

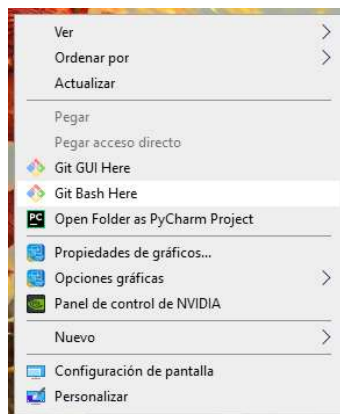


GitHub

Esta guía tiene como finalidad presentar el método de autenticación de su repositorio para el uso de su cuenta en computadores externos al personal.

Inicialización de la clave

1. Dirigirse a la página de Git para Windows ([descargar aquí](#)) y descargar el programa. Puede seguir el ejemplo mostrado en el siguiente ejemplo – [haga clic aquí](#).
2. Una vez instalado, puede abrir el programa *Git Bash* dando clic derecho sobre el escritorio.



3. Puede abrir el siguiente enlace de *Gitdocs*, donde encontrará la documentación referente a la generación de claves SSH y que utilizaremos durante esta.

<https://docs.github.com/es/authentication/connecting-to-github-with-ssh/generating-a-new-ssh-key-and-adding-it-to-the-ssh-agent>

Generación de claves SSH

1. Primero deberá ingresar el siguiente código para crear las contraseñas públicas y privadas SSH.

Facultad de ingeniería
Programa de Ing. Mecatrónica
Guía autenticación SSH GitHub



UNIVERSIDAD DE
SAN BUENAVENTURA



- Ubicado en dicho directorio, escribirá el comando `ls` para listar los elementos que contiene dicho directorio, debería ver creados dos archivos que contienen las credenciales pública y privada.

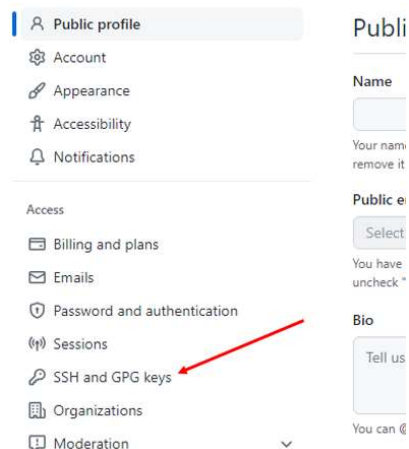
```
Mode                LastWriteTime         Length Name
----                -
-a-----          [redacted]          2655 [redacted]
-a-----          [redacted]          576 [redacted].pub
```

Nota: La clave terminada en `.pub` es la clave pública, mientras que la otra clave es la privada que no debe de compartir con nadie.

- A continuación, escribirá el siguiente código en la consola *Git Bash* para que le muestre la clave pública generada; esta sería la clave que utilizaría para poder iniciar sesión en cualquier otro equipo, pero realmente para esto la configuraremos en nuestro perfil de *GitHub* más adelante. No cierre la consola, porque se necesitará dicha clave más adelante

```
cat <Nombre de su archivo>.pub
```

- En el navegador acceda a su cuenta de GitHub y en el costado superior derecho de la pantalla dan clic en *settings*. Luego seleccionan la opción *SSH and GPG keys* donde se colocará la clave del paso anterior.



- Seguido seleccionan *new SSH key* para poder agregar la clave publica a nuestra cuenta de *GitHub*



SSH keys

New SSH key

There are no SSH keys associated with your account.

Check out our guide to [generating SSH keys](#) or [troubleshoot common SSH problems](#).

- Colocan un nombre con el que identifiquen fácilmente la llave (puede ser: Acceso_USB), seleccionan la opción *authentication key* y finalmente copian y pegan el texto de la llave pública del paso 3 en el campo *key*

Nota: recuerda que esa clave empieza con `ssh-rsa` y finaliza con `<TuEmail@academia.usbbog.edu.co>`.

Incorporación con la clave SSH

- En la consola de Git Bash, deberá ubicarse en el directorio del SSH (este paso ya lo había realizado anteriormente)

```
cd C:\<Su directorio del paso 2 anterior>\.ssh
```

- Escribirá el comando para abrir el agente de credenciales usando el comando

```
eval $(ssh-agent -s)
```

```
$ eval $(ssh-agent -s)
Agent pid 12345
```

Nota: Este agente le permitirá agregar la credencial de inicio de su sesión, la cual se debe instalar en cada ordenador que vaya a usar.

- Después de haber iniciado el agente de credenciales, se debe añadir la clave privada al agente escribiendo el siguiente código

```
ssh-add ~/.ssh/<nombre_del_archivo_clave_privada>
```

4. A partir de este momento, ya puedes generar autenticaciones por **SSH** puesto que **https** no ofrece autenticación. De acá en adelante todos los comandos funcionan normalmente a como se trabajan en la guía de funcionamiento GitHub.

