



TABLA 9: Evaluación
Familia Profesional: Informática y Comunicaciones
Curso de Especialización: 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%
% CE	Criterios de evaluación	Instrumentos de evaluación	% IE
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 teórico	100
25	b) Se ha establecido una normativa de protección del puesto de trabajo.	Presentación individual. FEM	50 50
25	c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.	Presentación individual	100
25	d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.	Práctica FEM	50 50
10	e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.	Examen teórico.	100

RA2	Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.		10%
% CE	Criterios de evaluación	Instrumentos de evaluación	% IE
10	a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización.	Examen teórico.	100
20	b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes.	Práctica FEM	50 50

TABLA 9: Evaluación

Familia Profesional: Informática y Comunicaciones
 Curso de Especialización: Ciberseguridad en
 Entornos de las Tecnologías de la Información
 Módulo Profesional: Incidentes de Ciberseguridad



RA2	Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.		10%
% CE	Criterios de evaluación	Instrumentos de evaluación	% IE
30	c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física	Práctica	100
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 (<i>OSINT: Open Source Intelligence</i>)	Práctica	100
10	e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.	Examen teórico	100

RA3	Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.		20 %
% CE	Criterios de evaluación	Instrumentos de evaluación	% IE
20	a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.	Práctica	50
		FEM	50
30	b) Se ha realizado un análisis de evidencias.	Práctica	100
20	c) Se ha realizado la investigación de incidentes de ciberseguridad	Práctica	100
10	d) Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que	Cuestionario multirespuesta	100

TABLA 9: Evaluación

Familia Profesional: Informática y Comunicaciones

Curso de Especialización: Ciberseguridad en

Entornos de las Tecnologías de la Información

Módulo Profesional: Incidentes de Ciberseguridad



RA3	Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.		20 %
% CE	Criterios de evaluación	Instrumentos de evaluación	% IE
	podrían hacer aportaciones al respecto.		
20	e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados	Cuestionario multirespuesta	100

RA4	Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.		30%
% CE	Criterios de evaluación	Instrumentos de evaluación	% IE
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 FEM	50 50
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	100
15	c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.	Trabajo grupal	100
15%	d) Se han llevado a cabo las tareas de restablecimiento de los servicios	Trabajo grupal	100

TABLA 9: Evaluación

Familia Profesional: Informática y Comunicaciones



Curso de Especialización: Ciberseguridad en

Entornos de las Tecnologías de la Información

Módulo Profesional: Incidentes de Ciberseguridad

RA4	Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.		30%
% CE	Criterios de evaluación	Instrumentos de evaluación	% IE
	afectados por un incidente hasta confirmar la vuelta a la normalidad.		
20%	e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de "lecciones aprendidas".	Práctica	100
15%	f) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.	Práctica	100

RA5	Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.		20 %
%CE	Criterios de evaluación	Instrumentos de evaluación	% IE
40	a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.	Trabajo individual	50
		FEM	50
15	b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.	Trabajo individual	100
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	100
15	d) Se ha notificado formalmente el incidente a los afectados, personal	Trabajo individual	100

TABLA 9: Evaluación

Familia Profesional: Informática y Comunicaciones

Curso de Especialización: Ciberseguridad en

Entornos de las Tecnologías de la Información

Módulo Profesional: Incidentes de Ciberseguridad



RA5	Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.		20 %
%CE	Criterios de evaluación	Instrumentos de evaluación	% IE
	interno, clientes, proveedores, etc., en caso de ser necesario.		
15	e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.	Trabajo individual	100