



TABLA 9: Evaluación

(hacer una tabla por cada RA)

Familia Profesional: Informática y Comunicaciones

Ciclo Formativo: Curso de Especialización en 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.	20 %
---	------

Criterios de evaluación:

%	CE	Inst. Evaluac.
15%	a) Se han comparado diferentes lenguajes de programación de acuerdo a sus características principales.	Prueba teórica
20%	b) Se han descrito los diferentes modelos de ejecución del software.	Prueba teórica
15%	c) Se han reconocido los elementos básicos del código fuente, dándoles significado.	Prueba práctica
20%	d) Se han ejecutado diferentes tipos de prueba de software.	Prueba práctica
30%	e) Se han evaluado los lenguajes de programación de acuerdo a la infraestructura de seguridad que proporcionan.	Tarea práctica individual.



RA2: Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.	20 %
--	------

Criterios de evaluación:

%	CE	Inst. Evaluac.
25%	a) Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (ASVS, "Application Security Verification Standard").	Tarea práctica individual.
25%	b) Se ha identificado el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos.	Trabajo de investigación individual.
25%	c) Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecido.	Tarea práctica individual.
25%	d) Se han reconocido los principales riesgos de las aplicaciones desarrolladas, en función de sus características.	Trabajo de investigación individual.



RA3: Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web.

20 %

Criterios de evaluación:

%	CE	Inst. Evaluac.
10%	a) Se han validado las entradas de los usuarios.	Prueba práctica
15%	b) Se han detectado riesgos de inyección tanto en el servidor como en el cliente.	Prueba práctica
15%	c) Se ha gestionado correctamente la sesión del usuario durante el uso de la aplicación.	Prueba práctica
15%	d) Se ha hecho uso de roles para el control de acceso.	Prueba práctica
15%	e) Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario.	Tarea práctica individual.
15%	f) Se han configurado servidores web para reducir el riesgo de sufrir ataques conocidos.	Tarea práctica individual.
15%	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).	Prueba teórica



RA4: Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.	20 %
--	------

Criterios de evaluación:

%	CE	Inst. Evaluac.
20%	a) Se han comparado los diferentes modelos de permisos de las plataformas móviles.	Prueba teórica
20%	b) Se han descrito técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.	Tarea práctica individual.
20%	c) Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.	Prueba práctica
20%	d) Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.	Tarea práctica individual.
20%	e) Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible.	Prueba teórica



RA5: Implanta sistemas seguros de despliegado de software, utilizando herramientas para la automatización de la construcción de sus elementos.	20 %
--	------

Criterios de evaluación:

%	CE	Inst. Evaluac.
20%	a) Se han identificado las características, principios y objetivos de la integración del desarrollo y operación del software.	Prueba práctica
15%	b) Se han implantado sistemas de control de versiones, administrando los roles y permisos solicitados.	Prueba teórica
15%	c) Se han instalado, configurado y verificado sistemas de integración continua, conectándolos con sistemas de control de versiones.	Prueba práctica
15%	d) Se han planificado, implementado y automatizado planes de despliegado de software.	Prueba teórica
15%	e) Se ha evaluado la capacidad del sistema desplegado para reaccionar de forma automática a fallos.	Tarea práctica individual.
10%	f) Se han documentado las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres.	Tarea práctica individual.
10%	g) Se han creado bucles de retroalimentación ágiles entre los miembros del equipo.	Tarea práctica individual.