplicaciones web para asegurarse de que no sean vulnerables a ningún ataque malicioso.
	Criptografía familiar	0,4	0,1	0,3	En este chapter podremos repasar la criptografía desde su inicio hasta revisar como usarla correctamente. Una de las piezas más importantes de la seguridad en las aplicaciones es la criptografía y realizar un correcto uso de esta. El uso de algoritmos criptográficos obsoletos, o la ausencia de su uso en algunas funcionalidades claves en la protección de los datos de usuario, hacen que la criptografía tenga una relevancia de peso a la hora de desarrollar aplicaciones.

6. Modalidad: En línea tutorizada

- Fase síncrona: 16 horas