

# Criptografia de chaves públicas

*Por Ricardo Paulino*

Criptografia é um método utilizado para cifrar um texto ou sentença escrita de modo a torná-lo ininteligível. Desse modo grandes empresas e/ou pessoas e processos em que estão envolvidos objetos que requerem sigilo são enviados a outras pessoas, organizações e/ou outros processos.

Um exemplo do uso de criptografia é para guardar repositórios para controle de versão na rede, com esse recurso podemos manter uma cópia dos códigos fontes de nossos programas em repositórios na rede e assim controlarmos suas versões de acordo com nossas necessidades.

O NetBeans é um software que fornece um ambiente integrado de desenvolvimento que quando tem o controle de versão configurado mantém repositórios atualizados em sincronia com as gravações de seus arquivos.

Desse modo eu posso voltar a versão de um arquivo fonte quando acho que algo deu errado e mantenho um controle bem mais sistemático da minha programação. Aconselho aos programadores que ainda não usam esse tipo de tecnologia a experimentarem esses recursos, não vão se arrepender.

Com o uso adequado das ferramentas de criptografia é possível enviar informações sigilosas através de e-mail ou através de comunicação remota, é o que faz o NetBeans, mantendo-se um nível de segurança bem aceitável para a troca de informações.

De um modo geral os dois tipos de **ambientes** onde mais é usada a criptografia:

1. Aquela utilizada para cifrar informações em arquivo ou cartas utilizando uma sequência de convenções combinadas para transformar a informação original de modo a torna-las ilegíveis por parte de quem viola a mensagem.
2. Aquela utilizada também para cifrar informações de cunho político, diplomático, militar e etc. Neste caso ocorre a modificação codificada de um texto de forma a impedir a sua compreensão por pessoas não autorizadas e que não tenham acesso à tabelas de conversão de caracteres para decifrar a mensagem.

Existem dois algoritmos básicos utilizados para se realizar a **criptografia**, são eles os **algoritmos de chave simétrica** e os **algoritmos de chave assimétrica**. Os **algoritmos de chave simétrica** são uma classe de algoritmos muito utilizados na criptografia, eles usam uma única chave para as operações de cifragem e decifragem de textos e códigos.

Enquanto as operações envolvidas na criptografia de chave simétrica se utilizam operações mais simples a **criptografia de chave pública ou assimétrica** utiliza duas chaves, sendo a primeira para a distribuição a todos os correspondentes de forma **pública**, por isso a chamamos de chave pública, e a outra sendo conhecida apenas pelo seu  **dono** permanecendo, em grande parte das vezes, no ambiente físico de sua máquina, a qual chamamos de **chave privada**.

O algoritmo [RSA](#) é um algoritmo de chave assimétrica que usa números para cifragem da ordem de  $10^{100}$  tornando a decifragem do código por que não possui a chave pública muito difícil. Esse é o algoritmo que possibilita a assinatura digital, ele já colocou por terra todas as tentativas de quebrá-lo .

Algoritmos de chave pública podem ser utilizados para conferir autenticidade e confidencialidade aos dados de um documento, esse é o caso da assinatura digital, vejamos estes conceitos:

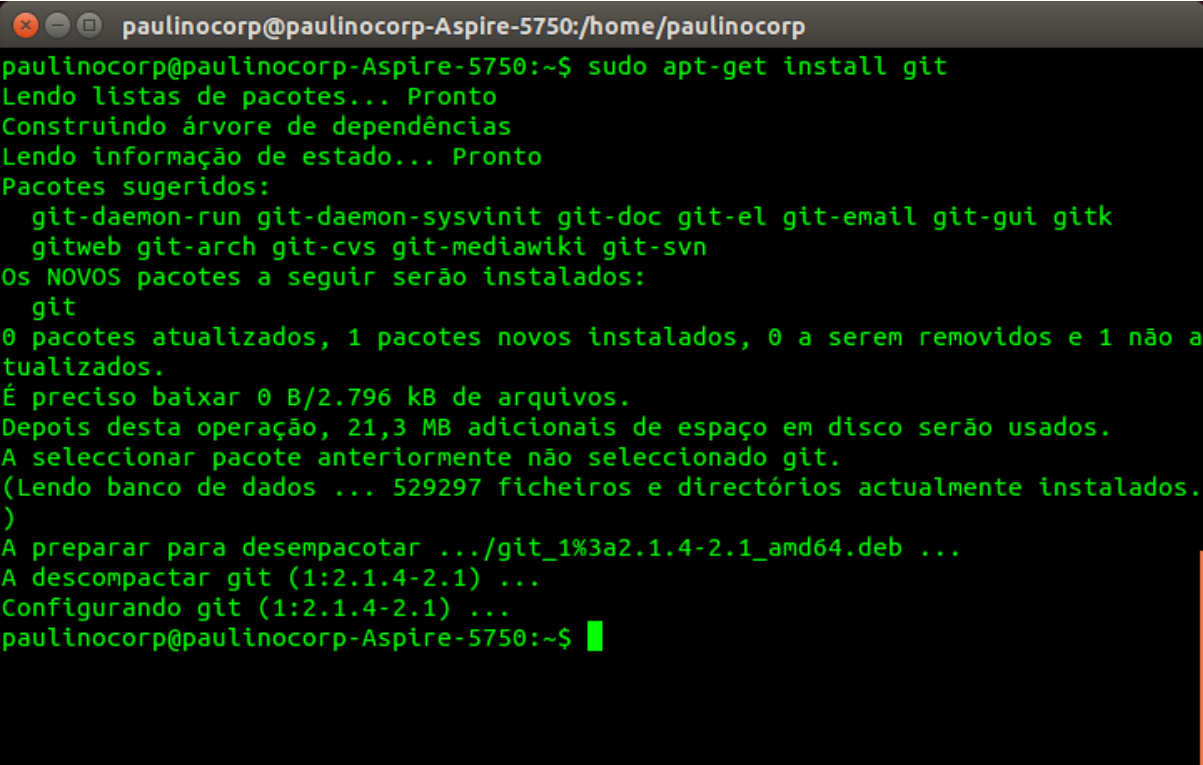
- **Confidencialidade:** A chave pública é utilizada para cifrar o texto de uma mensagem ou código garantindo que apenas o seu dono e o portador da chave privada possam decifrá-la, evitando assim que terceiros possam ler a mensagem ou o código. Através desse mecanismo você garante ao cliente [ssh](#) utilizado para comunicações através de protocolos seguros de comunicação o acesso para alterar dados desde que ele seja portador da chave privada e esta esteja na máquina onde a chave foi criada, ou seja autorizada a acessar o meio físico de dados onde está o seu fonte original. Desse modo um cliente [ssh](#) pode por exemplo alterar configurações de servidores e até mesmo instalar e desinstalar programas em servidores localizados na nuvem acessando seus dados remotamente acessados via [putty](#).
- **Autenticidade:** A chave privada, como já dissemos, é usada para decifrar a mensagem, com isso garantimos que apenas o criador daquela chave a poderia ter criado, viabilizando assim transações seguras como no caso citado acima.

Agora, para fixar este conhecimento, vamos criar um par de chaves assimétricas para acesso aos diretórios do [git](#).

Vamos instalar o **git** no **ubuntu**:

```
sudo apt-get install git
```

a imagem abaixo mostra o comando sendo executado no **shell**:

A terminal window with a dark background and green text. The window title is 'paulinocorp@paulinocorp-Aspire-5750:/home/paulinocorp'. The user has entered the command 'sudo apt-get install git'. The terminal output shows the package manager's response, including dependency resolution and the installation of the 'git' package. The output is as follows:

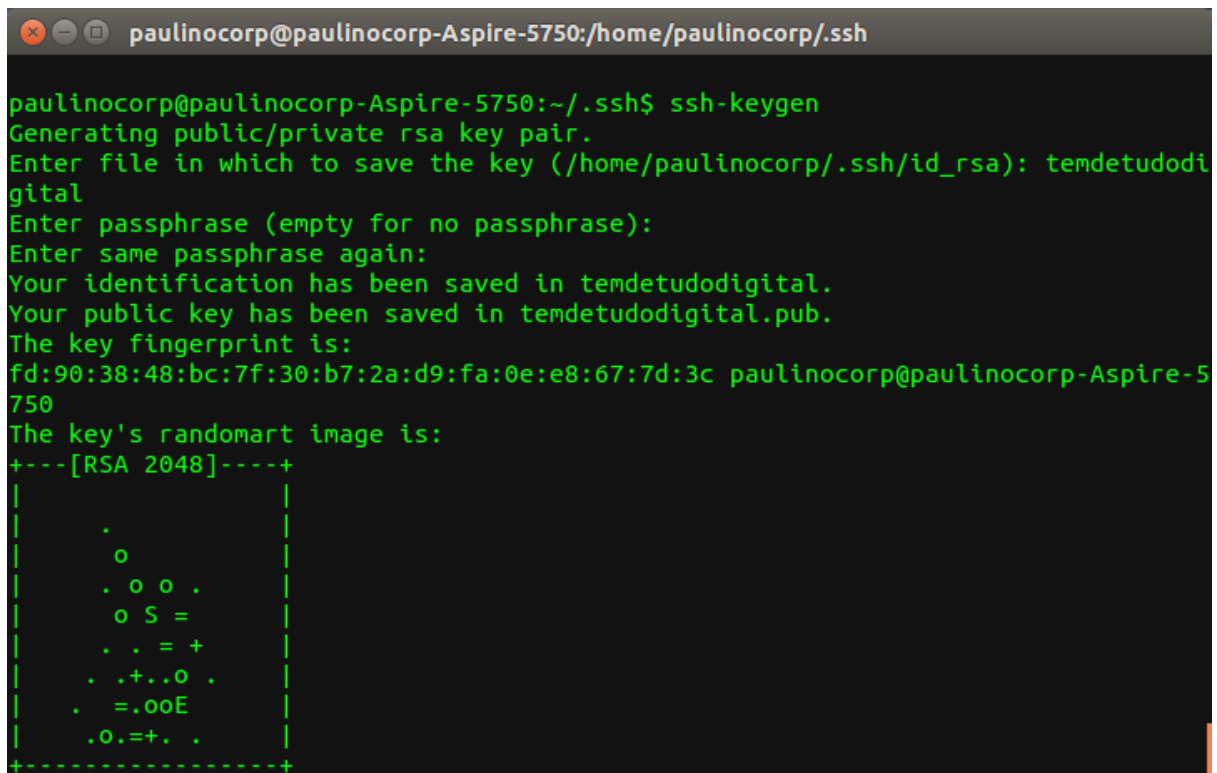
```
paulinocorp@paulinocorp-Aspire-5750:~$ sudo apt-get install git
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
Pacotes sugeridos:
  git-daemon-run git-daemon-sysvinit git-doc git-el git-email git-gui gitk
  gitweb git-arch git-cvs git-mediawiki git-svn
Os NOVOS pacotes a seguir serão instalados:
  git
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos e 1 não a
tualizados.
É preciso baixar 0 B/2.796 kB de arquivos.
Depois desta operação, 21,3 MB adicionais de espaço em disco serão usados.
A seleccionar pacote anteriormente não seleccionado git.
(Lendo banco de dados ... 529297 ficheiros e directórios actualmente instalados.
)
A preparar para desempacotar .../git_1%3a2.1.4-2.1_amd64.deb ...
A descompactar git (1:2.1.4-2.1) ...
Configurando git (1:2.1.4-2.1) ...
paulinocorp@paulinocorp-Aspire-5750:~$
```

Agora para poder ter acesso seguro ao seu repositório deverá criar na sua pasta pessoal a chave pública e a chave privada que irão autenticar seu acesso com o site github.com e permitira a transferência e a manipulação dos arquivos deste repositório.

Para criar as chaves usaremos o comando a seguir:

```
ssh-keygen
```

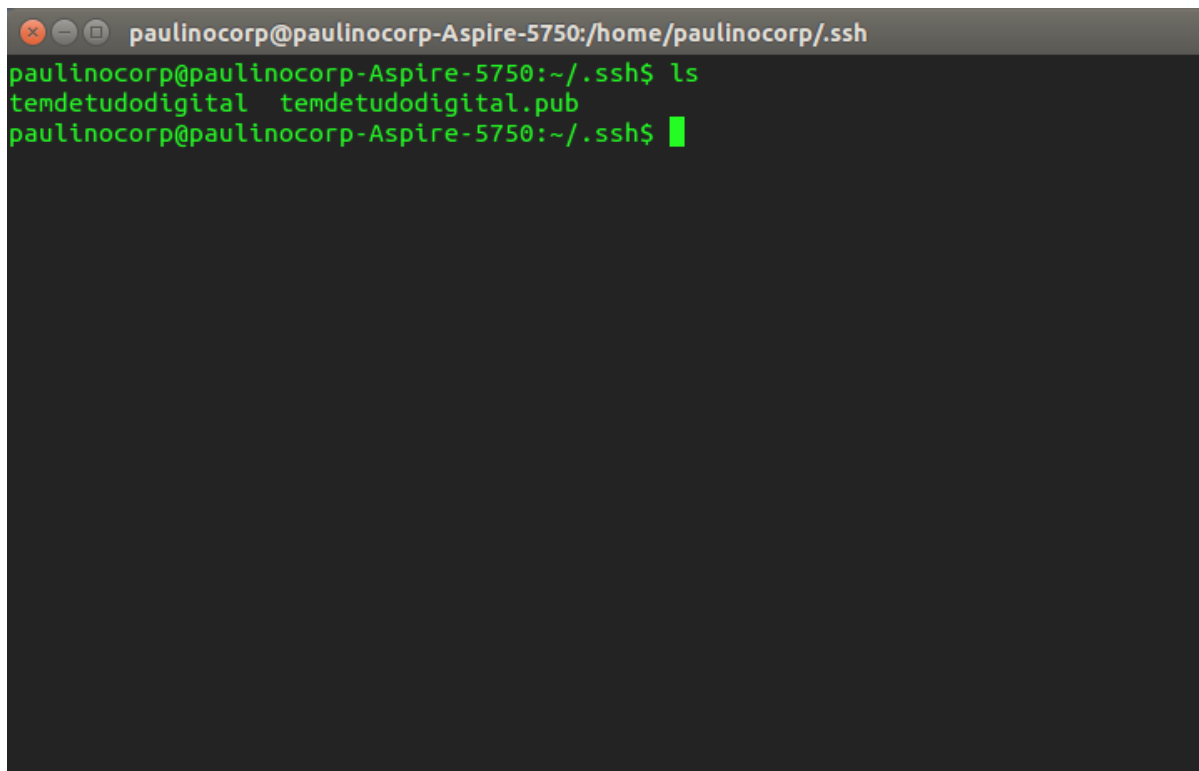
a imagem abaixo mostra esse comando sendo executado:



```
paulinocorp@paulinocorp-Aspire-5750:/home/paulinocorp/.ssh
paulinocorp@paulinocorp-Aspire-5750:~/ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/paulinocorp/.ssh/id_rsa): temdetudodigital
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in temdetudodigital.
Your public key has been saved in temdetudodigital.pub.
The key fingerprint is:
fd:90:38:48:bc:7f:30:b7:2a:d9:fa:0e:e8:67:7d:3c paulinocorp@paulinocorp-Aspire-5750
The key's randomart image is:
+---[RSA 2048]---+
|
|      .
|      o
|     . o o .
|    o S =
|   . . = +
|  . .+.o .
| . =.ooE
| .O.=+ .
+-----+

```

vamos dar uma olhada no arquivos gerados no diretório padrão do linux para chaves assimétricas:

A terminal window with a dark background and green text. The title bar shows 'paulinocorp@paulinocorp-Aspire-5750:/home/paulinocorp/.ssh'. The prompt is 'paulinocorp@paulinocorp-Aspire-5750:~/.ssh\$'. The command 'ls' has been entered, and the output is 'temdetudodigital temdetudodigital.pub'. The prompt is now 'paulinocorp@paulinocorp-Aspire-5750:~/.ssh\$' with a green cursor.

```
paulinocorp@paulinocorp-Aspire-5750:/home/paulinocorp/.ssh
paulinocorp@paulinocorp-Aspire-5750:~/.ssh$ ls
temdetudodigital  temdetudodigital.pub
paulinocorp@paulinocorp-Aspire-5750:~/.ssh$ █
```

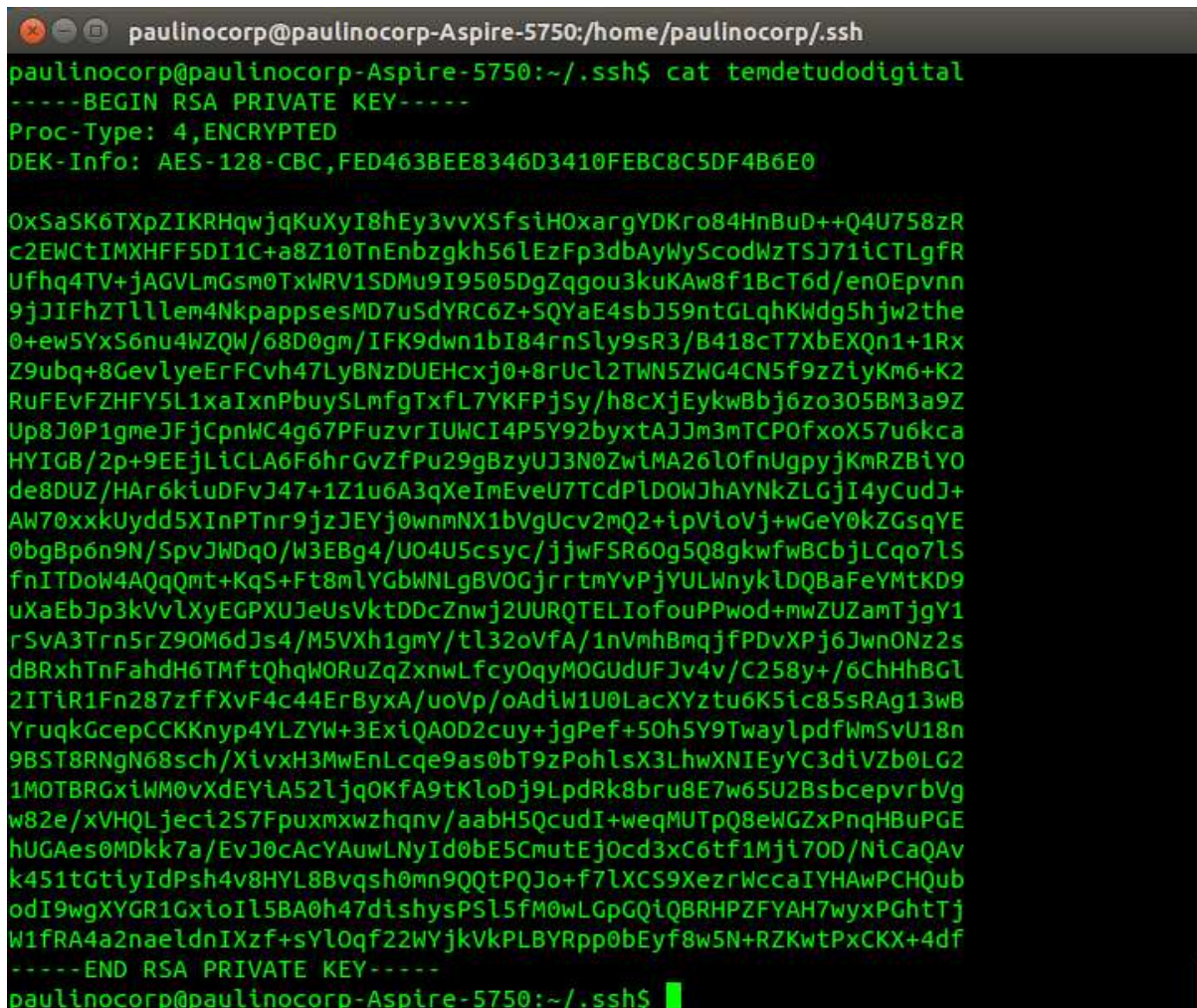
foram criados dois arquivos, um contendo a chave pública, que pode ser distribuída para quem tiver o acesso permitido por você e uma chave privada.

vamos ver o conteúdo desses arquivos:

O conteúdo deste arquivo corresponde à chave privada, para ver seu conteúdo usaremos o comando `cat`:

```
cat temdetudodigital
```

abaixo podemos ver o comando sendo executado:



```
paulinocorp@paulinocorp-Aspire-5750:/home/paulinocorp/.ssh
paulinocorp@paulinocorp-Aspire-5750:~/./.ssh$ cat temdetudodigital
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,FED463BEE8346D3410FEB8C5DF4B6E0

0xSaSK6TXpZIKRHqwjQKuXyI8hEy3vvXSfsiH0xargYDKro84HnBuD++Q4U758zR
c2EWctIMXHFF5DI1C+a8Z10TnEnbzgkh56lEzFp3dbAyWyScodWzTSJ71iCTLgFR
Ufhq4TV+jAGVlmgSm0TxWRV1SDMu9I9505DgZqgou3kuKAw8f1BcT6d/en0Epvnn
9jJIFhZTlllem4NkpappsesMD7uSdYRC6Z+SQYaE4sbJ59ntGLqhKwdg5hjw2the
0+ew5YxS6nu4WZQW/68D0gm/IFK9dwn1bI84rnSly9sR3/B418cT7XbEXQn1+1Rx
Z9ubq+8GevlyeErFCvh47LyBNzDUEHcxj0+8rUcl2TWN5ZWG4CN5f9zZiyKm6+K2
RuFEVfZHFY5L1xaIxnPbuySLmfgTxfL7YKFPjSy/h8cXjEykwBbj6zo305BM3a9Z
Up8J0P1gmeJFjCpnWC4g67PFuzvrIUWCI4P5Y92byxtAJJm3mTCPOfxoX57u6kca
HYIGB/2p+9EEjLiCLA6F6hrGvZfPu29gBzyUJ3N0ZwiMA26lOfnUgpyjKmRZBiYO
de8DUZ/HAR6kiuDFvJ47+1Z1u6A3qXeImEveU7TCdPlDOWJhAYNkZLGjI4yCudJ+
AW70xxkUydd5XInPTnr9jzJEYj0wnmNX1bVgUcv2mQ2+ipVioVj+wGeY0kZGsqYE
0bgBp6n9N/SpvJWDq0/W3EBg4/U04U5csyc/jjwFSR60g5Q8gkwfWBCbjLCqo7LS
fnITDoW4AQqQmt+KqS+Ft8mLYGbWNLgBVOCjrrtmYvPjYULWnykLDQBafEYmTKD9
uXaEbJp3kVvLxyEGPXUJeUsVktDDcZnwj2UURQTELIofouPPwod+mWZUZamTjgY1
rSvA3Trn5rZ90M6dJs4/M5VXh1gmY/tl32oVfA/1nVmhbmqjfpDvXPj6JwnONz2s
dBRxhTnFahdH6TMftQhqW0RuZqZxnwLfcyOqyMOGUdUFJv4v/C258y+/6ChHhBGL
2ITiR1Fn287zffXvF4c44ErByxA/uoVp/oAdiW1U0LacXYztu6K5ic85sRag13WB
YruqkGcepCCKNyp4YLZYW+3ExiQAOD2cuy+jgPef+50h5Y9TwaylpdfWmSvU18n
9BST8RNgN68sch/XivxH3MwEnLcqe9as0bT9zPohlSx3LhwXNIEyYC3diVZb0LG2
1MOTBRGxiWM0vXdEYiA52ljQkFA9tKl0Dj9LpdRk8brU8E7w65U2BsbcervbVg
w82e/xVHQLjeci2S7Fpuxmxwzhqnv/aabH5QcudI+weqMUTpQ8eWGZxPnqHBuPGE
hUGAes0MDkk7a/EvJ0cAcYAuwLNyId0bE5CmutEj0cd3xC6tf1Mji70D/NiCaQAV
k451tGtiyIdPsh4v8HYL8Bvqsh0mn9QQtPQJo+f7LXCS9XezrWccaIYHAWPCHQub
odI9wgXYGR1GxioIl5BA0h47dishysPSl5fM0wLgPQiQBRHPZFYAH7wyxPGhtTj
W1fRA4a2naeldnIXzf+sYlOqf22WYjkVklBYRpp0bEyf8w5N+RZKwtPxCKX+4df
-----END RSA PRIVATE KEY-----
paulinocorp@paulinocorp-Aspire-5750:~/./.ssh$
```

Este arquivo servirá tanto para autenticação da sua máquina no acesso remoto como para decifrar o conteúdo de seus arquivos e torná-los compreensíveis.

Do mesmo modo vamos agora verificar o conteúdo do arquivo `temdetudodigital.pub` que contém a chave pública, para isso utilizaremos o mesmo comando mudando apenas o nome do arquivo:

A imagem abaixo mostra o conteúdo do arquivo *temdetudodigital.pub*:

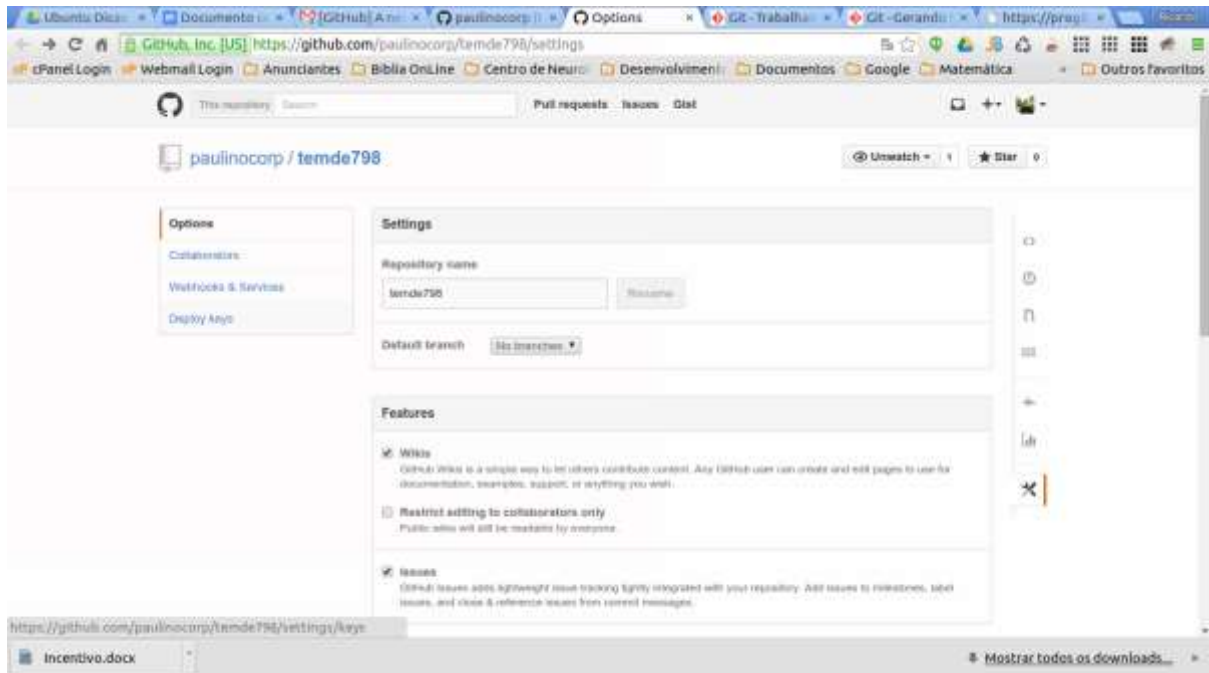
```
paulinocorp@paulinocorp-Aspire-5750:/home/paulinocorp/.ssh$ cat temdetudodigital.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDPXBcdmTRV3sBgfk0m0y1KbWffs7ICMLAvItyN0JUN
PbpUtNuTIyZ2LMgbhL1YR8+/cyza6g90gRcEkWwmJeUmEXPbYq8z4drMVrtBFHOL40sUQdmgApVW8wA
En6mUmnoVa4DNLEfsJJ5FFyI+bmzC7dBeVPcazH0L98v4oTLkd//f2GTk00DU65II9d7sd6398zt6HQU
YeolcMSCoxzRXinaOfx9Bj9uGkFNM2sR14hvYwK2ew7R0eF9GhUFSiB045T4H0RIg+qbq1C8bWU/fiRv
4k4XcY592/Inmz900VTDK0I/IL8siZQM5Iy5MNFkd9TwXpI/yeG3X4rkBAqj paulinocorp@paulino
corp-Aspire-5750
paulinocorp@paulinocorp-Aspire-5750:~/ssh$ █
```

Nesta fase, geradas as chaves deveremos incluir a chave pública no site do *git*, o github.

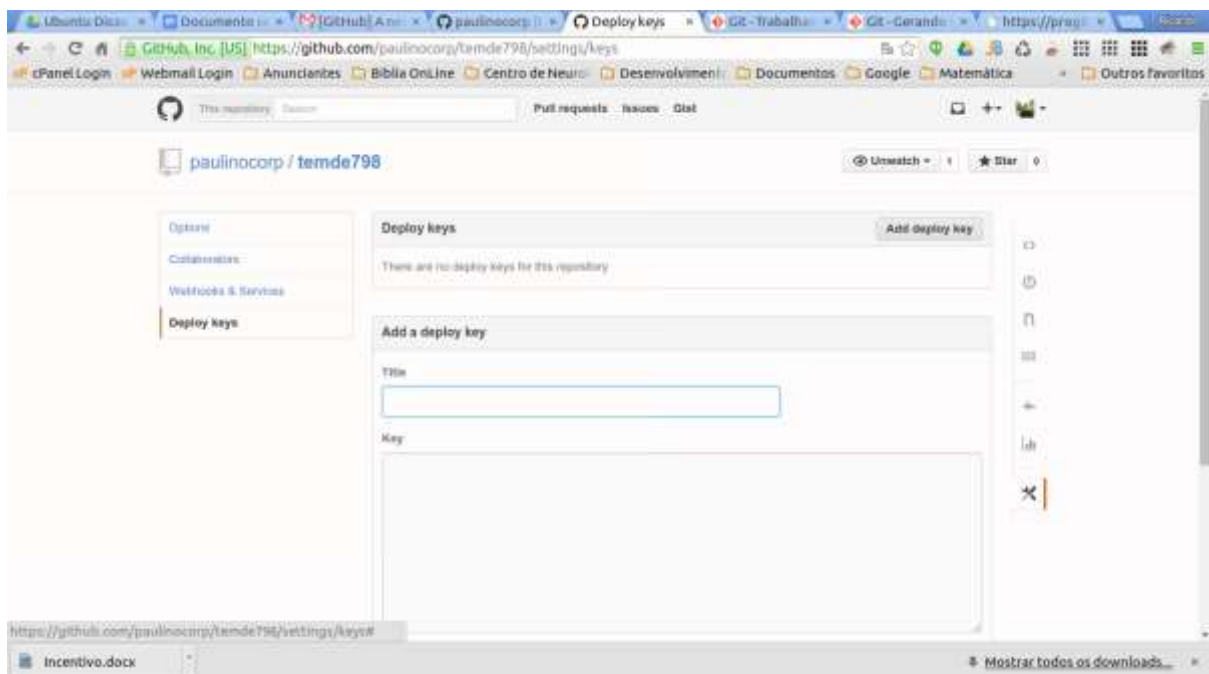
The screenshot shows the GitHub profile page for Ricardo Paulino (paulinocorp). The page includes a profile picture, name, and email address. A dropdown menu is open, showing options like 'Signed in as paulinocorp', 'Your profile', 'Your alerts', 'Explore', 'Help', 'Settings', and 'Sign out'. The 'Settings' option is highlighted. Below the profile information, there are sections for 'Popular repositories' (listing 'ajax-file-upload' and 'temdet798') and a 'Contributions' graph. The graph shows a grid of colored squares representing contributions over time. At the bottom, there is a message about a quick guide for creating a repository.



Entrando em *setins* encontraremos a opção **deploy keys**:

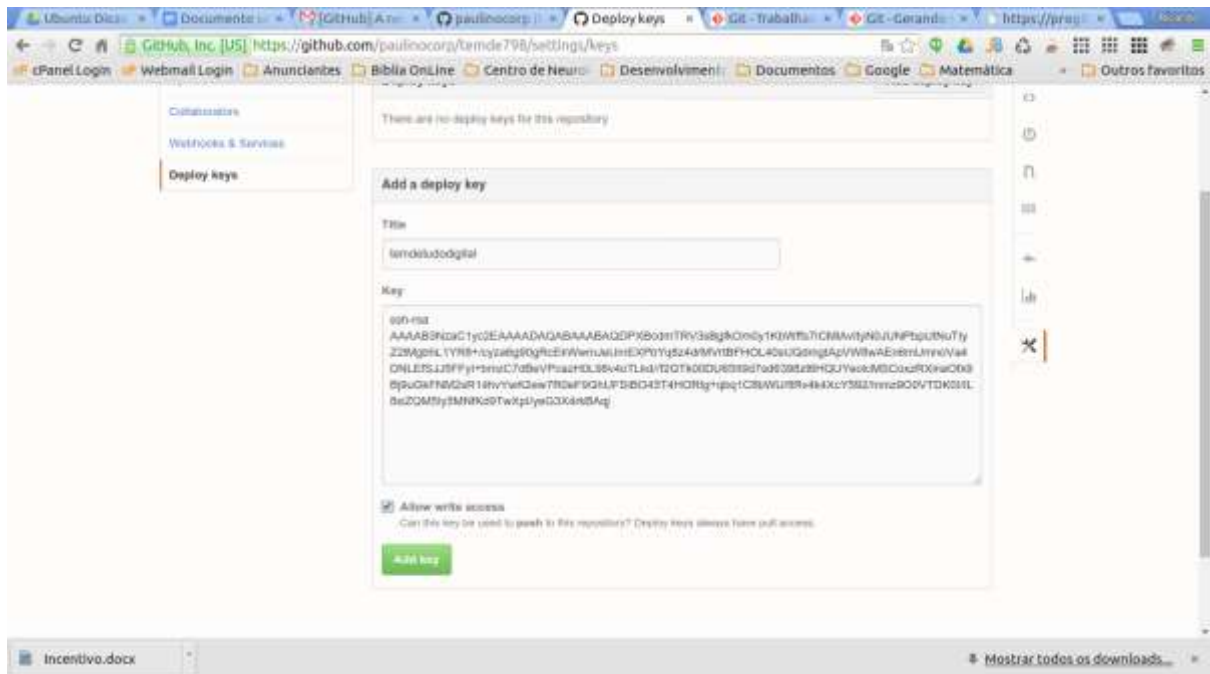


Ao clicarmos com o *mouse* nesta opção aparecerá a tela a seguir:

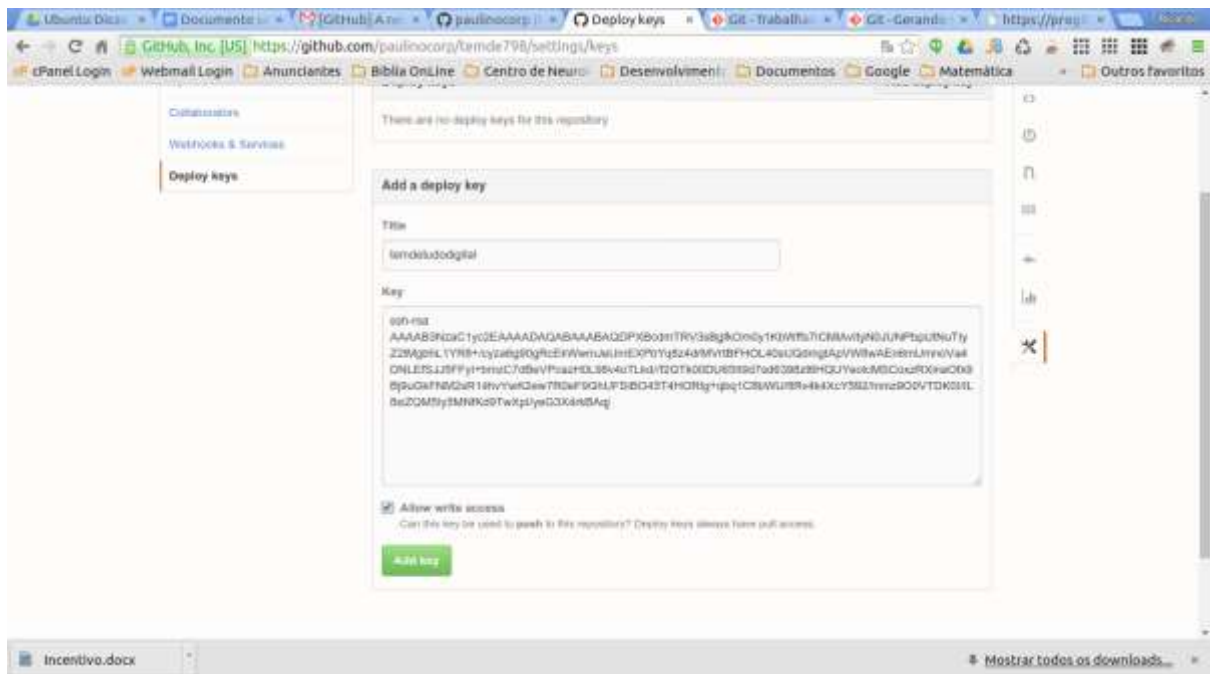


Devemos clicar no botão **Add deploy key** e depois no campo **title** colocar o título para o repositório e no campo **key** o conteúdo da chave pública.





Veremos na próxima página apresentada pelo site **github** que a nossa chave primária foi incluída com sucesso no site.



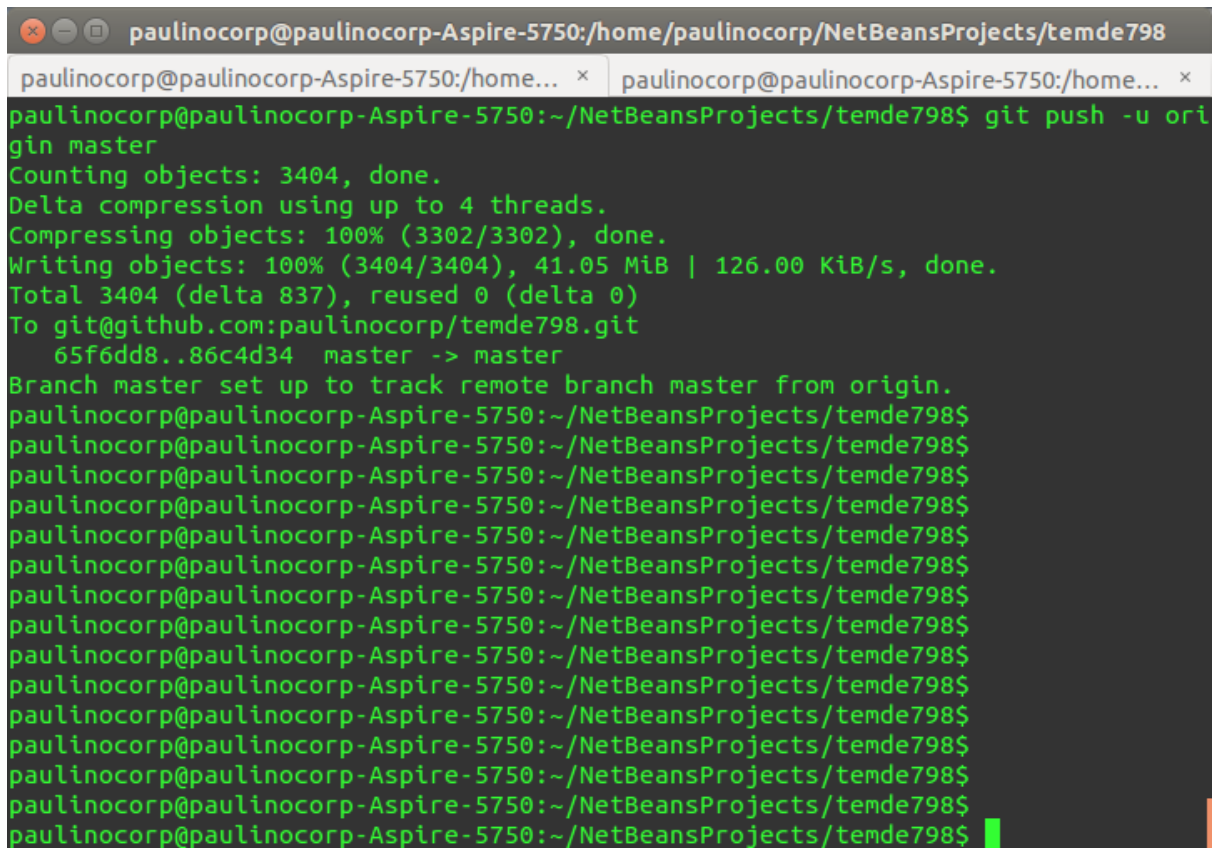
Isto tudo serve para garantir o acesso ao nosso repositório ponde enviá-lo, modificá-lo, importá-lo, fazer *clonagem* bem como purgá-lo.



```
paulinocorp@paulinocorp-Angira-5790:~/NetBeansProjects/temde798$ git add --all
warning: CRLF will be replaced by LF in articles/02-03-13/error_log.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in articles/02-12-13/error_log.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in articles/02-12-13/error_log.bkp.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in articles/05-08-13/error_log.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in articles/05-08-13/error_log.bkp.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in articles/07-07-13/error_log.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in articles/13-08-13/error_log.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in articles/16-08-13/error_log.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in articles/24-05-13/error_log.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in articles/24-08-13/error_log.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in articles/24-08-13/error_log.bkp.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in articles/25-08-13/error_log.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in articles/25-04-13/error_log.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in db/mysql-connector-java-5.1.29/README.txt.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in db/mysql-connector-java-5.1.29/doc/README.txt.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in db/mysql-connector-java-5.1.29/src/doc/sources/pon.xml.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in email/contact.php.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in js/A Mac OS X-style Dock In Javascript_files/MacstyleDock.compressed.js.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in js/A Mac OS X-style Dock In Javascript_files/shared.css.
The file will have its original line endings in your working directory.
warning: CRLF will be replaced by LF in js/Mac-style Dock Demonstration_files/MacstyleDock.compressed.js.
The file will have its original line endings in your working directory.
```

Um outro meio de exportar, verificar e atualizar o repositório é através dos seguintes comandos:

```
git remote add origin git@github.com:paulinocorp/temde798.git
git push -u origin master
```

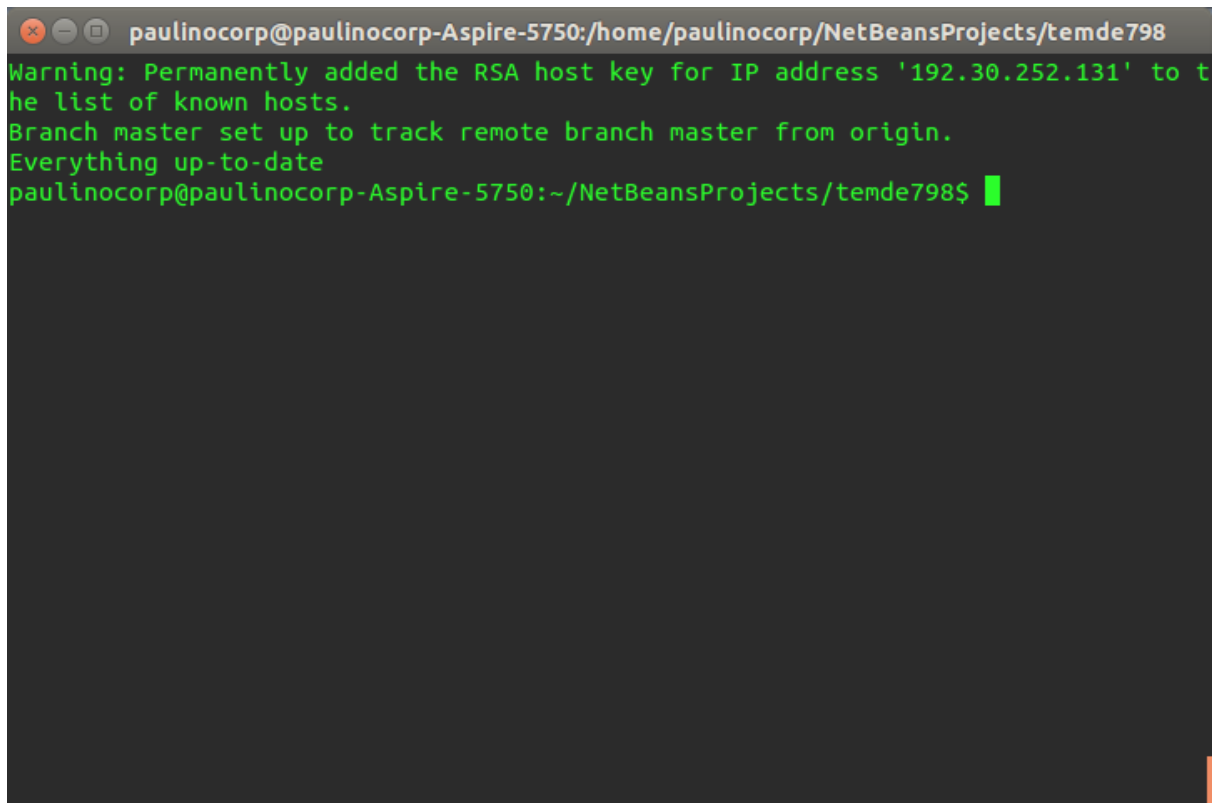
A terminal window screenshot showing the execution of a git push command. The terminal output includes: 'Counting objects: 3404, done.', 'Delta compression using up to 4 threads.', 'Compressing objects: 100% (3302/3302), done.', 'Writing objects: 100% (3404/3404), 41.05 MiB | 126.00 KiB/s, done.', 'Total 3404 (delta 837), reused 0 (delta 0)', 'To git@github.com:paulinocorp/temde798.git', '65f6dd8..86c4d34 master -> master', and 'Branch master set up to track remote branch master from origin.' The terminal prompt is green on a black background.

```
paulinocorp@paulinocorp-Aspire-5750:/home/paulinocorp/NetBeansProjects/temde798
paulinocorp@paulinocorp-Aspire-5750:/home... x paulinocorp@paulinocorp-Aspire-5750:/home... x
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$ git push -u ori
gin master
Counting objects: 3404, done.
Delta compression using up to 4 threads.
Compressing objects: 100% (3302/3302), done.
Writing objects: 100% (3404/3404), 41.05 MiB | 126.00 KiB/s, done.
Total 3404 (delta 837), reused 0 (delta 0)
To git@github.com:paulinocorp/temde798.git
 65f6dd8..86c4d34 master -> master
Branch master set up to track remote branch master from origin.
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$
```

Atualizamos o repositório com o seguinte comando executado no diretório raiz de nosso projeto conforme a imagem acima:

```
git push -u origin master
```

Se executarmos o comando novamente veremos que o **git** retornará a mensagem de que os arquivos estão atualizados.

A terminal window screenshot with a dark background and green text. The window title is 'paulinocorp@paulinocorp-Aspire-5750:/home/paulinocorp/NetBeansProjects/temde798'. The terminal output shows the following text: 'Warning: Permanently added the RSA host key for IP address '192.30.252.131' to the list of known hosts.', 'Branch master set up to track remote branch master from origin.', and 'Everything up-to-date'. The prompt is 'paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798\$' followed by a green cursor bar.

```
paulinocorp@paulinocorp-Aspire-5750:/home/paulinocorp/NetBeansProjects/temde798
Warning: Permanently added the RSA host key for IP address '192.30.252.131' to t
he list of known hosts.
Branch master set up to track remote branch master from origin.
Everything up-to-date
paulinocorp@paulinocorp-Aspire-5750:~/NetBeansProjects/temde798$ █
```

O **git** informa que os dados estão atualizados.

Caros amigos leitores, espero que com este simples artigo tenha atingido o objetivo de lhes trazer algo de útil.