FICHA DE ASIGNATURA

Título: Respuesta a Incidentes y Análisis Forense

Descripción:

El objetivo de este curso es presentar la metodología necesaria para dar respuesta a un incidente de seguridad, así como dar las herramientas técnicas y procedimentales para abordar una situación en la que se requiera un análisis forense teniendo especial cuidado de que las pruebas digitales presentadas sean admisibles ante un tribunal. El equipo docente que imparte el curso es experto en análisis forense y en actuar como perito informático en procedimientos judiciales de las distintas ramas del derecho.

Carácter*:* Obligatoria

Créditos ECTS: 6

Contextualización:

El programa de esta asignatura pretende proporcionar al alumno una serie de conocimientos en el campo del Análisis Forense Informático que les serán de utilidad en su formación como especialistas en seguridad, al proporcionarles los conceptos básicos para dar respuesta a los incidentes de seguridad y reunir y presentar las pruebas forenses correspondientes.

Modalidad*:* Online

Temario:

- Respuesta a Incidentes:
  - Metodología de gestión, normativa aplicable y notificaciones a organismos de referencia
  - Centros de respuesta a incidentes, centros de emergencias en seguridad y centros de operaciones
  - Plan de respuesta a incidentes (ISO 23301) y continuidad de negocio
- Análisis forense
  - Herramientas de ataque y evidencias en registros del sistema (redes, sistemas de ficheros y actividad maliciosa)
  - Evidencia electrónica: custodia, preservación de pruebas, peritaje y jurisprudencia
  - Artefactos de forense

Competencias Específicas:

CE4 – Identificar las vulnerabilidades, amenazas, y software malicioso a los que estén expuestos los diferentes activos de una organización.

CE7 - Conocer las tendencias actuales en ciberataques, técnicas de ocultación y principales vectores utilizados.

CE8 - Crear informes de carácter ejecutivo y de carácter científico-técnico que respondan a las necesidades de comunicación en términos de ciberseguridad dentro de una organización.

Actividades Formativas

Actividad Formativa	Horas	Presencialidad
Sesiones síncronas	30	100%
Desarrollo de actividades del portafolio	24	0
Trabajo autónomo del alumno	96	0

Metodologías docentes:

- Clase magistral
- Aprendizaje Basado en Problemas (ABP)
- Simulación - role play

Sistema de Evaluación*:*

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
Trabajos individuales dirigidos	40.0	60.0
Pruebas de conocimiento	40.0	60.0

Normativa específica*:*

Bibliografía:

- Gestión de incidentes de seguridad informática, Ester Chicano Tejada, 2014 https://ebookcentral.proquest.com/lib/universidadviusp/reader.action?docID=4184054
- Gestión de incidentes de seguridad informática, Álvaro Gómez Vieite, 2014 https://ebookcentral.proquest.com/lib/universidadviusp/reader.action?docID=3229340
- https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html
- https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf
- https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/respuesta-incidentes.pdf