

【NCS기반 채용 직무기술서: 전산개발】

| 채용분야 (채용직종) | 기술 | NCS 분류 체계 | 대분류 | 20.정보통신 | |
|----------------|--|--------------------|-----|----------------------------|----------------------------|
| | | | 중분류 | 01.정보기술 | |
| | | | 소분류 | 02.정보기술개발 | 06.정보보호 |
| | | | 세분류 | 05. NW엔지니어링 06. 보안엔지니어링 | 02.정보보호진단분석 03.보안사고분석대응 |
| 연구원 주요사업 | ○ 지질과학 연구, 지질자원 기반정보 구축·보급 및 지반·지하공간의 효율적 이용/광물자원 탐사·개발 및 순환·활용/지하 에너지자원 확보/지진, 지질재해 및 지구환경변화 대응/지하수자원의 탐사, 개발 및 보전 연구개발 등 | | | | |
| 핵심책무 | ○ (정보기술개발 및 정보보호) - 연구원 시스템/네트워크 환경구성을 이해하고 외부 사이버 해킹공격으로부터 내부 업무시스템/네트워크를 보호할 수 있는 보안정책을 수립하고 시행 - 업무시스템/홈페이지 웹취약점(OWASP) 및 시스템 취약점(Service Port 등) 점검/조치 업무 수행 - 개인정보보호법에 따른 개인정보 처리 업무 수행(수집이용, 저장관리, 제공위탁, 파기, 개인정보수준진단 등) - 연구원 사이버공격 및 침해사고 발생 시 사고분석(원인, 목적, 과정, 영향) 및 대응조치 업무 | | | | |
| 능력단위 | ○ (NW엔지니어링) 01.네트워크 환경분석 02.네트워크 프로토콜 분석 05.네트워크 자원관리 설계 10.네트워크 품질 평가 11.네트워크 프로젝트 관리 ○ (보안엔지니어링) 01.관리적 보안 구축 08.시스템 보안 구축 09.네트워크 보안 구축 10. 보안체계 운영관리 12.보안감사 수행 ○ (정보보호진단분석) 03.보안감사 06.보안대책설계 컨설팅 07.정보시스템 진단 ○ (보안사고분석대응) 05.침해사고분석 06.악성코드 분석 07.보안로그 분석 08.보안이벤트 대응 | | | | |
| 직무수행내용 | ○ (NW엔지니어링) 네트워크 프로토콜(TCP/IP)을 이해하고 다양한 형태의 네트워크 패킷 분석을 통해 최적화된 네트워크 환경(Topology)을 설계하고 구축하는 업무 ○ (보안엔지니어링) 정보보호 및 개인정보보호 관련 법률/정책 등을 이해를 바탕으로 이를 연구원 정보보안정책을 수립하고 네트워크/시스템에 적용/운영하는 업무. 또한 매년 수행하는 정보보안감사, 개인정보 수준진단 등 내/외부 감사 업무 ○ (정보보호진단분석) 매년 수행하는 내/외부 정보보안감사 수행/지원 업무, 정보보호관리체계에 관한 국제표준규격(ISO27001) 및 정보보호관리체계(ISMS)의 절차/관리/운영 사항을 연구원 정보보안관리지침에 적용하는 업무 ○ (보안사고분석대응) 연구원 사이버공격 및 침해사고의 예방활동, 위협정보를 탐지하고 분석, 피해현황 파악, 복구하는 등 신속하게 침해사고대응절차를 수행하는 업무 | | | | |
| 전형방법 | 1차 서류전형 → 2차 NCS기반역량평가 → 3차 종합면접 → 임용 | | | | |
| 일반요건 | 연령 | 무관 | | | |
| | 성별 | 무관 | | | |
| 교육요건 | 학력 | 무관 | | | |
| | 전공 | 컴퓨터공학 및 정보보호 관련 전공 | | | |

| 채용분야 (채용직종) | 기술 | NCS 분류 체계 | 대분류 | 20.정보통신 | |
|----------------|---|-----------------|-----|----------------------------|----------------------------|
| | | | 중분류 | 01.정보기술 | |
| | | | 소분류 | 02.정보기술개발 | 06.정보보호 |
| | | | 세분류 | 05. NW엔지니어링 06. 보안엔지니어링 | 02.정보보호진단분석 03.보안사고분석대응 |
| 필요지식 (K) | <ul style="list-style-type: none"> ○ (NW엔지니어링) 인터넷 프로토콜 모델, IP주소체계, 통신방식, 프로토콜 패킷 형식, 네트워크 패킷 송수신/흐름도/헤더 포맷, 유무선 네트워크 연결 구조, 네트워크 구성요소별 자원 측정 지표/절차/설정 ○ (보안엔지니어링) 정보보호관리체계에 관한 국제표준 규격(ISO27001), 정보보호관리체계(ISMS), 개인정보보호관리체계(PIMS), 서비스 공격유형, 시스템 아키텍처, 암호 알고리즘, 접근통제, 식별 및 인증, 보안 솔루션 종류 및 유형별 제공 기능, 네트워크 기반 공격 유형 및 QoS ○ (정보보호진단분석) 정보시스템 운영 정책, 위험평가 방법론, 취약점 분석평가 기준, 취약점 진단, 모의해킹 유형 관련 지식, 스크립트 코딩 관련 지식 ○ (보안사고분석대응) 침입대응, 분석 실무에 필요한 정보수집 및 활용 방법, 침해사고 대응절차, 원인과 사고과정 분석에 관한 지식, 보안위협 이벤트/원리이론 분석, 침해사고 관련 휘발성, 비휘발성 증거수집 방법, 네트워크와 시스템 취약점 관련 지식 | | | | |
| 필요기술 (S) | <ul style="list-style-type: none"> ○ (NW엔지니어링) 네트워크 제품/장비 활용 기술, SNMP 프로토콜 및 MIB 활용 기술, 네트워크 패킷 분석 툴 활용 기술, Raw 패킷 분석 능력, 네트워크 패킷 에러 발생 원인 분석 능력 ○ (보안엔지니어링) 시스템/네트워크 취약점 분석 툴 사용 기술, 로그 분석 도구 사용 기술, 서버 보안 소프트웨어 설치 및 운영기술, 보안 아키텍처 수립 기술, 운영체제의 환경 설정 기술 ○ (정보보호진단분석) DBMS, 네트워크 장비, 보안시스템, 서버(Unix, Linux, Windows) 운영 능력, 정보시스템별 스크립트 활용 능력, 취약점 판단 능력 ○ (보안사고분석대응) 침해사고 분석 기술(분석도구, 원인, 사고과정 분석 등), 네트워크 시스템 로그/보안취약점/분석 도구 사용 기술, 악성코드 행위 분석 기술, RootKit/악성코드 동작방식에 대한 지식, 파일/프로세스/리지스트리 구조/동작방식에 대한 지식 | | | | |
| 직무수행태도 (A) | <ul style="list-style-type: none"> ○ (공통) 객관적인 판단 및 논리적인 분석 태도, 투명하고 공정한 업무수행의 청렴성, 문제해결에 적극적인 의지, 창의적인 사고 노력, 의사결정 판단 자세, 주인의식 및 책임감 있는 태도, 경영자원 절약 자세, 수용적 의지 및 관찰 태도, 다양한 정보수집을 하려는 태도, 고객 지향적인 사고, 데이터 특성 및 분석 기술, 업무규정 준수, 상호업무협조 노력, 안전수칙 준수, 상황 판단력과 관찰력이 있는 자세 등 ○ (정보기술개발 및 정보보호) 정보보안 정책 및 운영에 대한 이해력을 바탕으로 효율적이고 안정적인 연구원 네트워크/업무시스템 운영관리를 수행할 수 있는 적극적이고 근면한 자세 | | | | |
| 필요자격 | ○ 정보보안 관련 자격증 우대(CISSP, CISA, 정보보안기사/기능사, CPPG 등) | | | | |
| 직업기초능력 | ○ 의사소통능력, 조직이해능력, 수리능력, 문제해결능력, 자기개발능력, 자원관리능력, 정보능력, 대인관계능력, 기술능력, 직업윤리 | | | | |
| 참고사이트 | ○ www.kigam.re.kr 및 www.ncs.go.kr 참조 | | | | |

* 2,3차 전형시에는 상기 직무의 필요지식, 필요기술, 직무수행능력태도에 대하여 평가 예정

* 상기 직무는 지원자가 입사 시 수행할 대표 직무이며, 입사 후 대표 직무 외에 다른 직무도 수행할 수 있음