

# Desarrollo Web en Entorno Cliente

## Tema 0





# Configuración de Git y GitLab



En el módulo de Desarrollo Web en Entorno Cliente se va a utilizar el programa *Git*, un software de control de versiones, diseñado por Linus Torvalds, el creador de Linux, para poder llevar de forma eficiente los cambios que se realizan en los archivos fuente de los diferentes proyectos.

Además, se va a utilizar *GitLab* como servidor de repositorios de *Git*.

El hosting que aloja este repositorio está en la siguiente dirección IP:

<http://143.47.39.127>

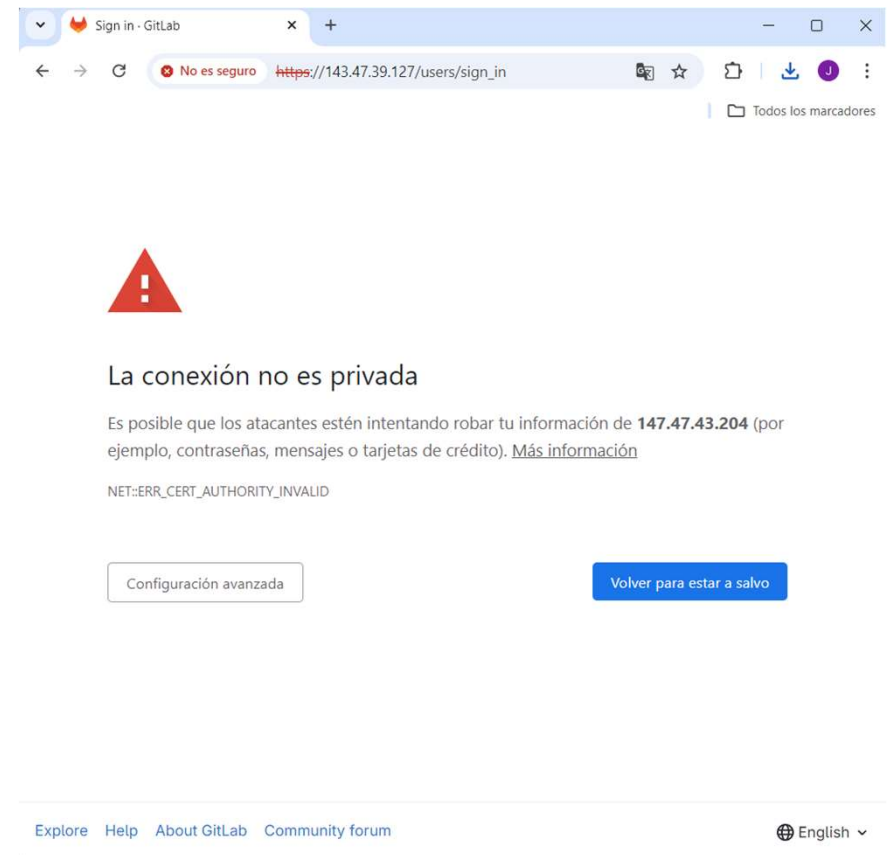
A screenshot of a web browser displaying the GitLab sign-in page. The browser's address bar shows the URL "https://143.47.39.127/users/sign\_in" with a warning icon and the text "No es seguro". The page features the GitLab logo (a red and orange fox head) at the top center, followed by the text "GitLab Community Edition". Below this, there are two input fields: "Username or primary email" and "Password". The password field has a toggle icon for visibility. To the right of the password field is a link that says "Forgot your password?". Below the input fields is a checkbox labeled "Remember me". At the bottom of the form is a blue "Sign in" button. Below the button is a link that says "Don't have an account yet? Register now". The footer of the page contains links for "Explore", "Help", "About GitLab", and "Community forum", along with a language selector set to "English".



El servidor *GitLab* utiliza el protocolo *HTTPS*, basado en *SSL/TLS*, que establece una conexión segura cifrando la información que se envía, lo que evita que usuarios malintencionados puedan espiar la red y averiguar las contraseñas.

Para poder utilizar *HTTPS* se necesita un certificado digital.

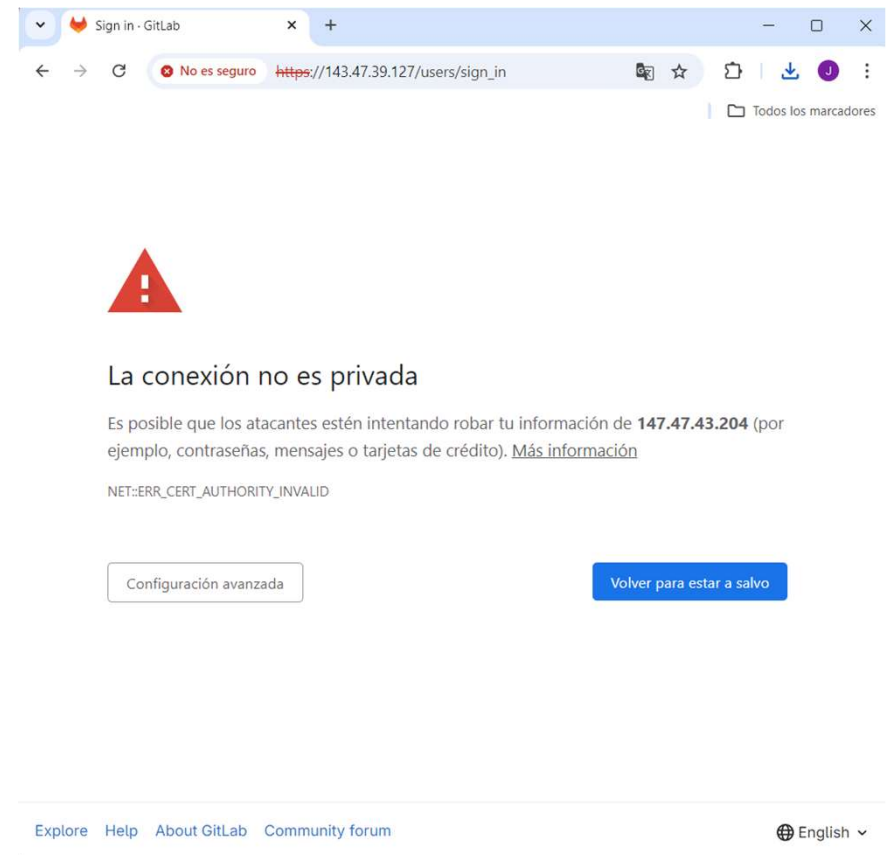
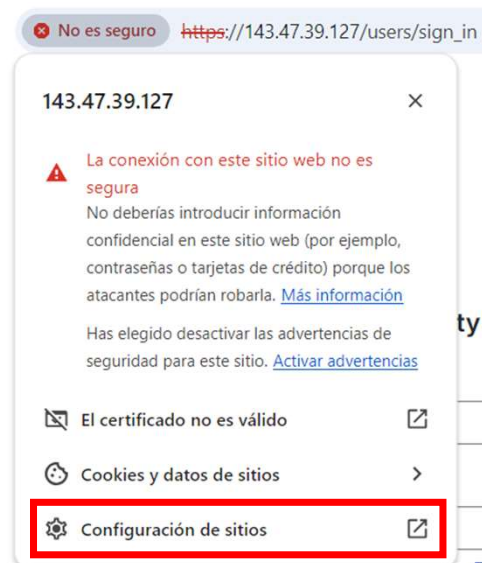
El certificado que se utiliza en el servidor donde se aloja *GitLab* es un “*autocertificado*”, se ha generado y firmado por la propia máquina, por lo que no hay ninguna empresa certificadora de confianza que lo avale. Esto hace que el navegador no aceptará el certificado e indicará el problema.



# [GitLab]

Para poder acceder al servidor *GitLab* se debe hacer clic en el botón *Configuración avanzada* y, a continuación, clic sobre *Acceder a 147.47.39.127* (*sitio no seguro*).

Para que la próxima vez *Chrome* u otro navegador deje acceder al sitio web directamente, hay que hacer clic izquierdo sobre la *exclamación* y seleccionar *Configuración de sitios* en el menú contextual:

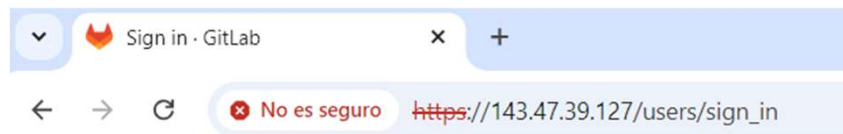















En el panel de configuración del navegador Chrome (o en el de *Edge* de Microsoft), en el apartado *Contenido no seguro* se habilita Permitir.

Esto parámetro permitirá que *Chrome*, cuando se acceda al sitio *143.47.39.127*, donde se aloja *GitLab*, ignorar el aviso de contenido no seguro.

De cualquier forma, en la barra del navegador seguirá apareciendo la advertencia de que el sitio no es seguro:



### Configuración

 Dispositivos HID	Preguntar (predeterminado) ▼
 IDs de contenido protegido Subtítulos automáticos de Chrome podría no funcionar	Permitir (predeterminado) ▼
 Portapapeles	Preguntar (predeterminado) ▼
 Controladores de pago	Permitir (predeterminado) ▼
 Contenido no seguro	Permitir ▼
 Inicio de sesión de terceros	Permitir (predeterminado) ▼
 Realidad aumentada	Preguntar (predeterminado) ▼
 Realidad virtual	Preguntar (predeterminado) ▼
 Uso de tu dispositivo	Preguntar (predeterminado) ▼
 Gestión de ventanas	Preguntar (predeterminado) ▼
 Fuentes	Preguntar (predeterminado) ▼

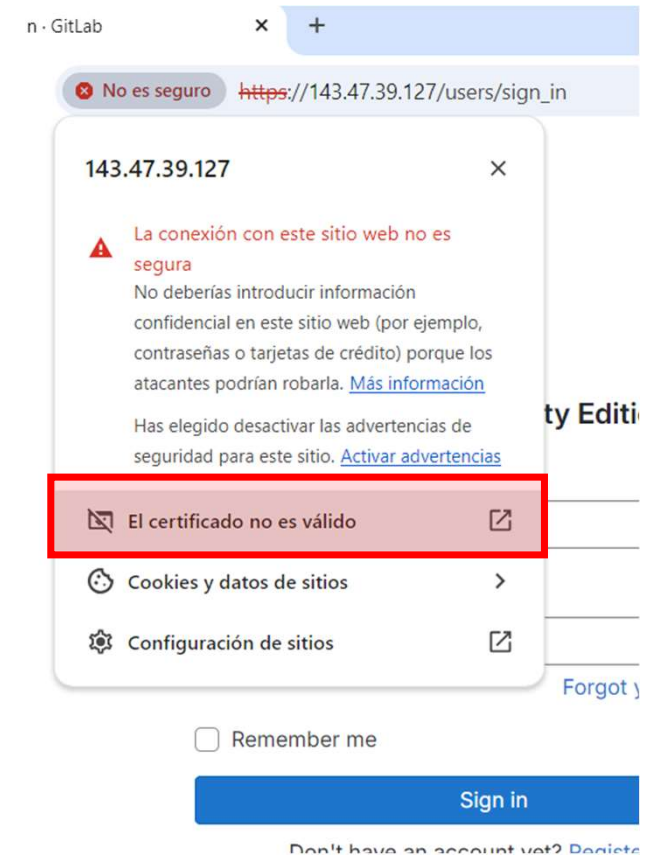
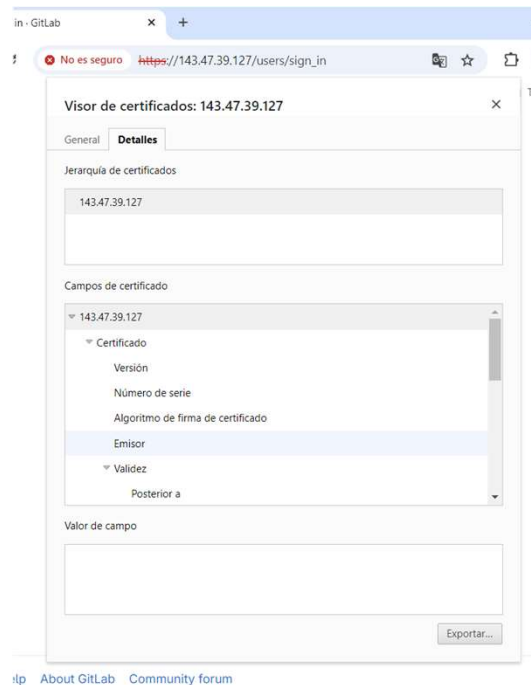


También se puede instalar el certificado en el sistema operativo Windows.

Para ello, se hace clic en la barra de direcciones sobre el texto *No es seguro*, y se selecciona la opción *El certificado no es válido*

En la ventana flotante que aparece, en la pestaña *Detalles* se hace clic sobre el botón *Exportar...*

Y se guarda el certificado en el ordenador, por ejemplo, en el Escritorio.

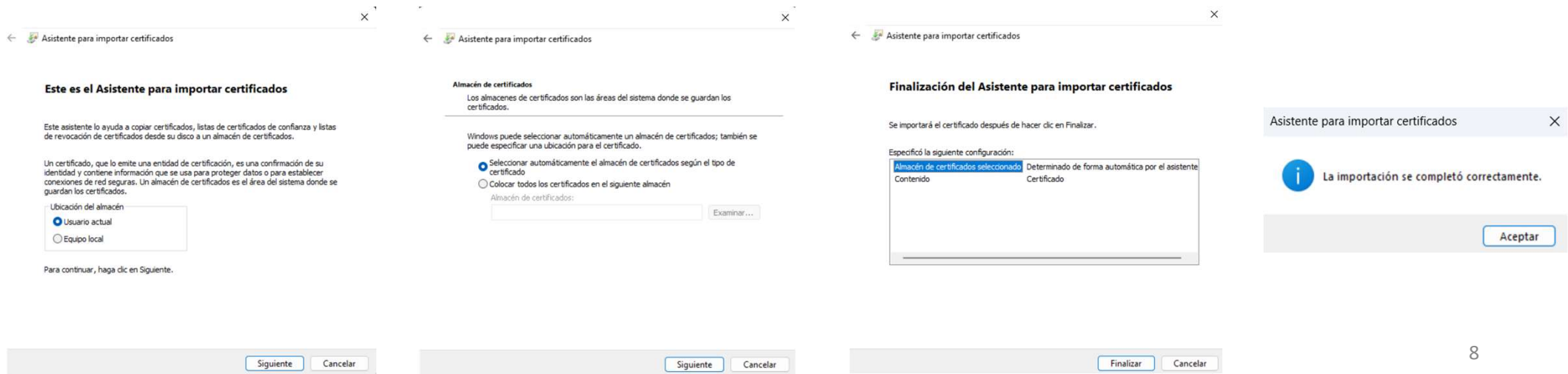
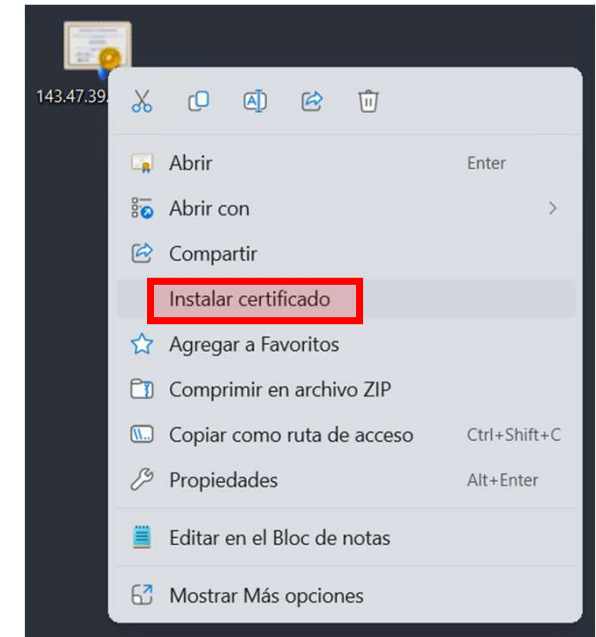




A continuación, se hace clic con el botón derecho del ratón, y en el menú contextual, se selecciona *Instalar certificado*.

En el asistente se selecciona *Usuario actual* y se hace clic en siguiente hasta obtener el mensaje que informa que se instaló el certificado correctamente.

Se repite todo el proceso de igual manera, pero seleccionado en esta ocasión en el asistente *Equipo local*.







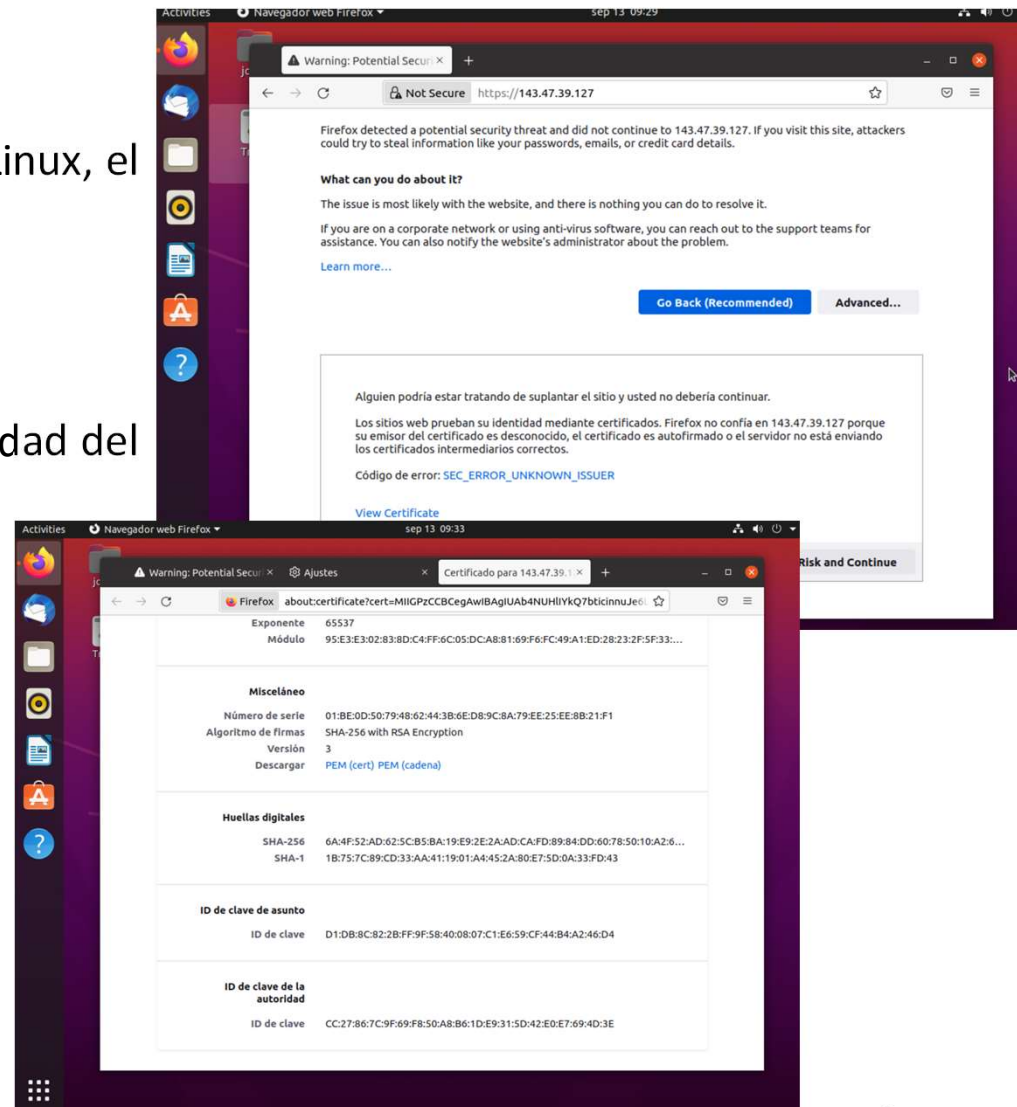
Desde otro navegador como *Firefox*, desde Windows o Linux, el proceso es muy similar.

Se accede a la URL <https://143.47.39.127>

El navegador informa que no puede verificar la autenticidad del certificado. Se hace clic en *Avanzado...*

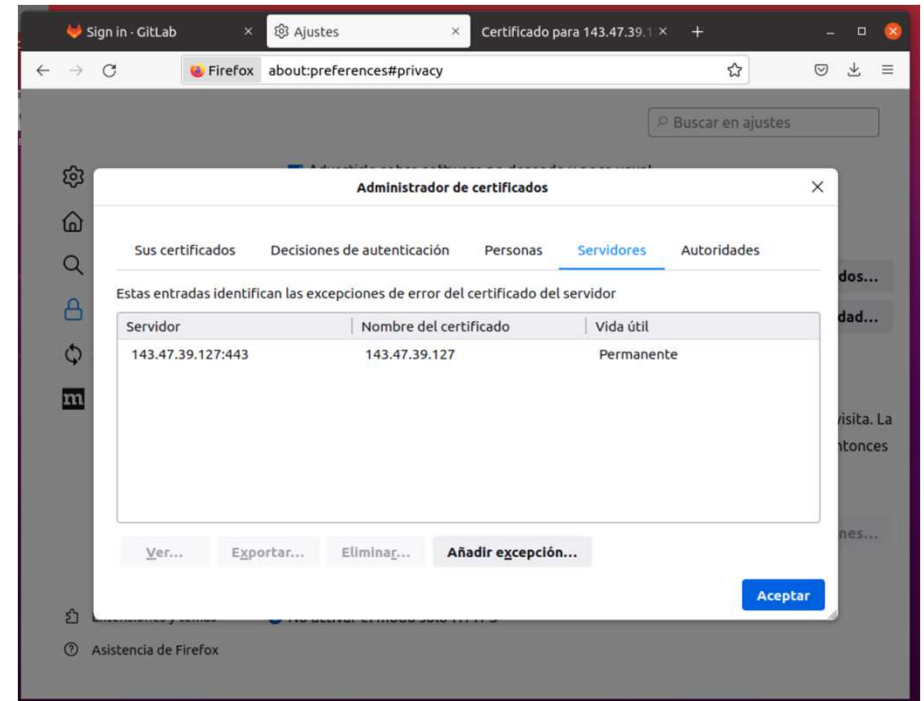
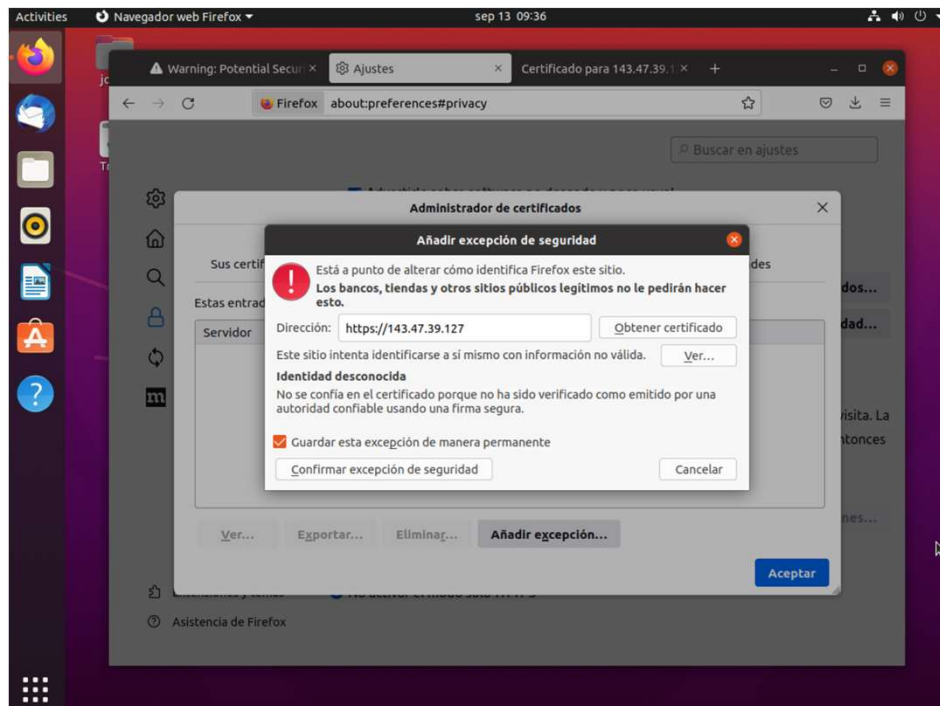
Se le da a la opción Ver certificado, y se descarga en la máquina.

A continuación, se abren los ajustes de Firefox, se busca la sección de certificados y se importa





A continuación, se abren los ajustes de *Firefox*, se busca la sección de certificados y en la pestaña de Servidores se Añade la excepción.



# Autenticación en GitLab mediante SSH

Git es un sistema de control de versiones distribuido, lo que significa que se puede trabajar en un ordenador de forma local y luego compartir o enviar los cambios realizados en la aplicación a un servidor de repositorios como *GitLab* o *GitHub*.

*GitLab* utiliza el protocolo *SSH* (*Secure Shell*) para comunicarse de forma segura con *Git*.

Cuando se utilizan claves SSH para autenticarse en el servidor remoto de *GitLab* no es necesario proporcionar el nombre de usuario y contraseña.

*GitLab* autentica al usuario en una máquina mediante un conjunto de claves pública y privada, por simplicidad se usará el algoritmo RSA, pero *GitLab* admite muchos más.



# Autenticación en GitLab mediante SSH

Para crear las credenciales SSH desde Windows, se abre una consola de comandos (*cmd*) y se teclea:

```
ssh-keygen -t rsa
```

Este comando forma parte de la suite *OpenSSH*, y generará una clave asimétrica, un par de claves una pública (*id\_rsa.pub*) y otra privada (*id\_rsa*), mediante el algoritmo RSA, por defecto se almacenan en la carpeta *.ssh* dentro de la cuenta de usuario, aunque se puede especificar la ubicación.

```
C:\Users\ibm_h>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\ibm_h/.ssh/id_rsa):
C:\Users\ibm_h/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\ibm_h/.ssh/id_rsa
Your public key has been saved in C:\Users\ibm_h/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:jLTcR2LPzgfl9xU2RHu5f+3Z06+k0SkFudvMizFTOT8 ibm_h@GeorgePC
The key's randomart image is:
+---[RSA 3072]---+
|                 o . +* |
|                . o = o. =|
|                 o ..= .o+|
|                 . o+ o .|=|
|                . S  o* ...|
|                . o  ...+ o|
|                 . . +* .E =|
|                 o=+* +=|
|                 ..+o.o*|
+-----[SHA256]-----+
C:\Users\ibm_h>
```

# Autenticación en GitLab mediante SSH

Windows utiliza, por defecto, la carpeta `.ssh`, dentro de la carpeta de usuario, para almacenar las contraseñas públicas y privadas, por lo que es preferible no cambiar esta ubicación.

Se puede especificar una frase o palabra de paso (*passphrase*) para que las claves sean más fuertes (por comodidad no se recomienda).

La palabra o frase de paso añade una capa adicional de seguridad a la clave, y cada vez que se quiera utilizar la clave privada se solicitará dicha palabra o frase de paso.

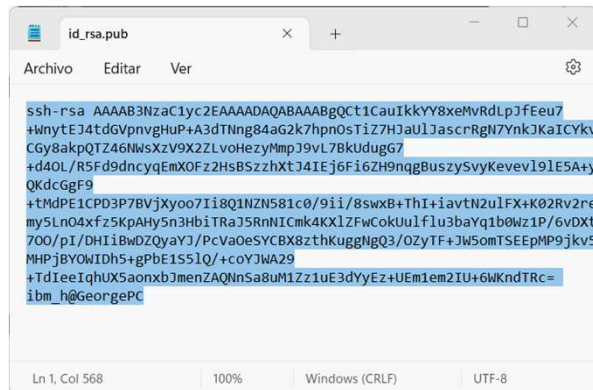
```
C:\Users\ibm_h>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\ibm_h/.ssh/id_rsa):
C:\Users\ibm_h/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\ibm_h/.ssh/id_rsa
Your public key has been saved in C:\Users\ibm_h/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:jLTcR2LPzgfl9xU2RHu5f+3Z06+k0SkFudvMizFTOT8 ibm_h@GeorgePC
The key's randomart image is:
+---[RSA 3072]---+
|                o . +* |
|               . o = o. =|
|                o ..= .o+|
|               . o+ o .|=|
|               . S o* ...|
|               . o ...+ o|
|               . . +* .E =|
|                o=+* +=|
|               ..+o.o*|
+-----[SHA256]-----+

C:\Users\ibm_h>
```

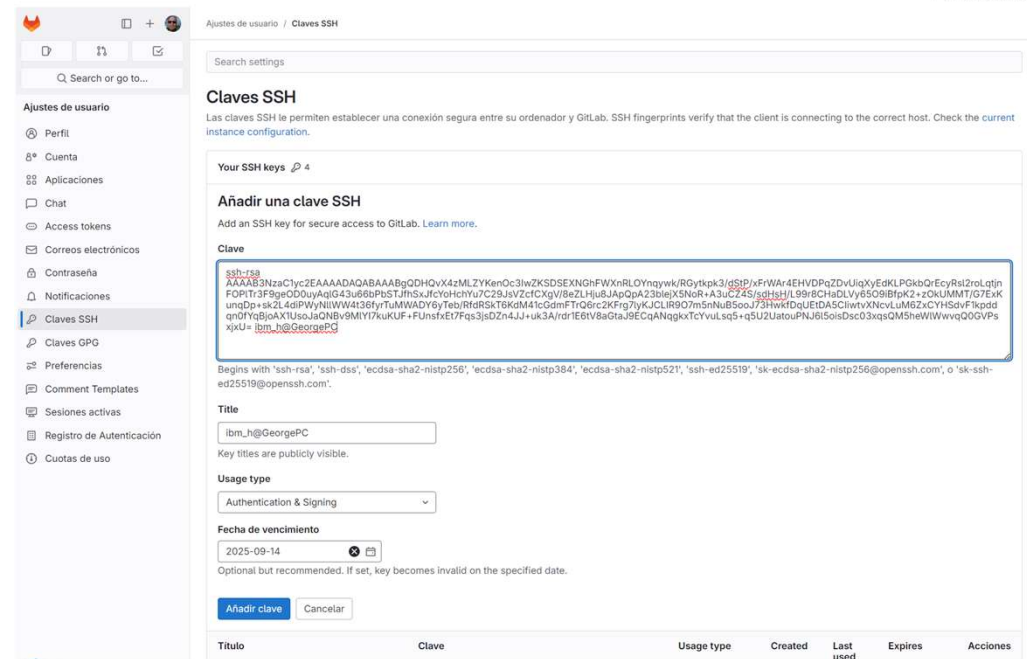
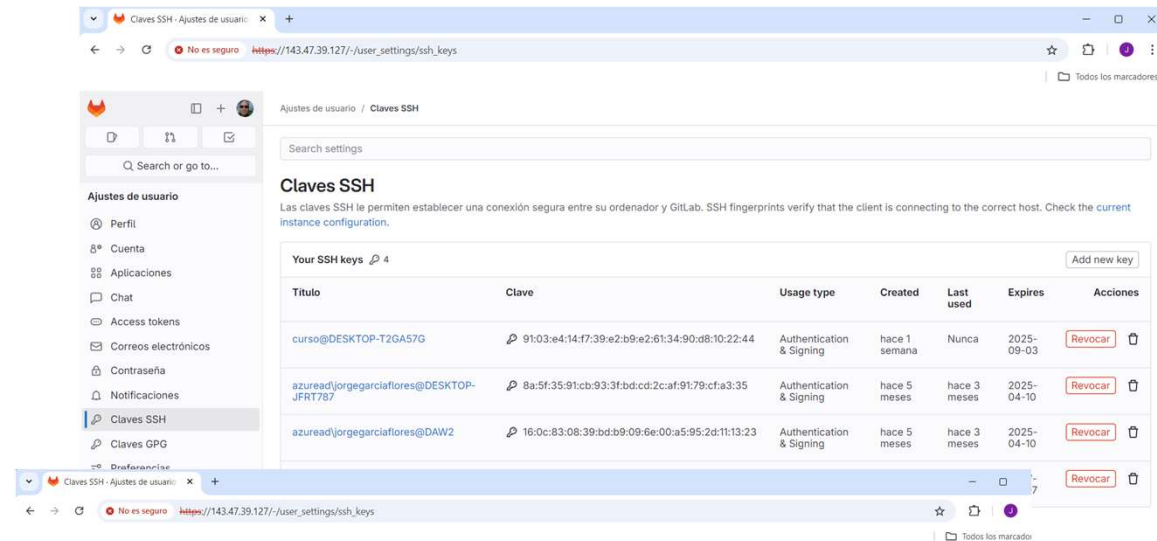
# Autenticación en GitLab mediante SSH

Desde *GitLab*, desde la opción *Editar Perfil*, se selecciona *Claves SSH* y se pulsa sobre el botón *Add new key* (añadir nueva clave).

Abrimos el fichero *id\_rsa.pub* y copiamos todos su contenido y lo pegamos en la entrada *Clave* y pulsamos el botón *Añadir clave*.



```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCT1CauIkYY8xMvRdLpJfEeu7
+WnytEJ4tdGVpvnGhUP+A3dTNng84aG2k7hpnOsTiZ7HJaUlJascRgN7Ynk3KaICykv
CGy8akpQTZ46NwSxZv9X2ZLvoHezyMmpJ9vL78kUdugG7
+d40L/R5Fd9dncyqEmXOFz2HsBSzZhXtJ4IEj6Fi6ZH9nqgBuszySvyKevev19IE5A+y
QKdcGgF9
+tMdPE1CPD3P7BVjXyoo7Ii8Q1NZN581c0/9ii/8swxB+ThI+iavtN2uLFX+K02Rv2re
my5Ln04xf25KpAHy5n3HbiTRAj5RnNICmk4KX1ZFwCokUu1flu3baYq1b0wz1P/6vDXt
700/pI/DHIiBwDZQyaYJ/PcVa0eSYCBX8zthKugngQ3/OzyTF+JW5omTSEEPMP9jKv5
MHPjBYOWIDh5+gPbE1S51Q/+coYJWA29
+TDIeeIqhUX5aonxbJmenZAQnSa8uM1Zz1uE3dYyEz+UEm1em2IU+6WkNdTRC=
ibm_h@GeorgePC
```





# Autenticación en GitLab mediante SSH

Mientras la clave sea válida, no se borre o sea revocada se puede acceder a *GitLab* sin utilizar nombre de usuario y contraseña.

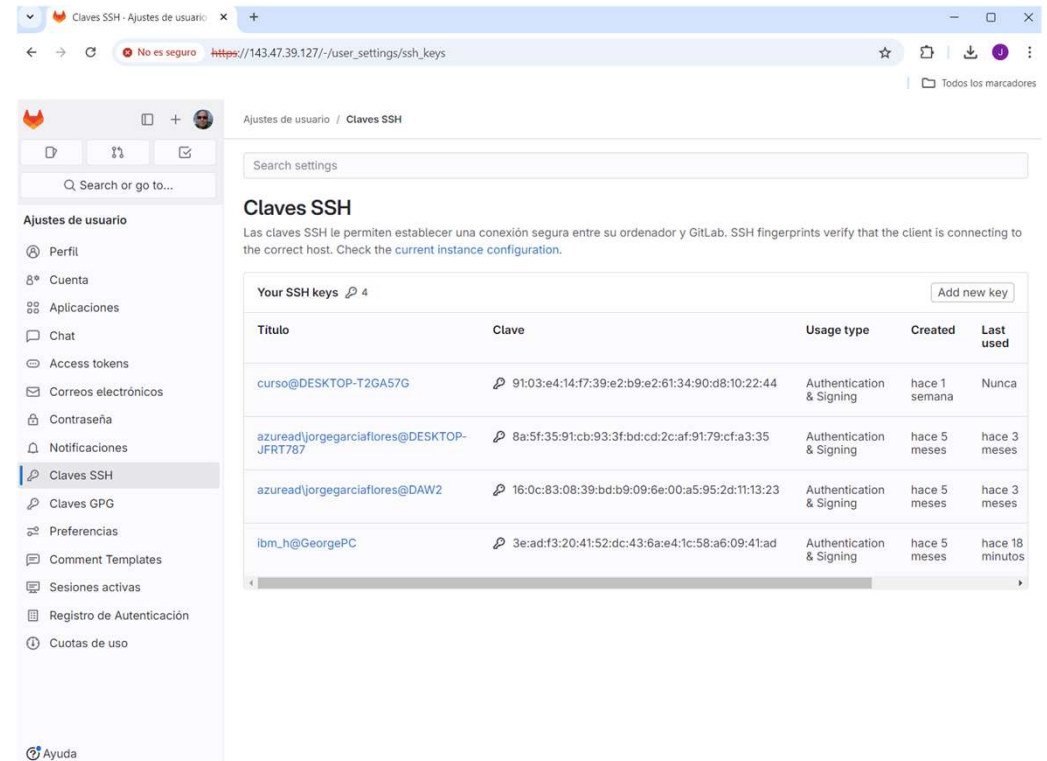
Para probarlo, se abre una ventana de comandos y se ejecuta la siguiente instrucción:

```
ssh -T git@143.47.39.127
```

Si el servidor responde con un *Welcome to GitLab* seguido con el nombre usuario, se ha configurado correctamente:

```
C:\Users\ibm_h>ssh -T git@143.47.39.127
Welcome to GitLab, @jorge!

C:\Users\ibm_h>
```



The screenshot shows the GitLab user settings page for SSH keys. The left sidebar contains a navigation menu with options like Perfil, Cuenta, Aplicaciones, Chat, Access tokens, Correos electrónicos, Contraseña, Notificaciones, Claves SSH (selected), Claves GPG, Preferencias, Comment Templates, Sesiones activas, Registro de Autenticación, and Cuotas de uso. The main content area is titled 'Claves SSH' and includes a search bar and a table of existing SSH keys. The table has columns for Title, Key, Usage type, Created, and Last used. There are four keys listed, each with a unique title and a corresponding SSH key fingerprint.

Titulo	Clave	Usage type	Created	Last used
curso@DESKTOP-T2GA57G	91:03:e4:14:f7:39:e2:b9:e2:61:34:90:d8:10:22:44	Authentication & Signing	hace 1 semana	Nunca
azuread@jorgegarciaflores@DESKTOP-JFRT787	8a:5f:35:91:cb:93:3f:bd:cd:2c:af:91:79:cf:a3:35	Authentication & Signing	hace 5 meses	hace 3 meses
azuread@jorgegarciaflores@DAW2	16:0c:83:08:39:bd:b9:09:6e:00:a5:95:2d:11:13:23	Authentication & Signing	hace 5 meses	hace 3 meses
ibm_h@GeorgePC	3e:ad:f3:20:41:52:dc:43:6a:e4:1c:58:a6:09:41:ad	Authentication & Signing	hace 5 meses	hace 18 minutos

# Autenticación en GitLab mediante SSH

El proceso en Linux es prácticamente el mismo, se abre una terminal y se teclea:

```
ssh-keygen -t rsa
```

En Linux, los ficheros con las claves pública (*id\_rsa.pub*) y privada (*id\_rsa*) se almacenan por defecto en la carpeta *.ssh* de la carpeta de conexión del usuario como, por ejemplo, en */home/jorge/.ssh*

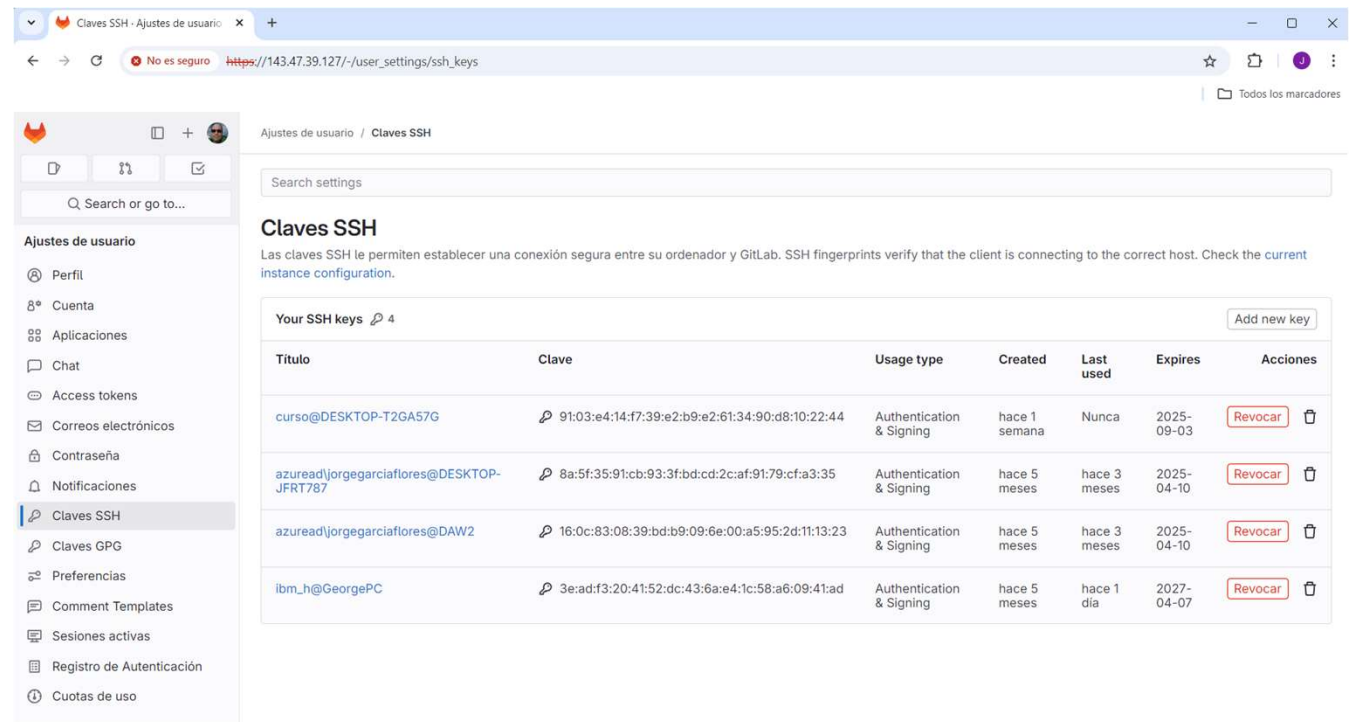
Con el comando *cat* se puede visualizar el contenido del fichero *id\_rsa.pub* para copiarlo y pegarlo fácilmente en el servidor *GitLab*.

```
jorge@jorge-Ubuntu:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jorge/.ssh/id_rsa):
/home/jorge/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/jorge/.ssh/id_rsa
Your public key has been saved in /home/jorge/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:qTC5NXXnnUiJeio7+12TQpuiQvWmhPwUmbcTwoDCBpU jorge@jorge-Ubuntu
The key's randomart image is:
+---[RSA 3072]-----+
|=. . . . .|
|o+E . . . .|
|o o o . . . .|
| B = . . . .|
|. o % O S . .|
| + = / O . .|
|. * O O o . .|
|+. B o . . .|
|=*o . . . .|
+---[SHA256]-----+
jorge@jorge-Ubuntu:~$ cat /home/jorge/.ssh/id_rsa.pub
```



# Autenticación en GitLab mediante SSH

Se pueden crear tantas claves en el servidor *GitLab* como se necesiten para poder acceder desde diferentes máquinas:



The screenshot shows the GitLab user settings page for SSH keys. The browser address bar indicates the URL is [https://143.47.39.127/-/user\\_settings/ssh\\_keys](https://143.47.39.127/-/user_settings/ssh_keys). The page title is "Claves SSH". Below the title, there is a search bar and a description: "Las claves SSH le permiten establecer una conexión segura entre su ordenador y GitLab. SSH fingerprints verify that the client is connecting to the correct host. Check the [current instance configuration](#)." Below this, there is a table titled "Your SSH keys" with 4 keys. The table has columns: Título, Clave, Usage type, Created, Last used, Expires, and Acciones. The keys are listed as follows:

Título	Clave	Usage type	Created	Last used	Expires	Acciones
curso@DESKTOP-T2GA57G	91:03:e4:14:f7:39:e2:b9:e2:61:34:90:d8:10:22:44	Authentication & Signing	hace 1 semana	Nunca	2025-09-03	<a href="#">Revocar</a> <a href="#">Eliminar</a>
azuread\jorgegarciaflores@DESKTOP-JFRT787	8a:5f:35:91:cb:93:3f:bd:cd:2c:af:91:79:cf:a3:35	Authentication & Signing	hace 5 meses	hace 3 meses	2025-04-10	<a href="#">Revocar</a> <a href="#">Eliminar</a>
azuread\jorgegarciaflores@DAW2	16:0c:83:08:39:bd:b9:09:6e:00:a5:95:2d:11:13:23	Authentication & Signing	hace 5 meses	hace 3 meses	2025-04-10	<a href="#">Revocar</a> <a href="#">Eliminar</a>
lbm_h@GeorgePC	3e:ad:f3:20:41:52:dc:43:6a:e4:1c:58:a6:09:41:ad	Authentication & Signing	hace 5 meses	hace 1 día	2027-04-07	<a href="#">Revocar</a> <a href="#">Eliminar</a>

# Autenticación en GitLab mediante SSH

Para utilizar otras claves con nombres o ubicaciones distintas a las de por defecto, hay que crear un fichero llamado *config* en la carpeta *.ssh*.

Dentro de este fichero se añade las siguientes líneas:

```
#GitLab de Daw 2
Host 143.47.39.127
    HostName 143.47.39.127
    User git
    IdentityFile C:\\Users\\ibm_h\\.ssh\\id_rsa_github
```

Donde a *IdentityFile* le sigue la ubicación y nombre del fichero con la clave privada (*id\_rsa\_github*), que se corresponde con la clave pública configurada en el servidor *GitLab*, en este caso, el servidor se identifica por su dirección IP, *143.47.39.127*.

# Autenticación en GitLab mediante SSH

En este fichero de configuración para *SSH* permite definir más credenciales para diferentes servidores *GitLab* o *GitHub* o para acceder a servidores Linux mediante *SSH*.

```
C:\Users\ibm_h>ssh -T git@143.47.39.127
Welcome to GitLab, @jorge!

C:\Users\ibm_h>
```

Una vez configurado correctamente podemos probar a trabajar con comandos de *Git* desde una ventana de comandos. Para verificarlo, se puede clonar el proyecto *Hola Mundo* alojado en el servidor *GitLab* para este fin, desde una ventana de comandos se teclea:

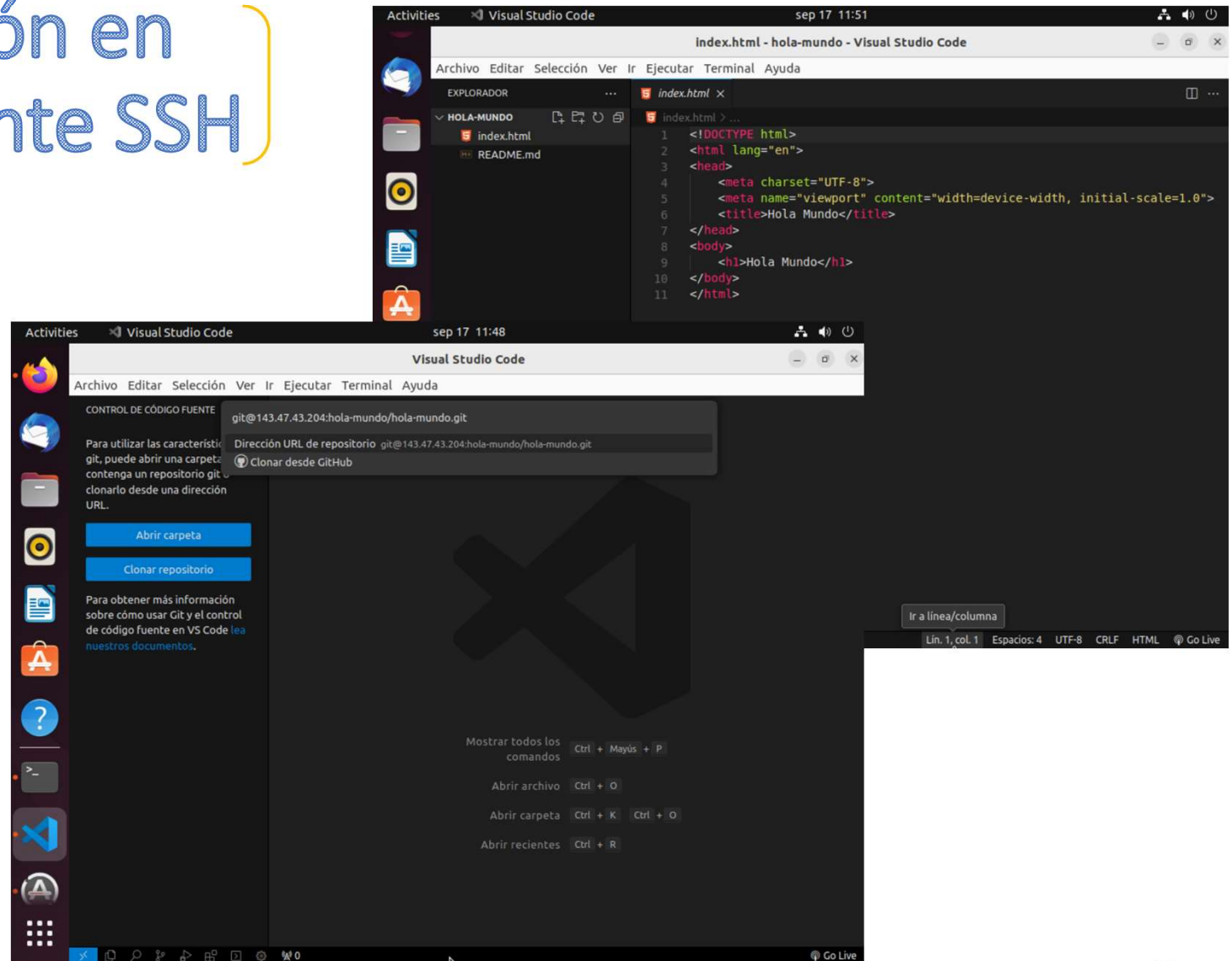
```
git clone git@143.47.39.127:hola-mundo/hola-mundo.git
```

```
C:\Users\ibm_h>git clone git@143.47.39.127:hola-mundo/hola-mundo.git
Cloning into 'hola-mundo'...
remote: Enumerating objects: 9, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 9 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (9/9), done.

C:\Users\ibm_h>|
```

# Autenticación en GitLab mediante SSH

También se puede comprobar que funciona directamente desde *Visual Studio Code* o desde otro editor o IDE que soporte *Git*.



# Bibliografía

- <https://docs.gitlab.com/ee/user/ssh.html>
- <https://medium.com/devops-with-valentine/2021-how-to-your-ssh-key-for-gitlab-on-linux-1b94e2a3a49a>
- <https://www.youtube.com/watch?v=j-zmv-ITQb8>
- <https://www.digitalocean.com/community/tutorials/how-to-configure-ssh-key-based-authentication-on-a-linux-server-es>
- <https://www.atlassian.com/es/git/tutorials/git-ssh>