

DESCRIPCIÓN DEL PUESTO DE TRABAJO

TÉCNICO DE ANÁLISIS FORENSE

| | |
|--|--|
| Misión | Llevar a cabo técnicamente las actividades de análisis forense e investigación de incidentes de seguridad de las TIC en cumplimiento de las funciones asignadas al Centro Criptológico Nacional. |
| Titulación | Formación Profesional Grado Medio en el ámbito de las nuevas tecnologías y las comunicaciones. |
| Funciones o responsabilidades principales | <p>Según la experiencia que se tenga, podrá tener como funciones o responsabilidades algunas de las detalladas a continuación:</p> <ul style="list-style-type: none"> • Análisis forense de soportes informáticos. • Análisis forense de dispositivos electrónicos. • Gestionar laboratorios y material. • Administrar redes y manejo de instrumental de laboratorio forense. |
| Experiencia / Conocimientos | <p>Experiencia en proyectos de Ciberseguridad de al menos 5 años y, en concreto en alguno de los siguientes ámbitos:</p> <ul style="list-style-type: none"> • Gestión y/o operación de Centro de Operaciones de Seguridad (SoC), abarcando el análisis y gestión de vulnerabilidades, monitorización y análisis de indicadores para la detección de las amenazas por parte de los sistemas SIEM, gestión de sistemas de detección y prevención de intrusiones, definición de reglas de correlación y gestión y respuesta ante incidentes de seguridad. • Realización de auditorías de seguridad, con experiencia en análisis forense y análisis de malware. Se incluye experiencia en pentesting, hacking ético y/o administración, gestión de evidencias y configuración de seguridad de redes, aplicaciones y dispositivos. • Se valorará disponer de experiencia previa en la administración de redes y sistemas y el conocimiento de normativas relacionadas con la Ciberseguridad. |
| Otros estudios valorables | <ul style="list-style-type: none"> • Certificaciones profesionales: CISP, OSCP, etc... • SANS Institute: Windows Forensic Analysis, Network Penetration Testing and Ethical Hacking, Securing Linux/Unix, Continuous Monitoring and Security Operations, etc... • Cursos o formaciones específicas en Ciberseguridad. |
| Idiomas | Se valorarán conocimientos de inglés a partir del nivel B2. |
| Competencias y otros aspectos relevantes | <ul style="list-style-type: none"> • Capacidad de aprendizaje . • Trabajo en equipo y de forma autónoma. • Iniciativa, proactividad y compromiso. • Disponibilidad, adaptabilidad y flexibilidad. • Gestión de equipos. • Vocación por la Ciberseguridad. |