DESCRIPCIÓN DEL PUESTO DE TRABAJO

TÉCNICO TIC. INCIDENTES DE SEGURIDAD EN CENTRO DE OPERACIONES DE CIBERSEGURIDAD

Misión	Llevar a cabo las actividades de análisis forense e investigación de incidentes de seguridad de las TIC (**Ciberseguridad**), en el COC (Centro de Operaciones de Ciberseguridad) en cumplimiento de las funciones asignadas al Centro Criptológico Nacional. Se considera muy valorable haber trabajado en un COS (Centro de Operaciones de Seguridad, SOC en inglés).
Funciones, responsabilidades principales	Principalmente: • Análisis y resolución de incidentes de seguridad. • Seguimiento y control mediante herramientas de ticketing. • Análisis de tráfico de red e identificación de anomalías. • Monitorización y correlación de alertas y eventos de seguridad y redes. • Monitorización y operación de elementos de seguridad: Firewalls, Proxy, AntiSPAM, Antivirus, EDR, SIEM, IDS, IPS, NIDS, etc. Además: • Análisis forense de soportes informáticos. • Análisis forense de dispositivos electrónicos. • Gestionar laboratorios y material. • Administrar redes y manejo de instrumental de laboratorio forense.
Titulación exigida	Formación Profesional Grado Medio en el ámbito de las nuevas tecnologías y las comunicaciones.
Experiencia valorable	Principalmente experiencia en proyectos de Ciberseguridad de al menos 5 años y, en concreto en alguno de los siguientes ámbitos: • Se valorará disponer de experiencia previa en la administración de redes, sistemas, bases de datos, elementos de seguridad y el conocimiento de normativas relacionadas con la Ciberseguridad. • Conocimientos técnicos en las siguientes tecnologías: Firewalls, WAF, Antivirus, EDR, AntiSPAM, ADDoS, IDS/IPS, HIDS, NIDS, SIEM, DLP, VPN, CASB, MTP, MDM, etc. • Conocimientos de productos y tecnologías de los principales fabricantes: Broadcom (Symantec/Bluecoat), Fortinet, PaloAlto Networks, Checkpoint, Cisco, Akamai, Forescout, TrendMicro, Sophos, ESET, Panda/Cytomic, McAfee, Zscaler, Microsoft, MobilIron, Airwatch, Kasperksy, etc. Además: • 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.
Conocimientos, certificaciones o estudios adicionales	Principalmente: • Certificación profesional: CEH (Certified Ethical Hacker). • Certificaciones fabricantes de seguridad: Checkpoint (CCSA, CCSE, CCES,..), Fortinet (NSE), PaloAlto Networks (PCNSA, PCNSE, PCSAE,…), etc. • Cursos o formaciones específicas en Big Data. Además: • Certificaciones profesionales: CISP y OSCP. • 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 B1.
Competencias, otros aspectos relevantes	• 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.