

## 【NCS기반 채용 직무기술서 : 정보보안】

채용분야	분류 체계	대분류	중분류	소분류	세분류
		20. 정보통신	01. 정보기술	02. 정보기술개발  06. 정보보호	06. 보안엔지니어링  03. 보안사고분석대응  *정보보호관리, 운영
능력단위	<b>(보안엔지니어링)</b> 02. 보안위험 평가 <b>(보안사고분석대응)</b> 05. 침해사고분석, 07. 보안로그 분석, 08. 보안이벤트 대응, *주요정보통신기반시설 취약점 분석, 평가, * EMS 취약점 점검 및 개선 <b>(정보보호관리, 운영)</b> CBP 취약점 점검 및 개선, 침해사고 대응관리, 침해사고 분석 및 대응, 보안관제망 정보보안 설비 구출 및 운영관리, 보안관제센터 위탁사업 관리, 웹페이지 자체 취약점 진단 및 개선, EMS 보안설비 운영 및 유지관리, CBP 보안 설비 운영 및 유지관리, OA 보안설비 운영 및 관리				
직무수행 내용	<b>(보안엔지니어링)</b> 보호하여야 할 자산을 식별, 분석하고 내재된 취약성을 도출하여 자산에 대한 위협의 종류와 영향을 분석, 평가함으로써 위협의 정도를 산정하는 일이다. <b>(보안사고분석대응)</b> 침해사고의 피해확산 방지를 위해 위협정보를 탐지하고, 시스템 복구와 예방 전략을 수립하는 일과 정보보호 침해사고를 분석하여 신속하게 대응하는 일이다. <b>(정보보호관리, 운영)</b> 정보보안 침해사고 및 사이버테러 발생 방지를 위한 정보보호 관련 기술적·물리적·관리적 조치를 하는 일이다.				
필요지식	<ul style="list-style-type: none"> <li>• 정보자산의 분류 정책에 대한 지식</li> <li>• 정보자산의 분류 표준, 지침, 절차에 대한 지식</li> <li>• 정보자산 평가방법(정량적 평가기준, 정성적 평가기준)과 관련된 지식</li> <li>• 정보자산 가치평가 기준(자산평가 기준표)과 관련된 지식</li> <li>• 정보보호 관련 수칙에 대한 지식</li> <li>• 노출계수(EF, Exposure Factor)에 대한 지식</li> <li>• 단일손실예상(SLE, Single Loss Expectancy)에 대한 지식</li> <li>• 연간발생빈도(ARO, Annualized Rate of Occurrence)에 대한 지식</li> <li>• 연간손실예상(ALE, Annual Loss Expectancy)에 대한 지식</li> <li>• 국내 정보보호 관련 법과 규정에서 정의된 보호조치 기준에 관한 지식</li> <li>• 침해사고 대응절차에 관한 지식</li> <li>• 침해사고 원인과 사고과정 분석 지침에 관한 지식</li> <li>• 네트워크와 시스템 취약점관련 지식</li> <li>• 보안시스템 별 탐지정책 및 이벤트 동작 메커니즘 관련 지식</li> <li>• 사이버 공격에 대한 이해 및 공격유형별 개념에 대한 지식</li> </ul>				
필요기술	<ul style="list-style-type: none"> <li>• 정보보호 아키텍처 분석 능력</li> <li>• 정보자산관리 도구 사용 기술</li> <li>• 정보보호 IT기술</li> <li>• 정보보호 위험분석 능력</li> <li>• 최신 침해사고 사례를 통한 침해대응 분석 기술</li> <li>• 침해사고 분석 도구 사용 기술</li> <li>• 침해사고 원인과 사고과정 분석 기술</li> <li>• 네트워크와 시스템 취약점 점검 기술</li> <li>• 보안시스템 정책 및 검색에 대한 활용기술</li> <li>• 보안시스템별 이벤트에 대한 분석 및 상세분석을 위한 조작 능력</li> <li>• 보안시스템에 대한 현황파악 및 분석능력</li> <li>• 취약점에 대한 로그 분석 도구 사용 기술</li> </ul>				

<b>직무수행 태도</b>	<ul style="list-style-type: none"> <li>• 조직의 보안시스템 구성과 현황을 지속적으로 숙지하려는 노력</li> <li>• 관련 이해당사자와의 협업을 위한 개방적 태도</li> <li>• 정보보안에 대한 논리적이고 객관적인 사고</li> <li>• 정의된 평가기준과 절차의 준수</li> <li>• 취약점과 위험요소의 누락을 방지하기 위한 적극적 노력</li> <li>• 최신 침해사고 동향을 파악하고 트렌드를 이해하려는 노력</li> <li>• 침해사고의 근본 원인을 파악하려는 노력</li> <li>• 보안위협 재발방지를 위해 철저히 대비하려는 의지</li> <li>• 보안위협의 효과적 대응을 목표로 전체 보안시스템을 효과적으로 사용하는 노력</li> <li>• 분석한 보안위협에 대해 신속하게 보고하고 대응하는 절차 준수</li> <li>• 모든 활동에 보안요구사항 준수</li> <li>• 신규 보안취약점 및 대응 방법에 대해 지속적으로 연구하는 노력</li> <li>• 분석을 위해 해당 로그만이 아닌 관련성을 찾을 수 있는 넓은 시야</li> </ul>
<b>직업 기초능력</b>	<ul style="list-style-type: none"> <li>• 의사소통능력, 수리능력, 문제해결능력, 자원관리능력, 조직이해능력, 직업윤리</li> </ul>
<b>관련 자격증</b>	<ul style="list-style-type: none"> <li>• 정보보안기사, CISSP, CISA, CEH, SIS</li> </ul>
<b>참고 사이트</b>	<p>NCS 홈페이지 : <a href="https://www.ncs.go.kr">https://www.ncs.go.kr</a></p> <p>전력거래소 홈페이지 : <a href="http://www.kpx.or.kr">www.kpx.or.kr</a></p>

\* 미개발된 NCS 분류체계로 인하여 세분류 ‘정보보호관리, 운영’은 자체개발하였음.

\* 미개발된 NCS 분류체계로 인하여 능력단위 ‘주요정보통신기반시설 취약점 분석, 평가’, ‘EMS 취약점 점검 및 개선’은 자체개발하였음.