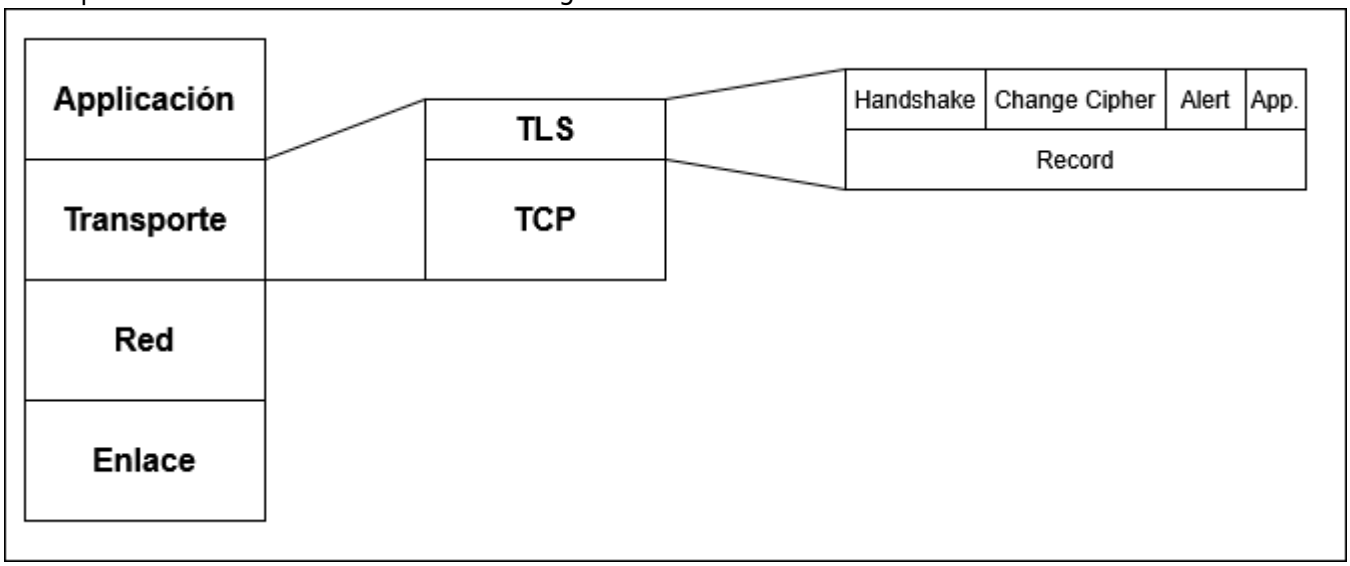
Seguridad a nivel de transporte [L4]

TLS (Transport Layer Security)

Es una evolución de SSL (Secure Socket Layer) para proveer comunicaciones seguras a través de infraestuctura insegura. Provee un canal seguro a un servicio arbitrario de internet. Garantiza autenticación, confidencialidad e integridad, tiene los siguientes objetivos:

- Seguridad Criptográfica
- Interoperabilidad
- Extensibildiad
- Eficiencia

La arquitectura de TLS en internet es la siguiente:



Competidores de TLS

- SSH (Secure Shell)
  - También en capa de aplicación
  - Usa cifrado de clave pública para la autenticación pero también puede usar contraseñas
  - Confiada basada en hosts conocidos e intercambio de claves en vez de PKI
  - Se suele usar para acceso remoto a servidores, transferencia de archivos o tunelado de otros protocolos.
- PGP(Pretty Good Privacy):
  - Confianza de web descentralizada en vez de usar PKI jerárquico.
  - Se suele usar para email, archivos y verificación de paquetes de software.

Protocolo TSL (1.2 y 1.3)

Transporta y, opcionalmente, cifra cada mensaje TLS entre 2 aplicaciones.