**1) Protocolo HTTP y HTTPS. Indicar las diferencias.**

**HTTP:** es un protocolo de transferencia de hipertexto, permitiendo así la transferencia de información en Internet, mediante documentos HTML.

**HTTPS:** es el protocolo de cifrado en internet, centrado en la seguridad y que usa una combinación de los protocolo HTTP y SSL/TLS, que hace que cualquier tipo de información que se transmita sea cifrada, mediante un certificado SSL.

**Las diferencias:**

- **Seguridad:** la principal diferencia es la seguridad, HTTPS es segura, y HTTP no, haciendo que la información sea interceptable.
- **Puertos:** HTTP hace uso del puerto 80, y HTTPS usa el 443.
- **Visibilidad en la web:** cuando un navegador detecte que una página no use HTTPS, avisará y lo mostrará indicando que no es segura, al contrario de HTTPS, que mostrará la seguridad con un candado.

https://es.godaddy.com/blog/diferencia-entre-http-y-https/
https://www.codedonostia.com/diferencias-entre-http-y-https/

**2) Mime y sus tipos.**

Mime es el acrónimo de Multipurpose Internet Mail Extensions, son un conjunto de especificaciones orientadas hacia el intercambio de cualquier tipo de archivo en internet.

**Sus características principales son:**

- Transferencia de texto en distintos idiomas, soportando así caracteres que no pertenezcan a US-ASCII.
- Enviar información adjuntada que no sea de tipo texto.
- Enviar correos con cuerpo dividido en múltiples partes.
- La información del encabezado del mensaje no está conformada por caracteres solamente ASCII.

**Sus tipos de datos son:**

- **text**
- **message:** este tipo encapsula en un mensaje contenido de otro. Admite subtipos como partial y rfc822 entre otros.
- **multipart:** Informa que el texto está conformado por varias partes independientes.
- **audio**
- **video**
- **image**
- **application**

https://es.wikipedia.org/wiki/Multipurpose_Internet_Mail_Extensions
https://lovtechnology.com/que-es-mime-y-para-que-se-emplea/

**3) Autenticación y control de acceso.**

El control de acceso y autenticación comprueba que los usuarios sean quienes son. De esta forma haces que los usuarios tengan el acceso a los datos y recursos de sistema que les correspondan.

**Tipos de control de acceso:**

- **Control de Acceso basado en Roles**
- **Control de Acceso Discrecional**
- **Control de Acceso Obligatorio**
- **Control de Acceso basado en Atributos**

https://www.redeszone.net/tutoriales/seguridad/control-de-acceso-que-es/
https://www.grupospec.com/es/blog/111-autenticacion-control-acceso

**4) Encriptación simétrica y asimétrica.**

**La encriptación simétrica** es el método que emplea la misma clave tanto para el cifrado como el descifrado de un mensaje. Por lo que el emisor y el receptor deben estar previamente de acuerdo y en conocimiento de la clave a utilizar.

**La encriptación asimétrica** es el proceso mediante el cual se usan un par de claves, una clave pública y otra privada, para cifrar y descifrar un mensaje, y protegerlo de accesos o usos no autorizados.

https://academy.bit2me.com/que-es-criptografia-simetrica/
https://www.gb-advisors.com/es/encriptacion-simetrica-y-asimetrica-conoce-sus-diferencias/

**5) Autoridad de certificación (AC)**

Una Autoridad de Certificación (AC, en inglés CA) es una entidad de confianza del emisor y del receptor del mensaje. Esto permite que cualquiera de los dos confíe a su vez en los documentos firmados por la Autoridad de Certificación, en particular, en los documentos que identifican cada clave pública con su propietario correspondiente y se denominan certificados.

https://www.dnielectronico.es/portaldnie/PRF1_Cons02.action?pag=REF_076&id_menu=6
https://www.sepe.es/HomeSepe/empresas/servicios-para-empresas/certificados/certificados-certificacion.html

**6) Infraestructura de Claves Públicas (ICP / PKI)**

La Public Key Infrastructure, por sus siglas en inglés, son un grupo de componentes y servicios informáticos que permiten gestionar, controlar y administrar la tarea de generar, brindar, revocar y validar toda clase de certificados digitales.

Está compuesto por:

- Certificados de clave pública
- Un repositorio de certificados
- Revocación de certificados

- Archivado y recuperación de claves
- Soporte técnico para no repudio de firmas digitales
- Actualización automática de pares de clave y certificados
- Gestión del historial de claves
- Soporte técnico para certificación cruzada
- Software cliente que interactúa de forma segura, sistemática y fiable con todo lo anterior.

https://www.docusign.mx/blog/pki
https://www.entrust.com/es/resources/certificate-solutions/learn/what-is-pki

**7) ACL o listas de control de acceso.**

El control del acceso se compone de recursos de información protegidos que especifican a quién puede otorgarse acceso para tales recursos.

**Un ACL puede realizar distintas tareas:**

Limitan el tráfico de la red para aumentar su rendimiento. Por ejemplo, si la política corporativa no permite el tráfico de video en la red, se pueden configurar y aplicar ACL que bloqueen el tráfico de video. Esto reduciría considerablemente la carga de la red y aumentaría su rendimiento.

Proporcionan control del flujo de tráfico. Las ACL pueden restringir la entrega de actualizaciones de routing para asegurar que las actualizaciones provienen de un origen conocido.

Proporcionan un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro host acceda a la misma área.

Filtran el tráfico según el tipo de tráfico. Por ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de Telnet.

Filtran a los hosts para permitirles o denegarles el acceso a los servicios de red. Las ACL pueden permitirles o denegarles a los usuarios el acceso a determinados tipos de archivos, como FTP o HTTP.

https://www.ibm.com/docs/es/ssw_aix_72/osmanagement/acl.htm
https://ccnadesdecero.es/listas-control-acceso-acl-router-cisco/

**8) Certificado digital**

Un Certificado Electrónico (o certificado digital) es un fichero digital emitido por una tercera parte de confianza (una Autoridad de Certificación) que garantiza la vinculación entre la identidad de una persona o entidad y su clave pública, por tanto, permite identificar a su titular de forma inequívoca.

**Un certificado cuenta con la siguiente información:**

- Identificación del titular del certificado: Nombre, dirección, etc.
- Clave pública del titular del certificado.
- Fecha de validez.

- Número de serie.
- Identificación del emisor del certificado.

https://www.aepd.es/es/preguntas-frecuentes/12-sede-electronica/FAQ-1205-que-es-un-certificado-electronico
https://www.xataka.com/basics/certificado-digital-que-que-tipos-hay-como-solicitarlo-activarlo

**9) Firma electrónica**

La firma electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

- Identificar al firmante de manera inequívoca
- Asegurar la integridad del documento firmado. Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación
- Asegurar el no repudio del documento firmado. Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento

https://www.docusign.com.es/blog/que-es-la-firma-electronica
https://firmaelectronica.gob.es/Home/Ciudadanos/Firma-Electronica.html

**10) Certificado SSL**

Un certificado SSL es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer (Capa de sockets seguros), un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.
Un certificado SSL contiene la siguiente información:

- El nombre del titular del certificado
- El número de serie del certificado y la fecha de vencimiento
- Una copia de la clave pública del titular del certificado
- La firma digital de la autoridad que emite el certificado

https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate
https://es.godaddy.com/help/que-es-un-certificado-ssl-542