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: Incidentes de Ciberseguridad

RA1: **Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección**	20 %

Criterios de evaluación:

%	CE	Inst. Evaluac.
15%	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.	Examen teorico
25%	b) Se ha establecido una normativa de protección del puesto de trabajo.	Presentación individual.
25%	c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.	Presentación individual
25%	d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.	Práctica
10%	e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.	Examen teórico.

RA2: **Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.**	10 %

Criterios de evaluación:

%	CE	Inst. Evaluac.
10%	a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización	Examen teórico.
20%	b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes	Práctica
30%	c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física	Práctica
30%	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*)	Práctica
10%	e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.	Examen teórico

RA3: **Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.**	20 %

Criterios de evaluación:

%	CE	Inst. Evaluac.
20%	a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.	Práctica
30%	b) Se ha realizado un análisis de evidencias.	Práctica
20%	c) Se ha realizado la investigación de incidentes de ciberseguridad	Práctica
10%	d) Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que podrían hacer aportaciones al respecto.	Cuestionario multirespuesta
20%	e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados	Cuestionario multirespuesta

RA4: **Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.**	30 %

Criterios de evaluación:

%	CE	Inst. Evaluac.
20%	a) Se han desarrollado procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.	Trabajo grupal
15%	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.	Trabajo grupal
15%	c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.	Trabajo grupal
15%	d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.	Trabajo grupal
20%	e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de “lecciones aprendidas”.	Práctica
15%	f) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.	Práctica

RA5: **Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.**	20 %

Criterios de evaluación:

%	CE	Inst. Evaluac.
40%	a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.	Trabajo individual
15%	b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.	Trabajo individual
15%	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.	Trabajo individual
15%	d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.	Trabajo individual
15%	e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.	Trabajo individual