Veamos un modelo jerárquico que contempla las bases de la Seguridad de la información, mediante seis capas. Analicemos el esquema de arriba a abajo.
En capa 6, se han enumerado varias de las aplicaciones seguras más populares actualmente: el correo electrónico seguro, dinero digital, comercio electrónico, votaciones electrónicas etc. Estas aplicaciones solo están disponibles si anteriormente de han puesto en marcha los protocolos de autenticación segura como SSL/TLS, IPSec, IEEE 802.11, etc. Todos ellos implementados la capa 5. Sin embargo, estos protocolos se nutren de la capa 4, que consiste en los servicios de seguridad habituales tales como: autenticación, integridad, no repudio y confidencialidad. Estos servicios de seguridad están respaldados por los dos pares de primitivas criptográficas representadas en la capa 3, a saber, cifrado/descifrado, firma digital/verificación. Ambos pares de primitivas criptográficas pueden ser implementadas mediante la combinación de los algoritmos de clave pública y clave privada, como los listados en la capa 2. Finalmente, para obtener un alto rendimiento de los algoritmos criptográficos, la capa 1 es indispensable ya que es necesario que la implementación de las operaciones aritméticas tales como, suma, resta, multiplicación, exponenciación, etc., sea eficiente.

Por estas razones hemos intentado que la asignatura que nos ocupa sea comprendida desde sus bases.