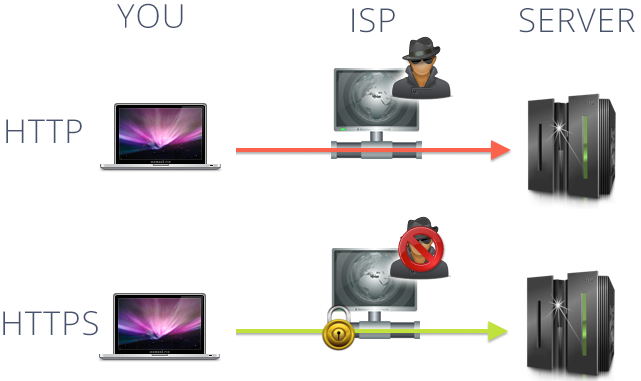
HTTPS

HTTPS (HyperText Transfer Protocol Secure, protocolo seguro de transferencia de hipertexto) es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio. Para esto se utilizan los certificados SSL/TLS

El certificado SSL/TLS proporciona tres capas de seguridad principales:

1. **Cifrado:** se cifran los datos intercambiados para mantenerlos a salvo de miradas indiscretas. Eso significa que, cuando un usuario está navegando por un sitio web, nadie puede "escuchar" sus conversaciones, hacer un seguimiento de sus actividades por las diferentes páginas ni robarle información.
2. **Integridad de los datos:** los datos no pueden modificarse ni dañarse durante las transferencias, ni de forma intencionada ni de otros modos, sin que esto se detecte.
3. **Autenticación:** demuestra que tus usuarios se comunican con el sitio web previsto. Proporciona protección frente a los ataques de intermediario y fomenta la confianza de los usuarios, lo que acaba creando otros beneficios empresariales



El proceso es el siguiente:

* El navegador intenta conectarse a un sitio protegido con SSL/TLS
* El navegador solicita que el servidor web se identifique
* El servidor envía una copia de su certificado SSL/TLS al navegador
* El navegador comprueba si el certificado SSL/TLS es de confianza. Si es así, envía un mensaje al servidor
* El servidor devuelve un acuse de recibo firmado digitalmente para comenzar una sesión SSL/TLS cifrada
* Los datos cifrados se comparten entre el navegador y el servidor (al URL del navegador se le añade un candado cerrado)

Si pulsamos sobre el candado, podemos comprobar la entidad que ha emitido dicho certificado, para quien ha sido emitido y el periodo de validez

Fuentes:

https://developers.google.com/search/docs/advanced/security/https?hl=es

<https://introbay.com/blog/https-que-es-y-para-que-sirve>

<https://youtu.be/6HJAWFenYx8?t=168>