TABLA 8: CE y Cb
Familia Profesional: Informática y Comunicaciones
Curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información
Módulo Profesional: Puesta en Producción Segura

RA1	Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución .	1. Prueba de aplicaciones web y para dispositivos móviles:		Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han comparado diferentes lenguajes de programación de acuerdo a sus características principales.	• Lenguajes de programación interpretados y compilados. • Código fuente y entornos de desarrollo.	Contenidos Básicos	• Comparar lenguajes de programación en base a las características de cada uno de ellos.	• Conocer las principales características de los lenguajes.
	b) Se han descrito los diferentes modelos de ejecución del software.	• Modelos de Ejecución de software. • Concepto y definición. • Tipos de modelos de ejecución del software.		• Identificación de los diferentes modelos de ejecución del software.	• Conocer los diferentes modelos de ejecución de software y sus características.
	c) Se han reconocido los elementos básicos del código fuente, dándoles significado.	• Fundamentos de la programación. • Elementos principales de los programas.		• Conocer los elementos básicos del código fuente.	• Saber dar significado a los elementos que constituyen el software.
	d) Se han ejecutado diferentes tipos de prueba de software.	• Pruebas. Concepto y definición. • Tipos de pruebas de software.		• Ejecutar pruebas de software.	• Saber diferenciar los distintos tipos de pruebas de software y sus características.
	e) Se han evaluado los lenguajes de programación de acuerdo a la infraestructura de seguridad que proporcionan.	• Seguridad en los lenguajes de programación y sus entornos de ejecución (“sandboxes”).		• Evaluar los lenguajes de programación en función de la seguridad que proporcionan.	• Saber diferenciar los lenguajes de programación y conocer sus características principales en relación con la seguridad que proporcionan.

TABLA 8: CE y Cb
Familia Profesional: Informática y Comunicaciones
Curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información
Módulo Profesional: Puesta en Producción Segura

RA2	Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados	2. Determinación del nivel de seguridad requerido por aplicaciones:		Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (ASVS, "Application Security Verification Standard").	• Comprobaciones de seguridad a nivel de aplicación: ASVS (Application Security Verification Standard).	Contenidos Básicos	• Comprobar la seguridad a nivel de aplicación.	• Saber realizar comprobaciones de seguridad a nivel de aplicación.
	b) Se ha identificado el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos.	• Fuentes abiertas para el desarrollo seguro.		• Identificar los niveles de verificación de seguridad que requieren las aplicaciones en base a los estándares reconocidos.	• Saber identificar los niveles de seguridad de aplicaciones según estándares reconocidos.
	c) Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecido.	• Requisitos de verificación necesarios asociados al nivel de seguridad establecido.		• Enumerar requisitos de verificación asociados a niveles de seguridad.	• Saber enumerar qué requisitos de verificación están asociados a cada nivel de seguridad.
	d) Se han reconocido los principales riesgos de las aplicaciones desarrolladas, en función de sus características.	• Listas de riesgos de seguridad habituales: OWASP Top Ten (web y móvil).		• Reconocer los riesgos en las aplicaciones desarrolladas.	• Saber identificar iesgos en aplicaciones desarrollada según sus características.

RA3	Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web.	3. Detección y corrección de vulnerabilidades de aplicaciones web:		Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han validado las entradas de los usuarios.	• − Estándares de autenticación y autorización. •	Contenidos	• Validar entradas de los usuarios.	• Saber aplicar los estándares de autenticación y autorización para validar entradas de los usuarios.
	b) Se han detectado riesgos de inyección tanto en el servidor como en el cliente.	• − Entrada basada en formularios. Inyección. Validación de la entrada.		• Detectar posibles riesgos de inyección en servidor y cliente.	• Saber identificar qué posibles riesgos de inyección se pueden producir en servidores y clientes.

TABLA 8: CE y Cb
Familia Profesional: Informática y Comunicaciones
Curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información
Módulo Profesional: Puesta en Producción Segura

RA3	Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web.	3. Detección y corrección de vulnerabilidades de aplicaciones web:	Saber Hacer	Saber Estar
		•		
	c) Se ha gestionado correctamente la sesión del usuario durante el uso de la aplicación.	• Seguridad de portales y aplicativos web. Soluciones WAF (Web Application Firewall).	• Gestionar las sesiones de usuario en el proceso de uso de la aplicación.	• Saber aplicar soluciones en la gestión de las sesiones de usuario durante el uso de una aplicación.
	d) Se ha hecho uso de roles para el control de acceso.	• Contramedidas. HSTS, CSP, CAPTCHAs, entre otros.	• Hacer uso de roles en relación con el control de acceso.	• Saber hacer uso de diferentes roles para el control de acceso.
	e) Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario	• – Almacenamiento seguro de contraseñas. •	• Utilizar algoritmos criptográficos para el almacenamiento de las contraseñas.	• Saber aplicar algoritmos criptográficos para almacenar contraseñas.
	f) Se han configurado servidores web para reducir el riesgo de sufrir ataques conocidos.	• – Vulnerabilidades web. • – Desarrollo seguro de aplicaciones web. • • – Listas públicas de vulnerabilidades de aplicaciones web. OWASP Top Ten. •	• Configurar servidores web para reducir la posibilidad de ataques.	• Saber configurar los servidores web para tratar de disminuir la posibilidad de recibir ataques.
	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).	• – Robo de sesión. •	• Incorporar medidas para evitar ataques a contraseñas.	• Saber aplicar diferentes medidas para minimizar la posibilidad de recibir ataques de contraseñas.

TABLA 8: CE y Cb
Familia Profesional: Informática y Comunicaciones
Curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información
Módulo Profesional: Puesta en Producción Segura

RA4	Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.	4. Seguridad de portales y aplicativos web. Soluciones WAF (Web Application Firewall).		Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han comparado los diferentes modelos de permisos de las plataformas móviles.	• – Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas.	Contenidos Básicos	• Comparar los modelos existentes de permisos en las plataformas móviles.	• Saber identificar los distintos 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.	• Fuga de información en los ejecutables.		• Describir técnicas de almacenamiento seguro.	• Saber identificar las diferentes técnicas de almacenamiento seguro de datos en los dispositivos.
	c) Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.	• Validación de compras integradas en la aplicación. • Firma y verificación de aplicaciones.		• Implantar sistemas de validación de compras haciendo uso de validación en el servidor.	• Saber realizar la implantación de sistemas de validación de compras en una aplicación.
	d) Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.	• Almacenamiento seguro de datos.		• Utilizar herramientas de monitorización de tráfico de red.	• Saber hacer uso de las diferentes herramientas de monitorización de tráfico de red para poder detectar protocolos no seguros de comunicaciones móviles.
	e) Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible.	• Soluciones CASB.		• Inspeccionar aplicaciones móviles en busca de posibles fugas de información.	• Saber aplicar técnicas de inspección en aplicaciones móviles para detectar posibles fugas de información sensible.

TABLA 8: CE y Cb
Familia Profesional: Informática y Comunicaciones
Curso de especialización de Ciberseguridad en Entornos de las Tecnologías de la Información
Módulo Profesional: Puesta en Producción Segura

RA5	Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos.	5. Implantación de sistemas seguros de desplegado de software:		Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han identificado las características, principios y objetivos de la integración del desarrollo y operación del software.	• Puesta segura en producción. • Escalado de servidores. Virtualización. Contenedores. • Orquestación de contenedores.	Contenidos Básicos	• Identificar características y objetivos para integrar el desarrollo y operaciones del software.	• Saber identificar las principales características para la integración de desarrollo del software.
	b) Se han implantado sistemas de control de versiones, administrando los roles y permisos solicitados.	• – Sistemas de control de versiones.		• Implantar sistemas de control de versiones.	• Saber realizar la implantación de sistemas de control de versiones.
	c) Se han instalado, configurado y verificado sistemas de integración continua, conectándolos con sistemas de control de versiones.	• Integración continua y automatización de pruebas.		• Administrar sistemas de integración continua.	• Saber gestionar sistemas de integración continua para conectarlos a sistemas de control de versiones.
	d) Se han planificado, implementado y automatizado planes de desplegado de software.	• Sistemas de automatización de construcción (build).		• Planificar planes de despliegue de software.	• Saber aplicar planes para desplegar software.
	e) Se ha evaluado la capacidad del sistema desplegado para reaccionar de forma automática a fallos.	• Herramientas de simulación de fallos.		• Evaluar la capacidad que ofrece el sistema para reaccionar ante fallos.	• Saber ser capaz de conocer la capacidad de un sistema para reaccionar a fallos de manera automática.
	f) Se han documentado las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres.	• Prácticas unificadas para el desarrollo y operación del software (DevOps).		• Documentar tareas y procedimientos para la recuperación ante desastres.	• Saber generar documentación de las acciones realizadas y procedimientos de recuperación ante desastres.
	g) Se han creado bucles de retroalimentación ágiles entre los miembros del equipo.	• Gestión automatizada de configuración de sistemas		• Crear bucles de retroalimentación en un equipo.	• Saber crear bucles de retroinformación entre miembros de un equipo.