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: Incidentes de Ciberseguridad

RA1	Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.	UT1. Desarrollo de planes de prevención y concienciación en ciberseguridad		Saber Hacer	Saber Estar
Criterios de Evaluación	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.	• Principios generales en materia de ciberseguridad.	Contenidos Básicos	• Define los principios generales de ciberseguridad que debe tener una empresa.	• Valora el grado de aplicación de dicha normativa al contexto de la empresa.
	b) Se ha establecido una normativa de protección del puesto de trabajo.	• Normativa de protección del puesto del trabajo		• Establece las politicas de seguridad necesarias para garantizar la seguridad informática en los lugares de trabajo.	•
	c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.	• Plan de formación y concienciación en materia de ciberseguridad.		• Desarrolla un plan de concienciación adaptado a la empresa	• Tiene en cuenta el conocimiento en materia de ciberseguridad de la plantilla de cara a la elaboración del plan de concienciación.
	d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.	• Materiales de formación y concienciación.		• Elabora material de concienciación y ejecuta activiades de ingeniería social como phishing en el lugar de trabajo.	•
	e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización	• Auditorías internas de cumplimiento en materia de prevención.		• Conoce la normativa referente a las auditorías, los tipos que existen, como se llevan a cabo y sabe aplicarlas.	• Pone en valor la realización periódica de una auditoría como método de mejorar de forma contínua el nivel de seguridad.

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: Incidentes de Ciberseguridad

RA2	Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.	UT2. Auditoría de incidentes de ciberseguridad:		Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización	• Taxonomía de incidentes de ciberseguridad	Contenidos Básicos	• Conoce lo que es una taxonomía y ejemplos de ellas en el ámbito de la clasificación de incidentes de ciberseguridad.	• Valora la importancia de una taxonomía de calidad a la hora de trabajar con los diferentes incidentes.
	b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes	• Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes: tipos y fuentes		• Implementa métodos de detección de incidentes basados en la monitorización de redes, losg, etc, empleando herramientas como un IDS o un SIEM.	• Reconoce el valor de los sistemas de detección y alerta de incidentes para la detección temprana y en pos de facilitar la mitigación posterior.
	c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física.	• Controles, herramientas y mecanismos de detección e identificación de incidentes de seguridad física		• Conoce los riesgos de una baja seguridad física y desarrolla mecanismos para mejorarla.	• Importancia de valorar la seguridad física y/o perimetral como un incidente o vector de ataque más de ciberseguridad.
	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*).	• Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT).		• Automatiza el proceso de detección de incidentes haciendo uso de fuentes abiertas.	
	e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.	• Clasificación, valoración, documentación, seguimiento inicial de incidentes de ciberseguridad.		• Aplica la taxonomía para clasificar los incidentes y mantiene canales de comunicación, documentación y control de los mismos	• Reconoce la importancia de una gestión organizada de los incidentes entre todos los miembros de la organización.

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: Incidentes de Ciberseguridad

R	Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.	UT3. Investigación de los incidentes de ciberseguridad:		Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.	• - Recopilación de evidencias.	Contenidos Básicos	• Recopila las diferentes evidencias del incidente.	• Es metodológico y ordenado a la hora de realizarlo.
	b) Se ha realizado un análisis de evidencias.	• Análisis de evidencias.		• Analiza las evidencias del incidente realizando una categorizacion inicial de su impacto y riesgo.	
	c) Se ha realizado la investigación de incidentes de ciberseguridad.	• Investigación del incidente		• Investiga el incidente para determinar las cuasas del mismo y conocer los servicios e información que se han visto afectados.	
	d) Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que podrían hacer aportaciones al respecto.	• Intercambio de información del incidente con proveedores u organismos competentes.		• Intercambia datos del incidente con otros organismos y entidades especializados en la ciberseguridad.	
	e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados	• Medidas de contención de incidentes.		• Toma medidas de prevención antes de que otros equipos, sistemas o datos se vean afectados por el incidente.	

RA4	Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.	UT4. Implementación de medidas de ciberseguridad:		Saber Hacer	Saber Estar
Cri ter	a) Se han desarrollado procedimientos de actuación detallados para dar respuesta,	• Desarrollar procedimientos de actuación detallados para	Co	• Desarrolla procedimientos de gestión de incidentes para dar una respuesta	

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: Incidentes de Ciberseguridad

RA4	Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.	UT4. Implementación de medidas de ciberseguridad:	Saber Hacer	Saber Estar
	mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.	dar respuesta, mitigar, eliminar o contener los tipos de incidentes.	rápida a aquellos más habituales o que pudieran tener un mayor impacto.	
	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.	• Implantar capacidades de ciberresiliencia.	• Implementa desarrollos de software que permiten ofrecer el servicio pese a la existencia de un ciberataque con técnicas de replicación y distribución de contenidos y alta disponibilidad.	
	c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.	• Establecer flujos de toma de decisiones y escalado interno y/o externo adecuados.		• Asume su responsabilidad y toma las decisiones que le corresponden durante el incidente.
	d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.	• Tareas para reestablecer los servicios afectados por incidentes.	• Lleva a cabo todas las tareas de restauración del servicio eliminando los daños realizados por el incidente durante el proceso de recuperación.	
	e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de “lecciones aprendidas”.	• Documentación	• Documenta el proceso de resolución del incidente para su aprovechamiento en el futuro.	
	f) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.	• Seguimiento de incidentes para evitar una situación similar.	• Desarrolla planes de prevención y de recuperación en base a los errores del incidente para evitar o minimizar daños futuros.	

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: Incidentes de Ciberseguridad

RA5	Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.	UT5. Detección y documentación de incidentes de ciberseguridad		Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.	• Desarrollar procedimientos de actuación para la notificación de incidentes.	Contenidos Básicos	• Elabora un plan de actuación para la notificación del incidente.	
	b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.	• Notificación interna de incidentes.		• Mantiene canales de información y documentación a empleados y colaboradores de la empresa.	
	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.	• Notificación de incidentes a quienes corresponda.		• Notifica por los canales adecuado y proporcionando la información necesaria la existencia de un incidente.	• Tiene en cuenta la normativa vigente en materia de notificación de incidentes a los CERT que correspondan.
	d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.	• Notificación de incidentes a quienes corresponda.		• Notifica el incidente a los afectados.	• Valora la importancia de la comunicación exterior de cara a la imagen de la empresa.
	e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.	• Notificación de incidentes a quienes corresponda.		• Comunica el incidente en medios de comunicación si fuera necesario.	• Valora la importancia de la comunicación exterior de cara a la imagen de la empresa.