	Fundamentos	Principiante	Intermedio	Especialista
Experiencia Laboral / Cargo	- Analista de Mesa de Ayuda - Soporte Técnico - Administrador de Infraestructura - Administrador de Redes	- Analista de Seguridad - Administrador de Redes - Administrador de Seguridad - Analista SOC	- Ingeniero de Respuesta a Incidentes - Analista Forense - Analista SOC Nivel II - Coordinador de SOC	- Lider de Respuesta a Incidentes - Líder de Investigación Forense - Lider de SOC
Conocimientos / Competencias	- **Sistemas Operativos**: Instalación de Windows, Linux OSX en Estaciones de Trabajo Instalación, Operación y Administración de Windows Server Instalación, Operación y Administración de Linux Sistemas de archivos FAT32, NTFS, EXT3, EXT4 , NFS, HFS Instalación de paquetes, programas y parches de seguridad - **Redes**: - Modelo OSI y TCP/IP - Configuración de servicios de red (DHCP, DNS, HTTP, SMTP, LDAP) - Configuración y Administración de Firewalls (iptables) - Identificar, Diseñar topologías de red - **Infraestructura**: Administrar un hipervisor (KVM, Hyper-V, VMware, QEMU) Desplegar y Administrar instancias windows/linux en la nube (AWS/Azure/Google) Despliegue, configuración y administración de contenedores Implementar un servicio de monitoreo (Zabbix, Nagios, Icinga, Cacti) Configurar, Administrar consolas de antivirus	- Definir controles de seguridad red y host - Implementar guías de aseguramiento (hardening) - Configurar y Administrar Sistemas de Detección de Intrusos - Ejecutar análisis de vulnerabilidades - Análisis de Logs de Seguridad - Análisis de Alertas de Seguridad - Analizar tráfico y flujos de red - Reconocer amenazas y vulnerabilidades - Desarrollo de scripts (bash, powershell, python) - Analizar arquitecturas de seguridad - Elaboración de informes técnicos	- Análisis forense en redes - Recuperación de Archivos - Análisis forense en sistemas operativos - Análisis forense en dispositivos móviles - Creación de firmas de Snort / Suricata - Elaboración y presentación de informes técnicos / ejecutivos - Análisis Forense en AWS / Azure - Adquisición de evidencia en vivo - Creación de imagenes forenses - Creación de Playbooks - Creación de casos de uso - Análisis de correos maliciosos - Definición de escenarios de riesgo - Elaboración de artículos técnicos (blog) - Expresiones Regulares - Análisis estático básico de Malware - Análisis de comportamiento de Malware	- Automatización y Orquestación de Procesos - Análisis de código malicioso - Ingeniería Inversa (Debugging, Dissasembly) - Criptografía - Elaboración y presentación de informes basados en riesgo - Gestión de Proyectos - Inteligencia de Amenazas - Elaboración de reportes de Inteligencia - Creación de reglas de YARA - Respuesta a Incidentes en Sistemas de Control Industrial - Liderazgo de equipos - Desarrollo de métricas - Elaboración de artículos técnicos (blog) - Desarrollo de scripts o herramientas para mejorar la detección de amenazas - Implementación y consolidación de CSIRTS - Investigaciones en tecnologías emergentes: - Drones - Vehiculos - IoT - Servicios Cloud
Certificaciones / Cursos	- CompTIA **A+** - CompTIA **Network +** - CompTIA **Linux+** - CompTIA **Server+** - Google IT Support - CISCO **CCNA**	- CompTIA **Security+** - CompTIA **Cloud+** - Mile2 **C)SP** - GIAC **GSEC** - EC-Council **CEH** - Mile2 **C)PTE**	- CompTIA **CySA+** - EC-Council **CSA** - EC-Council **ECIH** - EC-Council **CHFI** - Mile2 **C)IHE** - Mile2 **C)DFE** - Mile2 **C)NFE** - Cisco **CCNA Cyber Ops** - AWS **Certified Security** - Microsoft **Azure Security Engineer Associate** - GIAC **GMON** - GIAC **GCIA** - GIAC **GCFA** - GIAC **GNFA**	- ISC² **CISSP** - CSA **CCSK** - ISACA **CRISC** - ISACA **CISM** - CompTIA **CASP+** - GIAC **GREM** - GIAC **GRID** - GIAC **GCTI** - CISCO **CCIE** - AWS **Certified Advanced Networking**