Curso 2024 / 2025

Resumen Programaciones Didácticas

Curso

Departamento de informática

IES Rafael Alberti, Cádiz

Índice

1. Módulo Profesional. Incidentes de ciberseguridad (5021)

1.1 Objetivos del módulo

a) Identificar los principios de la organización y normativa de protección en ciberseguridad, planificando las acciones que es preciso adoptar en el puesto de trabajo para la elaboración del plan de prevención y concienciación.

b) Auditar el cumplimiento del plan de prevención y concienciación de la organización, definiendo las acciones correctoras que puedan derivarse para incluirlas en el plan de securización de la organización.

c) Detectar incidentes de ciberseguridad implantando los controles, las herramientas y los mecanismos necesarios para su monitorización e identificación.

d) Analizar y dar respuesta a incidentes de ciberseguridad, identificando y aplicando las medidas necesarias para su mitigación, eliminación, contención o recuperación.

q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.

r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.

s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.

t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.

u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

1.2 Resultados de aprendizaje

El Real Decreto 479/2020, de 7 de abril, establece los siguientes Resultados de aprendizaje, que se presentan desglosados según sus elementos:

RA	LOGRO	OBJETO	ACCIONES EN EL CONTEXTO DE APRENDIZAJE
RA 1	Desarrolla	planes de prevención y concienciación en ciberseguridad	estableciendo normas y medidas de protección
RA 2	Analiza	incidentes de ciberseguridad	utilizando herramientas, mecanismos de detección y alertas de seguridad
RA 3	Investiga	incidentes de ciberseguridad	analizando los riesgos implicados y definiendo las posibles medidas a adoptar
RA 4	Implementa	medidas de ciberseguridad en redes y sistemas	respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas
RA 5	Detecta y documenta	incidentes de ciberseguridad	siguiendo procedimientos de actuación establecidos.

1.3 Selección y secuencia de contenidos

UNIDADES DIDÁCTICAS		SESIONES	RA	CRITERIOS	
UD1	Desarrollo de planes de prevención y concienciación	30	RA1	a)..e)	1er trimestre (65 horas)
UD2	Analiza incidentes de ciberseguridad	35	RA2	a)..e)	
UD3	Investiga incidentes de ciberseguridad	30	RA3	a)..e)	2o trimestre (85 horas)
UD4	Implementa medidas de ciberseguridad en redes y sistemas	35	RA4	a)..f)	
UD5	Documenta y notifica incidentes de ciberseguridad	20	RA5	a)..e)	

1.4 Evaluación

A continuación, se especifica el peso de cada uno de los resultados de aprendizaje, así como el de los criterios de evaluación que lo componen. La mayor o menor ponderación de los criterios se obtiene en base

al nivel de dificultad y contenidos a desarrollar para cada criterio. La calificación de cada resultado de aprendizaje será la media ponderada de los distintos criterios de evaluación.

RA	CRITERIOS DE EVALUACIÓN	PESO RA	PESO CE	TÉCNICA
RA1	a) Se han definido los principios generales de la organización en materia de ciberseguridad, que deben ser conocidos y apoyados por la dirección de la misma.	15%	6,0%	Actividades teórico - prácticas
	b) Se ha establecido una normativa de protección del puesto de trabajo.		3,0%	
	c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.		3,0%	
	d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.		2,0%	
	e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.		1,0%	
RA2	a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización.	25%	2,0%	Actividades teórico - prácticas
	b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes.		11,0%	
	c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física.		1,0%	
	d) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT: Open Source Intelligence).		6,0%	
	e) Se ha realizado una clasificación, valoración, documentación y seguimiento de		5,0%	

RA	CRITERIOS DE EVALUACIÓN	PESO RA	PESO CE	TÉCNICA
	los incidentes detectados dentro de la organización.			
RA3	a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.	20%	3,0%	Actividades teórico - prácticas
	b) Se ha realizado un análisis de evidencias.		4,0%	
	c) Se ha realizado la investigación de incidentes de ciberseguridad.		5,0%	
	d) Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que podrían hacer aportaciones al respecto.		4,0%	
	e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados.		4,0%	
RA4	a) Se han desarrollado procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.	30%	6,0%	Actividades teórico - prácticas
	b) Se han preparado respuestas ciberresilientes ante incidentes que permitan seguir prestando los servicios de la organización y fortaleciendo las capacidades de identificación, detección, prevención, contención, recuperación y cooperación con terceros.		6,0%	
	c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.		6,0%	
	d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.		6,0%	

RA	CRITERIOS DE EVALUACIÓN	PESO RA	PESO CE	TÉCNICA
	e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de “lecciones aprendidas”.		3,0%	
	f) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.		3,0%	
RA5	a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.	10%	6,0%	Actividades teórico - prácticas
	b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.		1,0%	
	c) Se ha notificado el incidente de manera adecuada a las autoridades competentes en el ámbito de la gestión de incidentes de ciberseguridad en caso de ser necesario.		1,0%	
	d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.		1,0%	
	e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.		1,0%	

Para el cálculo de la calificación de cada evaluación parcial se tendrán en cuenta únicamente los criterios impartidos hasta la finalización de dicha evaluación. Dado que según la normativa vigente la calificación debe ser un entero numérico comprendido entre el 1 y el 10, el cálculo se realizará de la siguiente manera:

La calificación de cada criterio se obtendrá sobre su peso, es decir si un criterio tiene un peso del 1% su nota será un número real comprendido entre el 0 y el 1. Por otra parte, la calificación de cada uno de los resultados de aprendizaje se obtendrá mediante el redondeo de lo que resulte al aplicar la siguiente fórmula a los CE pertenecientes al RA:

Calificación Ev. Parcial \=(Calificación CE *%)

Esta misma fórmula permitirá obtener la nota parcial, no obstante esta calificación sólo será efectiva en el caso de que el alumno haya superado todos y cada uno de los Resultados de Aprendizaje impartidos en la evaluación. En el caso de que el alumno no haya superado algún Resultado de Aprendizaje y el resultado de

la anterior fórmula sea un número entero mayor o igual que 5, la calificación efectiva de la evaluación será igual a 4 hasta que el alumno supere todos los Resultados de Aprendizaje pendientes, momento en el que se realizará el recálculo de las calificaciones tal y como se indica en el apartado Evaluación Ordinaria.

La superación de una evaluación, no implica la superación del resto. Si llegado el caso de que alguna alumna o alumno superará la segunda evaluación, pero no hubiere superado la anterior, implica la no superación del curso, y por ello en el informe de evaluación se consignará como no superada. No se conservan partes -aprobadas o suspensas- de un curso a otro. Para el alumnado que no supere alguna de las evaluaciones, se prepararon actividades personalizadas de refuerzo/recuperación para el periodo de recuperación de fin de curso, siendo estas actividades de carácter obligatorio.

Se utilizarán los siguientes instrumentos de evaluación para comprobar el progreso y las dificultades del alumnado:

Trabajo diario individual y grupal:

- Observación sistemática sobre el trabajo en clase.
- Anotaciones sobre participación.
- Seguimiento de las actividades programadas y realizadas en el aula.
- Puntualidad y asistencia.

Prácticas y proyectos, individuales y grupales:

- Realización de prácticas planteadas durante el curso.
- Presentaciones sobre proyectos generados.

Pruebas teórico/prácticas individuales:

- Pruebas con ejercicios escritos y/o en el ordenador.

2. Módulo Profesional. Bastionado de redes y sistemas (5022)

2.1 Objetivos del módulo

e) Elaborar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad.

f) Diseñar e implantar planes de medidas técnicas de seguridad a partir de los riesgos identificados para garantizar el nivel de seguridad requerido.

g) Configurar sistemas de control de acceso, autenticación de personas y administración de credenciales para preservar la privacidad de los datos.

h) Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.

i) Configurar dispositivos de red para cumplir con los requisitos de seguridad.

j) Administrar la seguridad de sistemas informáticos en red aplicando las políticas de seguridad requeridas para garantizar la funcionalidad necesaria con el nivel de riesgo de red controlado.

q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.

r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.

s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.

t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.

u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

2.2 Resultados de aprendizaje

El Real Decreto 479/2020, de 7 de abril, establece los siguientes Resultados de aprendizaje, que se presentan desglosados según sus elementos:

RA	LOGRO	OBJETO	ACCIONES EN EL CONTEXTO DE APRENDIZAJE
RA 1	Diseña	Planes de securización	Incorporando buenas prácticas para el bastionado de sistemas y redes
RA 2	Configura	Sistemas de control de acceso y autenticación de personas	Preservando la confidencialidad y privacidad de los datos
RA 3	Administra	Credenciales de acceso a sistemas informáticos	Aplicando los requisitos de funcionamiento y seguridad establecidos
RA 4	Diseña	Redes de computadores	Contemplando los requisitos de seguridad
RA 5	Configura	Dispositivos y sistemas informáticos	Cumpliendo los requisitos de seguridad
RA 6	Configura	Dispositivos para la instalación de sistemas informáticos	Minimizando las probabilidades de exposición a ataques
RA 7	Configura	Sistemas informáticos	Minimizando las probabilidades de exposición a ataques

2.3 Selección y secuencia de contenidos

UNIDADES DIDÁCTICAS		SESIONES	RA	CRITERIOS	
UD1	Zero Trust	20	RA4, RA6	6a), 6b), 6c), 6d), 6e), 4a), 4b), 4c)	1er trimestre (60 horas)
UD2	Least-Privilege	20	RA2, RA3, RA4, RA7	2a), 2b), 2c), 2d), 2e). 3a), 4e), 7a) 7b)	
UD3	Reduce Attack Surface	20	RA5	5b)	
UD4	Under Control	40	RA3, RA4, RA5, RA7	3b), 3c), 3d), 3e), 4d), 5a), 5e), 7c), 7d), 7e)	2o trimestre (90 horas)
UD5	Risk Management	10	RA1	1a), 1b), 1c), 1d), 1e), 1f)	
UD6	Defense in Depth	40	RA5	5c), 5d)	

2.4 Evaluación

A continuación, se especifica el peso de cada uno de los resultados de aprendizaje, así como el de los criterios de evaluación que lo componen. La mayor o menor ponderación de los criterios se obtiene en base al nivel de dificultad y contenidos a desarrollar para cada criterio.

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	% RA	PESO C.E.	TÉCNICA
RA1. Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.	a) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.	15%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se ha evaluado las medidas de seguridad actuales.		B	
	c) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización		I	
	d) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.		A	
	e) Se ha diseñado y elaborado un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización.		I	
	f) Se han identificado las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización.		I	
RA2. Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y	a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.	7,5%	B	Proyectos aplicados y pruebas teórico-prácticas

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	% RA	PESO C.E.	TÉCNICA
privacidad de los datos.				
	b) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques.		B	
	c) Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.		B	
	d) Se han definido protocolos y políticas de autenticación basados en tokens, OTPs, etc., en base a las principales vulnerabilidades y tipos de ataques.		B	
	e) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.		B	
RA3. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.	a) Se han identificado los tipos de credenciales más utilizados.	7,5%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.		I	

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	% RA	PESO C.E.	TÉCNICA
	c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.		I	
	d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.		I	
	e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo RADIUS - Remote Access Dial In User Service).		I	
RA4. Diseña redes de computadores contemplando los requisitos de seguridad.	a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.	15%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).		I	
	c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.		I	
	d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).		B	
	e) Se ha establecido un túnel seguro de comunicaciones entre dos		I	

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	% RA	PESO C.E.	TÉCNICA
	sedes geográficamente separadas.			
RA5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.	a) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.	20%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.		I	
	c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.		I	
	d) Se han implementado contramedidas frente a comportamientos no deseados en una red.		B	
	e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.		B	
RA6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.	a) Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.	15%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.		B	
	c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia		I	

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	% RA	PESO C.E.	TÉCNICA
	de arranque con fines de acceso ilegítimo.			
	d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.		B	
	e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.		B	
RA7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.	a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.	20%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.		I	
	c) Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.		I	
	d) Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.		B	
	e) Se han instalado y configurado sistemas de copias de seguridad.		B	

La calificación de cada resultado de aprendizaje será la media ponderada de los distintos criterios de evaluación, repartidos en los siguientes pesos:
- Básicos (B): 4.
- Intermedios (I): 2.
- Avanzados (A): 1.

Por ejemplo, si un resultado de aprendizaje tiene 6 criterios de evaluación repartidos de la siguiente forma:

c1 (básico), c2 (básico), c3 (básico), c4 (intermedio), c5 (intermedio) y c6 (avanzado), se calcularía la calificación sumando las multiplicaciones de la nota de cada criterio por su peso correspondiente y dividiendo el resultado por la suma de todos los pesos. La fórmula matemática sería la siguiente:

$$ \text{Calificación del RA} = c_{14} + c_{24} + c_{34} + c_{42} + c_{52} + c_{614} + 4 + 4 + 2 + 2 + 1 $$

El alumnado que supere o iguale la calificación de 5 en cada uno de los Resultados de Aprendizaje tras aplicar estas ponderaciones, aprueba el módulo.
El alumno también tendrá posibilidad de subir nota y podrá solicitar al profesor un plan de mejora que consistirá en un conjunto de trabajos, prácticas o pruebas sobre los contenidos a los que están asociados los resultados de aprendizaje en los que desea mejorar su calificación.
Si no se han superado los contenidos del módulo a finales del mes de mayo, se desarrollará la recuperación de los R.A pendientes durante el mes de junio y consistirá en un conjunto de prácticas y/o pruebas sobre los contenidos a los que están asociados los resultados de aprendizaje no superados.

3. Módulo Profesional. Puesta en producción segura (5023)

3.1 Objetivos del módulo

k) Aplicar estándares de verificación requeridos por las aplicaciones para evitar incidentes de seguridad.

l) Automatizar planes de despliegue de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un desplegado seguro.

q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.

r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.

s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.

t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.

u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

3.2 Resultados de aprendizajes

Los Resultados de Aprendizaje establecidos por la normativa para este módulo de Puesta en producción segura son 5 que se enumeran a continuación y se presentan desglosado según sus elementos:

RA	LOGRO	OBJETO	ACCIONES EN EL CONTEXTO DE APRENDIZAJE
RA 1	Prueba	Aplicaciones web y aplicaciones para dispositivos móviles	Analizando la estructura del código y su modelo de ejecución
RA 2	Determina	El nivel de seguridad requerido por aplicaciones	Identificando los vectores de ataque habituales y sus riesgos asociados
RA 3	Detecta y corrige	Vulnerabilidades de aplicaciones web	Analizando su código fuente y configurando servidores web
RA 4	Detecta	Problemas de seguridad en las aplicaciones móviles	Monitorizando su ejecución y analizando ficheros y datos
RA 5	Implanta	Sistemas seguros de desplegado de software	Utilizando herramientas para la automatización de la construcción de sus elementos.

3.3 Selección y secuencia de contenidos

UNIDADES DIDÁCTICAS		SESIONES	RA	CRITERIOS	
UT1	Fundamentos del Software	16	RA1	a, b, c, d, e	1er trimestre (48 horas)
UT2	Verificación de seguridad en las aplicaciones	15	RA 2	a, b, c, d	
UT4	Detección y corrección vulnerabilidades	30	RA3	a, b, c, d, e, f, g	
					2o trimestre (72 horas)
UT3	Desplegado de software seguro	44	RA5	a, b, c, d, e	
UT5	Seguridad en aplicaciones móviles	15	RA4	a, b, c, d, e	

3.4 Evaluación

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	% RA	PESO C.E.	TÉCNICAS
RA1 Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.	a) Se han comparado diferentes lenguajes de programación de acuerdo a sus características principales.	11 %	2 %	Proyecto de desarrollo y testing
	b) Se han descrito los diferentes modelos de ejecución de software.		2%	
	c) Se han reconocido los elementos básicos del código fuente, dándoles significado.		2 %	
	d) Se han ejecutado diferentes tipos de prueba de software.		3 %	
	e) Se han evaluado los lenguajes de programación de acuerdo a la infraestructura de seguridad que proporcionan.		2 %	
RA2 Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.	a) Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (ASVS, “Application Security Verification Standard”).	12 %	2 %	Trabajo: Análisis y verificación de software
	b) Se ha identificado el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos.		2 %	
	c) Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecido.		4 %	

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	% RA	PESO C.E.	TÉCNICAS
	d) Se han reconocido los principales riesgos de las aplicaciones desarrolladas, en función de sus características.		4 %	
RA3 Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web.	a) Se han validado las entradas de los usuarios.	35 %	5 %	Actividades teórico / prácticas
	b) Se han detectado riesgos de inyección tanto en el servidor como en el cliente.		5 %	
	c) Se ha gestionado correctamente la sesión del usuario durante el uso de la aplicación.		5 %	
	d) Se ha hecho uso de roles para el control de acceso.		5 %	
	e) Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario.		5 %	
	f) Se han configurado servidores web para reducir el riesgo de sufrir ataques conocidos.		5 %	
	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).		5 %	
RA4 Detecta problemas de seguridad en las aplicaciones para dispositivos móviles,	a) Se han comparado los diferentes modelos de permisos de las plataformas móviles.	10%	2 %	Actividades teórico / prácticas

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	% RA	PESO C.E.	TÉCNICAS
monitorizando su ejecución y analizando ficheros y datos				
	b) Se han descrito técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.		2 %	
	c) Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.		2 %	
	d) Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.		2 %	
	e) Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible.		2 %	
RA5 Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos.	a) Se han identificado las características, principios y objetivos de la integración del desarrollo y operación del software.	32 %	2%	Proyecto de puesta en producción
	b) Se han implantado sistemas de control de versiones, administrando los roles y permisos solicitados.		6%	
	c) Se han instalado, configurado y verificado sistemas de integración continua, conectándolos con sistemas de control de versiones.		6%	

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	% RA	PESO C.E.	TÉCNICAS
	d) Se han planificado, implementado y automatizado planes de desplegado de software.		6%	
	e) Se ha evaluado la capacidad del sistema desplegado para reaccionar de forma automática a fallos.		4%	
	f) Se han documentado las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres.		4%	
	g) Se han creado bucles de retroalimentación ágiles entre los miembros del equipo.		4%	

Todas las actividades son evaluables, sin entender la evaluación como un proceso de recogida de información, pero no todas son objeto de calificación, sólo aquellas recogidas en la tabla anterior y que hemos asociado a los criterios de evaluación y a los resultados de aprendizaje y se suelen denominar actividades de evaluación.

Además, llevaremos un registro en Excel de la calificación de cada RA, unidad, por actividad y criterio.

A la puntuación obtenida en la unidad se le aplicará la ponderación correspondiente a los Resultados de Aprendizaje, los cuales los RA 3 y 5 tienen mayor peso en la nota final, un 35% y 28% y los RA 1, 2 y 4 tienen entre 10-15%. Esta elección es debida a la dedicación profesional que harán de este módulo, ya que los dos primeros resultados de aprendizaje comentados anteriormente, atañan un gran peso a nivel profesional, debido a que son parte del proceso habitual en el trabajo de la puesta en producción segura, y el resto de unidades componen recursos complementarios para ayudar a esa puesta en producción.

Para calificar cada unidad utilizaremos aquellas actividades de evaluación planteadas, en la que se ponderan los CE y para establecer la nota de cada evaluación, atenderemos a las siguientes consideraciones:

- En el primer trimestre se evaluarán completos los RA 1, 2 clasificando con el sistema de ponderación establecido, llevándolo al 100% para puntuar en Séneca por el sistema tradicional. Es decir, un alumno/a que tenga un diez en todas las unidades del primer trimestre habrá obtenido un 27% de los RA, pero nosotros puntuaremos con un 10 la evaluación.
- En la segunda se evaluarán del mismo modo los criterios que nos resten de los RA 3 y de forma completa 4 y 5 .
- Para calcular la nota final, como ya hemos comentado, se aplicarán los porcentajes de los todos Resultados de Aprendizaje (RA).
- Para obtener la nota de la evaluación extraordinaria se deberá realizar un plan de recuperación personalizado a cada alumno o alumna, dependiendo de los RA que no haya superado.

Para obtener una calificación positiva en los trimestres y en la nota final todos los RA deben ser alcanzados, tras aplicar el sistema de ponderación, en un 50% cada uno de los RA, lo que es lo mismo si traducimos al

lenguaje de calificación tradicional la puntuación deberá ser al menos un 5, de forma excepcional el alumnado que obtenga un 5 en la valoración global, pero tenga algún RA con puntuación entre 4 y 4,99 habría superado el módulo, sin necesidad de recuperar ese RA. No obstante, los alumnos que alcance unos RA y otros no se le dará diferentes oportunidades de obtenerlos, realizándose pruebas de recuperación y oportunidades de mejoras del proyecto.

4. Módulo Profesional. Análisis forense informático (5024)

4.1 Objetivos del módulo

m) Aplicar técnicas de investigación forense en sistemas y redes en los ámbitos del almacenamiento de la información no volátil, de los dispositivos móviles, del Cloud y de los sistemas IoT (Internet de las cosas), entre otros, para la elaboración de análisis forenses.

n) Analizar informes forenses identificando los resultados de la investigación para extraer conclusiones y realizar informes.

q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.

r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.

s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.

u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

4.2 Resultados de aprendizaje

El Real Decreto 479/2020, de 7 de abril, establece para este módulo profesional, los siguientes Resultados de aprendizaje:

RA	LOGRO	OBJETO	ACCIONES EN EL CONTEXTO DE APRENDIZAJE
RA 1	Aplica	Metodologías de análisis forense	Caracterizando las fases de preservación, adquisición, análisis y documentación
RA 2	Realiza	Análisis forenses en dispositivos móviles	Aplicando metodologías establecidas, actualizadas y reconocidas
RA 3	Realiza	Análisis forenses en Cloud	Aplicando metodologías establecidas, actualizadas y reconocidas
RA 4	Realiza	Análisis forense en dispositivos de IoT	Aplicando metodologías establecidas, actualizadas y reconocidas
RA 5	Documenta	Análisis forenses	Elaborando informes que incluyan la normativa aplicable

4.3 Selección y secuencia de contenidos

UNIDADES DIDÁCTICAS		SESIONES	RA	CRITERIOS	
UD1	Evidence Acquisition and Preservation	12	1	a, b, c	1er trimestre (48 horas)
UD2	Windows Forensics	32	1	d, e	
UD3	Documentation and Reporting	4	5	a, b, c, d, e, f	
UD4	Memory Forensics	12	1	g	2o trimestre (72 horas)
UD5	Linux Forensics	20	1	f	
UD6	Cloud Forensics	8	3	a, b, c, d, e, f	
UD7	Mobile Device Forensics	16	2	a, b, c, d	
UD8	IoT Forensics	16	4	a, b, c, d, e, f, g, h, i	

4.4 Evaluación

A continuación, se especifica para cada unidad didáctica los resultados de aprendizaje y los criterios de evaluación correspondientes a la misma, así como los instrumentos de evaluación que se usarán para calificar cada uno de ellos.

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	INSTRUMENTOS
RA1. Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.	a) Se han identificado los dispositivos a analizar para garantizar la preservación de evidencias.	Proyecto integrado y actividades teórico-prácticas
	b) Se han utilizado los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.	
	c) Se ha asegurado la escena y conservado la cadena de custodia.	
	d) Se ha documentado el proceso realizado de manera metódica.	
	e) Se ha considerado la línea temporal de las evidencias.	
	f) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.	
	g) Se han presentado y expuesto las conclusiones del análisis forense realizado.	
RA2. Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.	a) Se ha realizado el proceso de toma de evidencias en un dispositivo móvil.	Proyecto integrado y actividades teórico-prácticas
	b) Se han extraído, decodificado y analizado las pruebas conservando la cadena de custodia.	
	c) Se han generado informes de datos móviles, cumpliendo con los requisitos de la industria forense de telefonía móvil.	
	d) Se han presentado y expuesto las conclusiones del análisis forense realizado a quienes proceda.	
RA3. Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas.	a) Se ha desarrollado una estrategia de análisis forense en Cloud, asegurando la disponibilidad de los recursos y capacidades necesarios una vez ocurrido el incidente.	Proyecto integrado y actividades teórico-prácticas
	b) Se ha conseguido identificar las causas, el alcance y el impacto real causado por el incidente.	

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	INSTRUMENTOS
	c) Se han realizado las fases del análisis forense en Cloud.	
	d) Se han identificado las características intrínsecas de la nube (elasticidad, ubicuidad, abstracción, volatilidad y compartición de recursos).	
	e) Se han cumplido los requerimientos legales en vigor, RGPD (Reglamento general de protección de datos) y directiva NIS (Directiva de la UE sobre seguridad de redes y sistemas de información) o las que eventualmente pudieran sustituirlas.	
	f) Se han presentado y expuesto las conclusiones del análisis forense realizado.	
RA4. Realiza análisis forense en dispositivos de IoT, aplicando metodologías establecidas, actualizadas y reconocidas.	a) Se han identificado los dispositivos a analizar garantizando la preservación de las evidencias.	Proyecto integrado y actividades teórico-prácticas
	b) Se han utilizado mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias	
	c) Se ha garantizado la autenticidad, completitud, fiabilidad y legalidad de las evidencias extraídas.	
	d) Se han realizado análisis de evidencias de manera manual y mediante herramientas.	
	e) Se ha documentado el proceso de manera metódica y detallada.	
	f) Se ha considerado la línea temporal de las evidencias.	
	g) Se ha mantenido la cadena de custodia	
	h) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.	
	i) Se han presentado y expuesto las conclusiones del análisis forense realizado.	
RA5. Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.	a) Se ha definido el objetivo del informe pericial y su justificación.	Proyecto integrado y actividades teórico-prácticas

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	INSTRUMENTOS
	b) Se ha definido el ámbito de aplicación del informe pericial.	
	c) Se han documentado los antecedentes.	
	d) Se han recopilado las normas legales y reglamentos cumplidos en el análisis forense realizado.	
	e) Se han recogido los requisitos establecidos por el cliente.	
	f) Se han incluido las conclusiones y su justificación.	

5. Módulo Profesional. Hacking ético (5025)

5.1 Objetivos del módulo

ñ) Combinar técnicas de hacking ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados.

q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.

r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.

s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.

t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.

u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

5.2 Resultados de aprendizaje

El Real Decreto 479/2020, de 7 de abril, establece para este módulo profesional, los siguientes Resultados de aprendizaje:

RA	LOGRO	OBJETO	ACCIONES EN EL CONTEXTO DE APRENDIZAJE
RA 1	Determina	Herramientas de monitorización para detectar vulnerabilidades	Aplicando técnicas de hacking ético
RA 2	Ataca y defiende	Comunicaciones inalámbricas	Consiguiendo acceso a redes para demostrar sus vulnerabilidades
RA 3	Ataca y defiende	Redes y sistemas	Consiguiendo acceso a información y sistemas de terceros
RA 4	Consolida y utiliza	Sistemas comprometidos	Garantizando accesos futuros
RA 5	Ataca y defiende	Aplicaciones web	Consiguiendo acceso a datos o funcionalidades no autorizadas

5.3 Selección y secuencia de contenidos

UNIDADES DIDÁCTICAS		SESIONES	RA	CRITERIOS	
UD1	Cybersecurity Audit Fundamentals	12	1	a), b), c), d), e), f), g), h), i)	1er trimestre (48 horas)
UD2	Web app penetration testing	36	5	a), b), c), d), e), f)	
UD3	Host & Network Penetration Testing	40	3	a), b), c), d), e)	2o trimestre (72 horas)
UD4	Post Exploitation	20	4	a), b), c), d)	
UD5	Reporting	4	2	g)	
UD6	Wi-Fi Security and Pentesting	8	2	a), b), c), d), e), f)	

5.4 Evaluación

A continuación, se especifica para cada unidad didáctica los resultados de aprendizaje y los criterios de evaluación correspondientes a la misma, así como los instrumentos de evaluación que se usarán para calificar cada uno de ellos.

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	TÉCNICA
RA1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.	a) Se ha definido la terminología esencial del hacking ético.	Proyecto integrado y actividades teórico-prácticas
	b) Se han identificado los conceptos éticos y legales frente al ciberdelito.	
	c) Se ha definido el alcance y condiciones de un test de intrusión.	
	d) Se han identificado los elementos esenciales de seguridad: confidencialidad, autenticidad, integridad y disponibilidad.	
	e) Se han identificado las fases de un ataque seguidas por un atacante.	
	f) Se han analizado y definido los tipos de vulnerabilidades.	
	g) Se han analizado y definido los tipos de ataque.	
	h) Se han determinado y caracterizado las diferentes vulnerabilidades existentes.	
	i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.	
RA2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.	a) Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas.	Proyecto integrado y actividades teórico-prácticas
	b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.	
	c) Se han generado informes de datos móviles, cumpliendo con los requisitos de la industria forense de telefonía móvil.	
	d) Se ha accedido a redes inalámbricas vulnerables.	

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	TÉCNICA
	e) Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades.	
	f) Se han utilizado técnicas de “Equipo Rojo y Azul”.	
	g) Se han realizado informes sobre las vulnerabilidades detectadas.	
RA3. Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.	a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas.	Proyecto integrado y actividades teórico-prácticas
	b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas	
	c) Se ha interceptado tráfico de red de terceros para buscar información sensible.	
	d) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos.	
	e) Se han comprometido sistemas remotos explotando sus vulnerabilidades.	
RA4. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.	a) Se han administrado sistemas remotos a través de herramientas de línea de comandos.	Proyecto integrado y actividades teórico-prácticas
	b) Se han comprometido contraseñas a través de ataques de diccionario, tablas rainbow y fuerza bruta contra sus versiones encriptadas.	
	c) Se ha accedido a sistemas adicionales a través de sistemas comprometidos.	
	d) Se han instalado puertas traseras para garantizar accesos futuros a los sistemas comprometidos.	
RA5. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo	a) Se han identificado los distintos sistemas de autenticación web, destacando sus debilidades y fortalezas.	Proyecto integrado y actividades teórico-prácticas

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	TÉCNICA
acceso a datos o funcionalidades no autorizadas.		
	b) Se ha realizado un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación web.	
	c) Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación web durante su uso normal.	
	d) Se han examinado manualmente aplicaciones web en busca de las vulnerabilidades más habituales.	
	f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.	

6. Módulo Profesional. Normativa de ciberseguridad (5026)

6.1 Objetivos del módulo

o) Identificar el alcance de la aplicación normativa dentro de la organización, tanto internamente como en relación con terceros para definir las funciones y responsabilidades de todas las partes.

p) Revisar y actualizar procedimientos de acuerdo con normas y estándares actualizados para el correcto cumplimiento normativo en materia de ciberseguridad y de protección de datos personales.

q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.

r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.

s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.

t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.

u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

6.2 Resultados de aprendizaje

El Real Decreto 479/2020, de 7 de abril, establece para este módulo profesional, los siguientes Resultados de aprendizaje:

RA	LOGRO	OBJETO	ACCIONES EN EL CONTEXTO DE APRENDIZAJE
RA 1	Identifica	Los puntos principales de aplicación para asegurar el cumplimiento normativo	Reconociendo funciones y responsabilidades
RA 2	Diseña	Sistemas de cumplimiento normativo	Seleccionando la legislación y jurisprudencia de aplicación
RA 3	Relaciona	La normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos	Recopilando y aplicando las normas vigentes
RA 4	Aplica	La legislación nacional de protección de datos de carácter personal	Relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia
RA 5	Recopila y aplica	La normativa vigente de ciberseguridad de ámbito nacional e internacional	Actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia

6.3

6.4 Selección y secuencia de contenidos

UNIDADES DIDÁCTICAS		SESIONES	RA	CRITERIOS	
UD1	Fundamentos Jurídicos de la Seguridad Informática	4	1	a	1er trimestre (22 horas)
UD2	Principios y Buenas Prácticas de la Seguridad de la Información	8	1	b, c, d, e	
UD3	Gestión de Riesgos	10	2	a, b, c, d	
UD4	Normativas, Regulaciones y Legislación	14	4	a, b, c, d, e, f, g	2o trimestre (38 horas)
UD5	Sistemas de Gestión de la Seguridad de la Información	16	5	a, b, c, d, e	
UD6	Legislación para el Cumplimiento de la Responsabilidad Penal	8	3	a, b, c, d	

6.5 Evaluación

A continuación, se especifica el peso de cada uno de los resultados de aprendizaje, así como el de los criterios de evaluación que lo componen. La mayor o menor ponderación de los criterios se obtiene en base

al nivel de dificultad y contenidos a desarrollar para cada criterio. La calificación de cada resultado de aprendizaje será la media ponderada de los distintos criterios de evaluación.

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	PESO RA	PESO CE	TÉCNICA
RA1. Identifica los puntos principales de aplicación para asegurar el cumplimiento normativo reconociendo funciones y responsabilidades.	a) Se han identificado las bases del cumplimiento normativo a tener en cuenta en las organizaciones.	20%	4%	Proyecto integrado y actividades teórico-prácticas
	b) Se han descrito y aplicado los principios de un buen gobierno y su relación con la ética profesional.		4%	
	c) Se han definido las políticas y procedimientos, así como la estructura organizativa que establezca la cultura del normativo dentro de las organizaciones.		4%	
	d) Se han descrito las funciones o competencias del responsable del cumplimiento normativo dentro de las organizaciones.		4%	
	e) Se han establecido las relaciones con terceros para un correcto cumplimiento normativo.		4%	
RA2. Diseña sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación.	a) Se han recogido las principales normativas que afectan a los diferentes tipos de organizaciones.	25%	5%	Proyecto integrado y actividades teórico-prácticas
	b) Se han establecido las recomendaciones válidas para diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 19.600 entre otras).		5%	

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	PESO RA	PESO CE	TÉCNICA
	c) Se han realizado análisis y evaluaciones de los riesgos de diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 31.000 entre otras).		7,5%	
	d) Se ha documentado el sistema de cumplimiento normativo diseñado.		7,5%	
RA3. Relaciona la normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos, recopilando y aplicando las normas vigentes.	a) Se han identificado los riesgos penales aplicables a diferentes organizaciones.	10%	2%	Proyecto integrado y actividades teórico-prácticas
	b) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados.		2%	
	c) Se ha establecido un sistema de gestión de cumplimiento normativo penal de acuerdo con la legislación y normativa vigente (Código Penal y UNE 19.601, entre otros).		3%	
	d) Se han determinado los principios básicos dentro de las organizaciones para combatir el soborno y promover una cultura empresarial ética de acuerdo con la legislación y normativa vigente (ISO 37.001 entre otros).		3%	

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	PESO RA	PESO CE	TÉCNICA
RA4. Aplica la legislación nacional de protección de datos de carácter personal, relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia.	a) Se han reconocido las fuentes del Derecho de acuerdo con el ordenamiento jurídico en materia de protección de datos de carácter personal.	20%	2%	Proyecto integrado y actividades teórico-prácticas
	b) Se han aplicado los principios relacionados con la protección de datos de carácter personal tanto a nivel nacional como internacional.		3%	
	c) Se han establecido los requisitos necesarios para afrontar la privacidad desde las bases del diseño.		2%	
	d) Se han configurado las herramientas corporativas contemplando el cumplimiento normativo por defecto.		3%	
	e) Se ha realizado un análisis de riesgos para el tratamiento de los derechos a la protección de datos		3%	
	f) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados en la protección de datos.		4%	
	g) Se han descrito las funciones o competencias del delegado de protección de datos dentro de las organizaciones.		3%	

RESULTADOS DE APRENDIZAJE	CRITERIOS DE EVALUACIÓN	PESO RA	PESO CE	TÉCNICA
RA5.Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.	a) Se ha establecido el plan de revisiones de la normativa, jurisprudencia, notificaciones, etc. jurídicas que puedan afectar a la organización.	25%	5%	Proyecto integrado y actividades teórico-prácticas
	b) Se ha detectado nueva normativa consultando las bases de datos jurídicas siguiendo el plan de revisiones establecido.		5%	
	c) Se ha analizado la nueva normativa para determinar si aplica a la actividad de la organización.		5%	
	d) Se ha incluido en el plan de revisiones las modificaciones necesarias, sobre la nueva normativa aplicable a la organización, para un correcto cumplimiento normativo.		5%	
	e) Se han determinado e implementado los controles necesarios para garantizar el correcto cumplimiento normativo de las nuevas normativas. incluidas en el plan de revisiones.		5%	

7. Registro de versiones

RESPONSABLE	ACCIÓN (REDACTADO, REVISADO)	FECHA	VERSIÓN
Carmona Martos, Alejandro Fenández Oliver, Eduardo Rivas Sánchez, Manuel Romero Santos, David	Redactado	28/10/2022	1.0
Carmona Martos, Alejandro Fenández Oliver, Eduardo Rivas Sánchez, Manuel Romero Santos, David	Revisado		1.1
Fenández Oliver, Eduardo Rivas Sánchez, Manuel Romero Santos, David Ureña Lara, Fernando	Revisado	06/11/2023	1.2
Fenández Oliver, Eduardo Ortega Nogueras, Francisco Javier Rivas Sánchez, Manuel Romero Santos, David	Revisado		1.3