MINISTERIO
DE DEFENSA

DESCRIPCIÓN DEL PUESTO DE TRABAJO

INGENIERO/A TIC. INCIDENTES DE SEGURIDAD EN CENTRO DE OPERACIONES DE CIBERSEGURIDAD

Misión	Tratamiento y gestión de incidentes de seguridad complejos (**Ciberseguridad**) para el **COC (Centro de Operaciones de Ciberseguridad)** de la AGE (Administración General del Estado). Manejo de fuentes humanas. Impulsar, liderar y gestionar las actividades de desarrollo de las funciones del Centro Criptológico Nacional. Se considera muy valorable haber trabajado en un COS (Centro de Operaciones de Seguridad, SOC en inglés).
Funciones, responsabilidades principales	• Principalmente: definición, diseño, seguimiento y ejecución de planes de acción para la mejora de servicios de seguridad. Además: • Diseño e instalación de sistemas de seguridad de sistemas de información. • Administración de seguridad y mantenimiento de sistemas de información. • Detección temprana de fallos. Diagnóstico y resolución de Incidencias • Análisis de incidentes de seguridad. • Realización de auditorías de seguridad. • Desarrollo de procedimientos y normativa TIC y de seguridad. • Diseño e instalación de sistemas de cifra hardware y software. • Impartición de formación sobre Ciberseguridad.
Titulación exigida	Ingeniería Superior, Licenciatura o Grado con máster en alguna de las ramas de las TIC: Telecomunicación, Electrónica, Sistemas de Tratamiento de Información, Programación, Matemáticas o Computación.
Experiencia valorable	• Conocimiento en el diseño y análisis de arquitecturas de seguridad y redes. • Provisión de nuevos servicios de seguridad. • Gestión y resolución de incidentes de seguridad. • Configuración de seguridad de redes, aplicaciones y dispositivos. • Redes de comunicaciones: TPC IP, IPv4, IPv6, DNS, HTTP/HTTPS, OSI, LAN/WAN, Wi-Fi, etc • Routing & switching: OSPF, BGP, VLAN, STP. • Seguridad de redes: IPSEC, SSL, VPN, TLS, GRE, NAT, ACL. • Sistemas de monitorización de eventos de redes y sistemas. • Sistemas Operativos (Windows, Linux, Mac, iOS y Android), bases de datos y aplicaciones web. • 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. • Conocimientos sobre desarrollo seguro de aplicaciones. • Experiencia en auditorías de seguridad de sistemas, redes y aplicaciones. • Herramientas de escaneo y evaluación de seguridad: Nessus, OpenVAS, Burp Suite, Metasploit, etc. Además: • Conocimientos de normativas de seguridad: ENS, NIST, GDPR, etc • Experiencia en optimización y diseño de algoritmos complejos. • Ingeniería inversa de software. • Gestión y/o operación de Centro de Operaciones de Seguridad (SoC). • Experiencia en auditorías de seguridad, en análisis forense y análisis de malware, en pentesting, hacking ético y/o administración, en gestión de evidencias. • Administración de redes y sistemas y el conocimiento de normativas relacionadas con la Ciberseguridad.
Conocimientos, certificaciones o estudios adicionales	• Certificaciones fabricantes de seguridad: Checkpoint (CCSA, CCSE, CCES,..), Fortinet (NSE), PaloAlto Networks (PCNSA, PCNSE, PCSAE,…), etc. • Cursos o formaciones específicas en Big Data. • Certificaciones profesionales: CISM, CEH, CISCO (CCNA, CCNP,…), ISO27001, OSCP, CISA, CISPS, etc… Además: • Cursos o formaciones específicas en Ciberseguridad. • Lenguajes de programación de circuitos integrados y FPGA, Criptología y seguridad de las comunicaciones, optimización de algoritmos complejos, ingeniería inversa de software, programación en lenguaje de alto nivel. • SANS Institute: Windows Forensic Analysis, Network Penetration Testing and Ethical Hacking, Securing Linux/Unix, Continuous Monitoring and Security Operations, etc.
Idiomas	Se valorarán conocimientos de inglés a partir del nivel B2.
Competencias, otros aspectos relevantes	• Capacidad para la toma de decisiones. • Capacidad de liderazgo de equipos multidisciplinares. • Gestión y coordinación de grupos técnicos de seguridad. • Diseño de procedimientos. • Generación, revisión y presentación de informes. • 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.

Si te interesa esta oferta y consideras que puede encajar con tu objetivo profesional, envíanos tu CV a **oferta.empleo@cni.es** con el asunto **"Nombre de la oferta – VIU – Apellidos, nombre"** e incluyendo los siguientes datos personales: Nombre y apellidos; Fecha y lugar de nacimiento; NIF; Teléfono móvil; Correo electrónico, motivo por el que quieres unirte al CNI y área de interés profesional.

Departamento de Selección