ITINERARIO FORMATIVO CIBERSEGURIDAD

“DFIR- Digital Forensic and Incident Response”

(300 horas)

- **Objetivo general**

A través de este curso se pretende dotar de conocimientos y competencias a los alumnos para que sean capaces de gestionar incidentes de seguridad, conociendo el marco legal del desarrollo de la actividad y pudiendo evolucionar/profesionalizar hacia la rama de FORENSE DIGITAL. Una vez finalizado, los alumnos también pueden formar parte de los equipos de blue team (equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva), realizando las labores de detección y respuesta.

- **Objetivos específicos**

- Adquirir una visión horizontal del mundo de la Ciberseguridad y de los empleos relacionados.
- Conocer la realidad del estado del cibercrimen y el negocio que este genera.
- Disponer de una metodología para la implantación de un plan de respuesta ante incidentes en la empresa.
- Conocer las bases de Sistemas operativos y redes sobre la que se sustentan tanto los ataques informáticos como la detección y gestión de estos.
- Capacitar en el uso de herramientas de uso empresarial en el campo de la respuesta ante incidentes, IR.
- Capacitar al alumno en los requisitos de recogida y tratamiento de evidencias en modo forense, de modo que puedan ser presentadas ante tribunales.

- Realizar el informe forense, como entregable de la actividad pericial.
- Gestionar los esfuerzos en materia de securización bajo el modelo basado en el riesgo.
- Aplicar el análisis y gestión de riesgos bajo metodologías reconocidas del mercado.
- Tratar los datos de carácter personal según legislación vigente. GDPR.

➢ **Contenidos**:

- Sistemas operativos y virtualización
- Redes
- Normativa y análisis de riesgos
- Respuesta ante incidentes
- Análisis forense