IC03.- Investigación de los Incidentes de Ciberseguridad.

Orientaciones Alumnado

En esta unidad de trabajo aprenderás los mecanismos y procedimientos que se emplean para investigar en detalle los incidentes de ciberseguridad.

La investigación de incidentes tiene características análogas a la labor que efectúa la Policía Científica, con la que además mantiene una estrecha relación. En esta línea, la labor tiene que ver con recopilación de pruebas, verificación de su validez, custodia controlada de las mismas, y análisis detallado de todas ellas, de forma que no sólo sirvan para determinar y erradicar la causa raíz de un incidente, sino también para constituir pruebas de cargo en un juicio, en un momento dado.

Para fijar las ideas y asimilar la importancia de los conceptos, la unidad incluye un conjunto de ejercicios resueltos que te resultarán de gran interés.

Datos generales de la Unidad de Trabajo

Nombre completo del MP	Incidentes de Ciberseguridad	**Siglas MP**	IC
Nº y título de la UT	03.- Investigación de los Incidentes de Ciberseguridad		
Índice o tabla de contenidos	1.- Recopilación de Evidencias. 1.1.- Principios durante la recolección de evidencias. 1.1.1.- Orden de volatilidad. 1.1.2.- Acciones que deben evitarse. 1.1.3.- Consideraciones sobre la privacidad. 1.2.- Procedimiento de recolección. 1.2.1.- Transparencia. 1.2.2.- Pasos. 1.3.- El procedimiento de almacenamiento. 1.3.1.- Cadena de custodia. 1.3.2.- Dónde y cómo almacenar las evidencias. 1.4.- Herramientas necesarias. 1.5.- Conclusiones de la Recopilación. 2.- Análisis de Evidencias. 3.- Investigación del Incidente. 4.- Intercambio de Información del Incidente con Proveedores u Organismos Competentes. 5.- Medidas de Contención de Incidentes. 6.- Bibliografía.		
Objetivos	Con el estudio de esta unidad serás capaz de: ✓ Efectuar la recopilación detallada y consistente de evidencias, almacenándolas de forma segura y custodiándolas hasta el momento de su utilización. ✓ Analizar las evidencias recopiladas para investigar las causas de los incidentes. ✓ Intercambiar la información obtenida con entidades públicas y privadas, con objeto de contener futuros incidentes.		
Temporalización (estimación)	**Tiempo necesario para estudiar los contenidos (h)**	11	
	Tiempo necesario para completar la tarea (h)	2	
	Tiempo necesario para completar el examen (h)	1	
	Nº de días que se recomienda dedicar a esta unidad	13	
	La temporalización anterior es una estimación media, ya que el tiempo a invertir dependerá de las circunstancias personales de cada alumno.		
Consejos y recomendaciones	✓ La materia del módulo está estructurada de forma progresiva, por lo que es importante que completes el estudio de cada unidad y asimiles sus contenidos, antes de proseguir con el estudio del resto de las unidades. ✓ Los ejercicios técnicos incluidos en las cinco primeras unidades del módulo son ilustrativos. Su misión es concienciarte y brindarte experiencia directa sobre ciertos temas, por lo que es muy conveniente que los ejecutes por tu cuenta en tu propio entorno, siempre que esto sea posible. ✓ Además, estos ejercicios tienen una misión secundaria también muy importante, que es brindarte conocimientos con objeto de que tengas la soltura necesaria para abordar las dos últimas unidades, que son esencialmente prácticas de laboratorio de mayor envergadura.		