Seguridad para IS

La ciberseguridad o seguridad informática es definida como la práctica de proteger los sistemas más importantes y la información confidencial ante ataques digitales. Se trata uno de los campos en los que un ingeniero en software se puede desempeñar y por ende, podemos asumir que debemos saber todo lo que consideramos como el “tronco” general de la ingeniería en software en el caso de los conocimientos, competencias y habilidades. Pero a esto se pueden añadir algunos puntos específicos de este campo y que es mejor reforzar si se planea entrar a esta área.

- **Conocimientos**

  Estos se pueden resumir en terminología y tecnología básica del ámbito (firewalls, IDS/IPS, SIEM, DLP, VPNS, etc.), Análisis de malware y ciberdelitos, gestión de incidentes, metodologías de ciberseguridad, bases de datos y lenguajes de programación (Siendo Python, Powershell scripting, y Bash scripting).

  Usualmente se requieren certificaciones o estudios de mayor grado para poder entrar al ámbito sin problemas, por lo que hay ser consiente de que conocimientos faltan, cuales se pueden desarrollar y como.

- **Habilidades**

  La autonomía, adaptabilidad, iniciativa, trabajo en equipo, autodidáctica y habilidades para investigación son las habilidades esenciales. A pesar de que en el entorno estudiantil se pueden llegar a promover estas habilidades, depende de uno mismo saber qué hace falta para dominarlas totalmente.

- **Competencias**

  Comprensión de criptografías y hacking ético, análisis y detección de técnicas de ocultación de ataques a sistemas y redes, conocimientos de tendencias de ciberataques, etc. Son solo algunas de las competencias especificas que uno debe disponer en ciberseguridad, se podría decir que giran entorno al conocimiento, análisis, comprensión y aplicación de conocimientos tanto generales como específicos al campo.