CONTENIDOS DE LA UNIDAD, CRITERIOS DE EVALUACIÓN Y RESULTADOS DE APRENDIZAJE

La siguiente tabla responde al REAL DECRETO 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo. Se incluye también una columna con las unidades didácticas que forman el curso, en las que se desarrollas los diferentes bloques de contenidos.

CONTENIDOS	CRITERIOS DE EVALUACIÓN	RESULTADOS DE APRENDIZAJE	UNIDAD TRABAJO
Bloque 1. Desarrollo de Planes de Prevención y Concienciación en Ciberseguridad.			
Desarrollo de planes de prevención y concienciación en ciberseguridad: ▪ Principios generales en materia de ciberseguridad. ▪ Normativa de protección del puesto del trabajo. ▪ Plan de formación y concienciación en materia de ciberseguridad. ▪ Materiales de formación y concienciación. ▪ Auditorías internas de cumplimiento en materia de prevención.	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. b) Se ha establecido una normativa de protección del puesto de trabajo. c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados. d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados. **e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.**	RA1. Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.	U.T. 1

Bloque 2. Auditoría de Incidentes de Ciberseguridad.			
Auditoría de incidentes de ciberseguridad: ▪ Taxonomía de incidentes de ciberseguridad. ▪ Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes: tipos y fuentes. ▪ Controles, herramientas y mecanismos de detección e identificación de incidentes de seguridad física. ▪ Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT). ▪ Clasificación, valoración, documentación, seguimiento inicial de incidentes de ciberseguridad.	a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización. b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física. 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). **e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.**	RA2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.	U.T. 2
Bloque 3. Investigación de los Incidentes de Ciberseguridad.			
Investigación de los incidentes de ciberseguridad: ▪ Recopilación de evidencias. ▪ Análisis de evidencias. ▪ Investigación del incidente ▪ Intercambio de información del incidente con proveedores u organismos competentes. ▪ Medidas de contención de incidentes.	**a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.** **b) Se ha realizado un análisis de evidencias.** **c) Se ha realizado la investigación de incidentes de ciberseguridad.** d) Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que podrían hacer aportaciones al respecto. e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados.	RA3. Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.	U.T. 3

Bloque 4. Implantación de Medidas de Ciberseguridad.			
Implementación de medidas de ciberseguridad: ▪ Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes. ▪ Implantar capacidades de ciberresiliencia. ▪ Establecer flujos de toma de decisiones y escalado interno y/o externo adecuados. ▪ Tareas para reestablecer los servicios afectados por incidentes. ▪ Documentación. ▪ Seguimiento de incidentes para evitar una situación similar.	**a) Se han desarrollado procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.** 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. c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados. **d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.** **e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de "lecciones aprendidas".** f) **Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.**	RA4. Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.	U.T. 4
Bloque 5. Detección y Documentación de Incidentes de Ciberseguridad.			
Detección y documentación de incidentes de ciberseguridad: ▪ Desarrollar procedimientos de actuación para la notificación de incidentes. ▪ Notificación interna de incidentes. ▪ Notificación de incidentes a quienes corresponda.	**a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.** b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones. **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.** d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario. e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.	RA5. Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.	U.T. 5

Bloque 6. IDS/IPS Snort.			
Prototipo de un SOC: ▪ Prevención de Intrusiones. ▪ Snort - El IDS/IPS de Código Abierto. ▪ Instalación y Configuración de Snort. ▪ Inicio, Arranque y Parada de Snort. ▪ Ficheros de Configuración Básica de Snort. ▪ Fichero de Registro de Alertas de Snort. ▪ Torre de Protocolos ISO-OSI. ▪ Detección de Tráfico ICMP con Snort. ▪ Detección de Tráfico SSH con Snort.	a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización. **b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes.** c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física. 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). e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.	RA2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.	U.T. 6
Bloque 7. SIEM ELK.			
Escenario de Trabajo SIEM: ▪ Premisas para la Práctica SIEM. ▪ Instalación de OpenJDK. ▪ Instalación de Elasticsearch. ▪ Instalación de Logstash. ▪ Instalación de Kibana. ▪ Configuración SIEM. ▪ Visualización SIEM.	a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización. **b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes.** c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física. 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). e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.	RA2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.	U.T. 7

C.E. CIBERSEGURIDAD: INCIDENTES DE CIBERSEGURIDAD

Este módulo profesional contiene la formación necesaria para desempeñar las funciones de análisis, detección y respuesta a los incidentes de ciberseguridad de la organización.

La función de análisis y detección de incidentes de ciberseguridad incluye aspectos como la monitorización de los sistemas para la recopilación de evidencias que permita dar una respuesta adecuada a los incidentes detectados.

Las actividades profesionales asociadas a esta función se aplican mediante la instalación y configuración de las herramientas necesarias para hacer frente a los ciberataques.

La formación del módulo contribuye a alcanzar los objetivos generales a), b), c), d), q), r), s), t), u) y v) y las competencias a), b), k), l), m), n) y ñ) del curso de especialización.

Las líneas de actuación en el proceso de enseñanza aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

- La elaboración de planes de prevención y concienciación de ciberseguridad.
- La detección de incidentes mediante distintas herramientas de monitorización.
- La implantación de las medidas necesarias para responder a los incidentes detectados.
- Identificación de la normativa nacional e internacional aplicable en la organización.
- La notificación de incidentes tanto interna como externa, si procede, mediante los procedimientos adecuados.