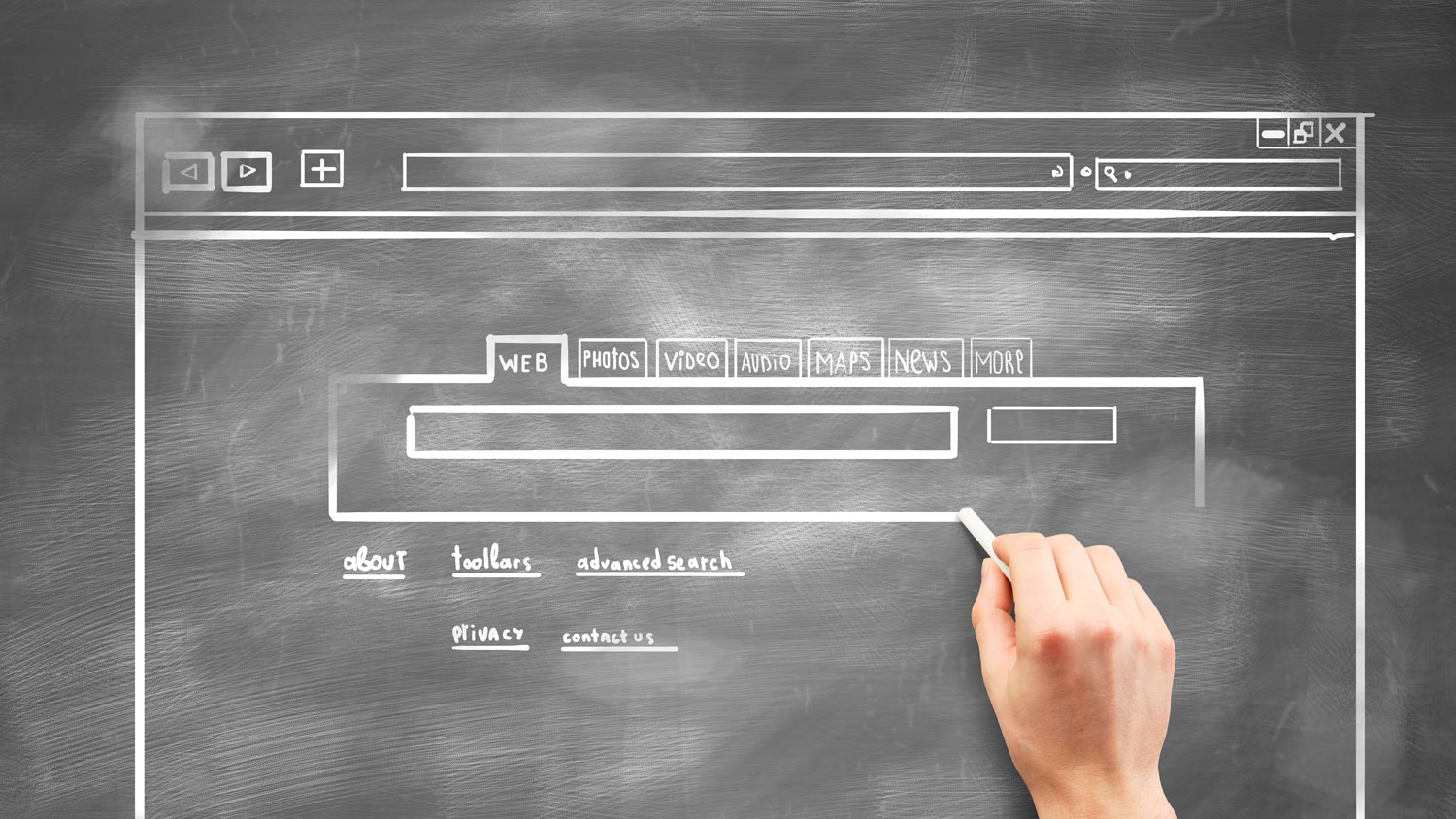
# 5.5 Plataformas Tecnológicas

El ciberespacio, compuesto por millones de sitios web en todo el mundo, existe gracias a una serie de plataformas tecnológicas complementarias.



**Arquitectura de la información web:** es la disciplina encargada de la organización y estructuración de la información en los *websites*.

**Servidor web:** es un programa diseñado para transferir hipertextos, páginas web o páginas HTML (HyperText Markup Language). Estos son textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores musicales. El programa implementa el protocolo HTTP (HyperText Transfer Protocol) que pertenece a la capa de aplicación del modelo OSI. Ejecutado en un ordenador, el servidor web se mantiene a la espera de peticiones por parte de un navegador web y responde a estas peticiones adecuadamente, mediante una página web que se exhibirá en el navegador o mostrando un mensaje si se detectó algún error.

A manera de ejemplo, si escribimos www.google.com en nuestro navegador, éste hará una petición HTTP al servidor de dicha dirección. Acto seguido, el servidor responderá al cliente enviando el código HTML de la página. Luego el cliente recibe el código, lo interpreta y lo exhibe en pantalla. La interpretación del código HTML consiste en mostrar las fuentes, los colores y la disposición de los textos y objetos de la página. Por su parte, el servidor se limita a transferir el código de la página sin realizar interpretación alguna.

**Servicio DNS:** en castellano se denomina sistema de nombres de dominio. Se trata de un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a internet o a una red privada. Asocia información variada con nombres de dominios asignados a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, con la finalidad de localizar y direccionar estos equipos mundialmente. Otra función clave de los protocolos DNS es la asignación de nombres a direcciones IP. Cada sitio web cuenta con una dirección IP, pero para tener acceso a ellas no digitamos dichas direcciones sino su nombre precedido de www y con una terminación como .org, .com, etc. La mayoría de usuarios acceden a los sitios web empleando estos nombres y no las direcciones IP.

**Sistemas operativos:** quizá es el programa más complejo e importante para una computadora. El sistema operativo "despierta" a la PC y le hace reconocer al CPU, la memoria, el teclado, el sistema de vídeo, la impresora y las unidades de disco. También facilita la comunicación para que los usuarios se comuniquen con la computadora y sirve de plataforma a partir de la cual se corran programas de aplicación.

*Los sistemas operativos más conocidos son: DOS, Windows 3.1, OS/2, Mac OS y UNIX.*

**Sistema gestor de la base de datos:** es un conjunto de programas no visibles por el usuario final que se encargan de la privacidad, integridad y seguridad de los datos, así como de la interacción con el sistema operativo. Permite la interfaz entre los datos, los programas que los manejan y los usuarios finales.

**Navegadores web:** son softwares elaborados para la búsqueda de páginas web y mostrar en pantalla la lista de opciones de búsqueda. Las búsquedas abarcan textos y gráficos. Los principales navegadores son: Google Chrome, Mozilla firefox, Opera, Avanti browser, Internet Explorer, Netscape y Safari.

# 5.6 Seguridad E Interoperabilidad.

La característica principal de un Servicio Web es que le permite cierto grado de **flexibilidad**, **accesibilidad** y**interoperabilidad**. Esto permite que los desarrolladores abstraigan la lógica de negocio y se centren en el desarrollo del servicio sin preocuparse de los criterios anteriormente citados.

Como objetivos básicos a cubrir por la seguridad de un servicio WEB

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) define interoperabilidad como la habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada.

La característica principal de un Servicio Web es que le permite cierto grado de flexibilidad, accesibilidad y interoperabilidad. Esto permite que los desarrolladores abstraigan la lógica de negocio y se centren en el desarrollo del servicio sin preocuparse de los criterios anteriormente citados.

Como objetivos básicos a cubrir por la seguridad de un servicio WEB

* Es necesario asegurar que existe una autenticación mutua entre el cliente que accede a los servicios web y el proveedor de dichos servicios.
* Se debe mantener una política de autorización del acceso a recursos y, más importante, a operaciones y procesos en un entorno en el que debe administrarse y controlarse el acceso de clientes, proveedores, vendedores, competidores y los posibles ataques que reciban de personal externo.
* Mantener al cliente identificado, de manera que se identifique una sola vez y pueda acceder a servicios en diversos sistemas, sin que resulte necesario identificarse nuevamente en cada uno de ellos.
* Controlar y asegurar la confidencialidad de los datos intercambiados, ya que SOAP no es capaz de cifrar la información, la cual viaja en claro a través de la red.Es necesario asegurar la comunicación con algún estándar que permita crear un canal seguro de comunicación. El estándar ya firmemente establecido de creación de canales seguros SSL y el cifrado de partes específicas de documentos mediante el cifrado XML son las direcciones que se están siguiendo en este terreno.
* Se debe asegurar la integridad de los datos, de manera que estén protegidos a los posibles ataques o a manipulaciones fortuitas. En este campo se está utilizando el estándar de firmas XMLDSIG, que permiten la firma de partes específicas del documento XML.
* Comprobar que no se repudian las operaciones, para lo cual es necesario mantener firmas en XML.

Los protocolos de seguridad para servicios web comienzan por la especificación WS-Security que define una arquitectura basada en señales para comunicaciones seguras. Existen seis principales especificaciones de componentes construidas sobre esa base:

* **WS-Policy** y sus especificaciones relacionadas, que definen las reglas de políticas sobre la interacción de servicios.
* **WS-Trust**, que define el modelo confiable para el intercambio seguro.
* **WS-Privacy**, que define cómo se mantiene la privacidad de las informaciones.
* **WS-Secure Conversation**, que define cómo establecer una sesión protegida entre servicios para intercambiar datos usando las reglas definidas en WS-Policy, WS-Trust, y WS-Privacy.
* **WS-Federation**, que define las reglas de identidad distribuida y de la gestión de esa identidad.
* **WS-Authorization**, que maneja el procesamiento de autorización para acceder a los datos e intercambiarlos.

Además del modelo de seguridad, existen las especificaciones específicas de las aplicaciones, incluyendo el lenguaje de ejecución de procesos empresariales para servicios web (BPEL4WS), que define las operaciones de flujos de trabajo, y WS-Transaction y WS-Coordination, que funcionan en conjunto para manejar el procesamiento distribuido de transacciones.

Actualmente está en desarrollo una especificación para la gestión distribuida de servicios web que trata de la gestión administrativa de software de todos los servicios y de la arquitectura orientada a servicios. Por fin, existen especificaciones para interfaces de usuario (WS-InteractiveApplications) y acceso remoto a servicios web (*WS-RemotePortals*).

Las especificaciones y protocolos para servicios web aún están siendo definidas y sólo están comenzando a explicar cómo los servicios deben interactuar. Sin embargo, no pueden abarcar todas las situaciones y combinaciones posibles. Así, el Web Services Interoperability Group (WS-I), constituido por prácticamente todos los grandes y pequeños proveedores involucrados en el desarrollo de los servicios web, se encargó de la tarea de desarrollar estudios de caso, ejemplos de aplicaciones, casos de ejemplo de implementación y herramientas de prueba para asegurar que esos estándares y especificaciones realmente funcionarán los unos con los otros, independientemente de las implementaciones de productos de los proveedores.

WS-I ha definido su primer Basic Profile 1.0 para servicios web y también ha lanzado sus casos de ejemplo, ejemplos de aplicaciones y herramientas de prueba para evaluar y comparar resultados de varias implementaciones de acuerdo con los casos de ejemplo.

Además de WS-I, una buena parte del trabajo de los estándares está siendo realizado por la Organización para el Avance de Estándares de Informaciones Estructuradas (OASIS), el World Wide Web Consortium (W3C) y el Grupo de Trabajo de Ingeniería de Internet (IETF).