LDAP (389-DS)

Instalación, Configuración y Acceso

Instalación del servidor

Instalación del servidor

```
# apt install 389-ds
# dscreate interactive
```

```
root@bravo:~# dscreate interactive
Install Directory Server (interactive mode)
===========================================
selinux is disabled, will not relabel ports or files.

Selinux support will be disabled, continue? [yes]:

Enter system's hostname [bravo.sivigo.site]:

Enter the instance name [bravo]:

Enter port number [389]:

Create self-signed certificate database [yes]: no

Enter Directory Manager DN [cn=Directory Manager]:

Enter the Directory Manager password:
Confirm the Directory Manager Password:

Enter the database suffix (or enter "none" to skip) [dc=bravo,dc=sivigo,dc=site]:

Create sample entries in the suffix [no]: yes

Do you want to start the instance after the installation? [yes]:

Are you ready to install? [no]: yes
Starting installation ...
Validate installation settings ...
Create file system structures ...
selinux is disabled, will not relabel ports or files.
Create database backend: dc=bravo,dc=sivigo,dc=site ...
Perform post-installation tasks ...
Completed installation for instance: slapd-bravo
root@bravo:~#
```

Alta de usuarios

Creación de cuentas y ajuste de contraseña

```
# dsidm acme user create
```

```
root@bravo:~# dsidm bravo user create
Enter password for cn=Directory Manager on ldap://bravo.sivigo.site:
Enter value for uid : bob
Enter value for cn : bob
Enter value for displayName : Bob Esponja
Enter value for uidNumber : 1101
Enter value for gidNumber : 1101
Enter value for homeDirectory : /home/bob
Successfully created bob
root@bravo:~# _
```

Introducir datos:

- Identificador de usuario (uid)
- Nombre (cn)
- Nombre representativo (displayName)
- Número de usuario (uidNumber)
- Número de grupo (gidNumber)
- Carpeta “home” (homeDirectory)

Establecimiento de contraseña

```
# dsidm acme account reset_password uid=alice,ou=people,dc=acme,dc=com
```

```
root@bravo:~# dsidm bravo account reset_password uid=alice,ou=people,dc=bravo,dc=sivigo,dc=site
Enter password for cn=Directory Manager on ldap://bravo.sivigo.site:
Enter new password for uid=alice,ou=people,dc=bravo,dc=sivigo,dc=site :
CONFIRM - Enter new password for uid=alice,ou=people,dc=bravo,dc=sivigo,dc=site :
reset password for uid=alice,ou=people,dc=bravo,dc=sivigo,dc=site
root@bravo:~# _
```

Gestión de usuarios

Alta de usuario:

```
# dsidm acme user create
```

Establecimiento de contraseña:

```
# dsidm acme account reset_password uid=alice,ou=people,dc=acme,dc=com
```

Modificar algún dato del usuario:

```
# dsidm acme user modift alice “replace:displayName:Alice Cooper”
```

Baja de usuario:

```
# dsidm acme user delete uid=alice,ou=people,dc=acme,dc=com
```

Configuración del cliente

Instalación del software (Debian y compatibles)

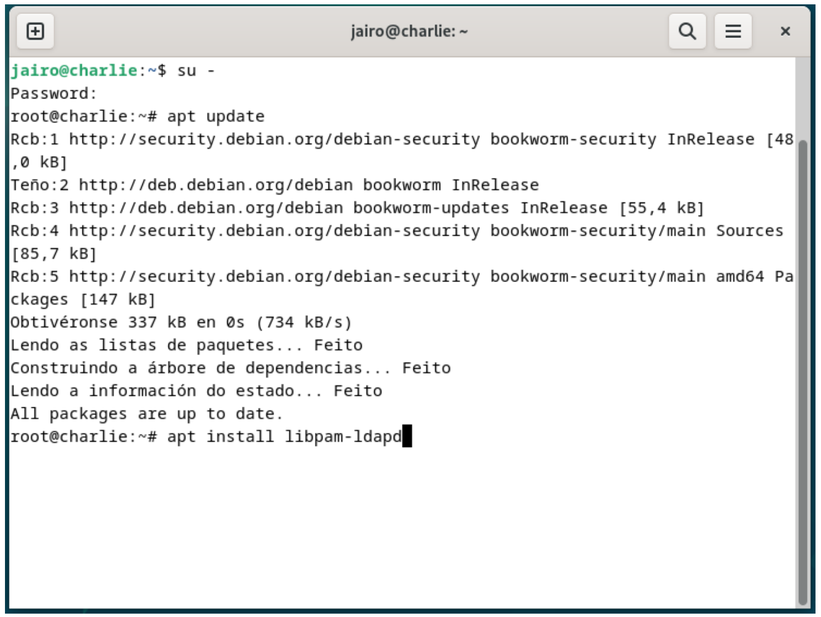
```
# apt update
# apt install libpam-ldapd
```

- LDAP server URI:
  Ejemplo: *ldap://bravo.sivigo.site*
  (Es posible que haya que configurar /etc/hosts)

- LDAP search base:
  Ejemplo: *ou=people,dc=bravo,dc=sivigo,dc=site*

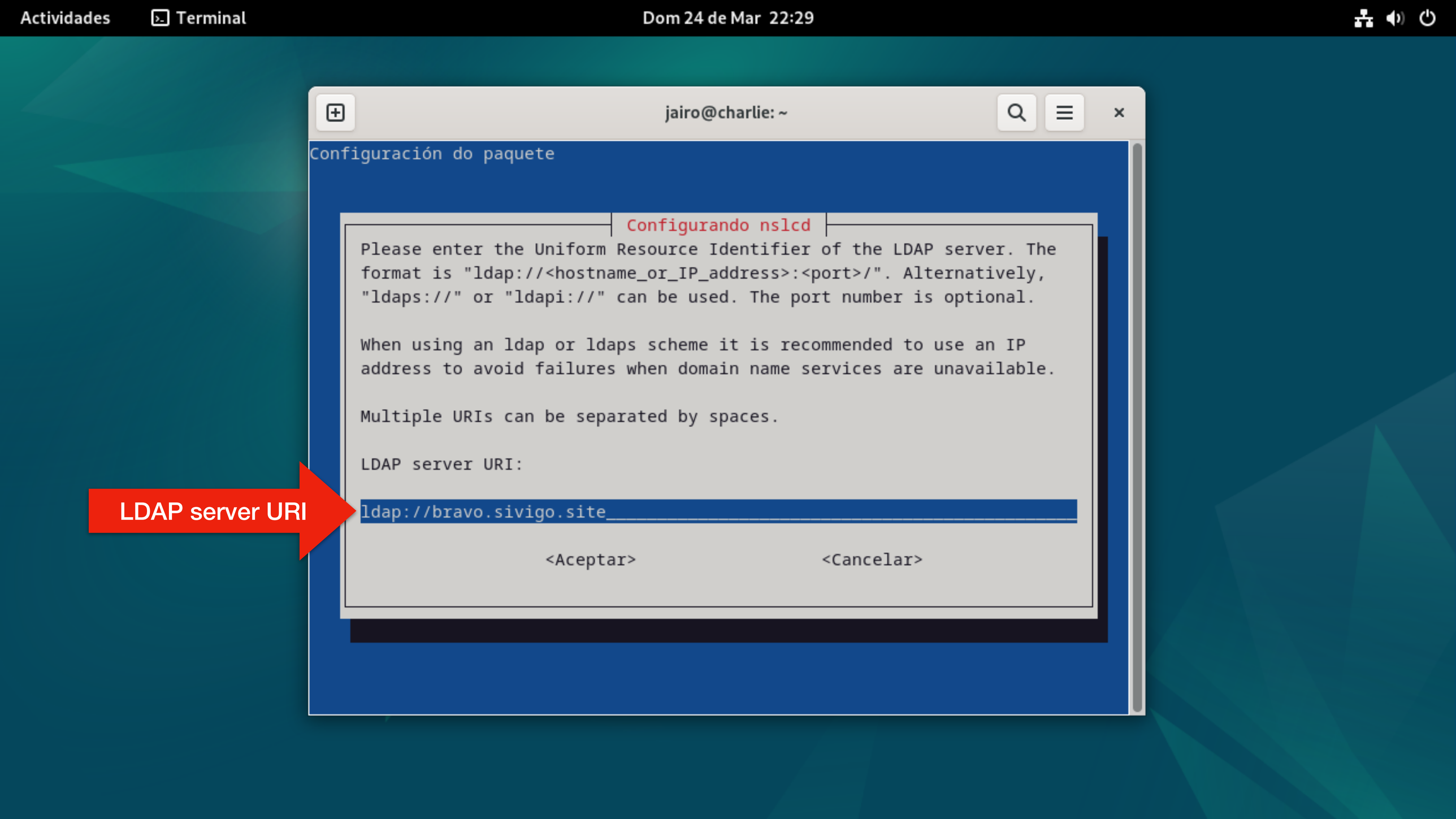
- LDAP authentication: **simple**

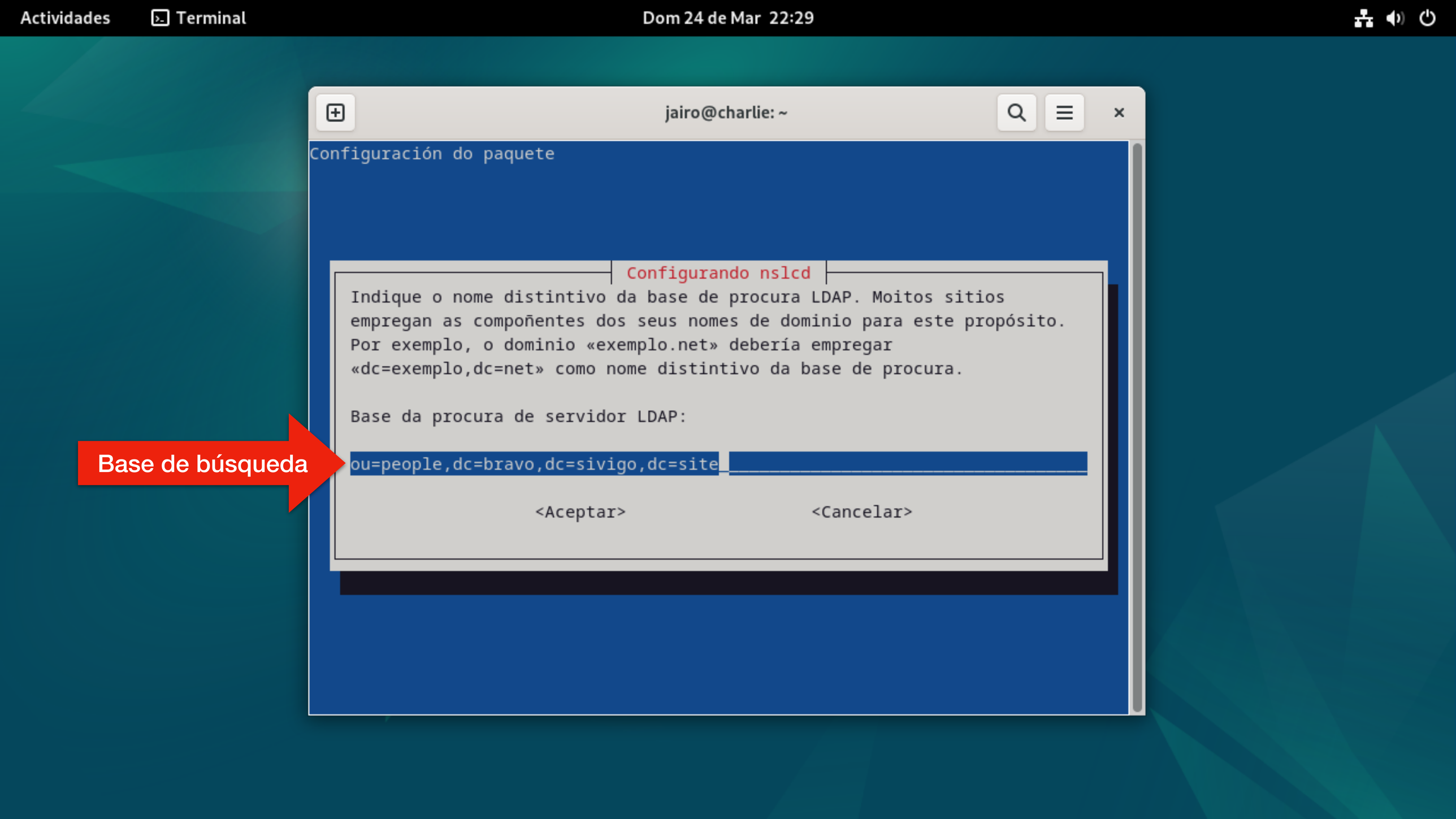
- (SSL cert: **none** si no hay SSL, **demand** en caso de haberlo)

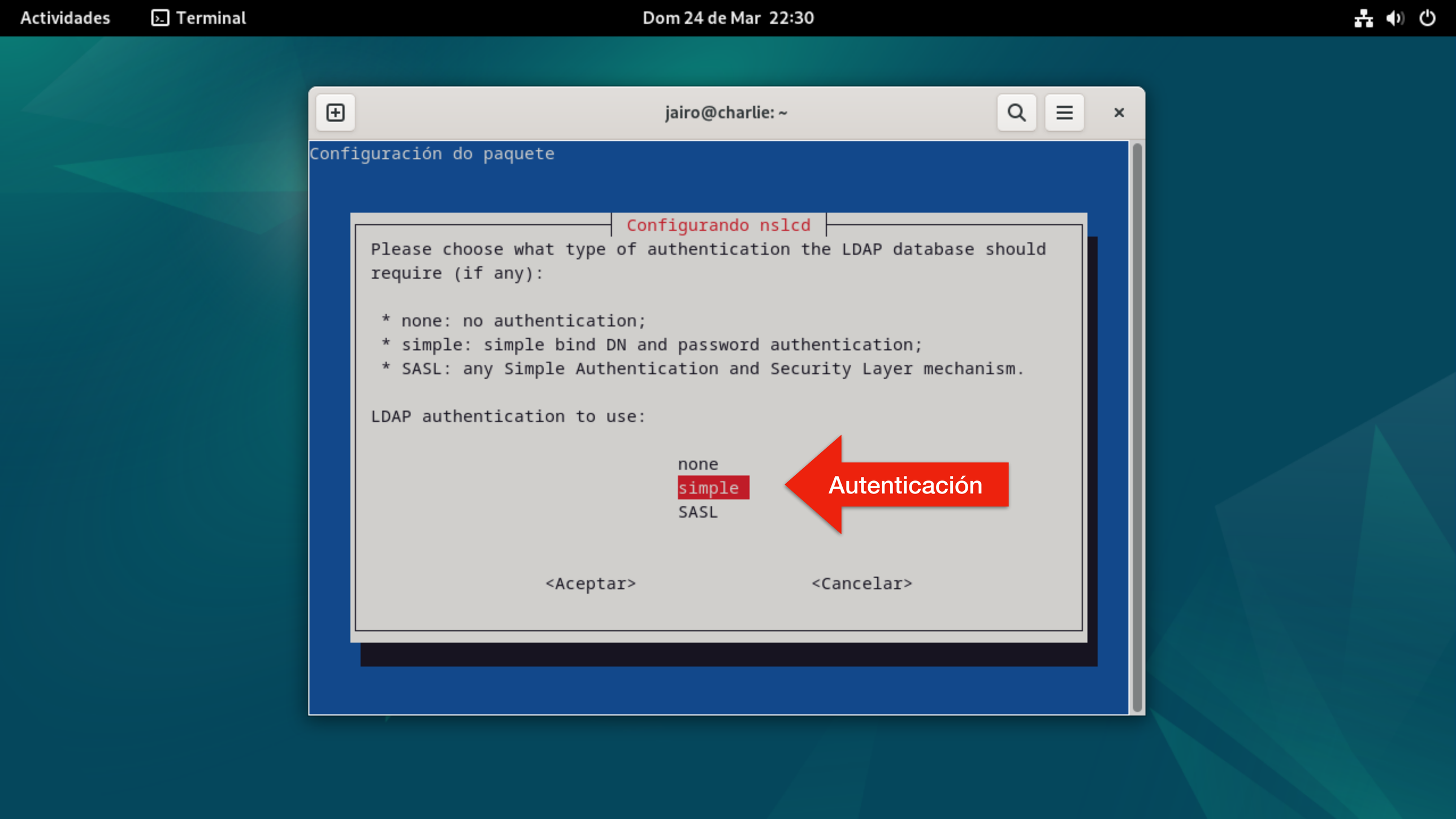


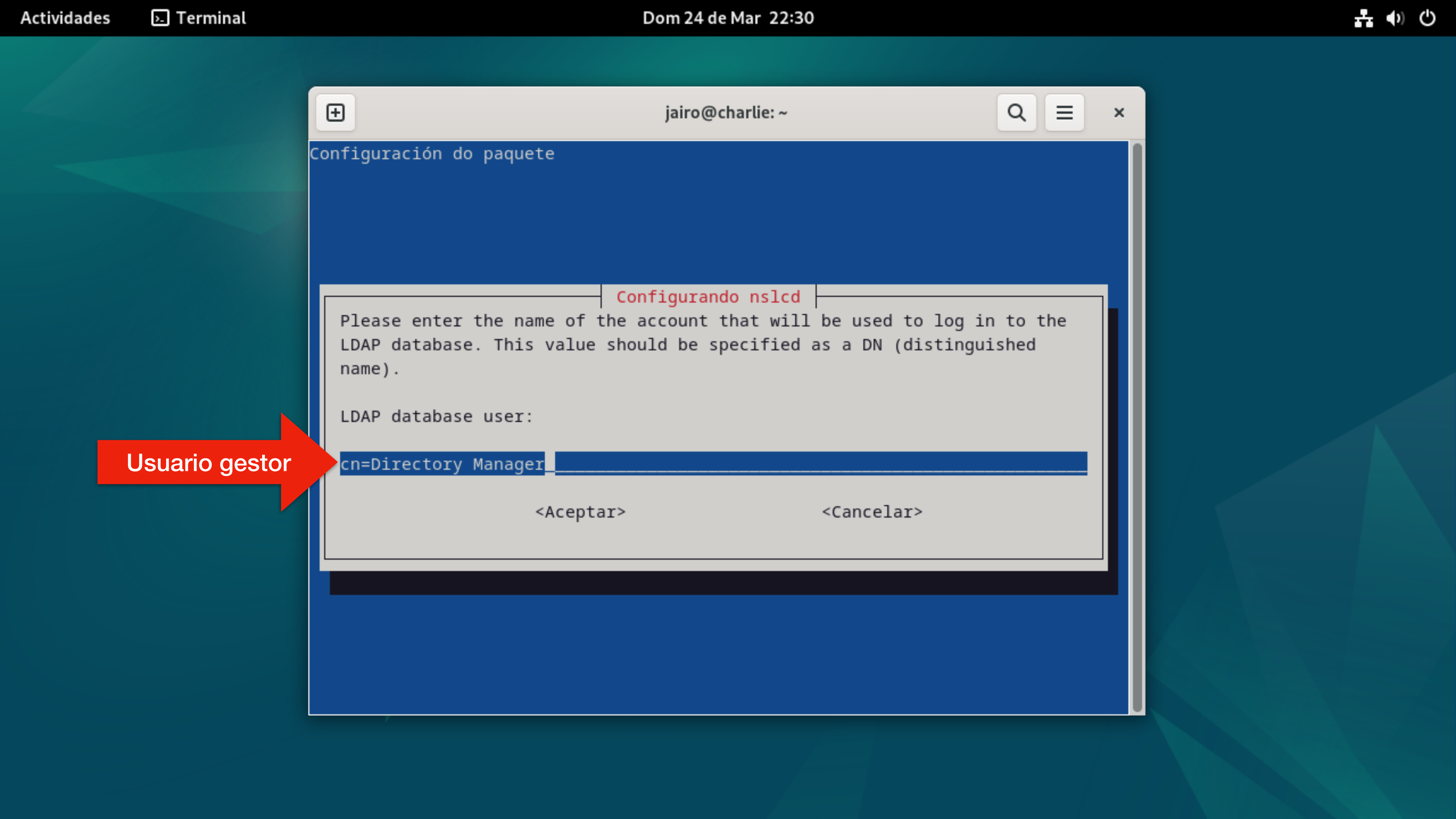
En caso de error o cambios, se puede volver a configurar con:

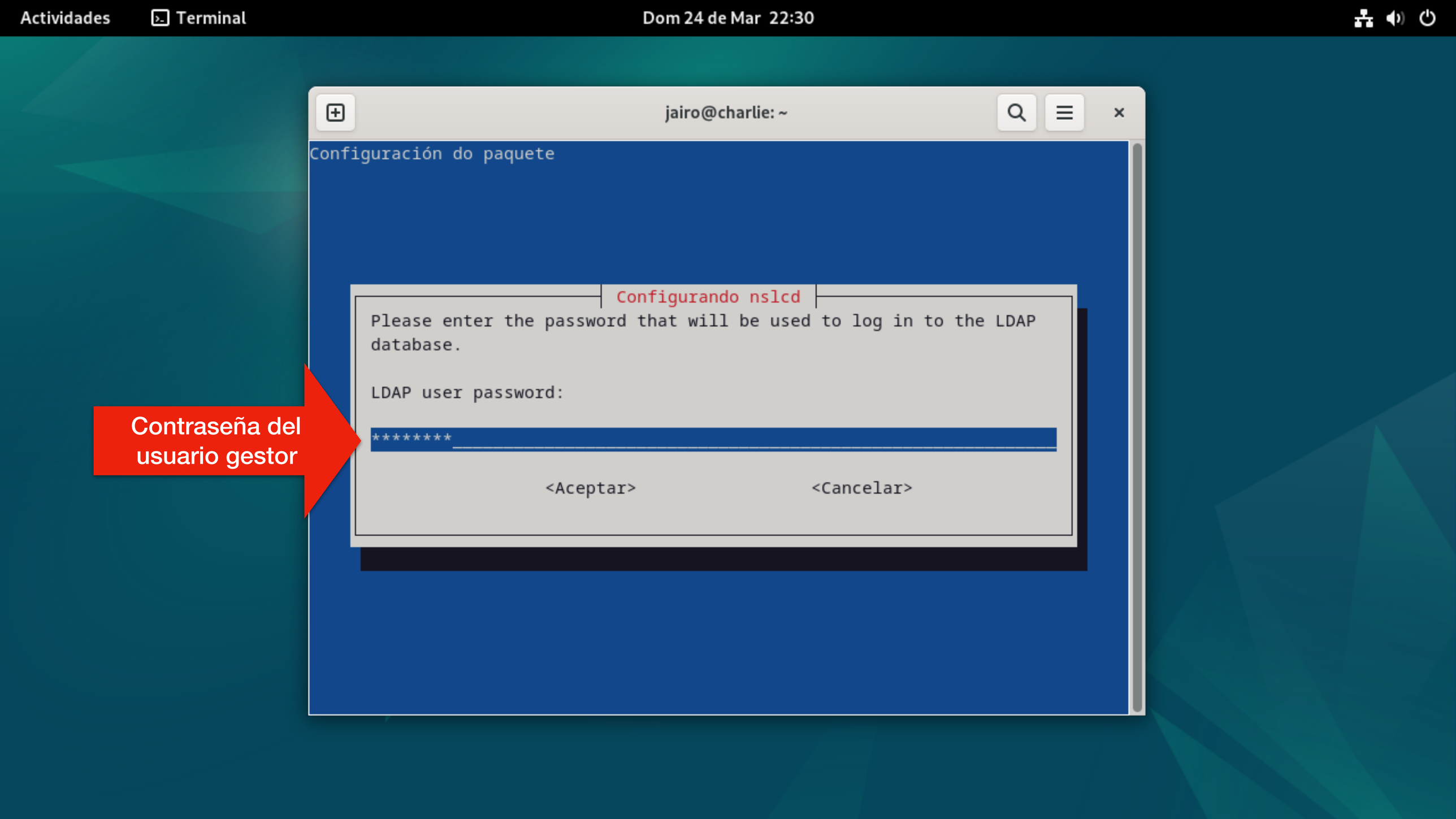
```
dpkg-reconfigure nslcd
dpkg-reconfigure libnss-ldapd
```

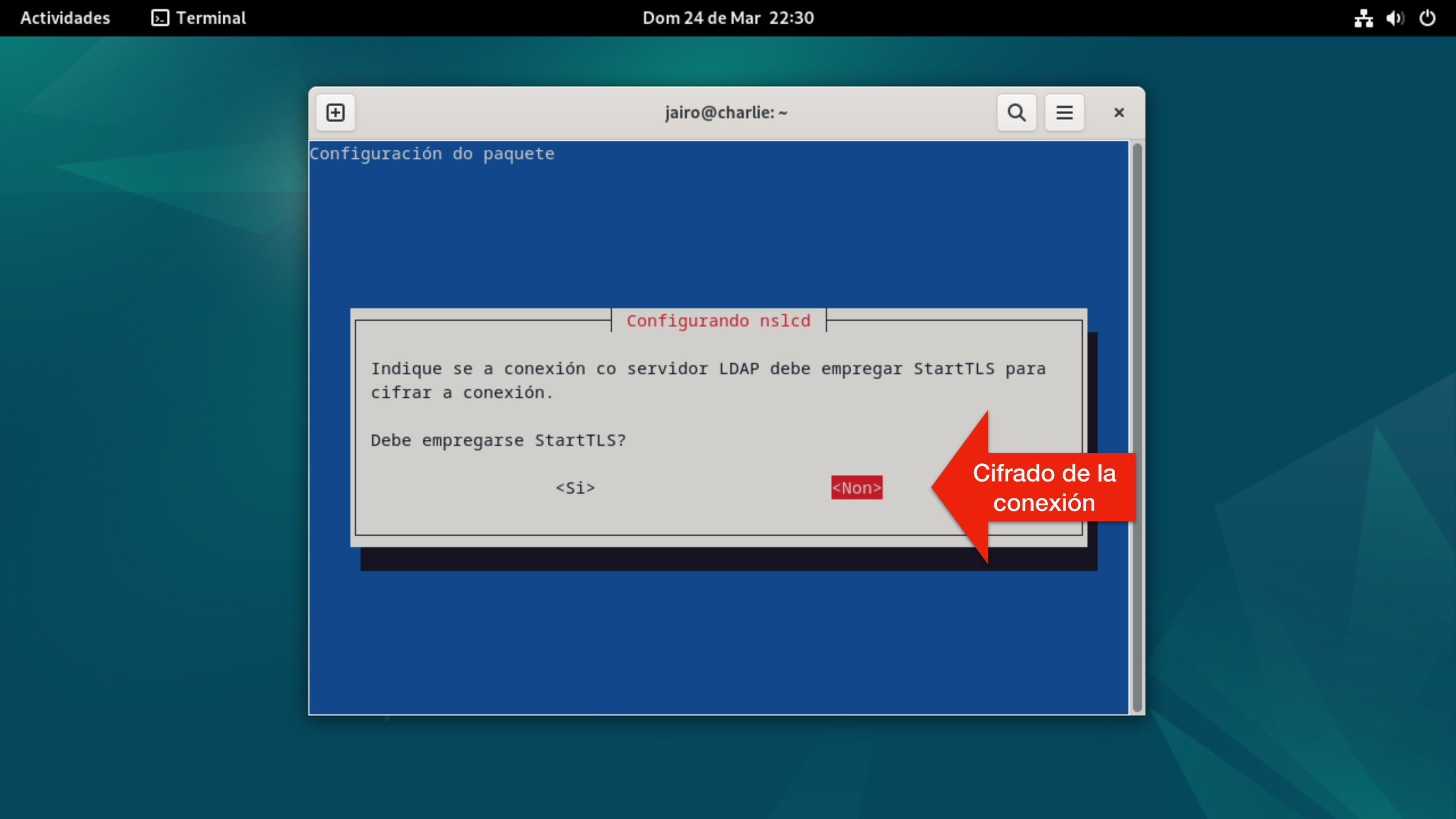

Actividades
Terminal
Dom 24 de Mar 22:29
jairo@charlie: ~
Configuración do paquete
Configurando nslcd
Please enter the Uniform Resource Identifier of the LDAP server. The format is "ldap://<hostname_or_IP_address>:<port>/". Alternatively, "ldaps://" or "ldapi://" can be used. The port number is optional.
When using an ldap or ldaps scheme it is recommended to use an IP address to avoid failures when domain name services are unavailable.
Multiple URIs can be separated by spaces.
LDAP server URI:
ldap://bravo.sivigo.site
<Aceptar>
<Cancelar>
LDAP server URI

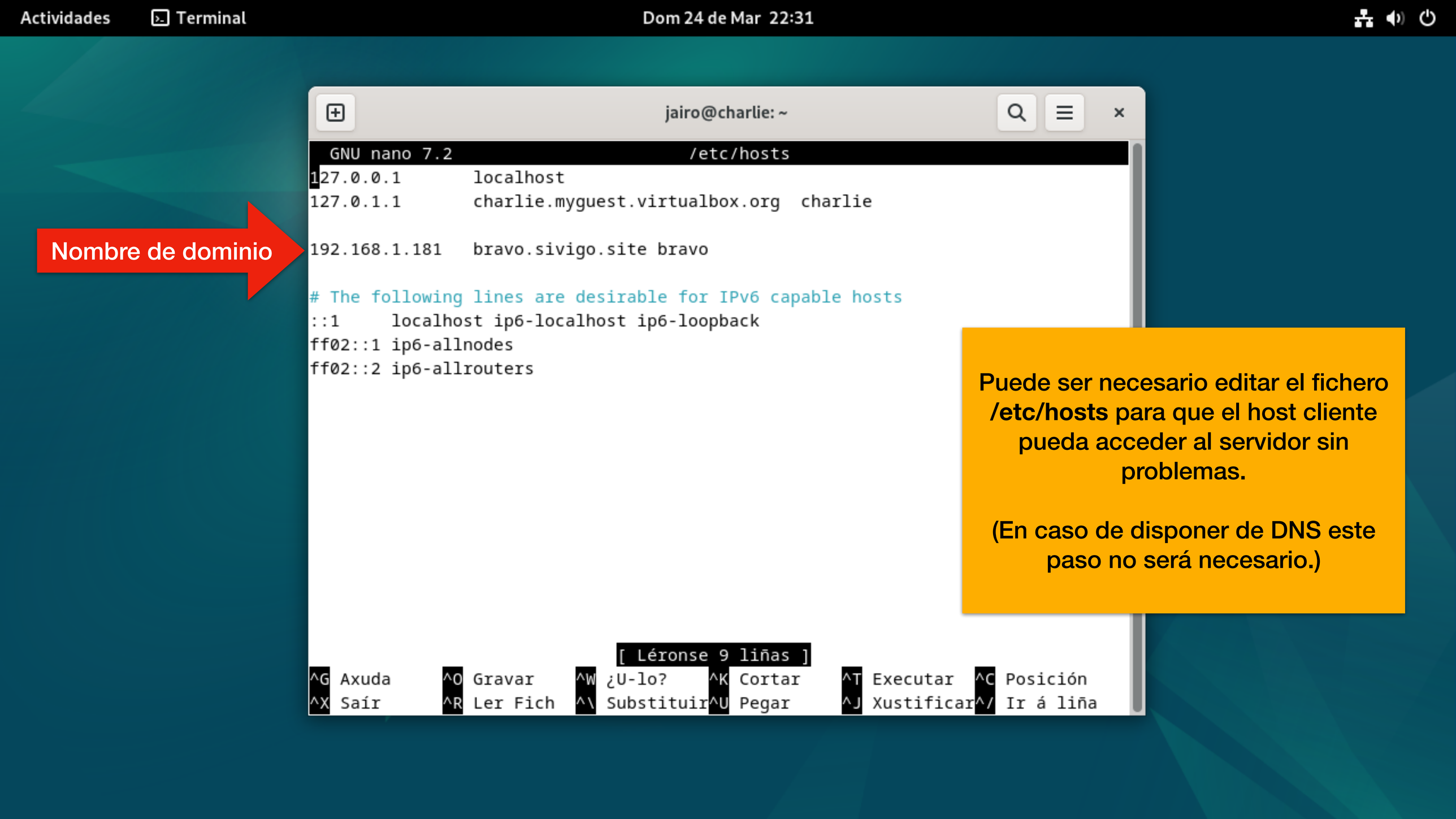

Actividades
Terminal
Dom 24 de Mar 22:29
jairo@charlie: ~
Configuración do paquete
Configurando nslcd
Indique o nome distintivo da base de procura LDAP. Moitos sitios
empregan as compoñentes dos seus nomes de dominio para este propósito.
Por exemplo, o dominio «exemplo.net» debería empregar
«dc=exemplo,dc=net» como nome distintivo da base de procura.
Base da procura de servidor LDAP:
ou=people,dc=bravo,dc=sivigo,dc=site
<Aceptar>
<Cancelar>
Base de búsqueda


Actividades
Terminal
Dom 24 de Mar 22:30
jairo@charlie: ~
Configuración do paquete
Configurando nslcd
Please choose what type of authentication the LDAP database should require (if any):
* none: no authentication;
* simple: simple bind DN and password authentication;
* SASL: any Simple Authentication and Security Layer mechanism.
LDAP authentication to use:
none
simple
SASL
Autenticación
<Aceptar>
<Cancelar>


Actividades
Terminal
Dom 24 de Mar 22:30
jairo@charlie: ~
Configuración do paquete
Configurando nslcd
Please enter the name of the account that will be used to log in to the LDAP database. This value should be specified as a DN (distinguished name).
LDAP database user:
cn=Directory Manager
<Aceptar>
<Cancelar>
Usuario gestor


Actividades
Terminal
Dom 24 de Mar 22:30
jairo@charlie: ~
Configuración do paquete
Configurando nslcd
Please enter the password that will be used to log in to the LDAP database.
LDAP user password:
****
<Aceptar>
<Cancelar>
Contraseña del usuario gestor


Actividades
Terminal
Dom 24 de Mar 22:30
jairo@charlie: ~
Configuración do paquete
Configurando nslcd
Indique se a conexión co servidor LDAP debe empregar StartTLS para cifrar a conexión.
Debe empregarse StartTLS?
<Si>
<Non>
Cifrado de la conexión


Actividades
Terminal
Dom 24 de Mar 22:31
jairo@charlie: ~
GNU nano 7.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 charlie.myguest.virtualbox.org charlie
192.168.1.181 bravo.sivigo.site bravo
The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
[Léronse 9 liñas]
^G Axuda ^O Gravar ^W ¿U-lo? ^K Cortar ^T Executar ^C Posición
^X Saír ^R Ler Fich ^\ Substituir ^U Pegar ^J Xustificar ^/ Ir á liña
Nombre de dominio
Puede ser necesario editar el fichero /etc/hosts para que el host cliente pueda acceder al servidor sin problemas.
(En caso de disponer de DNS este paso no será necesario.)

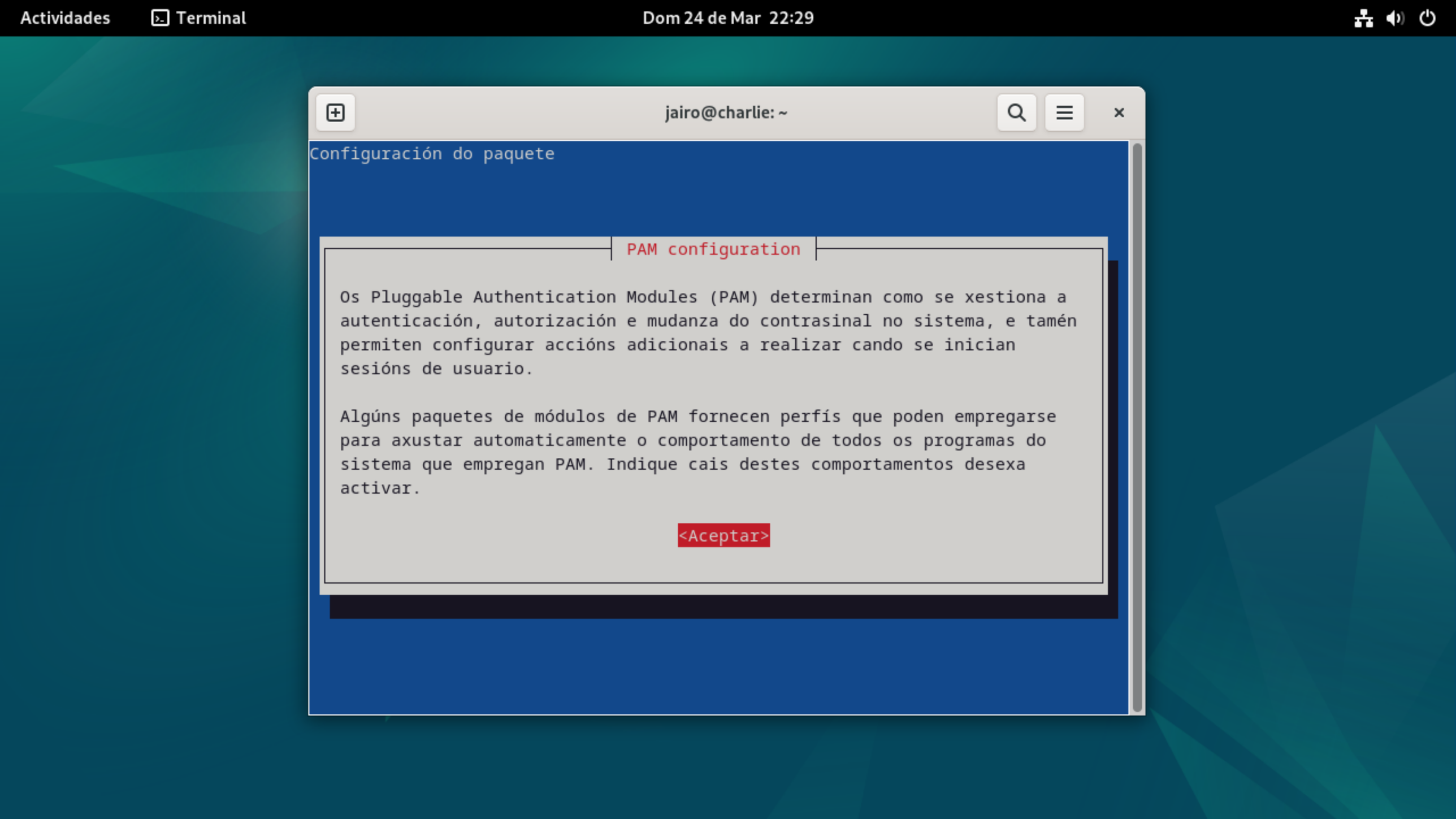
Configuración del login

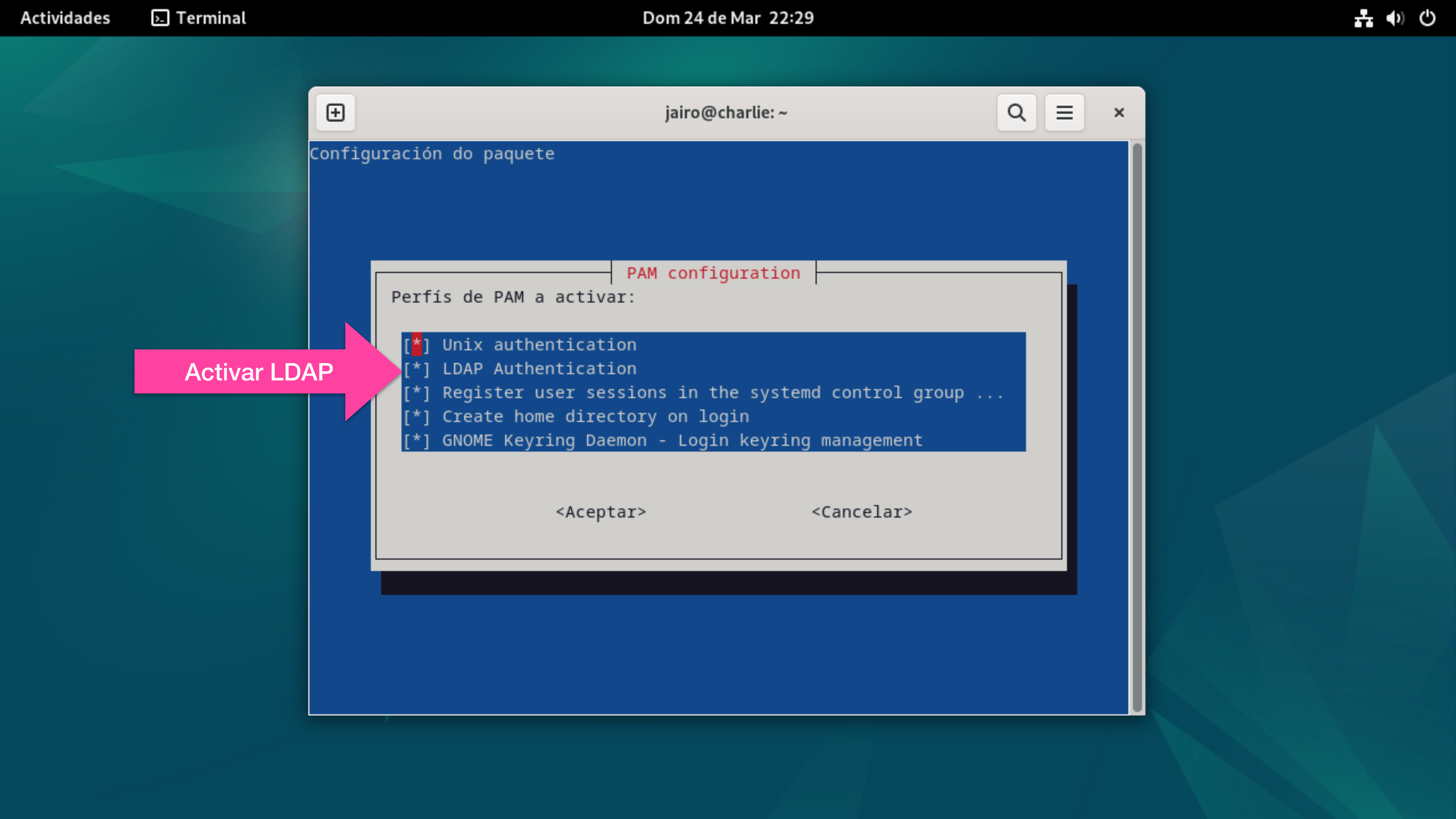
```
# pam-auth-update
```

Activar:

- LDAP
- Crear directorios home

```
# systemctl restart nscd.service nslcd.service
```


Actividades
Terminal
Dom 24 de Mar 22:29
jairo@charlie: ~
Configuración do paquete
PAM configuration
Os Pluggable Authentication Modules (PAM) determinan como se xestiona a autenticación, autorización e mudanza do contrasinal no sistema, e tamén permiten configurar accións adicionais a realizar cando se inician sesións de usuario.
Algúns paquetes de módulos de PAM fornecen perfís que poden empregarse para axustar automaticamente o comportamento de todos os programas do sistema que empregan PAM. Indique cais destes comportamentos desexa activar.
<Aceptar>


Actividades
Terminal
Dom 24 de Mar 22:29
jairo@charlie: ~
Configuración do paquete
PAM configuration
Perfís de PAM a activar:
[*] Unix authentication
[*] LDAP Authentication
[*] Register user sessions in the systemd control group ...
[*] Create home directory on login
[*] GNOME Keyring Daemon - Login keyring management
<Aceptar>
<Cancelar>
Activar LDAP

Pruebas

Verificación del servicio

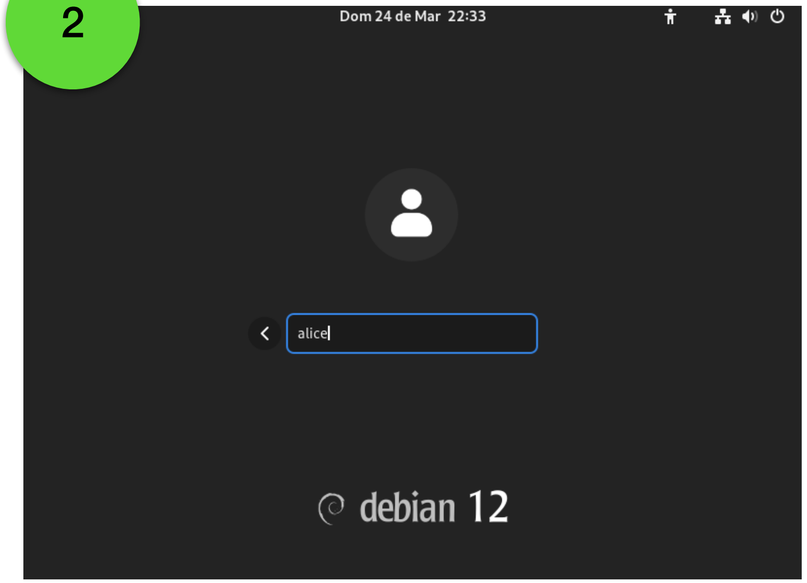
```
> ldapwhoami -H ldap://acme.com -D uid=alice,ou=people,dc=acme,dc=com -W -x
```

```
# login
```

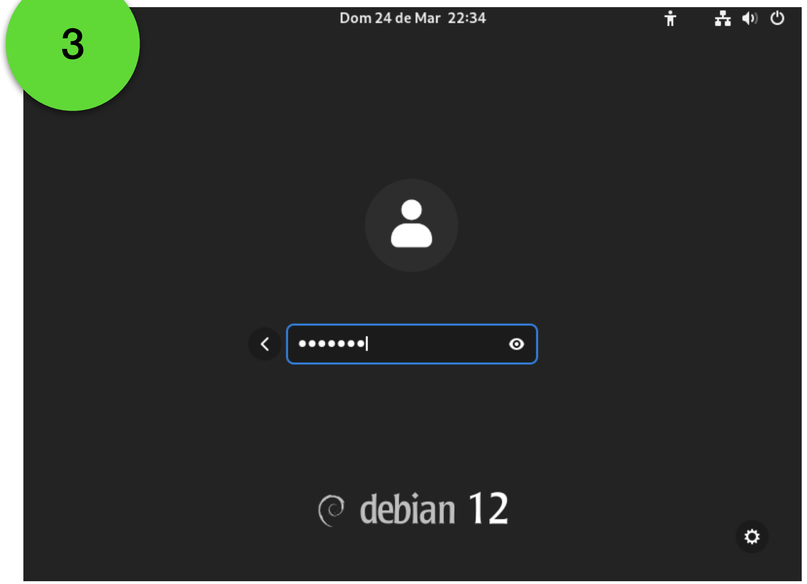
1


Dom 24 de Mar 22:35
jairo
alice
bob
Non está na lista?
Acceder aquí
debian 12

2


Dom 24 de Mar 22:33
alice
debian 12

3


Dom 24 de Mar 22:34
debian 12

Referencias

- “389 Directory Server - Quick Start”
  https://www.port389.org/docs/389ds/howto/quickstart.html
- “389 Directory Server - Howto: Install 389 Directory Server”
  https://www.port389.org/docs/389ds/howto/howto-install-389.html
- “389 Directory Server - Howto: Users and Groups”
  https://www.port389.org/docs/389ds/howto/howto-users-and-groups.html
- “LDAP-login on Debian 11/12”
  https://www.flofaber.com/log/debian-ldap-auth