

DESPLIEGUE WEB: CONFIGURANDO TU HOST Y SERVIDOR



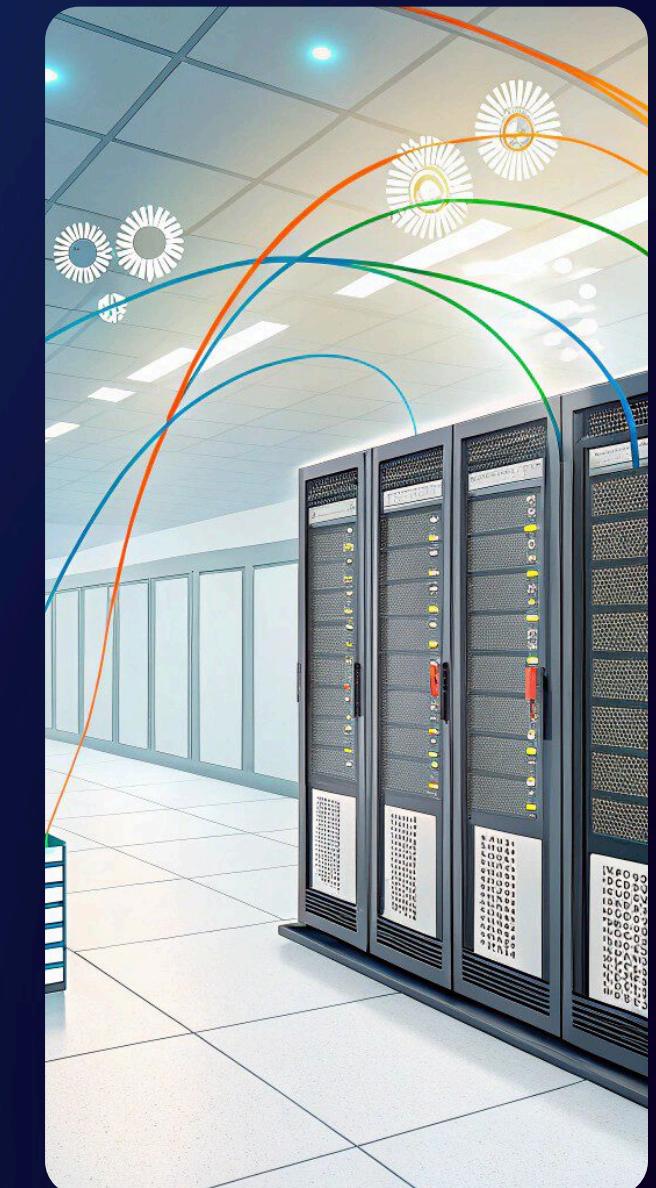


1. ¿QUÉ ES EL DESPLIEGUE WEB?

El despliegue web es el proceso de publicar una página o aplicación en internet. Consiste en trasladar los archivos desde tu computadora local a un servidor para que las personas puedan acceder a tu sitio desde cualquier parte del mundo.

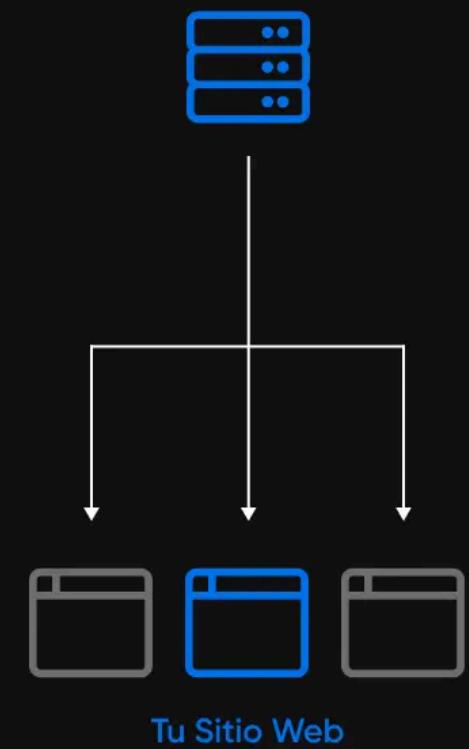
2. COMPONENTES DEL DESPLIEGUE

Para poner una web en línea se necesitan tres elementos principales:
El dominio, que es el nombre del sitio (por ejemplo, www.misitio.com).
El hosting, que es el servicio donde se guardan los archivos.
Y el servidor web, que entrega la información al navegador del usuario.

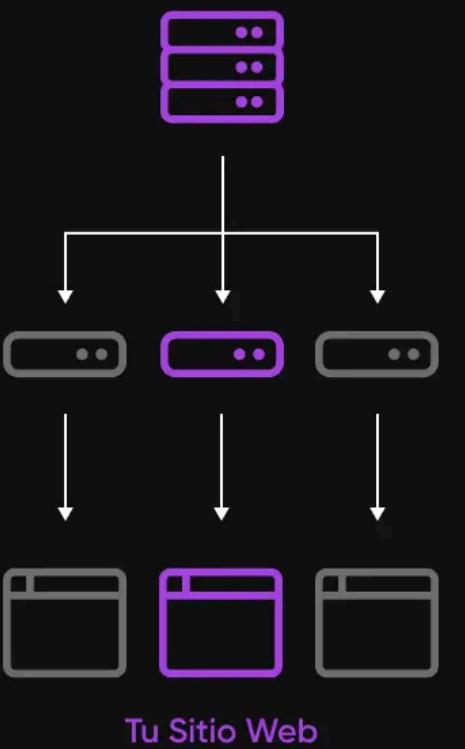


Opciones de Alojamiento: **Compartido vs. VPS vs. Dedicado**

COMPARTIDO



VPS



DEDICADO



3. TIPOS DE HOSTING

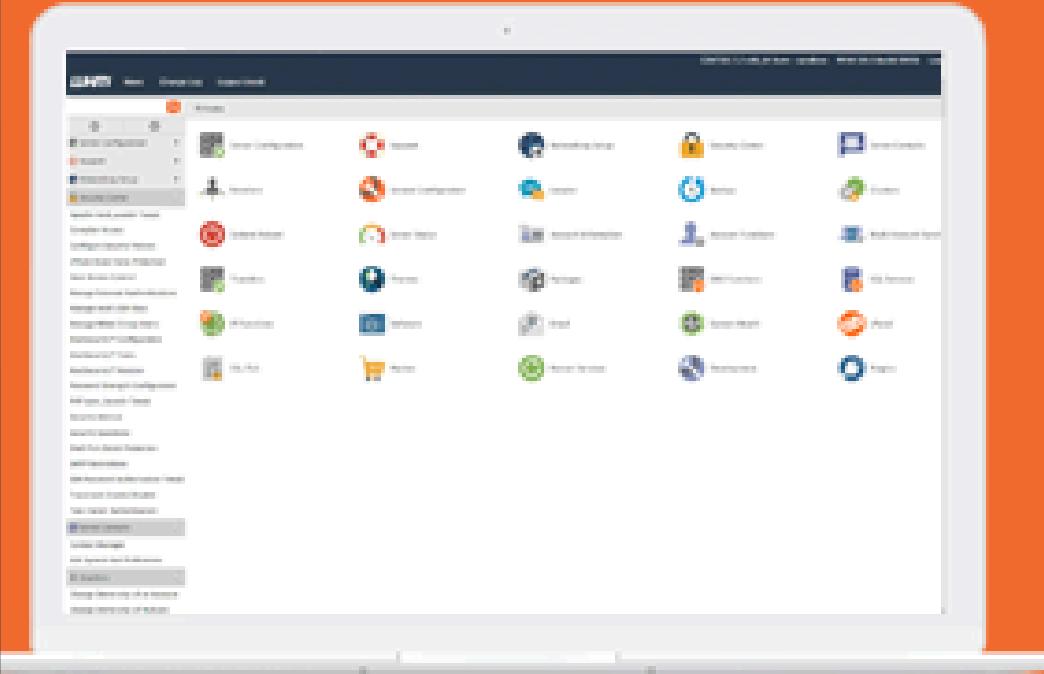
Existen varios tipos de hosting según el tamaño del proyecto.

El hosting compartido es económico y sirve para páginas pequeñas.

El VPS ofrece más control y recursos, ideal para proyectos medianos.

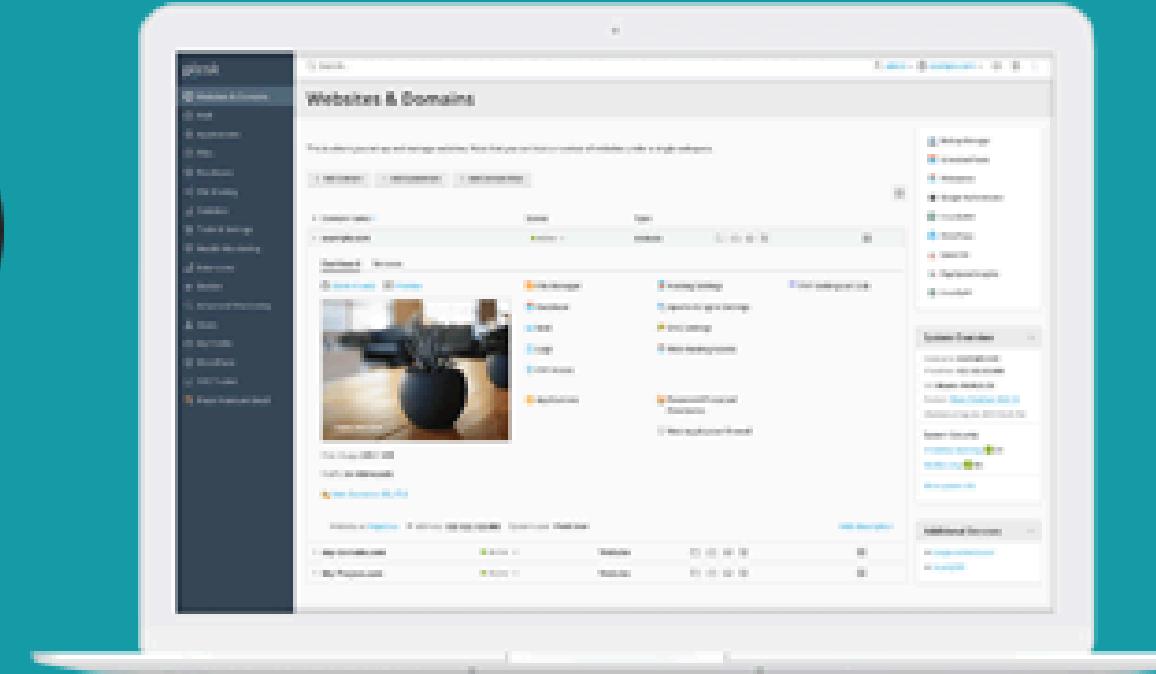
El servidor dedicado se usa en empresas grandes o sitios con mucho tráfico.

cPanel®



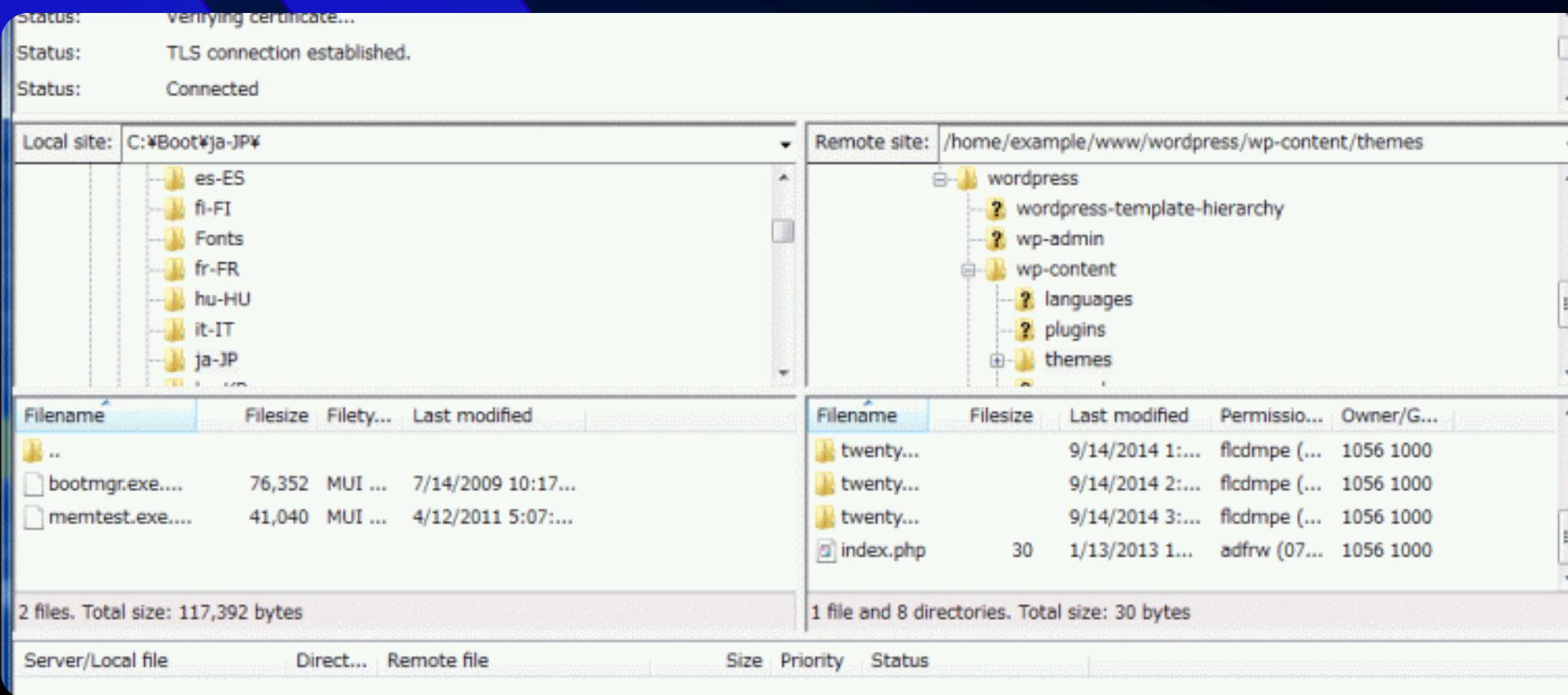
VS

plesk



4. ACCESO Y CONFIGURACIÓN DEL HOST

Al contratar un hosting, se reciben datos como usuario, contraseña y nombre del host. Con ellos puedes ingresar al panel de control, generalmente cPanel o Plesk. Desde ahí puedes gestionar archivos, bases de datos, correos y dominios. También se debe conectar el dominio al hosting usando los servidores DNS.



5. SUBIDA DE ARCHIVOS

Los archivos del sitio se pueden subir de dos maneras:

La primera es por FTP, usando programas como FileZilla para transferir los archivos al servidor.

La segunda es mediante el Administrador de Archivos dentro del panel de control, donde puedes subirlos directamente desde el navegador.

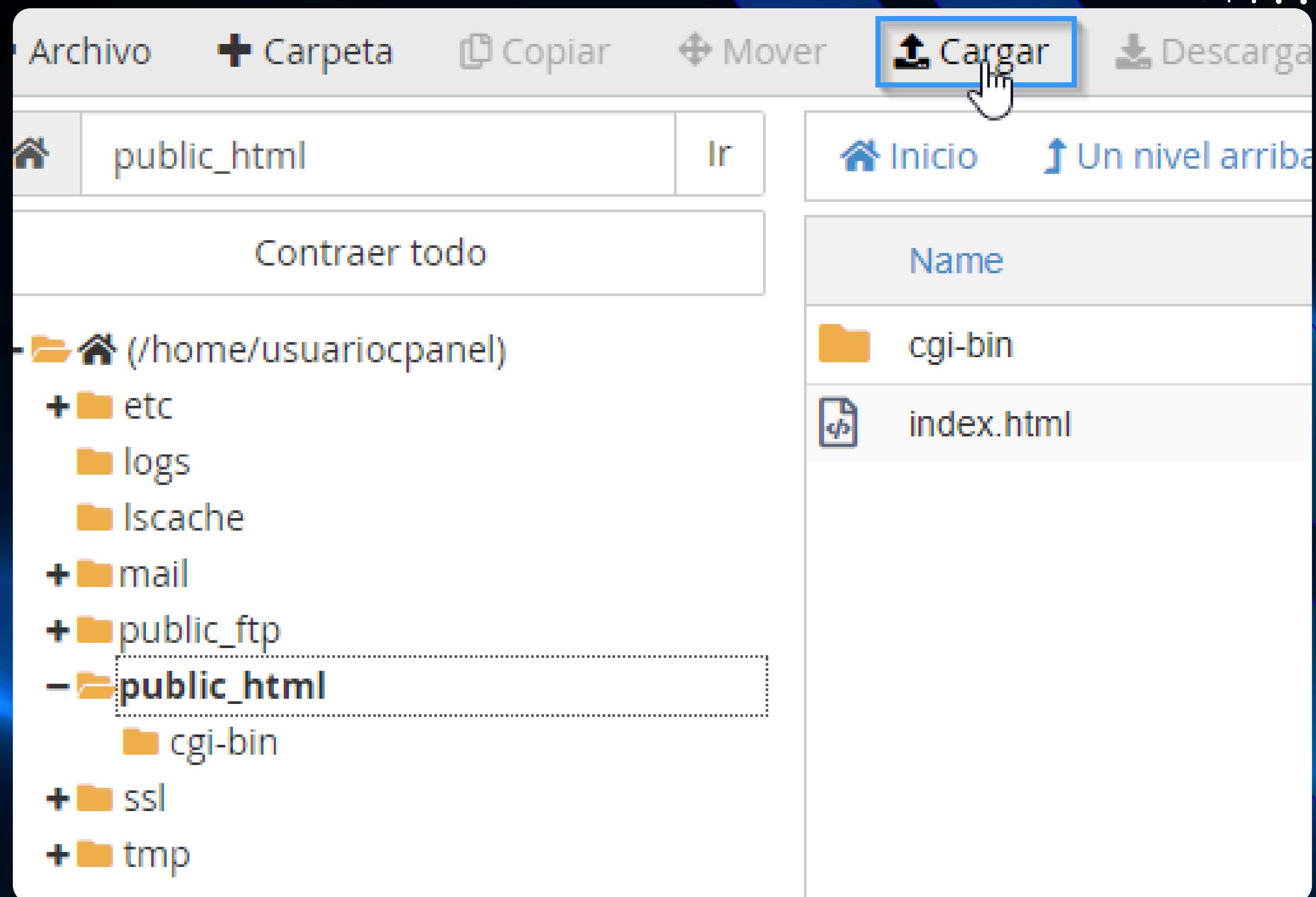
The screenshot shows the cPanel File Manager interface. The left sidebar (1) displays a tree view of the directory structure under '/home/usuariopanel', including 'etc', 'logs', 'Iscache', 'mail', 'public_ftp', 'public_html', 'ssl', and 'tmp'. The main area (2) shows a list of files with columns for Name, Size, Last Modified, Type, and Permissions. The listed files are: etc (71 bytes, httpd/unix-directory, 0750), logs (182 bytes, httpd/unix-directory, 0700), Iscache (6 bytes, httpd/unix-directory, 2770), mail (157 bytes, mail, 0751), public_ftp (22 bytes, publicftp, 0750), public_html (103 bytes, publichtml, 0750), ssl (77 bytes, httpd/unix-directory, 0755), tmp (290 bytes, httpd/unix-directory, 0755), access-logs (34 bytes, httpd/unix-directory, 0777), and www (11 bytes, publichtml, 0777).

Name	Size	Last Modified	Type	Permissions
etc	71 bytes	6 mar. 2020 17:04	httpd/unix-directory	0750
logs	182 bytes	Hoy 13:05	httpd/unix-directory	0700
Iscache	6 bytes	28 feb. 2020 18:36	httpd/unix-directory	2770
mail	157 bytes	28 feb. 2020 18:35	mail	0751
public_ftp	22 bytes	28 feb. 2020 18:35	publicftp	0750
public_html	103 bytes	Hoy 12:09	publichtml	0750
ssl	77 bytes	28 feb. 2020 18:41	httpd/unix-directory	0755
tmp	290 bytes	10 mar. 2020 13:20	httpd/unix-directory	0755
access-logs	34 bytes	28 feb. 2020 18:43	httpd/unix-directory	0777
www	11 bytes	28 feb. 2020 18:35	publichtml	0777

6. UBICACIÓN DE LOS ARCHIVOS

Los archivos del sitio deben colocarse en la carpeta principal llamada public_html o www.

El archivo principal del sitio debe llamarse index.html o index.php, ya que el servidor lo reconoce automáticamente como la página de inicio.



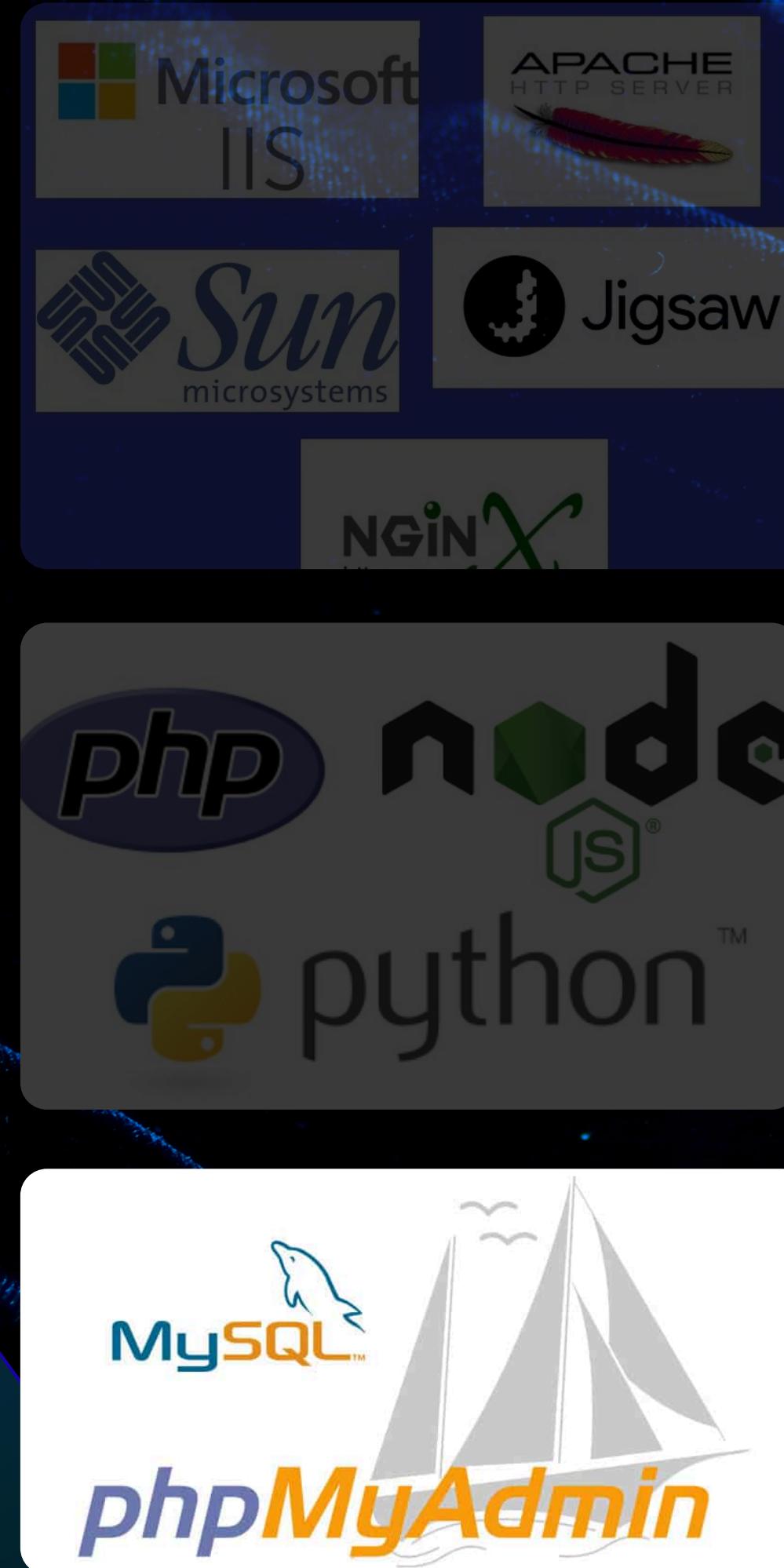
7. ESPECIFICACIONES DEL SERVIDOR WEB

Los servidores web más comunes son Apache, Nginx y IIS.

Deben estar configurados para soportar los lenguajes que use la página, como PHP, Python o Node.js.

Si el sitio usa base de datos, se configura una MySQL, que se gestiona desde phpMyAdmin.

También es importante activar un certificado SSL/TLS para usar el protocolo seguro HTTPS.



8. SEGURIDAD Y PERMISOS

Un servidor seguro protege los datos de los usuarios.

Se deben aplicar permisos correctos a los archivos y carpetas usando CHMOD (por ejemplo, 644 para archivos y 755 para carpetas).

Además, mantener el software actualizado y usar contraseñas seguras evita vulnerabilidades.

dueño

6



110

↖ ↘ ↗
r w x

grupo

4



100

↖ ↘ ↗
r w x

otros

4



100

↖ ↘ ↗
r w x