CONTENIDOS DE LA UNIDAD, CRITERIOS DE EVALUACIÓN Y RESULTADOS DE APRENDIZAJE

La siguiente tabla responde al Real Decreto 479/2020, de 7 de abril (junto con las modificaciones del Real Decreto 261/2021, de 13 de abril y del Real Decreto 497/2024, de 21 de mayo), por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo. Se incluye también una columna con las unidades didácticas que forman el curso, en las que se desarrollas los diferentes bloques de contenidos.

CONTENIDOS	CRITERIOS DE EVALUACIÓN	RESULTADOS DE APRENDIZAJE	UNIDAD DIDÁCTICA
Bloque 1			
Prueba de aplicaciones web y para dispositivos móviles: – Fundamentos de la programación. – Lenguajes de programación interpretados y compilados. – Código fuente y entornos de desarrollo. – Ejecución de software. – Elementos principales de los programas. – Pruebas. Tipos. – Seguridad en los lenguajes de programación y sus entornos de ejecución (“sandboxes”).	a) Se han comparado diferentes lenguajes de programación de acuerdo a sus características principales. b) Se han descrito los diferentes modelos de ejecución de software. c) Se han reconocido los elementos básicos del código fuente, dándoles significado. d) Se han ejecutado diferentes tipos de prueba de software. e) Se han evaluado los lenguajes de programación de acuerdo a la infraestructura de seguridad que proporcionan	Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.	1
Bloque 2.			
Determinación del nivel de seguridad requerido por aplicaciones:	a) Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (ASVS, “Application Security Verification Standard”).	Determina el nivel de seguridad requerido por aplicaciones	2

– Fuentes abiertas para el desarrollo seguro. – Listas de riesgos de seguridad habituales: OWASP Top Ten (web y móvil). – Requisitos de verificación necesarios asociados al nivel de seguridad establecido – Comprobaciones de seguridad a nivel de aplicación: ASVS (Application Security Verification Standard).	b) Se ha identificado el nivel de verificación de seguridad requerido porlas aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos. c) Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecida. d) Se han reconocido los principales riesgos de las aplicaciones desarrolladas, en función de sus características.	identificando los vectores de ataque habituales y sus riesgos asociados.	
Bloque 3.			
Detección y corrección de vulnerabilidades de aplicaciones web: – Desarrollo seguro de aplicaciones web. – Listas públicas de vulnerabilidades de aplicaciones web. OWASP Top Ten. – Entrada basada en formularios. Inyección. Validación de la entrada. – Estándares de autenticación y autorización. – Robo de sesión. – Vulnerabilidades web. – Almacenamiento seguro de contraseñas. – Contramedidas. HSTS, CSP, CAPTCHAs, entre otros. – Seguridad de portales y aplicativos web. Soluciones WAF (Web Application Firewall).	a) Se han validado las entradas de los usuarios. b) Se han detectado riesgos de inyección tanto en el servidor como en el cliente. c) Se ha gestionado correctamente la sesión del usuario durante el uso de la aplicación. d) Se ha hecho uso de roles para el control de acceso. e) Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario. f) Se han configurado servidores web para reducir el riesgo de sufrir ataques conocidos. g) Se han incorporado medidas para evitar los ataques a contraseñas, envío masivo de mensajes o registros de usuarios a través de programas automáticos (bots)	Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web.	3
Bloque 4.			

Detección de problemas de seguridad en aplicaciones para dispositivos móviles: – Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas. – Firma y verificación de aplicaciones. – Almacenamiento seguro de datos. – Validación de compras integradas en la aplicación. – Fuga de información en los ejecutables. – Soluciones CASB.	a) Se han comparado los diferentes modelos de permisos de las plataformas móviles. b) Se han descrito técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información. c) Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor. d) Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles. e) Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible	Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.	4
Bloque 5.			
Implantación de sistemas seguros de desplegado de software: – Puesta segura en producción. – Prácticas unificadas para el desarrollo y operación del software (DevOps). – Sistemas de control de versiones. – Sistemas de automatización de construcción (build). – Integración continua y automatización de pruebas. – Escalado de servidores. Virtualización. Contenedores. – Gestión automatizada de configuración de sistemas – Herramientas de simulación de fallos. – Orquestación de contenedores.	a) Se han identificado las características, principios y objetivos de la integración del desarrollo y operación del software. b) Se han implantado sistemas de control de versiones, administrando los roles y permisos solicitados. c) Se han instalado, configurado y verificado sistemas de integración continua, conectándolos con sistemas de control de versiones. d) Se han planificado, implementado y automatizado planes de desplegado de software. e) Se ha evaluado la capacidad del sistema desplegado para reaccionar de forma automática a fallos. f) Se han documentado las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres. g) Se han creado bucles de retroalimentación ágiles entre los miembros del equipo.	Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos.	5