

Permisos de Usuarios

Francisco Javier Otero Herrero

Grupo ATU

10-4-2025

Permisos de Usuarios

Permisos de Usuarios

Contenido

<i>Proceso de autenticación de usuarios.....</i>	<i>3</i>
<i>Puntos Básicos de Seguridad</i>	<i>7</i>

Permisos de Usuarios

Contamos con un servidor web propio de una empresa en la que cada uno de los trabajadores tiene un usuario con los accesos permitidos a diferentes carpetas. Se va a incorporar un nuevo trabajador y es necesario prepararle un equipo con un nuevo usuario y crearle acceso a la carpeta donde accederá a los archivos con los que va a trabajar.

Proceso de autenticación de usuarios

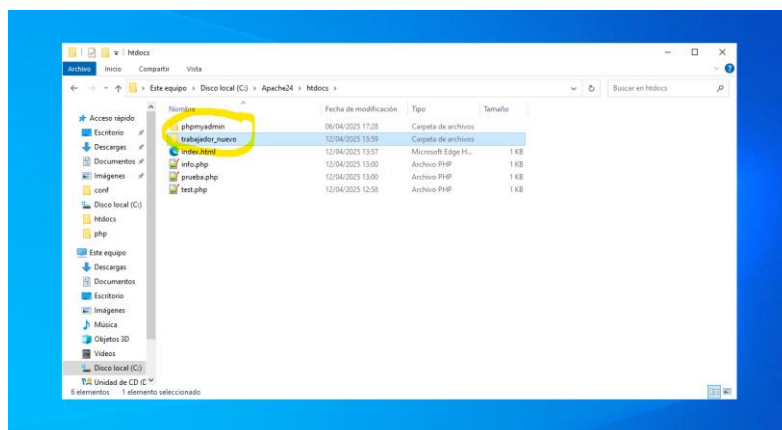
1. Explicar cómo se realiza la autenticación de usuarios y el acceso a los contenidos con servidor web Apache e indica los pasos a seguir para conceder permiso al usuario a la carpeta específica.

- Apache permite controlar el acceso a carpetas o archivos mediante:
 - Autenticación básica (Basic Authentication) con `.htaccess` y `.htpasswd`.
 - Control de permisos por IP, grupos, usuarios, etc.
 - En Windows también se pueden usar permisos del sistema de archivos (NTFS) como extra.

Lo más habitual es usar archivos `.htaccess` junto con un archivo `.htpasswd` que contiene las credenciales.

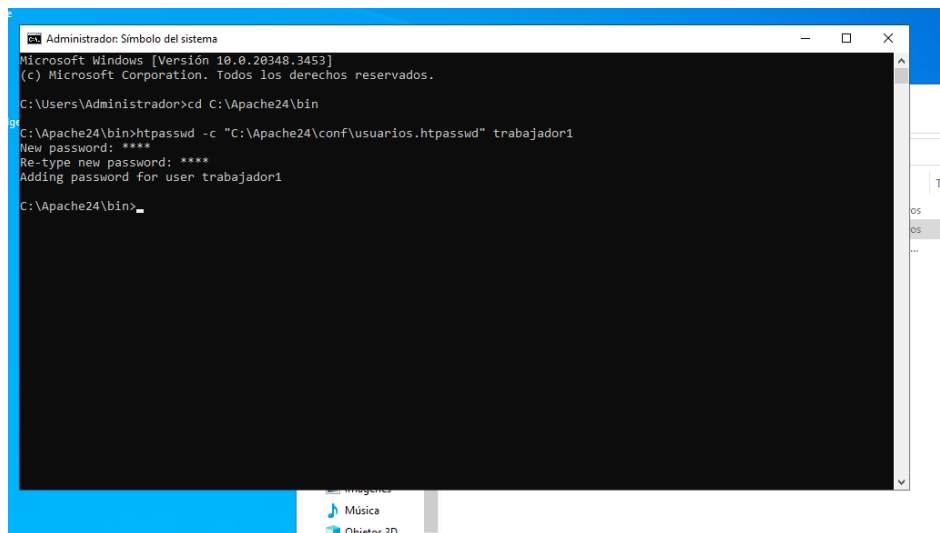
✓ **Pasos para conceder acceso a una carpeta a un nuevo trabajador:**

El primer paso será crear la carpeta del nuevo trabajador, dentro de la siguiente ruta:
`C:\Apache24\htdocs:`



Permisos de Usuarios

Ahora vamos a crear el archivo **.htpasswd**, con las credenciales del nuevo trabajador. En nuestro caso hemos usado la herramienta **htpasswd.exe** que suele venir con Apache, y también se puede descargar e instalar, o usar una versión online, en esta práctica ya venía instalada con Apache por suerte. Abrimos un CMD con permisos de administrador, una vez dentro nos movemos por los directorios para llegar a la siguiente ruta y mediante el siguiente comando: **cd C:\Apache24\bin**. El siguiente paso será lanzar el siguiente comando, con el que crearemos el archivo .htpasswd mencionado: **htpasswd -c "C:\Apache24\conf\usuarios.htpasswd" trabajador1**.



```

Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.20348.3453]
(c) Microsoft Corporation. Todos los derechos reservados.

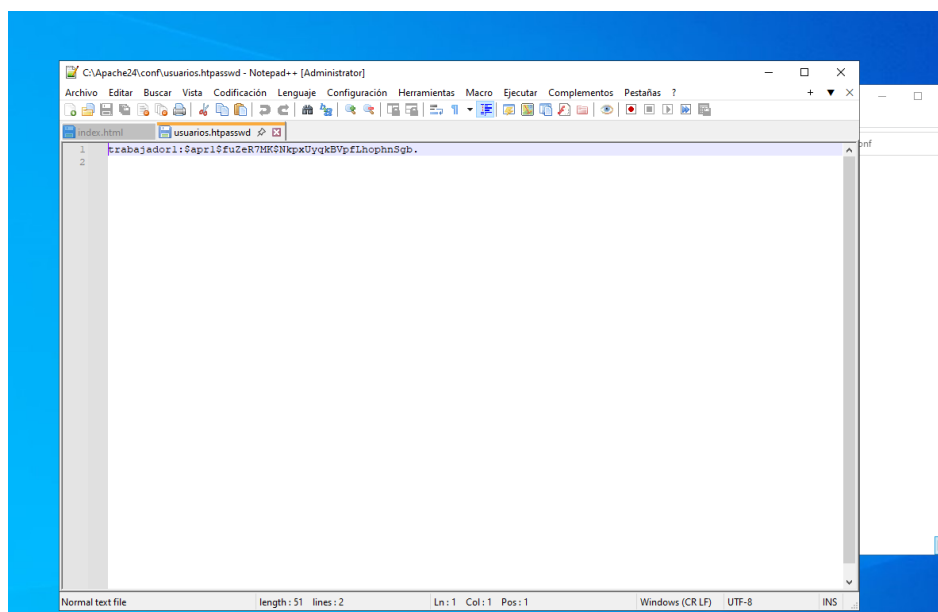
C:\Users\Administrador>cd C:\Apache24\bin
C:\Apache24\bin>htpasswd -c "C:\Apache24\conf\usuarios.htpasswd" trabajador1
New password: ****
Re-type new password: ****
Adding password for user trabajador1
C:\Apache24\bin>

```

El parámetro **-c** crea el archivo, (solo se usa la primera vez)

Apache nos pedirá introducir y confirmar la contraseña del trabajador.

Con ello conseguimos crear un archivo **usuarios.htpasswd** con el usuario **trabajador1** y su contraseña cifrada.



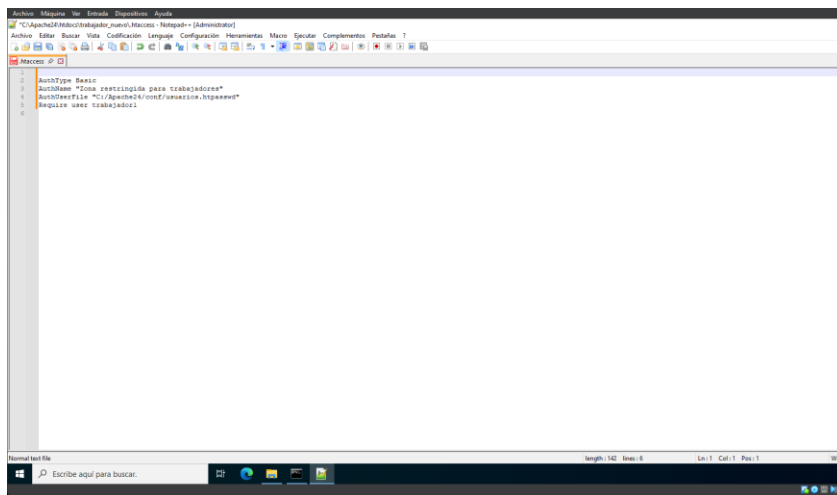
```

C:\Apache24\conf\usuarios.htpasswd - Notepad++ [Administrator]
Archivo  Editor  Buscar  Vista  Codificación  Lenguaje  Configuración  Herramientas  Macro  Ejecutar  Complementos  Pestañas  ?
index.html  usuarios.htpasswd
1
2
trabajador1:Saprl$FuZeR7MK$NkpxDyqkBYpFLhophnSgb.

```

Permisos de Usuarios

Ahora debemos configurar el archivo **.htaccess** en la carpeta protegida. Dentro de la carpeta que creamos para el trabajador 1, creamos dicho archivo con el siguiente contenido:



- **AuthType Basic:** Tipo de autenticación.
- **AuthName:** Texto que se muestra en el navegador.
- **AuthUserFile:** Ruta al archivo .htpasswd con los usuarios.
- **Require user trabajador1:** Solo este usuario tiene acceso.
-

Ahora debemos habilitar el uso del fichero **.htaccess** en Apache, para ello debemos revisar el fichero **httpd.conf** y verificar si está habilitado, en caso contrario deberemos hacer un cambio en el código de ese fichero.

```

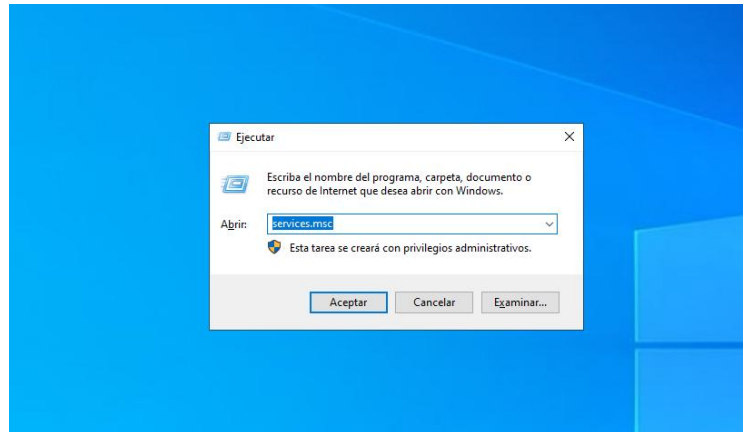
#
#ServerName www.example.com:80
#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory "C:/Apache24/htdocs/trabajador_nuevo">
    AllowOverride All
    Require all granted
</Directory>
#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your

```

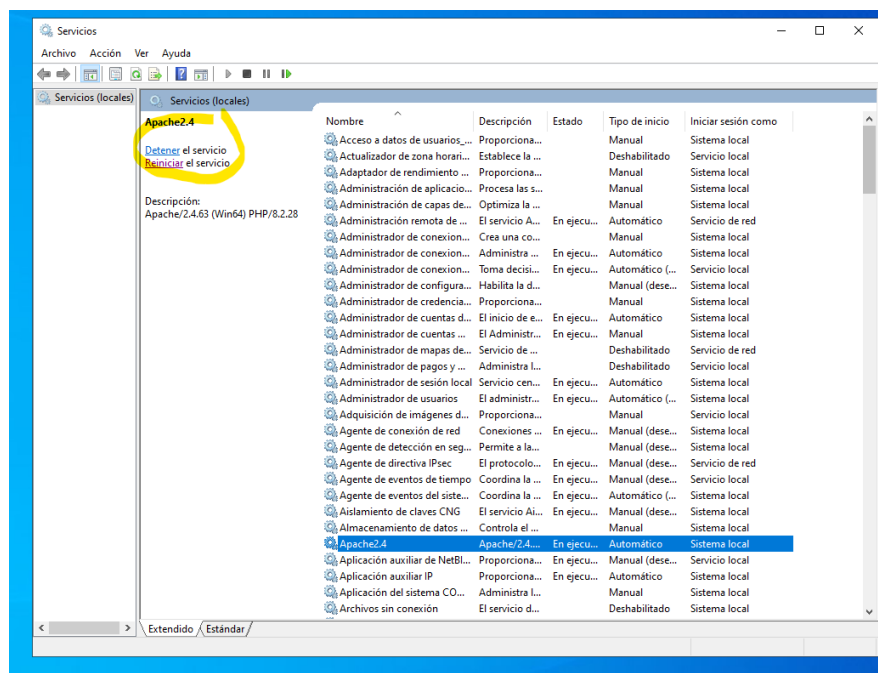
En esta práctica tuvimos que modificar el código y añadiendo ese código que podemos ver en la imagen anterior.

Permisos de Usuarios

Ahora debemos reiniciar Apache, para ello tenemos varias opciones, bien desde la línea de comandos o desde la interfaz del servidor si pulsamos las teclas **Windows + r** se nos abrirá una ventana en la que debemos introducir **services.msc** y pulsar intro.



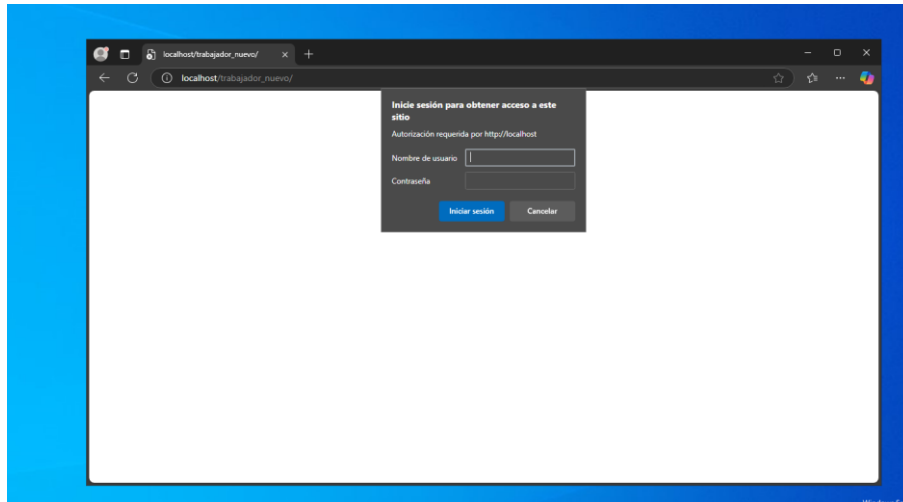
Se nos abrirá la ventana de servicios locales.



Desde aquí podemos reiniciar los servicios de Apache y a continuación probaremos desde el navegador para ver si la configuración es correcta.

Permisos de Usuarios

Abrimos el navegador e introducimos: ***http://localhost/trabajador_nuevo*** y al dar intro deberá abrir una ventana del navegador en la que nos pedirá usuario y contraseña:



En este punto podemos confirmar que la configuración fue correcta y todo funciona como se esperaba.

Puntos Básicos de Seguridad

2. Además, el nuevo trabajador hará uso de internet en su desempeño diario por lo que debemos conocer algunos puntos básicos en la seguridad de aplicaciones web para hacérselo saber. Enumera alguno de ellos.

La seguridad en aplicaciones web es fundamental, especialmente si el nuevo trabajador utilizará internet como parte de su desempeño diario. A continuación, se enumeran algunos puntos básicos de seguridad de aplicaciones web que podemos comunicarle para que esté informado y adopte buenas prácticas:

- ✓ Usar contraseñas **seguras**: Las contraseñas deben ser largas (al menos 12 caracteres), combinando letras mayúsculas, minúsculas, números y símbolos. *No reutilizar contraseñas y considerar el uso de un gestor de contraseñas.*
- ✓ Mantener el Software actualizado: Los navegadores, sistemas operativos y aplicaciones deben mantenerse actualizados para corregir vulnerabilidades conocidas. *Habilitar actualizaciones automáticas siempre que sea posible.*

Permisos de Usuarios

- ✓ Identificar y evitar el **phishing**: El phishing es un método común para robar credenciales o información sensible mediante correos electrónicos o sitios falsos. *Verificar la URL antes de ingresar credenciales y desconfiar de correos sospechosos o mensajes inesperados.*
- ✓ Usar conexiones cifradas (**HTTPS**): Siempre acceder a sitios web que usen HTTPS (el candado en la barra de direcciones indica una conexión segura). *Evitar ingresar datos personales o sensibles en sitios sin cifrado.*
- ✓ No descargar archivos de fuentes no confiables: Los archivos descargados pueden contener malware o software malicioso. Descargar solo de sitios oficiales o confiables y escanear archivos con antivirus antes de abrirlos.
- ✓ Proteger la sesión de usuario: Cerrar sesión después de usar aplicaciones web, especialmente en dispositivos compartidos. Usar autenticación multifactor (MFA) siempre que esté disponible.
- ✓ Conocer las políticas de privacidad y seguridad: Entender cómo las aplicaciones web manejan los datos personales y qué medidas de seguridad implementan. Leer las políticas de privacidad y evitar compartir datos sensibles innecesariamente.
- ✓ Reportar incidentes de seguridad: Si detecta algo sospechoso (como acceso no autorizado o comportamiento extraño), debe reportarlo inmediatamente. Tener claro a quién contactar dentro de la empresa para reportar problemas de seguridad.

Estos puntos son fundamentales para garantizar que el nuevo trabajador utilice internet y aplicaciones web de manera segura. Comunicar estas prácticas le ayudará a proteger tanto su información personal como los recursos de la empresa.