ANEXOS

ANEXO A: Salida en pantalla de comandos Linux

A continuación presentamos la salida de los comandos importantes para la administración y verificación de la salud de un servidor Linux.

1. Comando free

Ejecutamos lo siguiente:

```
[root@pruebas~]# free -m
```

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@casa ~]# free -m
              total        used        free      shared  buff/cache   available
Mem:           1748        1368          75          38         304         170
Swap:          1023         960          63
[root@casa ~]#
```

2. Comando top

Ejecutamos lo siguiente:

```
[root@pruebas~]# top
```

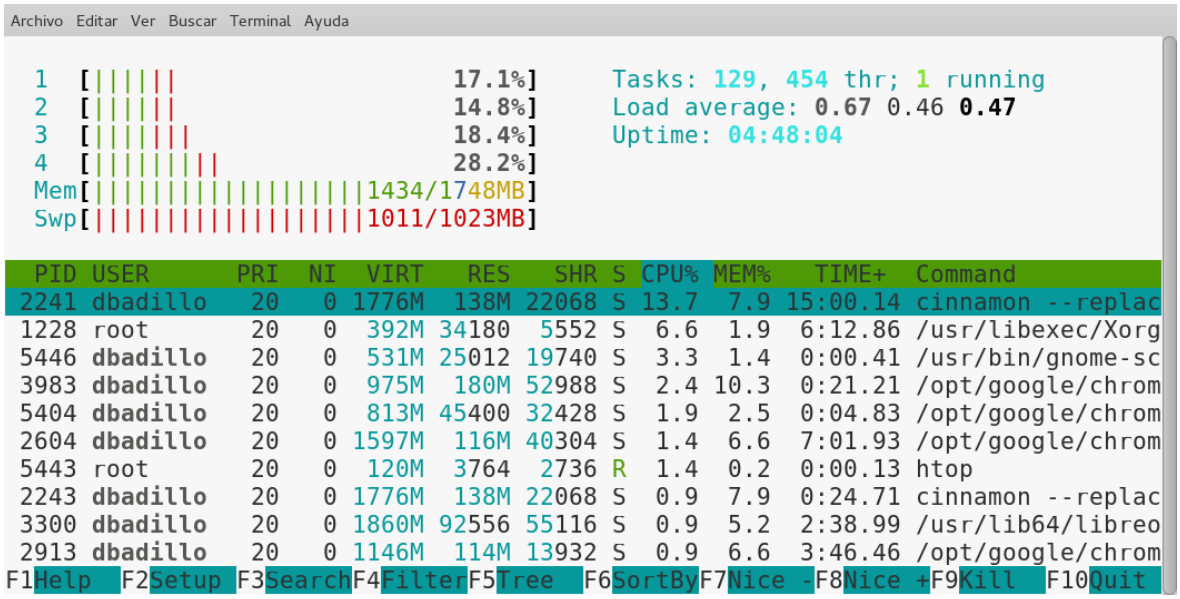
```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
top - 21:03:24 up  4:32,  1 user,  load average: 0,26, 0,53, 0,50
Tasks: 242 total,   1 running, 240 sleeping,   1 stopped,   0 zombie
%Cpu(s): 10,0 us,  3,1 sy,  0,0 ni, 85,7 id,  1,2 wa,  0,0 hi,  0,0 si,  0,0 st
KiB Mem :  1790552 total,    81672 free,  1358976 used,   349904 buff/cache
KiB Swap:  1048572 total,    43464 free,  1005108 used.   218944 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 2241 dbadillo  20   0 1816000 131636  22196 S  24,3  7,4  13:43.42 cinnamon
 1228 root      20   0  401972  39716  10500 S  10,0  2,2   5:25.66 Xorg.bin
 5332 dbadillo  20   0  543768  25428  20160 S   9,3  1,4   0:00.28 gnome-scre+
 4855 dbadillo  20   0 1141876 135252  24156 S   4,3  7,6   0:40.03 chrome
 2604 dbadillo  20   0 1635620 103456  33820 S   1,7  5,8   6:31.52 chrome
 2913 dbadillo  20   0 1174384 117572  14044 S   1,7  6,6   3:33.59 chrome
 3489 dbadillo  20   0  541652  15036   9792 S   1,0  0,8   0:21.17 gnome-term+
    7 root      20   0       0      0      0 S   0,7  0,0   0:39.99 rcu_sched
 2138 dbadillo  20   0 1141924   7924   5140 S   0,7  0,4   0:06.91 cinnamon-s+
 2669 dbadillo  20   0  702628  68412  20880 S   0,7  3,8   3:58.71 chrome
    9 root      20   0       0      0      0 S   0,3  0,0   0:10.55 rcuos/0
   25 root      20   0       0      0      0 S   0,3  0,0   0:20.73 rcuos/2
 1080 root      20   0  145200   1564   1512 S   0,3  0,1   0:18.97 teamviewerd
```

3. Comando htop

Ejecutamos lo siguiente:

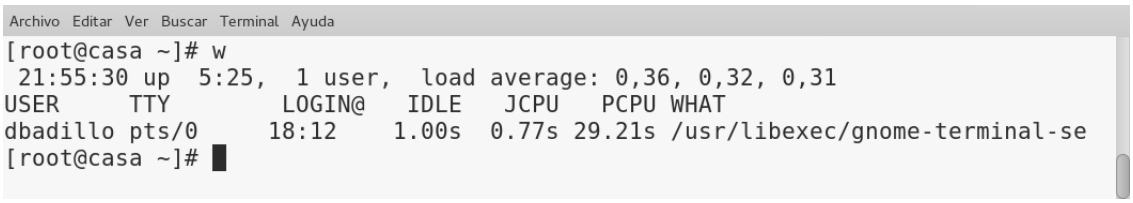
```
[root@pruebas~]# htop
```



4. Comando w

Ejecutamos lo siguiente:

```
[root@pruebas~]# w
```



5. Comando ps

Ejecutamos lo siguiente:

[root@pruebas~]# ps -aux

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.0  0.2 186440  3704 ?        Ss   16:30   0:03 /usr/lib/syste
md/systemd --switched-root --system --deserialize 20
root          2  0.0  0.0      0     0 ?        S    16:30   0:00 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    16:30   0:00 [ksoftirqd/0]
root          5  0.0  0.0      0     0 ?        S<   16:30   0:00 [kworker/0:0H]
root          7  0.2  0.0      0     0 ?        S    16:30   0:49 [rcu_sched]
root          8  0.0  0.0      0     0 ?        S    16:30   0:00 [rcu_bh]
root          9  0.0  0.0      0     0 ?        S    16:30   0:13 [rcuos/0]
root         10  0.0  0.0      0     0 ?        S    16:30   0:00 [rcuob/0]
root         11  0.0  0.0      0     0 ?        S    16:30   0:00 [migration/0]
root         12  0.0  0.0      0     0 ?        S    16:30   0:00 [watchdog/0]
root         13  0.0  0.0      0     0 ?        S    16:30   0:00 [watchdog/1]
root         14  0.0  0.0      0     0 ?        S    16:30   0:00 [migration/1]
root         15  0.0  0.0      0     0 ?        S    16:30   0:00 [ksoftirqd/1]
root         17  0.0  0.0      0     0 ?        S<   16:30   0:00 [kworker/1:0H]
root         18  0.0  0.0      0     0 ?        S    16:30   0:02 [rcuos/1]
root         19  0.0  0.0      0     0 ?        S    16:30   0:00 [rcuob/1]
root         20  0.0  0.0      0     0 ?        S    16:30   0:00 [watchdog/2]
root         21  0.0  0.0      0     0 ?        S    16:30   0:00 [migration/2]
root         22  0.0  0.0      0     0 ?        S    16:30   0:02 [ksoftirqd/2]
root         24  0.0  0.0      0     0 ?        S<   16:30   0:00 [kworker/2:0H]
root         25  0.1  0.0      0     0 ?        S    16:30   0:25 [rcuos/2]
```

6. Comando df

Ejecutamoslo siguiente:

[root@pruebas~]# df -h

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@casa ~]# df -h
S.ficheros           Tamaño Usados  Disp Uso% Montado en
devtmpfs               863M      0  863M   0% /dev
tmpfs                  875M    22M  853M   3% /dev/shm
tmpfs                  875M   964K  874M   1% /run
tmpfs                  875M      0  875M   0% /sys/fs/cgroup
/dev/mapper/dsk-root   9,5G   391M  8,7G   5% /
/dev/mapper/dsk-usr     15G   4,7G  9,0G  35% /usr
tmpfs                  875M   2,0M  873M   1% /tmp
/dev/sda1              477M   165M  283M  37% /boot
/dev/mapper/dsk-home   385G   263G  103G  72% /home
/dev/mapper/dsk-var    7,1G   1,9G  4,9G  28% /var
tmpfs                  175M    28K  175M   1% /run/user/1000
/dev/sdb2              432G   148G  284G  35% /run/media/dbadillo/WINDOWS
/dev/sdb1              493G   259G  234G  53% /run/media/dbadillo/LINUX
[root@casa ~]#
```

7. Comando isof

Ejecutamos lo siguiente:

```
[root@pruebas~]# lsof -p PID
```

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@casa ~]# echo $$
5796
[root@casa ~]# lsof -p 5796
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
COMMAND  PID USER   FD   TYPE DEVICE  SIZE/OFF   NODE NAME
bash    5796 root  cwd    DIR  253,1      4096 129796 /root
bash    5796 root  rtd    DIR  253,1      4096      2 /
bash    5796 root  txt    REG  253,2   1012808 521408 /usr/bin/bash
bash    5796 root  mem    REG  253,2 106370640 657627 /usr/lib/locale/locale-archive
bash    5796 root  mem    REG  253,2     62072 261568 /usr/lib64/libnss_files-2.20.so
bash    5796 root  mem    REG  253,2   2082456 261546 /usr/lib64/libc-2.20.so
bash    5796 root  mem    REG  253,2     19512 261562 /usr/lib64/libdl-2.20.so
bash    5796 root  mem    REG  253,2    173136 262357 /usr/lib64/libtinfo.so.5.9
bash    5796 root  mem    REG  253,2    163176 261586 /usr/lib64/ld-2.20.so
bash    5796 root  mem    REG  253,2     26254 262851 /usr/lib64/gconv/gconv-modules.cache
bash    5796 root    0u   CHR  136,0       0t0      3 /dev/pts/0
bash    5796 root    1u   CHR  136,0       0t0      3 /dev/pts/0
bash    5796 root    2u   CHR  136,0       0t0      3 /dev/pts/0
bash    5796 root  255u   CHR  136,0       0t0      3 /dev/pts/0
[root@casa ~]#
```

8. Comando ifstat

Ejecutamos lo siguiente:

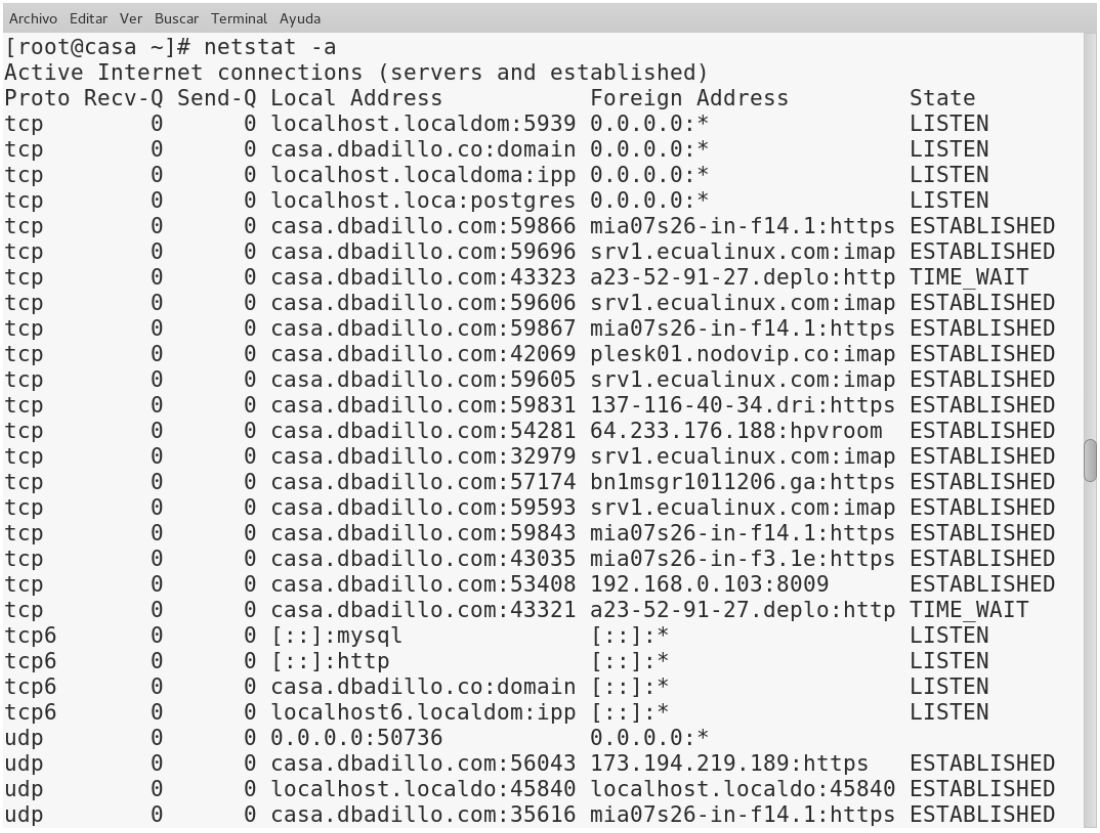
```
[root@pruebas~]# ifstat
```

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@casa ~]# ifstat
#kernel
Interface        RX Pkts/Rate    TX Pkts/Rate    RX Data/Rate    TX Data/Rate
                 RX Errs/Drop    TX Errs/Drop    RX Over/Rate    TX Coll/Rate
lo                   249 0           249 0         17646 0         17646 0
                       0 0             0 0             0 0             0 0
enp2s0                 0 0             0 0             0 0             0 0
                       0 0             0 0             0 0             0 0
wlp3s0             40844 0         35393 0        34696K 0         6445K 0
                       0 0             0 0             0 0             0 0
virbr0                 0 0             0 0             0 0             0 0
                       0 0             0 0             0 0             0 0
[root@casa ~]#
```

9. Comando netstat

Ejecutamos lo siguiente:

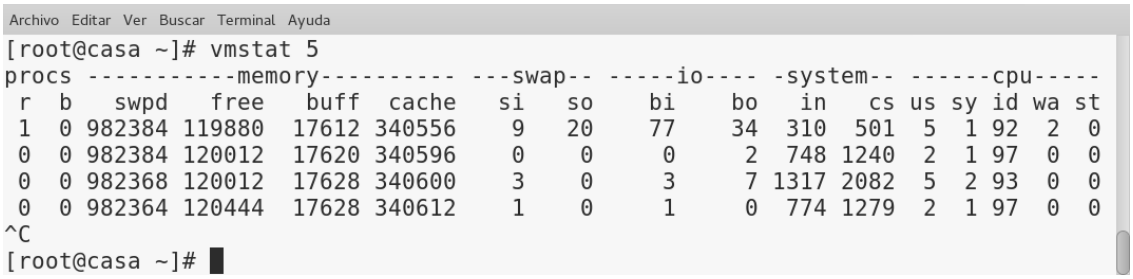
[root@pruebas~]# netstat -a



10. Comando vmstat

Ejecutamos lo siguiente:

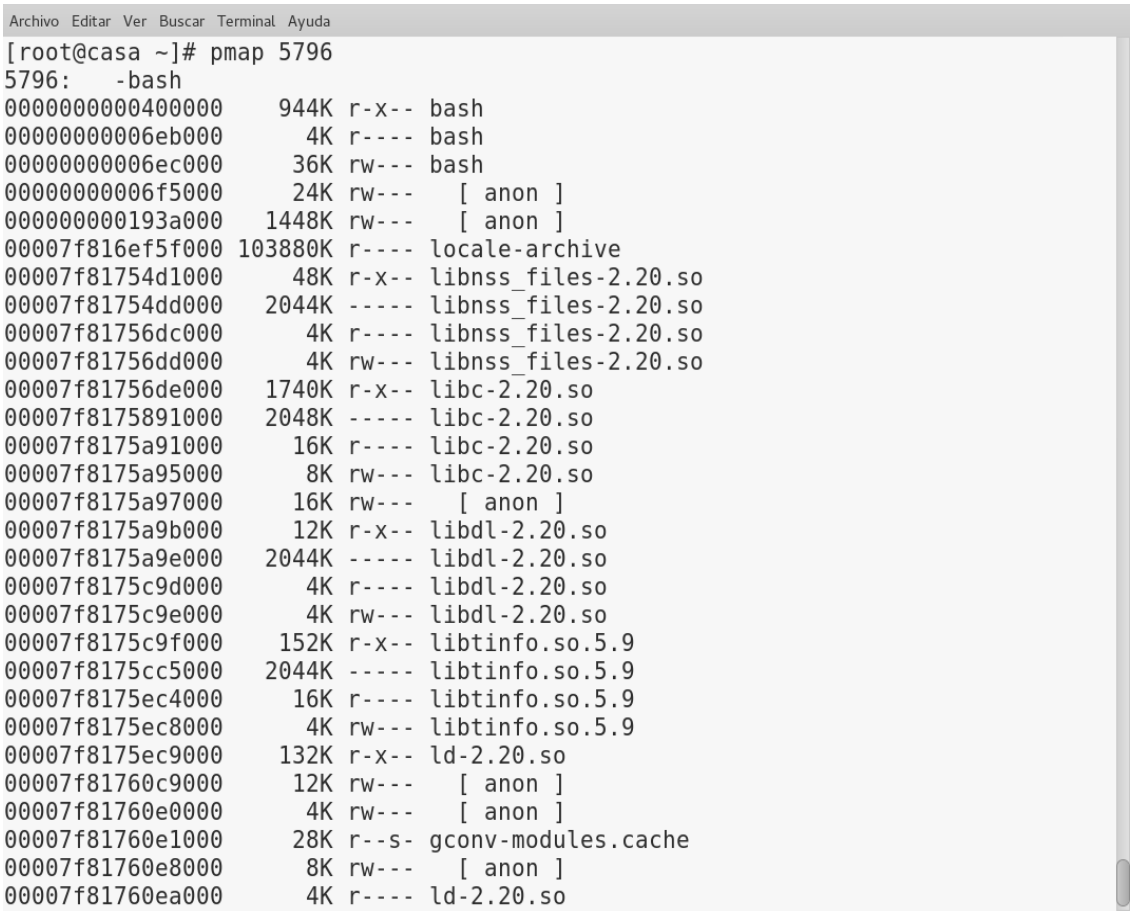
[root@pruebas~]# vmstat



11. Comando pmap

Ejecutamos lo siguiente:

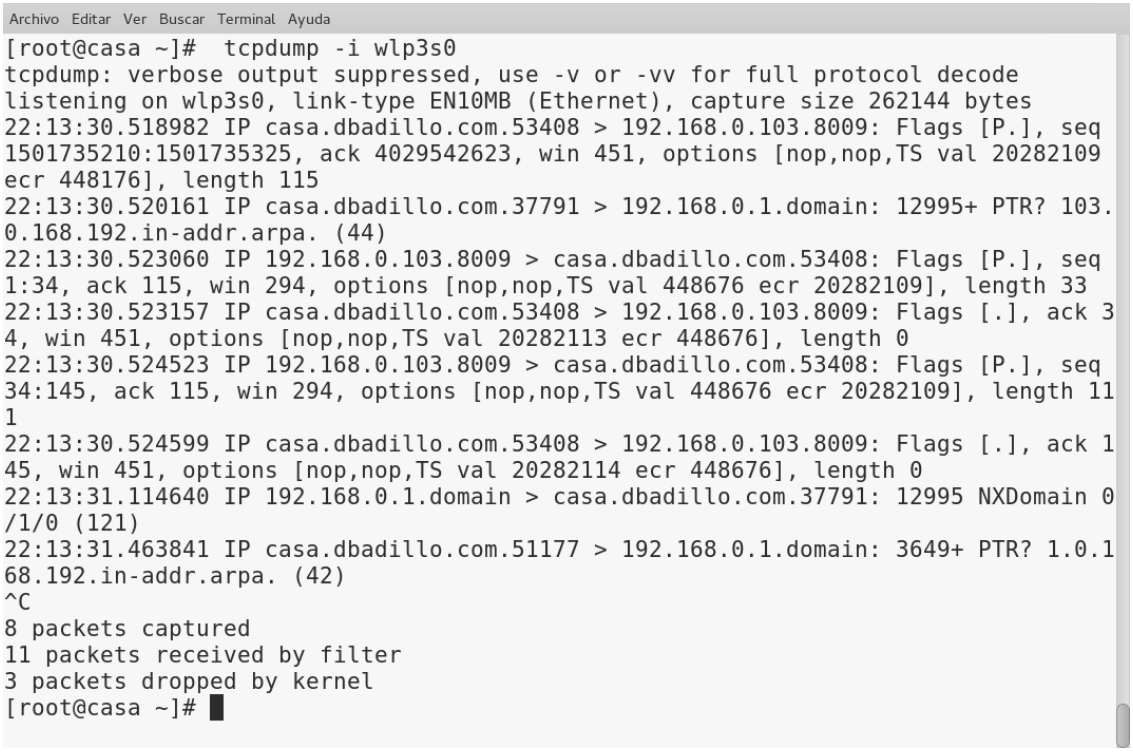
```
[root@pruebas~]# pmap PID
```



12. Comando tcpdump

Ejecutamos el comando:

```
[root@pruebas~]# tcpdump
```



ANEXO B. Características Distribuciones Linux

En este anexo presentamos las características generales de 20 distribuciones Linux, las cuales son muy utilizadas a nivel mundial. Luego del análisis de estas distros, se pudo determinar cuáles son orientadas a brindar servicios en redes de comunicación.

1. Kali Linux

Nombre de la Distribución:	*Kali Linux*
País de Origen:	Suiza
Página Web Oficial:	www.kali.org
Versión Actual	1.1.0
Fecha de Lanzamiento	10/08/2004
Precio	Gratuito
Escritorio por Defecto:	GNOME
Gestor de Paquetes:	DEB
Arquitectura:	Armel, armhf, i386, x86_64
Categoría:	Test de Seguridad

Esta distribución tenía el nombre de BackTrack y fue lanzada en el año 2004. El objetivo fundamental de esta distro, es brindar una gran colección de herramientas de seguridad y de informática forense. Mediante este sistema, podemos realizar test de seguridad tanto a nivel de servidores como dentro de una red.

Esta distribución no está orientada a brindar servicios de red, por esta razón no la incluiremos en la comparación.

2. Fedora

Nombre de la Distribución:	*Fedora*
País de Origen:	Estados Unidos
Página Web Oficial:	getfedora.org
Versión Actual	Fedora Core 22
Fecha de Lanzamiento	05/11/2003
Precio	Gratuito
Escritorio por Defecto:	GNOME
Gestor de Paquetes:	RPM (dnf)
Arquitectura:	Armhfp, i686, x86_64
Categoría:	Escritorio, Servidor

Fedora es una distribución Linux patrocinada por Red Hat, busca innovar tecnologías que luego las pueda implementar en versiones posteriores de Red Hat. A este tipo de distribuciones se las conoce como sandbox (caja de arena), la que se nutre de los reportes de error que envían los usuarios, para que estos sean corregidos y al momento de tener un producto estable sean implementados en Red Hat.

El lanzamiento de las nuevas versiones son muy frecuentes, por ejemplo en el año 2013 se publicaron 3: 18 (spherical), 19 (schrodingers) y 20 heisenbug.

Si bien es cierto esta distribución provee de paquetes para levantar varios servicios de red, de ninguna manera es recomendable que se lo use en producción. Fedora es una distribución de pruebas, que puede presentar algunos errores propios de la innovación del software, esto afecta a la estabilidad de un servidor. Por otro lado la comunidad desarrolladora de Fedora no se compromete a dar solución a los problemas reportados.

Sin duda por lo innovadora de esta distribución, es muy popular para ser instalada en equipos de escritorio obteniendo muy buenos resultados. Se considera como una de las distribuciones más usadas en nuestro medio para equipos orientados a usuarios finales.

En mayo del 2010, esta distribución adopta por defecto a systemd, que hoy en día es soportado por Red Hat, Dabian Suse entre otras distribuciones Linux.

Para nuestro estudio, no la vamos a tomar en cuenta, como explicamos por la frecuencia de las actualizaciones y por tener un grupo de software muy innovador, no es una distribución estable. Definitivamente Fedora no debe ser utilizada para ser instalada en un servidor de producción.

3. CentOS (Red Hat)

Nombre de la Distribución:	***C****ommunity* ***ENT****repise* ***O****perating* ***S****ystem*
País de Origen:	Estados Unidos
Página Web Oficial:	www.centos.org
Versión Actual	Entrepise Linux 7
Fecha de Lanzamiento	24/05/2004
Precio	Gratuito

Escritorio por Defecto:	GNOME
Gestor de Paquetes:	RPM (yum)
Arquitectura:	x86_64
Categoría:	Servidor

CentOS es una distribución clon de Red Hat, esto quiere decir que sus características son iguales, para entender de mejor manera debemos puntualizar lo siguiente.

Red Hat definitivamente es una de las distribuciones más influyentes en el desarrollo de Linux, por esta razón es considerada como un sistema operativo estable y robusto, a ser instalado en servidores que tengan una gran carga de trabajo; esta distribución está diseñada para grandes proyectos informáticos.

Red Hat tiene un costo por licencia de uso, la cual es plenamente justificada por el servicio que esta empresa brinda; sin embargo por estos costos, esta distribución no puede ser asequible por Pymes. Red Hat publica todo el grupo de software, bajo licencia GPL, lo que obliga a entregar el código fuente de todos los paquetes distribuidos por Red Hat.

CentOS se encarga de recompilar todos los paquetes liberados por Red Hat y los distribuye de manera gratuita, de esta manera las Pymes se ven directamente beneficiadas, al tener un sistema operativo robusto a muy bajo costo.

Red Hat tiene una prohibición de uso sobre la imagen corporativa de la empresa, esto es lo único que no puede adoptar CentOS, por lo demás es una distribución idéntica en sus características.

CentOS en nuestro medio es la distribución muy utilizada por los beneficios que brinda y por ser cien por ciento gratuita; sin embargo debemos recalcar que CentOS no brinda las ventajas de soporte técnico especializado como lo hace Red Hat.

Red Hat desde marzo del 2014 patrocina el proyecto CentOS, estrechando mucho más la relación entre estas dos distribuciones. Para la presente comparación utilizaremos a CentOS.

4. Arch Linux

Nombre de la Distribución:	*ArchLinux*
País de Origen:	Canadá
Página Web Oficial:	www.archlinux.org
Versión Actual	2015.05.01
Fecha de Lanzamiento	11/03/2002
Precio	Gratuito
Escritorio por Defecto:	Ninguno
Gestor de Paquetes:	Pacman
Arquitectura:	Arm, i686,x86_64
Categoría:	Escritorio, Servidor

Arch Linux es una distribución Linux orientada principalmente para equipos de escritorio, sin embargo permite también levantar varios servicios con opciones para usuarios experimentados en ambientes Linux.

Uno de los temas interesantes de esta distribución es que utiliza su propio gestor de paquetes llamado Pacman, el que maneja un formato de paquetes binarios con la extensión pkg.tar.xz. Mediante este gestor se permite la instalación, actualización y eliminación de software en Arch Linux.

También debemos señalar que esta distribución no se basa en lanzamientos (versiones); el gestor de paquetes permite una evolución constante del sistema operativo.

Para nuestro estudio, analizaremos las características de seguridad que brinda esta distribución al momento del manejo de servicios de red.

5. Ubuntu

Nombre de la Distribución:	*Ubuntu*
País de Origen:	Isle of Man
Página Web Oficial:	www.ubuntu.com
Versión Actual	15.04 (vivid)
Fecha de Lanzamiento	20/10/2004
Precio	Gratuito
Escritorio por Defecto:	Unity
Gestor de Paquetes:	DEB
Arquitectura:	i686,x86_64
Categoría:	Escritorio, Servidor

Ubuntu sin duda es una de las distribuciones Linux más populares a nivel mundial, basada en la distro Debian, es una de las primeras orientada a usuarios finales. Actualmente Ubuntu usa su propio entorno de escritorio llamado Unity.

Esta distribución Linux es patrocinada por Canonical, una empresa fundada por el sudafricano Mark Shuttleworth, esta compañía vende el soporte comercial de Ubuntu.

Existen varias distribuciones que se derivan de Ubuntu, estas son: Kubuntu, Xubuntu, Ubuntu MATE, Ubuntu Studio, Edubuntu, Lubuntu, entre otras.

Ubuntu publica nuevas versiones con una periodicidad de 6 meses, las cuales tienen un soporte por parte de Canonical de 9 meses, además tiene un sistema de versiones llamado LTS (Long Term Support), que se liberan cada 2 años y tienen un soporte de 5 años.

Como lo indicamos anteriormente esta distribución está originalmente orientada a usuarios finales, sin embargo desde el año 2011, Canonical lo separa en dos versiones: “Ubuntu Desktop Edition” y “Ubuntu Server Edition”. Bajo algunas investigaciones hemos determinado que algunas empresas han optado por esta distro para ser uso de servidor. Al tener la versión para servidores, tomaremos en cuenta a Ubuntu para la comparación.

6. Open Suse

Nombre de la Distribución:	*Open Suse*
País de Origen:	Alemania
Página Web Oficial:	www.opensuse.org
Versión Actual	13.2
Fecha de Lanzamiento	23/03/1998
Precio	Gratuito
Escritorio por Defecto:	KDE
Gestor de Paquetes:	RPM
Arquitectura:	i586,x86_64
Categoría:	Escritorio, Servidor

Es una distribución Linux que se considera de propósito general, está orientada a desarrolladores como usuarios finales. Esta se la puede usar en equipos de escritorio y servidores.

Open Suse es la versión comunitaria de SUSE Linux Enterprise que tiene el soporte comercial de la compañía estadounidense Novell. Open Suse es mantenida por la comunidad llamada “Proyecto openSUSE”.

OpenSUSE es gratuita mientras que SUSE Linux tiene costo por varios rubros: suscripción, soporte técnico y certificación.

Una característica muy interesante de esta distribución, es el administrador del sistema llamado YaST, que permite gestionar varios servicios del sistema como la administración de paquetes de software.

Al brindar servicios para la red, vamos a incluir a esta distribución para la comparación.

7. Debian

Nombre de la Distribución:	*Debian*
País de Origen:	No definido
Página Web Oficial:	www.debian.org
Versión Actual	8.0 Jessie
Fecha de Lanzamiento	17/06/1996
Precio	Gratuito
Escritorio por Defecto:	GNOME
Gestor de Paquetes:	DEB

Arquitectura:	i586,x86_64, armel, mipsel
Categoría:	Servidor

Debian es una distribución Linux liberada bajo un contrato social (https://www.debian.org/social_contract), que fundamentalmente garantiza que sea cien por ciento libre y no aplica discriminación a sus usuarios. Esta distribución es libre y gratuita.

Existe una gran cantidad de instituciones que usan esta distro, podemos obtener un listado en la siguiente dirección web: https://www.debian.org/users/ . Podemos comprobar que es muy usada a nivel mundial y que de ésta se derivan un sin número de distribuciones como: Ubuntu, Canaima, Kali, Educanix, Mint, entre muchas más.

Es considerado uno de los grandes proyectos de software libre, ya que cuenta con alrededor de mil desarrolladores, los cuales eligen cada año al líder del proyecto. Desde 1993 hasta la fecha, se han elegido trece líderes de diferentes nacionalidades; por esta razón no se ha definido un país de origen para esta distribución.

Para nuestro caso de estudio, tomaremos en cuenta a esta distribución, sin duda es una de las más importantes y activas dentro del mundo Linux.

8. Linux Mint

Nombre de la Distribución:	*Linux Mint*
País de Origen:	Irlanda
Página Web Oficial:	www.linuxmint.com
Versión Actual	17.1 (Rebecca)

Fecha de Lanzamiento	14/11/2006
Precio	Gratuito
Escritorio por Defecto:	Cinnamon, MATE
Gestor de Paquetes:	DEB
Arquitectura:	i386,x86_64
Categoría:	Escritorio

El propósito de esta distribución, es crear un sistema operativo orientado a usuario final que sea moderno, confortable, potente y fácil de usar.

Linux Mint actualmente ocupa el primer lugar de uso de las distribuciones Linux, esto es gracias a la facilidad en su manejo, gratuidad y proporciona alrededor de 30.000 paquetes de software.

En sus inicios Linux Mint se derivaba de Ubuntu, actualmente lo hace directamente de Debian.

Mint ha desarrollado varias herramientas para que la experiencia del usuario sea más rica, entre las que se destacan son:

- **MintSoftware.** Gestor de paquetes de software.
- **MintUpdate.** Gestor de actualizaciones.
- **MintInstall.** Gestor de instalación.
- **MintDesktop.** Gestor para la configuración del escritorio.
- **MintConfig.** Centro de control para la configuración del sistema.
- **MintAssistant.** Centro de ayuda para el uso del sistema.
- **MintUpload.** Cliente de FTP para la transferencia de archivos.
- **MintMenu.** Menú de escritorio personalizable.
- **MintBackup.** Gestor para respaldos y restauración de datos.
- **MintNanny.** Sistema para filtrado de contenidos web.

Mint se dedicó a la construcción de estas herramientas, todas son gráficas y permite un uso sencillo del sistema operativo, razón fundamental para la popularidad de Mint.

Como podemos ver está orientada a equipos de escritorio y en efecto consideramos que es una muy buena opción para usuarios que se inician en el mundo de Linux.

Para nuestra comparación no la tomaremos en cuenta, ya que el estudio está basado en las distribuciones Linux que son orientadas para brindar servicios de red.

9. Mageia

Nombre de la Distribución:	*Mageia*
País de Origen:	Francia
Página Web Oficial:	www.mageia.org
Versión Actual	4.1
Fecha de Lanzamiento	01/06/2011
Precio	Gratuito
Escritorio por Defecto:	KDE
Gestor de Paquetes:	RPM (urpmi)
Arquitectura:	i586,x86_64
Categoría:	Escritorio, Servidor

Mageia es una distribución Linux que pertenece a un proyecto comunitario sin fines de lucro originario de Francia, siendo una bifurcación de Mandriva Linux.

Esta distro utiliza como gestor de paquetes a URPMI, el que permite instalar, actualizar y eliminar el software.

La comunidad que la soporta está compuesta de diseñadores, desarrolladores, empaquetadores, probadores, usuarios de software, todos alineados al código abierto, a diferencia de Mandriva que tenía fines comerciales.

Dentro de las versiones que ofrece Mageia tenemos el uso para servidor, por esta razón la tomaremos en cuenta para la comparación.

10. Zorin

Nombre de la Distribución:	*Zorin*
País de Origen:	Irlanda
Página Web Oficial:	www.zorin-os.com
Versión Actual	9
Fecha de Lanzamiento	01/07/2009
Precio	Gratuito
Escritorio por Defecto:	Zorin
Gestor de Paquetes:	DEB
Arquitectura:	i386,x86_64
Categoría:	Escritorio

Zorin OS es una distribución Linux orientada para equipos de escritorio basada en Ubuntu. Tiene como objetivo principal brindar una interfaz gráfica y funcionalidades, similares a lo que ofrece Microsoft Windows.

Para brindar compatibilidad con Microsoft Windows la distro utiliza a Wine, software que permite ejecutar ciertos programas diseñados y desarrollados para Windows.

Zorin OS tiene como objetivo ser un reemplazo en software libre de Microsoft Windows, para ello, ha desarrollado herramientas que brindan ventajas similares a las que ofrece el sistema operativo más usado a nivel mundial.

Esta distro no está orientada a brindar servicios de red, pretende brindar las mayores prestaciones para usuarios finales.

Por lo expuesto no la podemos incluir dentro de la comparación, sin embargo puede ser una muy buena alternativa para usuarios que desean migrar del software comercial al software libre.

11. Elementary OS

Nombre de la Distribución:	*Elementary OS*
País de Origen:	Canadá
Página Web Oficial:	www.elementary.io
Versión Actual	0.3
Fecha de Lanzamiento	11/04/2015
Precio	Gratuito
Escritorio por Defecto:	Pantheon
Gestor de Paquetes:	DEB

Arquitectura:	i386,x86_64
Categoría:	Escritorio

Elementary OS es una distribución Linux basada en Ubuntu, está orientada a equipos de escritorio. Tiene como característica principal el uso del entorno de escritorio llamado Pantheon, que es más ligero que GNOME. Adicional ha desarrollado algunas herramientas propias de esta distribución, entre las principales tenemos:

- **Midori.** Navegador Web.
- **Scratch.** Editor para archivos de texto.
- **Birdie.** Cliente de Twitter.

Adicionalmente utiliza el gestor de ventanas llamado Gala, que permite dar una interfaz gráfica similar a la brindada por MacOS X.

Al ser una distribución Linux orientada a equipos de escritorio, no la tomaremos en cuenta en la comparación.

12. Lubuntu

Nombre de la Distribución:	*Lubuntu*
País de Origen:	Francia, Taiwan
Página Web Oficial:	www.lubuntu.net
Versión Actual	15.04 (Vivid)
Fecha de Lanzamiento	03/05/2010

Precio	Gratuito
Escritorio por Defecto:	LXDE
Gestor de Paquetes:	DEB
Arquitectura:	i386,x86_64
Categoría:	Netbooks

Lubuntu es una distribución Linux basada en Ubuntu, busca ser muy ligera para funcionar en equipos con recursos limitados, como dispositivos móviles, netbooks o computadores antiguos.

Para poder ser ligero y ofrecer una interfaz gráfica utiliza a LXDE, entorno de escritorio que consume muy pocos recursos de hardware, más aún si lo comparamos con la última versión de GNOME o KDE.

Los creadores de esta distro, manejan la frase “menos recursos y más eficiencia energética”, en clara tendencia a buscar la mayor optimización de hardware de un equipo.

Esta distribución cómo está construida, no brinda servicios de red, aunque como deriva de Ubuntu, puede ser que encontremos algunos demonios que levantar, sin embargo consideramos que no podemos tomarlo en cuenta en este estudio comparativo.

Es una muy buena opción si deseamos reutilizar nuestro computador antiguo.

13. LXLE

Nombre de la Distribución: *LXLE*

País de Origen:	Estados Unidos
Página Web Oficial:	www.lxle.net
Versión Actual	14.04.1
Fecha de Lanzamiento	23/10/2014
Precio	Gratuito
Escritorio por Defecto:	LXDE
Gestor de Paquetes:	DEB
Arquitectura:	x86_64
Categoría:	Escritorio

LXLE es una distribución Linux basada en Lubuntu, la cual se deriva de Ubuntu. Esta utiliza el entorno de escritorio LXDE.

Tiene la característica de usar versiones de Ubuntu LTS (Long Term Support), brinda un soporte de 5 años por parte de la distribución base, en este caso Ubuntu. El ciclo de desarrollo está directamente relacionado con las versiones de Lubuntu.

El desarrollador de la distro, indica que el tiempo de arranque de este sistema es menor a un minuto, ratificando lo liviano y poco consumidor de recursos de hardware.

Al igual que Lubuntu es una distribución que no está orientada a brindar servicios de red, sus características le permiten instalar en cualquier computador y está orientada a equipos de escritorio para usuarios finales.

Por lo expuesto, no podemos tomar en cuenta a esta distribución para nuestra comparación.

14. Puppy Linux

Nombre de la Distribución:	*Puppy Linux*
País de Origen:	Australia
Página Web Oficial:	www.puppylinux.com
Versión Actual	6.0 (Tahrpup)
Fecha de Lanzamiento	15/05/2006
Precio	Gratuito
Escritorio por Defecto:	OpenBox
Gestor de Paquetes:	PET
Arquitectura:	i386
Categoría:	Escritorio

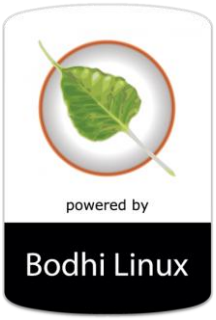
Puppy Linux es una mini distribución Linux, que está disponible en un Live CD. Tiene como objetivo el permitir al usuario trabajar en tareas básicas del computador como: navegar por Internet, manejar una suite de ofimática, editar archivos de imágenes, uso de audio y video.

Se puede guardar en un CD, su tamaño no sobrepasa de los 200 MB, se recomienda que el computador donde va a correr, tenga al menos 256 MB de memoria principal (RAM).

La idea de esta distro es que pueda ser usada en hardware antiguo con recursos limitados, equipos en los cuales no se pueden instalar sistemas operativos modernos, por ser muy consumidores de recursos.

Al igual que Lubuntu y LXLE, por sus característica no es diseñada para brindar servicios de red, no la tomaremos en cuenta para la comparación.

15. Bodhi Linux



Nombre de la Distribución:	*Bodhi Linux*
País de Origen:	Estados Unidos
Página Web Oficial:	www.bodhilinux.com
Versión Actual	3.0.0
Fecha de Lanzamiento	22/03/2012
Precio	Gratuito
Escritorio por Defecto:	Enlightenment
Gestor de Paquetes:	DEB
Arquitectura:	i386,x86_64
Categoría:	Escritorio

Bodhi Linux es una distribución Linux muy liviana que se diferencia del resto de distros, al presentar tras la instalación, solamente el software básico, a saber: navegador Web, explorador de archivos y emulador de terminal. Esta distribución está basada en Debian.

Bodhi está orientada a equipos de escritorio, por esta razón no la tomaremos en cuenta en este estudio.

16. PCLinuxOS

Nombre de la Distribución:	*PCLinuxOS*
País de Origen:	Estados Unidos
Página Web Oficial:	www.pclinuxos.com
Versión Actual	2014.12
Fecha de Lanzamiento	21/11/2005
Precio	Gratuito
Escritorio por Defecto:	KDE
Gestor de Paquetes:	RPM (APT)
Arquitectura:	i586,x86_64
Categoría:	Escritorio

PCLinuxOS es una distribución Linux, derivada de Mandriva, busca brindar una interfaz amigable para el usuario. PCLinuxOS brinda soporte de una variedad de tarjetas gráficas y de audio, que le hace muy compatible con diferentes equipos de hardware. Ofrece algunos paquetes de software para usuarios finales.

Esta distribución es orientada para equipos de escritorio, por lo tanto no la tomaremos en cuenta para la comparación.

17. Linux Deepin

Nombre de la Distribución:	*Linux Deepin*
País de Origen:	China
Página Web Oficial:	www.deepin.org
Versión Actual	2014.3
Fecha de Lanzamiento	22/07/2004
Precio	Gratuito
Escritorio por Defecto:	Deepin DE
Gestor de Paquetes:	DEB
Arquitectura:	i386,x86_64
Categoría:	Escritorio

Deepin es una distribución Linux basada en Ubuntu, originaria en China para usuarios finales. Ha desarrollado su propio entorno de escritorio llamado (Deepin Desktop Enviroment) basado en GNOME.

Debemos recalcar que está disponible en mandarín e inglés. Al ser una distribución orientada a usuarios finales, no la tomaremos en cuenta en este estudio.

18. Manjaro

Nombre de la Distribución:	*Manjaro Linux*
País de Origen:	Austria, Alemania y Francia
Página Web Oficial:	www.manjaro.org
Versión Actual	0.8.11
Fecha de Lanzamiento	26/11/2013
Precio	Gratuito
Escritorio por Defecto:	KDE, XFCE
Gestor de Paquetes:	Pacman
Arquitectura:	i686,x86_64
Categoría:	Escritorio, Netbooks

Manjaro Linux es una distribución Linux basada en Arch Linux, por esta razón utiliza el gestor de paquetes Pacman. Ofrece un sistema de instalación sencillo y muy intuitivo, que realiza una detección automática del hardware para el uso de los controladores.

Manjaro es una distribución orientada a usuarios finales, por esta razón no la tomaremos en cuenta en esta comparación.

19. Ultimate Edition

Nombre de la Distribución:	*Ultimate Edition*
País de Origen:	Estados Unidos
Página Web Oficial:	www.ultimateedition.info
Versión Actual	4.5
Fecha de Lanzamiento	26/01/2008
Precio	Gratuito
Escritorio por Defecto:	XFCE
Gestor de Paquetes:	DEB
Arquitectura:	x86_64
Categoría:	Escritorio

Ultimate Edition es una distribución Linux, basada en Linux Mint. Busca ofrecer una solución integral en Linux y fácil de mantener, por ejemplo actualizar el sistema con un solo clic. Brinda un gran número de repositorios para instalación de paquetes, así como temas en 3D para el escritorio. Es una distro orientada al usuario final, por lo que no la incluiremos en esta comparación.

20. Xubuntu

Nombre de la Distribución:	*Xubuntu*
País de Origen:	Isle of Man
Página Web Oficial:	www.xubuntu.org
Versión Actual	15.04 (Vivid)
Fecha de Lanzamiento	01/06/2006
Precio	Gratuito
Escritorio por Defecto:	XFCE
Gestor de Paquetes:	DEB
Arquitectura:	i386,x86_64
Categoría:	Escritorio

Xubuntu es una distribución Linux basada en Ubuntu, que usa como entorno de escritorio a Xfce. Esta cuenta con el apoyo de Canonical.

El objetivo de Xubuntu es brindar todas las ventajas que tiene Ubuntu pero para equipos con recursos limitados.

Podríamos decir que Xubuntu es la competencia de Lubuntu, distribución antes estudiada, pues comparten los mismos objetivos.

Es una distro orientada a equipos de escritorio, por esta razón no la tomaremos en cuenta en la comparación.

ANEXO C: Procesos de instalación Distribuciones Linux

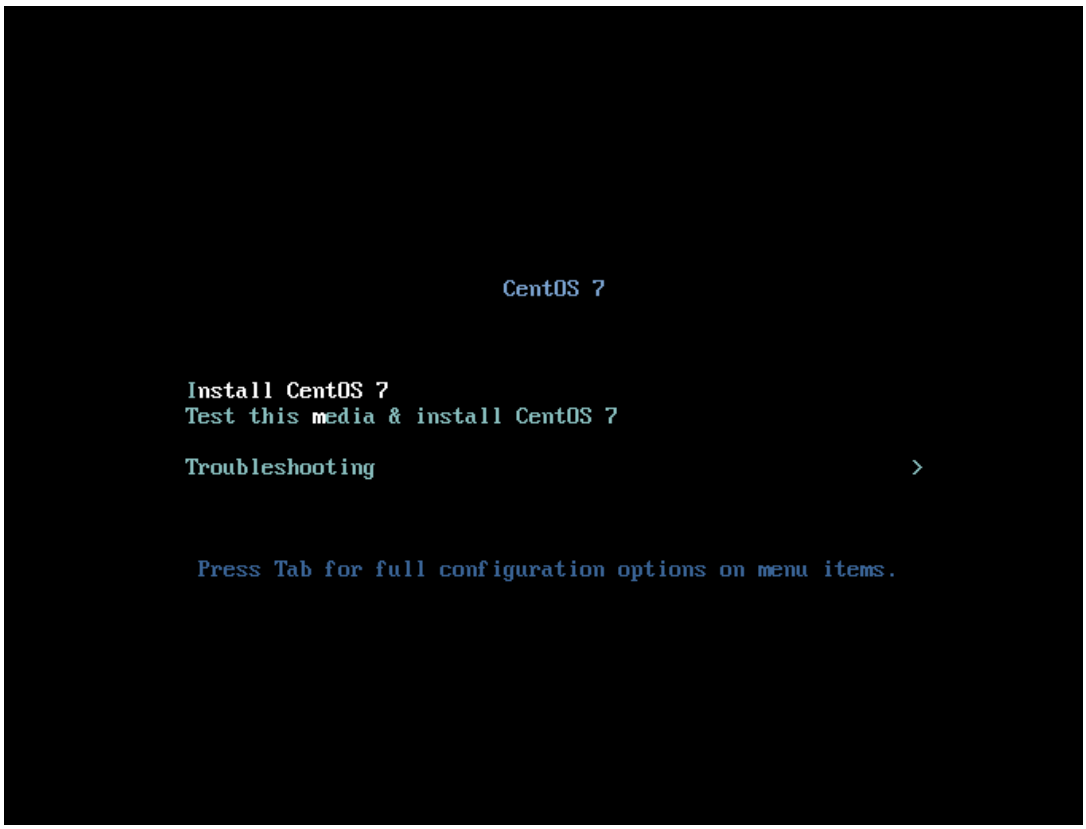
Para poder realizar el estudio comparativo se prepararon escenarios de pruebas mediante la virtualización con KVM. Se crearon máquinas virtuales con las distribuciones Linux a ser analizadas. Este anexo detalla el proceso de instalación de cada una de ellas.

1. Instalación y configuración básica de CentOS

Una vez cargado el instalador, se presenta la pantalla con las siguientes opciones:

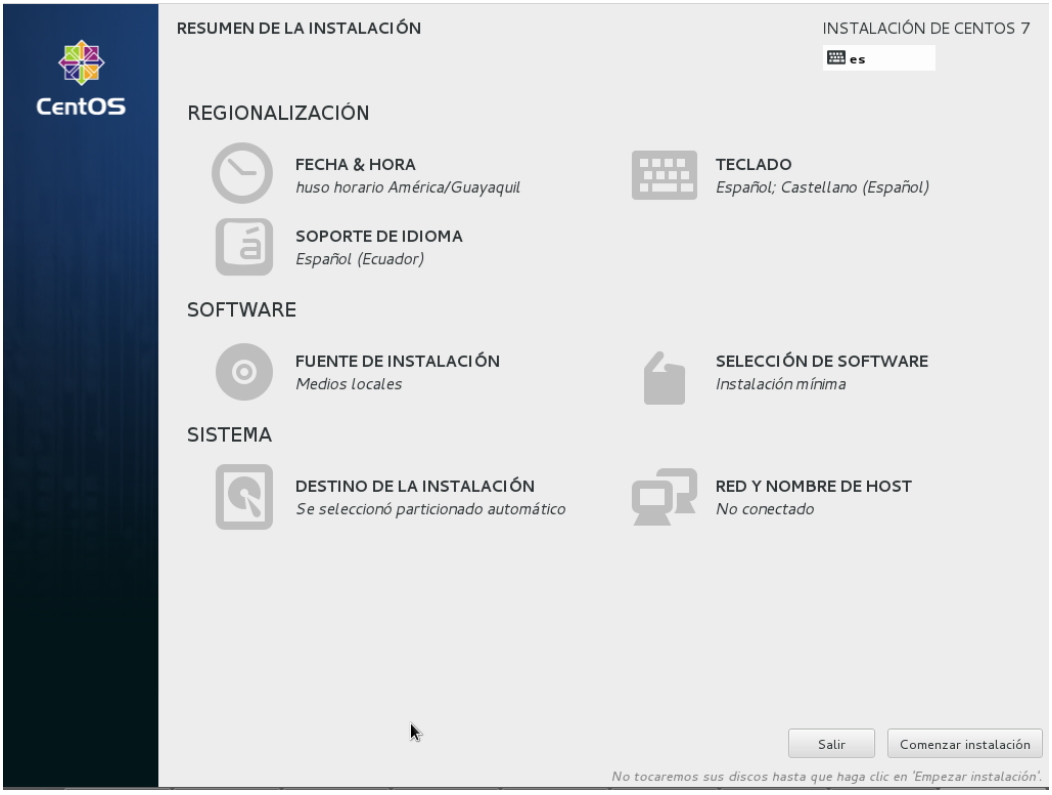
- **Install CentOS 7.** Dispara el instalador gráfico de CentOS.
- **Test this media & install CentOS 7.** Realiza un test del DVD y posteriormente dispara el instalador gráfico de CentOS.
- **Troubleshooting.** Arranca en modo de rescate, el cual permite solucionar problemas en equipos que tienen instalado a CentOS.

Elegimos la primera opción “Install CentOS 7”, arrancará el gestor de instalación llamado Anaconda.



Una vez que elegimos el idioma pasamos a la siguiente pantalla del instalador, esta presenta algunas opciones a configurar:

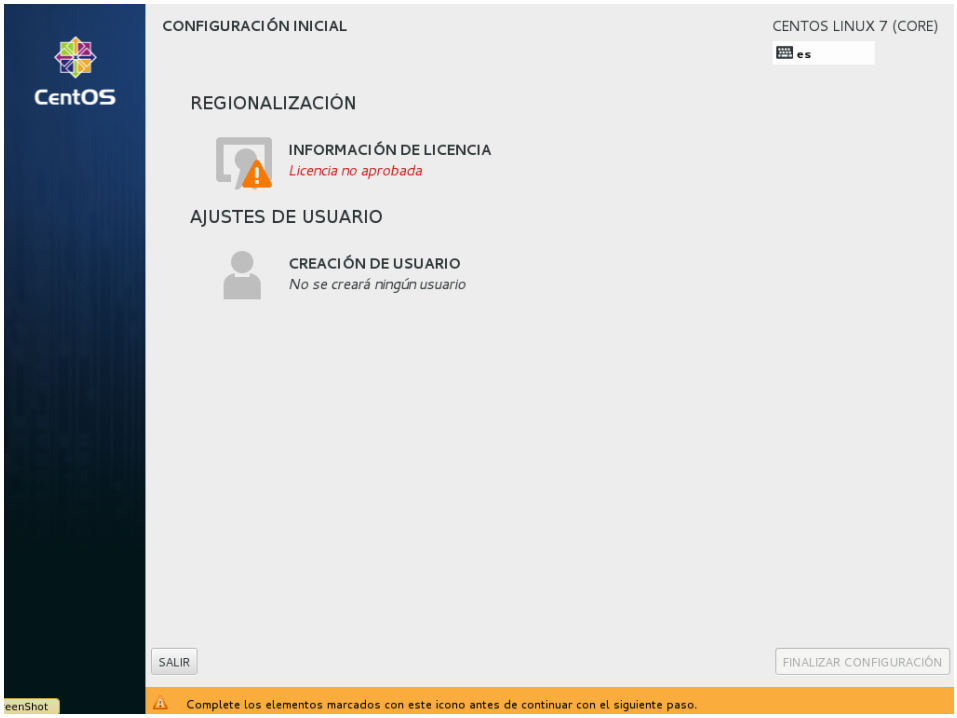
- **Fecha y Hora.** Permite elegir la zona horaria, en nuestro caso seleccionamos “América/Guayaquil”.
- **Teclado.** Permite elegir la distribución del teclado. Debemos reconocer el tipo de teclado que tenemos, No tiene la misma distribución el en español (tiene la tecla @ en el número 2) que la distribución del latinoamericano (tiene la tecla @ en la letra Q).
- **Soporte de Idioma.** Permite seleccionar el idioma en el cual trabajará el sistema operativo, elegimos Español.
- **Fuente de Instalación.** Permite elegir la fuente desde la cual se copiarán los archivos para realizar la instalación, seleccionamos la unidad óptica. Otra opción podría ser usar un servidor mediante la red.
- **Selección de Software.** En esta sección debemos elegir qué tipo de instalación queremos realizar, teniendo varias opciones.
  En nuestro caso elegimos la opción “Servidor con GUI”, esto quiere decir que vamos a destinar al equipo para servidor y que se instale el entorno gráfico. Si se tiene la suficiente experiencia, se recomienda realizar una instalación mínima para posteriormente agregar los paquetes estrictamente necesarios.
- **Destino de la Instalación.** Es la sección más importante en la cual elegimos el disco duro para instalar el sistema operativo. Podemos realizar un particionamiento avanzado con el uso de volúmenes. Para el uso de pruebas no es necesario crear particiones, así que elegimos la opción de “Configurar el particionado automáticamente”. De esta manera el sistema de instalación Anaconda, creará las particiones necesarias para el funcionamiento del mismo, sin tener un diseño de particiones avanzado como lo hemos analizado en este documento. Una vez seleccionado el disco y elegido las opciones de almacenamiento, podemos dar clic en el botón “Listo”, ubicado en la parte superior de la pantalla.
- **Red y nombre de Host.** En esta sección podemos configurar las propiedades necesarias para que el equipo se conecte a una red y al Internet



Una vez completada todas las secciones procedemos a dar clic en el botón “Comenzar instalación”. Mientras se copian los archivos y se instala el sistema, tenemos dos íconos que se encuentran con símbolo de advertencia (!), estos son: Contraseña de root y creación de usuarios. Este signo (!) nos indica que no se ha definido la contraseña de root y no se crearán usuarios adicionales al super administrador (root).Para definir la contraseña de root, le damos clic en “CONTRASEÑA DE ROOT”, se recomienda desde un inicio definir una contraseña segura que tenga al menos 8 caracteres combinados entre letras mayúsculas, letras minúsculas, números y caracteres especiales. Una vez que escribimos la contraseña, el sistema de instalación nos indica con una barra de colores, el nivel de seguridad de la misma.

Si no se requiere crear un usuario común, no es necesario ingresar a la sección “CREACIÓN DE USUARIO”. Para las pruebas utilizaremos el usuario root, por esta razón no es necesario crear usuarios adicionales.

Una vez que termina el proceso de instalación, el equipo se reiniciará y arrancará el sistema cargando lo necesario desde el disco duro. La primera vez que arranca el sistema, se solicita una configuración inicial.



Tenemos las opciones de “INFORMACIÓN DE LICENCIA” y nuevamente nos permite elegir si deseamos crear nuevos usuarios con la opción “CREACIÓN DE USUARIO”.

En la sección de “INFORMACIÓN DE LICENCIA”, nos aparecerá todo el texto del acuerdo de licencia que nos ofrece CentOS, es necesario que lo leamos para enterarnos de los detalles de la misma. Al final del texto, tenemos una casilla de verificación “Acepto el acuerdo de licencia”; para aceptar la misma, le damos un clic verificando que se señale con un visto. Seguidamente le damos clic en el botón “FINALIZAR CONFIGURACIÓN”. El sistema arrancará y estará listo para usarse.

2. Instalación y configuración básica de Arch Linux

La instalación de Arch Linux, es bajo consola de comandos, una vez que carga el instalador nos presentará la pantalla con las siguientes opciones:

- **Boot Arch Linux (x86_64).** Carga el instalador para procesadores de 64 bits.
- **Boot Arch Linux (i686).** Carga el instalador para procesadores de 32 bits.
- **Boot existing OS.** Arranca el equipo con el sistema operativo Arch Linux existente, si es el caso.
- **Run Memtest86+.** Corre un programa que realiza una prueba del correcto funcionamiento de la memoria RAM.
- **Hardware Information.** Corre un programa que presenta la información del hardware del equipo.
- **Reboot.** Reinicia el equipo
- **Power Off.** Apaga el equipo.

En nuestro caso poseemos un equipo con procesador de 64 bits, razón por la cual seleccionamos la primera opción. El equipo arrancará en modo texto, por lo que la instalación la debemos hacer con el uso de comandos.

La primera acción es establecer el lenguaje de instalación, ejecutamos el siguiente comando:

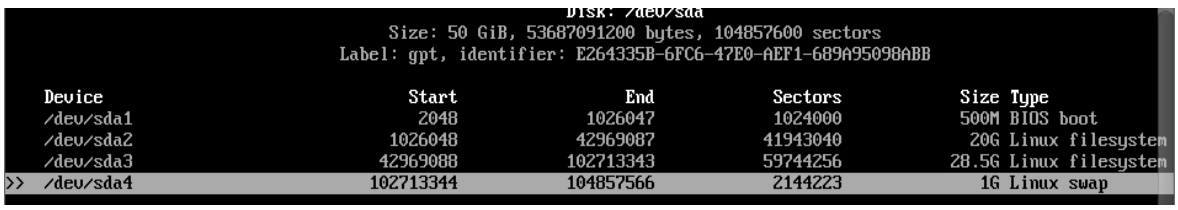
```
root@archiso ~# loadkeys es
```

Luego debemos crear las particiones del disco, tenemos varias opciones como: fdisk. gdisk, parted y cfdisk. En nuestro caso usaremos a cfdisk.


```
root@archiso ~# cfdisk
```

Hemos creado las siguientes particiones:

- **/dev/sda1** con punto de montaje /boot . Partición con 500Mb de espacio en disco, es donde se guardan las imágenes del kernel y todo lo necesario para el arranque del sistema.
- **/dev/sda2** con punto de montaje /. Partición con 20Gb de espacio en disco, es donde se guarda toda la información del sistema, excepto la información de las otras particiones creadas.
- **/dev/sda3** con punto de montaje /home. Partición de 28.5 Gb de espacio en disco, es donde se guarda la información de los usuarios.
- **/dev/sda4** para uso de swap. Partición de 1Gb de espacio en disco, es la memoria virtual.



Damos formato con el sistema de archivos ext4 a las particiones /dev/sda1, /dev/sda2 y /dev/sda3.

```
root@archiso ~# mkfs.ext4 -L boot /dev/sda1
root@archiso ~# mkfs.ext4 -L root /dev/sda2
root@archiso ~# mkfs.ext4 -L home /dev/sda3
```

Creamos la partición para el uso de memoria virtual (swap).

```
root@archiso ~# mkswap /dev/sda4
```

Activamos la memoria virtual.

```
root@archiso ~# swapon /dev/sda4
```

Ahora debemos montar las particiones creadas. La partición / la haremos en la carpeta /mnt.

```
root@archiso ~# mount /dev/sda2 /mnt
```

Posteriormente creamos las carpetas /boot y /home dentro de /mnt para poder montar esas particiones.

```
root@archiso ~# mkdir /mnt/boot
root@archiso ~# mkdir /mnt/home
```

Montamos las particiones boot y home.

```
root@archiso ~# mount /dev/sda1 /mnt/boot
root@archiso ~# mount /dev/sda3 /mnt/home
```

Ahora debemos probar que tengamos conexión a Internet, para ello usamos el comando ping de la siguiente manera:

```
root@archiso ~# ping www.google.com
PING www.google.com (200.63.214.53) 56(84) bytes of data.
64 bytes from 53.214.uio.satnet.net (200.63.214.53): icmp_seq=1 ttl=59 time=7.22 ms
64 bytes from 53.214.uio.satnet.net (200.63.214.53): icmp_seq=2 ttl=59 time=8.36 ms
64 bytes from 53.214.uio.satnet.net (200.63.214.53): icmp_seq=3 ttl=59 time=9.15 ms
64 bytes from 53.214.uio.satnet.net (200.63.214.53): icmp_seq=4 ttl=59 time=8.82 ms
^C
```

```
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 7.225/8.391/9.158/0.736 ms
```

Para instalar el sistema, Arch Linux pone a disposición un script llamado pacstrap, adicionalmente instalamos el paquete base-devel, para posterior compilación de paquetes.

```
root@archiso ~# pacstrap /mnt base base-devel
```

Ahora vamos a instalar el gestor de arranque GRUP.

```
root@archiso ~# pacstrap /mnt grub-bios
```

Luego instalamos el gestor de conexiones de red NetworkManager

```
root@archiso ~# pacstrap /mnt networkmanager
```

Debemos generar el archivo fstab, que trae la información de las particiones creadas.

```
root@archiso ~# genfstab -U -p /mnt >> /mnt/etc/fstab
```

Para realizar algunas configuraciones adicionales, nos enjaulamos con el comando arch-chroot.

```
root@archiso ~# arch-chroot  /mnt
```

Una vez encerrados podemos configurar ciertas cosas iniciales, como por ejemplo la zona horaria.

```
root@archiso ~# ln -s /usr/share/zoneinfo/America/Guayaquil /etc/localtime
```

Definimos el nombre del equipo.

```
root@archiso ~# vi /etc/hostname
```

Generamos la localización, editando el archivo:

```
root@archiso ~# vi /etc/locale-gen
```

Descomentamos la línea correspodiente a ecuador con UTF8

```
root@archiso ~# locale-gen
```

Instalamos el grub:

```
root@archiso ~# grub-install /dev/sda
```

Creamos el archivo de configuración del grub

```
root@archiso ~# grub-mkconfig -o /boot/grub/grub.cfg
```

Generamos el ramdisk

```
root@archiso ~# mkinitcpio -p linux
```

Definimos la contraseña de root

```
root@archiso ~# passwd
```

Instalamos el entorno gráfico si lo requerimos.

```
root@archiso ~#  pacman -S cinnamon cinnamon-control-center cinnamon-desktop cinnamon-screensaver cinnamon-session cinnamon-settings-daemon cinnamon-translations nemo

root@archiso ~# systemctl enable lxdm.service
```

Finalmente reiniciamos el equipo. Como podemos analizar para la instalación de esta distribución, se requiere de algunos conocimientos básicos de Linux.

3. Instalación y configuración básica de Ubuntu Server

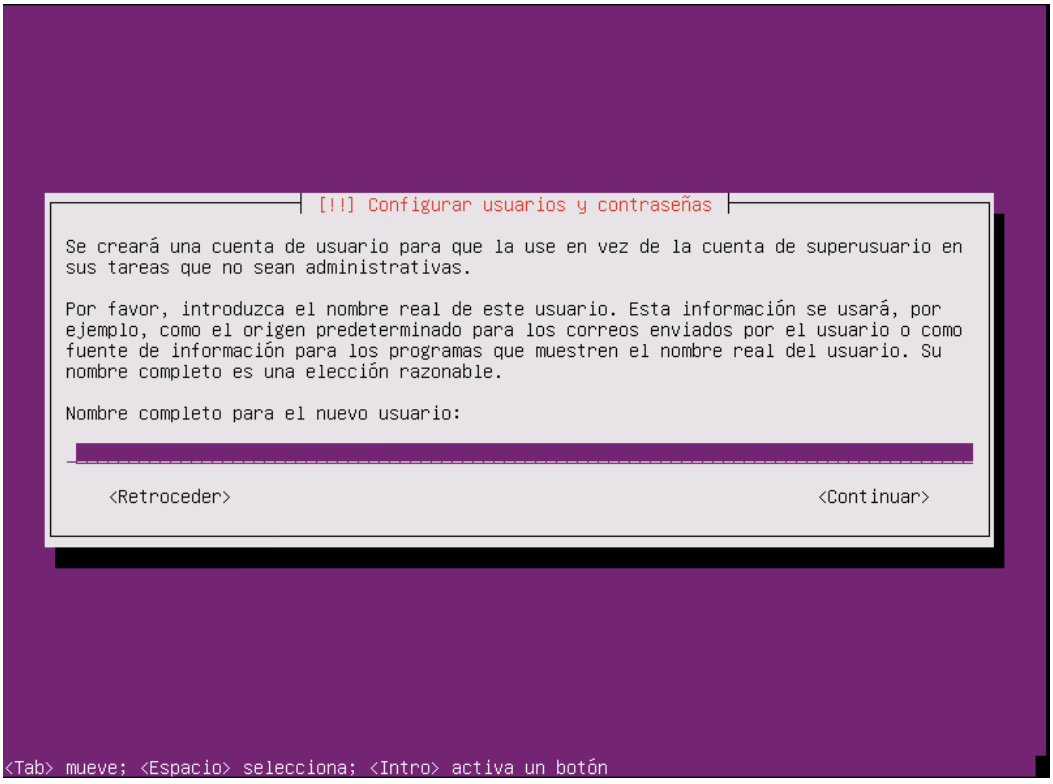
Ubuntu es una distribución que originalmente tiene una versión para equipos de escritorio, sin embargo Canonical provee la versión para servidores

Una vez cargada la imagen del instalador en la máquina virtual, la primera pantalla que obtenemos es para seleccionar el lenguaje de la instalación.

Luego de elegir el lenguaje para la instalación, se presenta la pantalla con las opciones que brinda el instalador, estas son:

- **Instalar Ubuntu Server.** Permite realizar una instalación nueva en el equipo.
- **Instalación de varios servidores con MAAS**. Permite instalar un servidor miembro de MAAS.
- **Comprobar defectos en el disco.** Comprueba si el disco duro tiene defectos.
- **Comprobar la memoria.** Realiza una prueba de memoria RAM.
- **Arrancar desde el primer disco duro.** Arranca el equipo desde una instalación preexistente.
- **Recuperar un sistema dañado.** Arranca el equipo a prueba de fallos, se usa cuando el sistema operativo instalado no arranca.

Elegimos la primera opción “Instalar Ubuntu Server”, mediante el cual arranca el instalador de Ubuntu Server.



La primera pantalla que presenta el gestor de instalación, permite elegir la zona horaria mediante la selección de país.

La siguiente pantalla facilita configurar el teclado, existen dos opciones: detectar automáticamente y elegir de una lista de opciones. La primera opción es la recomendable, siempre y cuando se mantenga el teclado al computador.

El siguiente paso de la instalación es la configuración de la red. Lo primero que nos solicita es el nombre del equipo. Si este es un servidor y está aliado a un dominio, le podemos asignar a éste como nombre del equipo. Si la máquina está dentro de una red LAN, se puede asignar un nombre que identifique al equipo.

Ubuntu es una distribución que no permite ingresar al sistema con el super usuario (root) con entorno gráfico, es por esta razón que se requiere crear una cuenta de usuario común para poder ingresar. La instalación está en modo texto, sin embargo se puede crear una cuenta de usuario y se le asigna una contraseña. Esta cuenta es la predeterminada y se la considera para el envío de correos por parte del sistema. No debemos olvidar asignar una contraseña segura que contenga al menos 8 caracteres y esté compuesta de una combinación de mayúsculas, minúsculas, números y caracteres especiales. La siguiente etapa de instalación es la configuración de la zona horaria.

El instalador en base a la localización del equipo, sugiere la zona horaria, en el caso de que sea correcta, simplemente debemos dar clic en “Sí” En nuestro ejemplo la zona horaria es “América/Guayaquil”.

El crear particiones del disco al igual que en las otras distribuciones, es el tema fundamental dentro de la instalación. Ububntu Server soporta volúmenes lógicos (LVM) de manera nativa, al igual que CentOS/RedHat, por su flexibilidad al manejo de particiones, es recomendable usar esta tecnología.

El instalador presenta las opciones para el particionado. Elegimos la que dice “Guiado – utilizar el disco completo y configurar LVM”.

El gestor de instalación realiza de manera automática la distribución de las particiones con LVM; sin embargo el mismo permite cambiar el tamaño de los volúmenes lógicos en el caso que se requiera. Para nuestro estudio al crear un entorno de pruebas, no se requiere cambiar la configuración creada automáticamente.

Una vez que se terminó con la creación de particiones, el sistema de instalación, presenta en pantalla el detalle de los cambios a ejecutarse en el disco y pregunta si se desea escribir dichos cambios o no. Aceptamos para que se aplique la configuración de las particiones en el disco.

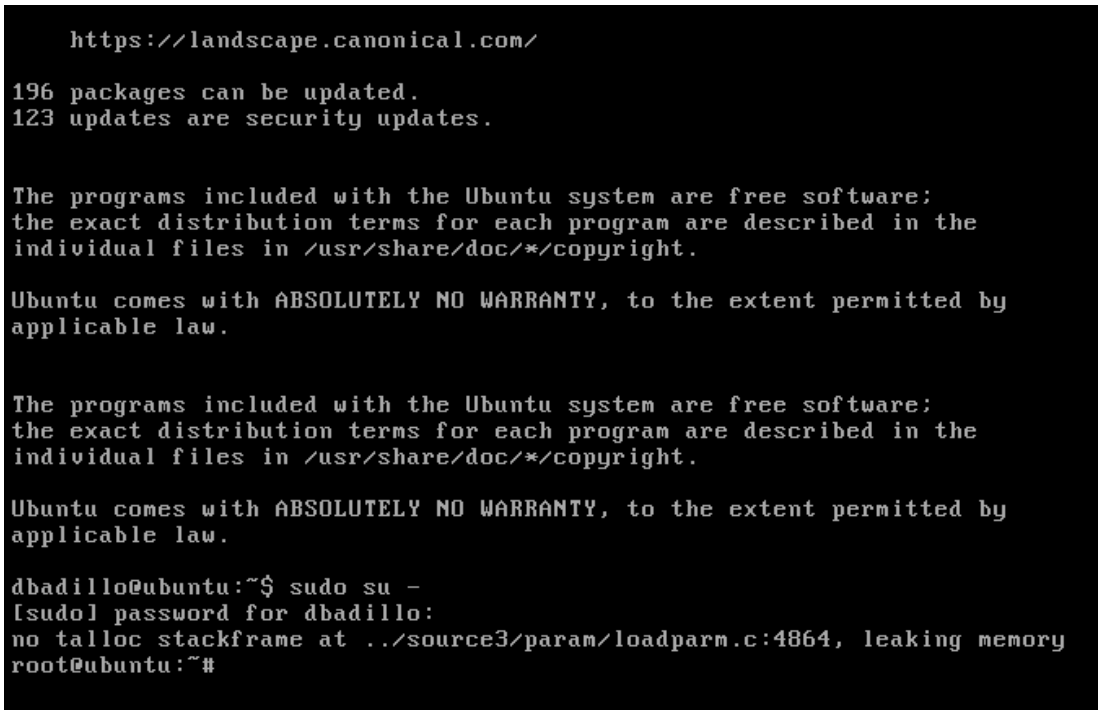
La siguiente pantalla del gestor de instalación, muestra las opciones para las actualizaciones del sistema, podemos configurar para que este proceso sea de manera automática o manual. Ubuntu presenta una herramienta llamada Landscape, la que permite actualizar, supervisar y gestionar el sistema Ubuntu; esta tiene un costo de licencia de uso. En nuestro caso elegimos la opción “Sin actualizaciones automáticas”, de esta manera se puede tener el control de qué se instala y cuando deseamos actualizar el sistema.

El gestor de instalación de Ubuntu detecta si existe un sistema operativo instalado en el equipo, esto se da cuando queremos configurar para que la máquina trabaje en modo dual.

En nuestro caso como es el único sistema, el instalador pregunta si deseamos cargar el gestor de arranque GRUB, le decimos que si; se instalará el gestor para seleccionar con que kernel deseamos arrancar el sistema, cada vez que prendamos o reiniciemos la máquina.

La última etapa de la instalación comprende la configuración de PAM, la cual coloca a este sistema de autenticación por defecto.

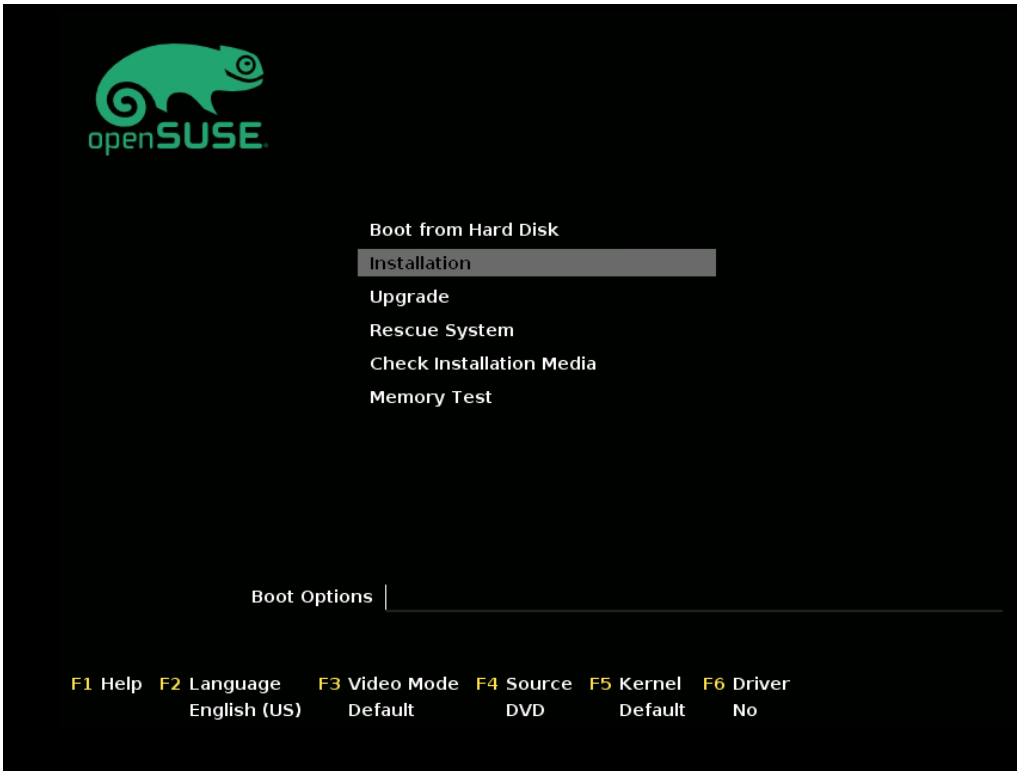
Una vez que termina el proceso de instalación, el equipo se reinicia para arrancar con el sistema cargado desde el disco duro. Cabe señalar que el sistema está en modo texto por lo que no tiene un entorno gráfico, se carga la consola de comandos.



La instalación de Ubuntu server, nos pareció muy intuitiva, sin inconvenientes en la configuración de los elementos que trae esta distribución. Al igual que para el resto de distros, se recomienda que una vez cargadas las aplicaciones requeridas, se realice una actualización del sistema para obtener los paquetes más recientes.

Ubuntu Server tiene un soporte de actualizaciones de 9 meses, sin embargo existe la versión LTS que para servidores brinda un soporte de 5 años. Se recomienda en el caso que se opte usar esta distribución, utilizar la versión LTS, de lo contrario 9 meses es un tiempo muy corto de soporte.

4. Instalación y configuración básica de Open Suse



Una vez creada la máquina virtual y cargada la imagen del instalador de esta distribución, aparece la pantalla con las siguientes opciones:

- **Boot from Hard Disk.** Permite arrancar desde el disco duro, en el caso de que exista un sistema previamente instalado..
- **Installation.** Arranca el gestor de instalación.
- **Rescue System.** Inicia el equipo en modo de rescate, para solucionar problemas de un sistema preexistente.
- **Check Installation Media.** Realiza una inspección del instalador.
- **Memory Test.** Ejecuta el test de la memoria RAM.

Le damos clic en la opción “Installation” para arrancar el gestor de instalación de esta distribución.

Lo primero que nos aparece es el acuerdo de licencia, se recomienda leer completamente este documento. Esta pantalla también selecciona el idioma de instalación y la distribución del teclado. Elegimos “Español” como lenguaje para la instalación y teclado.

Debemos recalcar que la distribución de teclas en español latinoamericano es diferente al del español castellano.

Se lo puede diferenciar por la posición de la @ que en el teclado latinoamericano se encuentra en la tecla Q, a diferencia del teclado en español que se encuentra en el número 2.

La siguiente pantalla presenta las opciones de instalación, estas son:

- **Añadir repositorios en línea antes de la instalación.** Agrega servidores de paquetes para ser tomados en cuenta al momento de instalar.

- **Incluir productos adicionales desde medios separados.** Permite que se pueda realizar la instalación de paquetes desde medios externos como CD-ROM o flash memory.

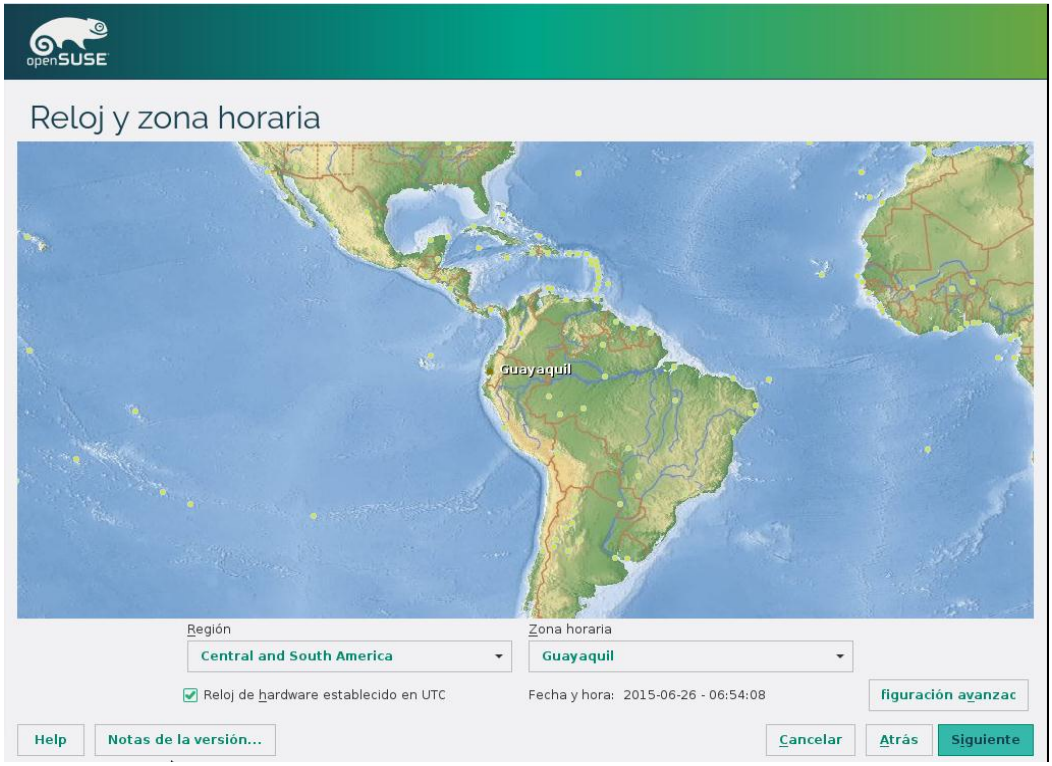
La primera opción es recomendable, sin embargo se descargarán paquetes desde el Internet, lo que puede ocasionar una demora en la instalación. En la segunda opción si tenemos paquetes adicionales la podemos usar, caso contrario no tiene objeto hacerlo.

Debemos recalcar que se deben agregar repositorios oficiales de la distribución, y así garantizar la calidad de los paquetes a instalarse. Cuando agregamos repositorios fantasmas, puede ser que el sistema presente problemas con diferentes paquetes de software. El comportamiento y estabilidad de un sistema Linux, depende directamente de los paquetes instalados, por lo que debemos garantizar que el software sea validado por la distribución, caso contrario aumenta un porcentaje considerable de que el equipo falle

Open SUSE realiza una propuesta de particionado de disco, si el usuario lo requiere puede personalizar esta configuración. Al igual que lo hicimos en la instalación de las otras distribuciones, procedemos en aceptar la propuesta realizada por el gestor.

La siguiente etapa de instalación, es la configuración del reloj y zona horaria. El instalador presenta un mapa para seleccionar la zona horaria, en el caso de que no se pueda ubicar por medio del mapa, en la parte inferior del mismo, nos ofrece dos cajas de selección. En la primera caja, elegimos el continente, en nuestro caso “Central and South America”. En la segunda caja, determinamos Guayaquil, no existe la opción Quito u otra ciudad del

Ecuador a excepción de Galápagos por estar en otro uso horario.



Como elegimos en un paso anterior el uso de repositorios en línea, la siguiente etapa de la instalación, presenta los repositorios disponibles para ser agregados. Seleccionamos las opciones de los repositorios: principal OSS, principal NON-OSS, actualizaciones de depuración, principal fuente y principal de actualizaciones.

No agregamos los repositorios DEBUG, ya que pueden contener paquetes de prueba, tampoco el repositorio que contiene paquetes que no son software libre, en todo caso posteriormente se puede agregar o quitar cualquier repositorio.

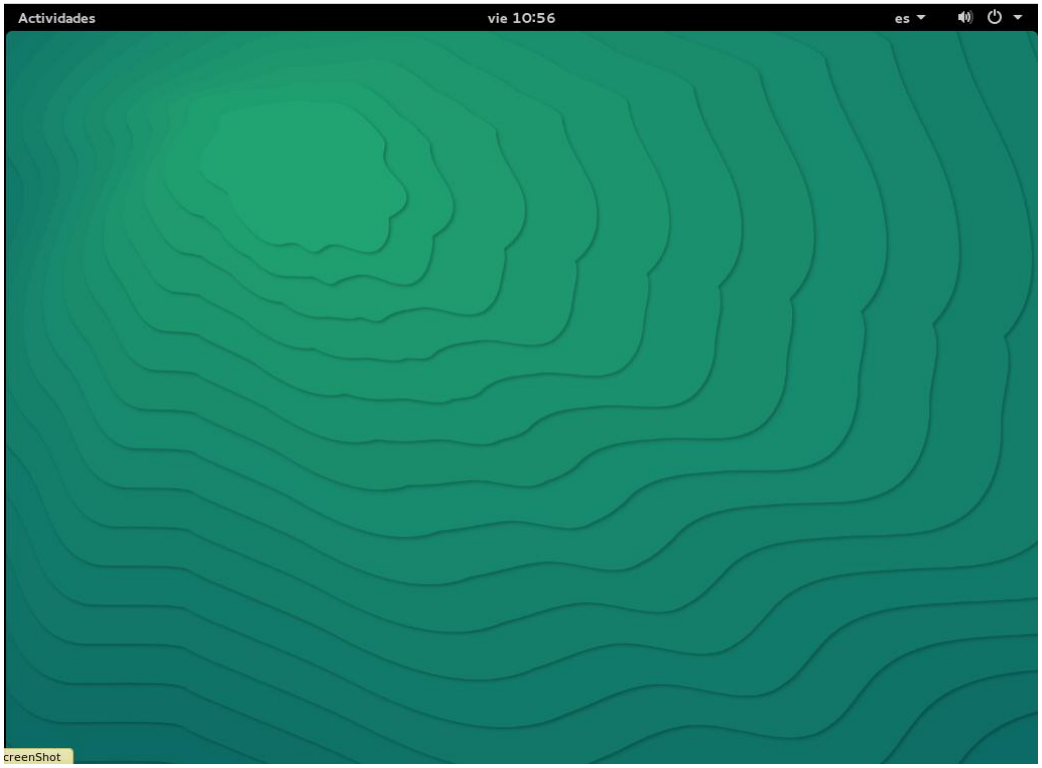
Open SUSE brinda la opción de seleccionar el entorno de escritorio; los principales son: GNOME Desktop y KDE Desktop. En nuestro caso elegimos a GNOME como entorno de escritorio.

El gestor de instalación pide se cree un usuario común al cual se le puede dar algunas opciones, estas son:

- Utilizar esta contraseña para administrar el sistema.
- Recibir correo del sistema.
- Inicio de sesión automático.

La etapa final de la instalación comprende un resumen de las configuraciones realizadas; en el caso que se encuentre un error en cualquiera de las etapas de instalación, podemos rectificar en este paso. Si todo está correcto procedemos a dar clic en “Instalar”. Luego de que se realice el proceso de instalación el equipo se reiniciará, seguidamente registramos a un usuario y estaremos listos para utilizar esta distribución.

.



5. Instalación y configuración básica de Debian

Una vez cargada la imagen del instalador de Debian, la primera pantalla nos presenta las opciones del instalador, estas son:

- **Install.** Carga el gestor de instalación en modo texto.
- **Graphical Install.** Inicia el gestor de instalación con interfaz gráfica
- **Advanced Options.** Ejecuta el gestor brindando opciones avanzadas para la instalación.
- **Help.** Presenta documentación de ayuda para la instalación.
- **Install with speech synthesis.** Arranca el gestor de instalación con síntesis de voz, una nueva herramienta de Debian.

En nuestro caso elegimos la segunda opción “Graphical Install”, permitirá cargar el gestor de instalación en modo gráfico.

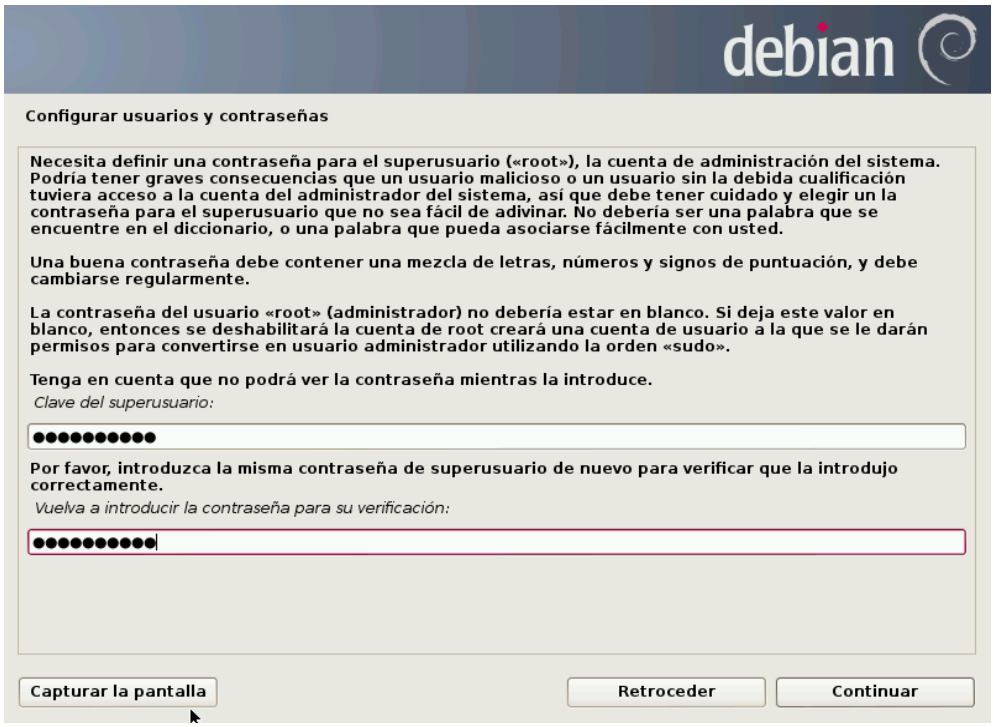
La primera pantalla del instalador, permite la selección del idioma para el sistema de Debian, en nuestro caso elegimos “Español”.

La siguiente pantalla permite determinar la ubicación geográfica, elegimos Ecuador.

A continuación debemos seleccionar la distribución del teclado. Al igual que lo detallamos en la instalación de las otras distribuciones, el teclado es “Español”.

Luego el instalador permite realizar la configuración de la red. Debemos ingresar el nombre del equipo.

Siguiendo el proceso de instalación, ubicamos la contraseña del super usuario root, debemos recalcar que esta contraseña debe ser muy segura, se recomienda que tenga al menos 8 caracteres combinados entre letras mayúsculas, minúsculas, números y caracteres especiales. Cuando se ingresan claves débiles, estamos exponiendo a nuestro servidor de manera peligrosa.



El super administrador permite realizar cualquier tarea dentro del sistema, razón por la cual, debemos tener el mayor cuidado al usar esta cuenta pues intencional o no, puede causar mucho daño al mismo.

Este paso permite ubicar la zona horaria, al igual que en las otras distribuciones, tenemos para el Ecuador dos zonas: Guayaquil (-5) y Galápagos (-6). La primera representa al Ecuador continental y la segunda a la región insular. Seleccionamos a Guayaquil.

El seleccionar la zona horaria ayudará a coordinar el tiempo mediante un servidor NTP, el que provee de fecha y hora para el equipo.

Es recomendable que todos los computadores, más aún servidores, tengan la información sincronizada. Los registros del sistema y otros utilitarios, deben guardar los datos de fecha y hora correcta; dependiendo la zona horaria en la que se encuentre la máquina.

Las opciones para la creación de particiones de disco son:

- **Guiado – utilizar todo el disco.** Crea las particiones necesarias para instalar el sistema, utilizando todo el espacio del disco duro.
- **Guiado – utilizar el disco completo y configurar LVM.** Realiza la misma configuración del punto anterior, con la diferencia que utiliza LVM

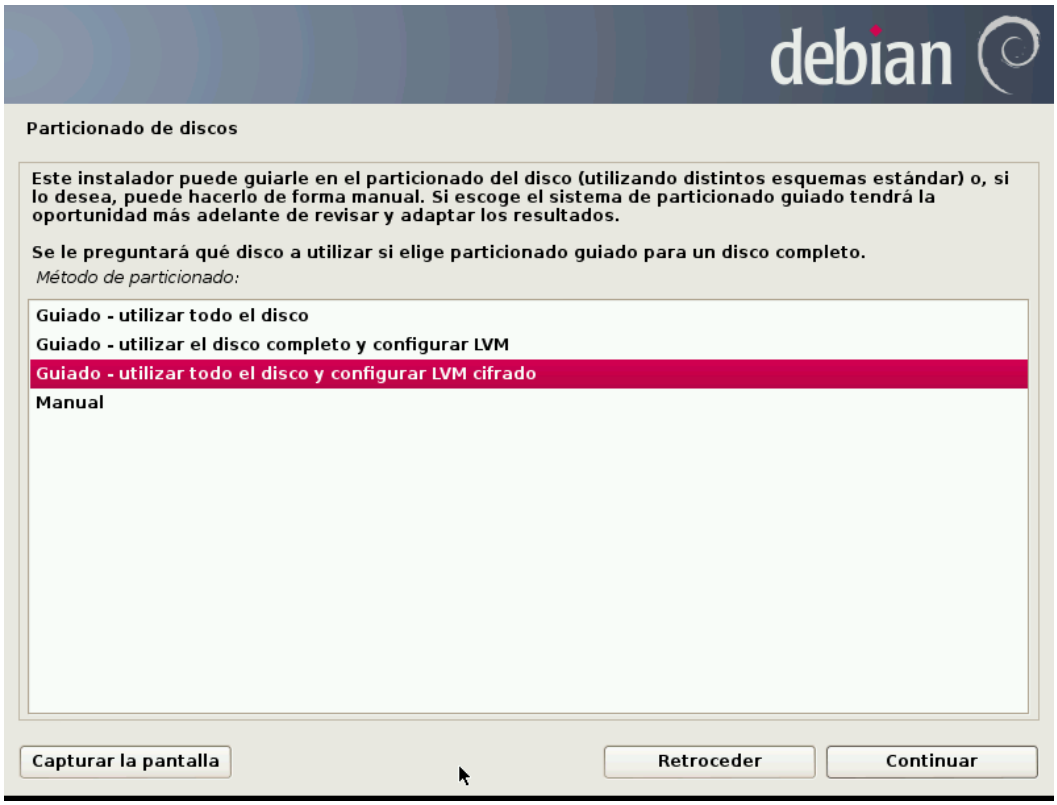
- **Guiado – utilizar todo el disco y configurar LVM cifrado.** En esta se añade la opción de cifrar las particiones.

- **Manual.** Permite crear las particiones de manera manual.

Seleccionamos la opción de “Guiado – utilizar todo el disco y configurar LVM cifrado”, nos permitirá utilizar volúmenes lógicos y cifrar las particiones.

El gestor de instalación presenta dos opciones para crear las particiones del disco:

- **Separar la partición /home.** Crea la partición para /home, en la cual se guardan los datos de los usuarios, el resto del sistema se guarda en la partición raíz (/).



- **Separar las particiones /home, /usr, /var y /tmp.** Separa en particiones las carpetas home, usr, var y tmp.

Elegimos la tercera opción, ya que tendremos una mejor organización de la información en el sistema, teniendo separados en particiones, los datos de los usuarios, programas y del sistema en general.

La siguiente pantalla permite determinar la contraseña para el cifrado de las particiones, en nuestro caso se encriptará la partición /home, la que contiene los datos de los usuarios. La contraseña puede tener máximo 20 caracteres, se sugiere tenga al menos 6 combinados entre letras mayúsculas, minúsculas, números y caracteres especiales.

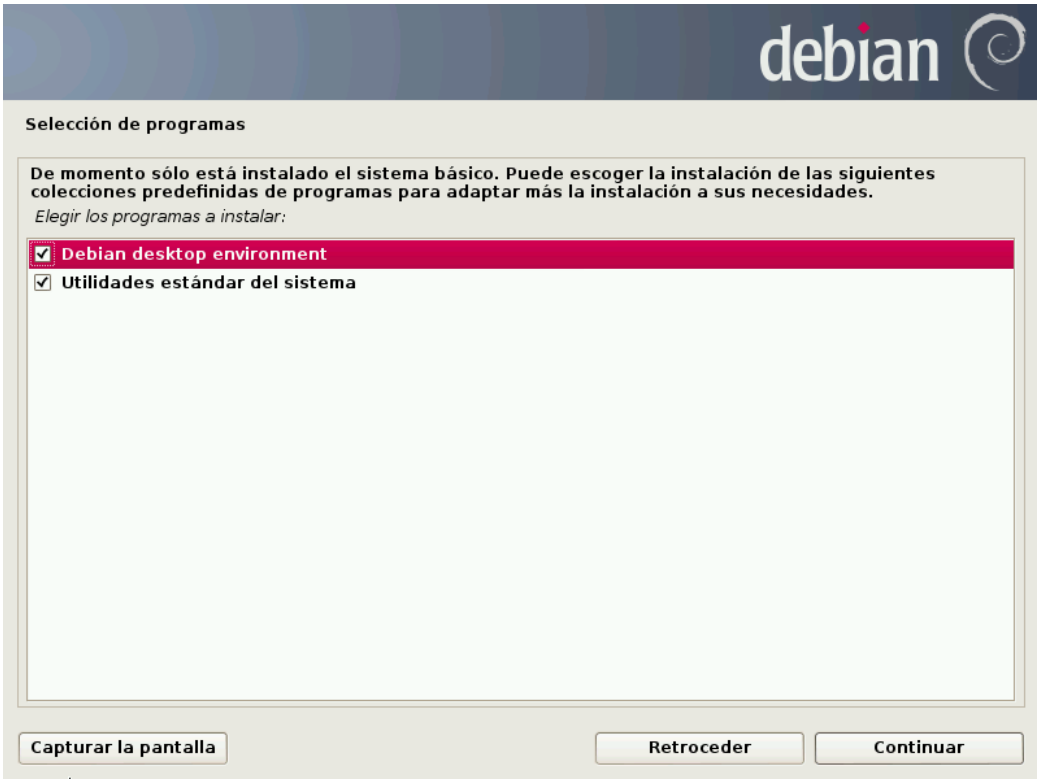
Luego se presenta un detalle de las particiones a crear en el disco, debemos revisar minuciosamente y aceptar en el caso de que no existan errores. Elegimos la opción que indica “Finalizar el particionado y escribir los cambios en el disco”.

Ahora debemos elegir los programas adicionales a instalar en el sistema, tenemos dos opciones:

- **Debian desktop environment.** Instala los paquetes necesarios para brindar una interfaz gráfica.

- **Utilidades estándar del sistema.** Carga paquetes adicionales a los necesarios del sistema.

Seleccionamos las dos opciones.



La última pantalla permite instalar el gestor de arranque GRUB, como no tenemos un sistema preexistente, le damos clic en “Sí” y continuamos con la instalación.

6. Instalación y configuración básica de Mageia

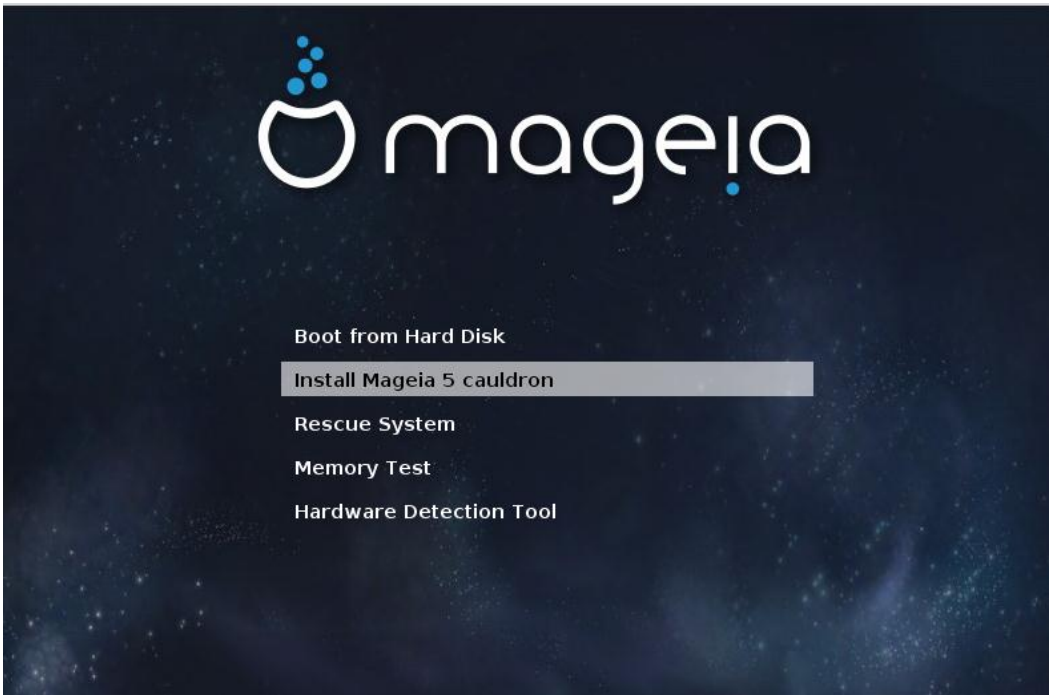
Una vez cargada la imagen del instalador de Mageia, se presenta la pantalla con las opciones de instalación, estas son:

- **Boot from Hard Disk.** Arranca el equipo desde el disco duro en el caso de que exista un sistema Linux instalado.

- **Install Mageia 5 cauldron.** Inicia el gestor de instalación de Mageia.

- **Rescue System.** Ejecuta el sistema en modo de rescate, para corregir errores del sistema previamente instalado.
- **Memory Test.** Realiza una prueba de la memoria RAM.
- **Hardware Detection Tool.** Herramienta para detectar los dispositivos de hardware del equipo.

Seleccionamos la opción “Install Mageia 5 cauldron” para arrancar el gestor de instalación.



La primera pantalla del gestor de instalación permite seleccionar el idioma, elegimos la opción “Español”.

La siguiente pantalla nos presenta el acuerdo de licencia, seleccionamos en “Aceptar” y continuamos con la instalación.

Luego la pantalla presenta la opción de seleccionar el teclado, en nuestro caso elegimos “Español”.

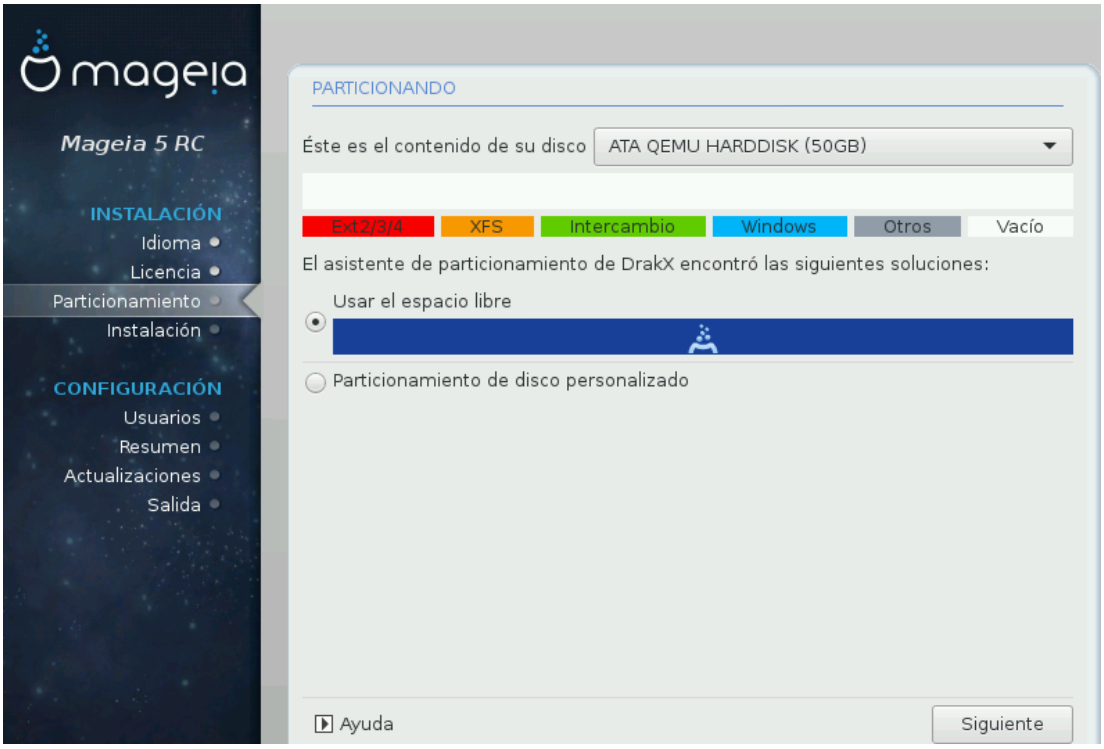
La siguiente página permite crear las particiones del disco, al igual que en otras distros, el gestor de instalación sugiere la distribución de particiones, estas son:

- **Usar espacio libre.** Crea una distribución del disco automáticamente por DrakX.

- **Particionamiento de disco personalizado.** Permite al usuario crear la distribución de particiones como lo desee, esta opción está diseñada para usuarios más experimentados.

Como es un entorno de prueba, seleccionamos la primera opción, en la que el gestor de instalación se encarga de crear las particiones automáticamente.

A continuación debemos elegir opcionalmente, algún medio como fuente para la instalación, diferente a la imagen cargada.

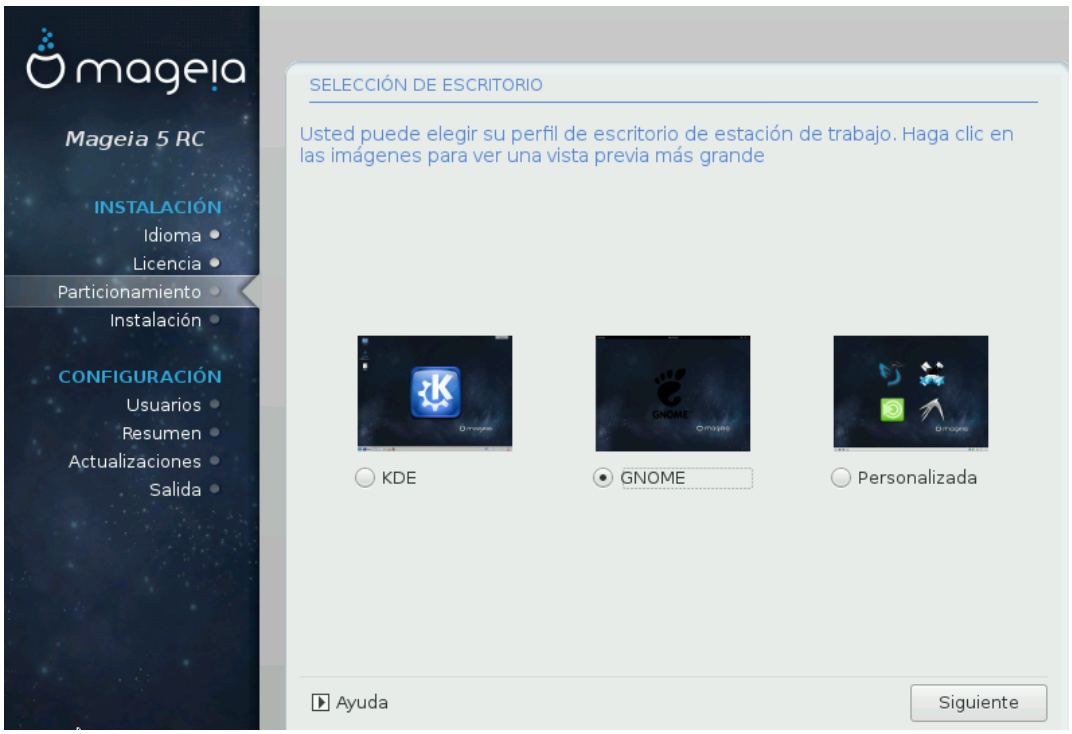


Es muy poco frecuente el uso de esta opción, ya que los paquetes están cargados en el mismo instalador. Determinamos la opción de “Ninguno” y continuamos con la instalación

La última pantalla de configuración previa a la instalación, presenta las opciones para seleccionar el entorno de escritorio a usar, estas son:

- KDE.
- GNOME
- Personalizada

Se puede seleccionar cualquiera de los entornos, todo depende del gusto del usuario, en nuestro caso utilizaremos GNOME.



Una vez ubicado el entorno de escritorio, damos clic en “Siguiente” y comenzará a instalar el sistema, luego de este proceso tendremos algunas opciones de configuración.

La primera pantalla post instalación presenta la opción para determinar la contraseña del super administrador (root) y la creación de usuarios comunes. En nuestro caso determinamos la contraseña de root.

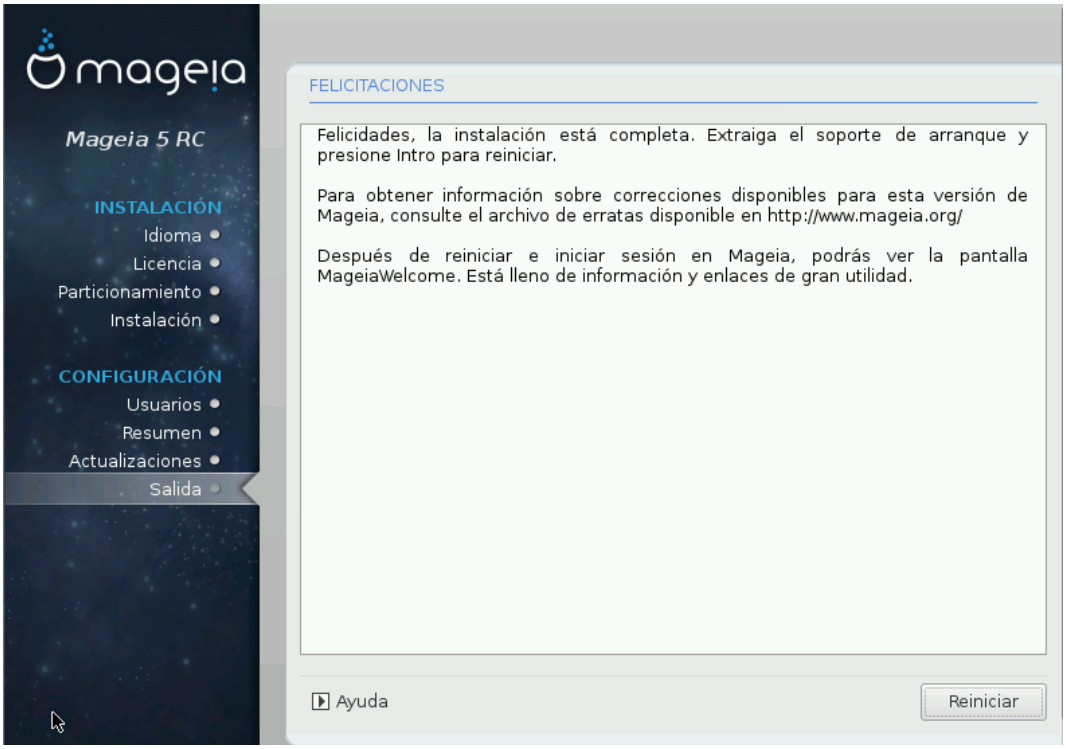
La segunda pantalla permite la configuración del monitor, elegimos la opción “plug and play”.

La tercera pantalla post instalación presenta el resumen de las configuraciones que realizamos en el proceso de instalación. En esta pantalla tenemos la opción de cambiar la configuración si se lo requiere.

La cuarta pantalla presenta la opción de actualizar el sistema. Como lo hemos sugerido es importante que se ejecuten las actualizaciones, esto permite muchas veces corregir problemas de seguridad que se pueden presentar en paquetes obsoletos. Mageia nos sugiere que lo hagamos antes de ingresar al sistema por primera vez. Seleccionamos “Sí”, este proceso puede tardar varios minutos ya que se deben descargar los paquetes de Internet e instalarse.

Luego de actualizado, Mageia presenta un mensaje de felicitaciones, indicando que el proceso de instalación se realizó con total éxito. Nos pide que debemos extraer el medio de arranque del instalador, para permitir que el equipo arranque desde el disco duro.

El proceso de instalación de esta distribución fue muy amigable e intuitivo, además que el gestor de instalación permite configurar varias características del sistema de manera muy fácil para el usuario. También debemos destacar que el gestor de instalación presenta leyendas en cada pantalla lo cual sirve de ayuda para entender lo que estamos configurando.



ANEXO D: Documento Guía – Instalación de CentOS7

1. Objetivo

Describir el proceso de instalación de Linux CentOS 7, paso a paso, para que este sirva de sistema base en la instalación de servicios de red.

2. Consideraciones

El proceso descrito en la presente guía de instalación está diseñado para sistemas Linux Red Hat Enterprise 7 o equivalente clon CentOS 7.

También debemos recalcar que el proceso descrito en la guía corresponde a la instalación de un sistema base, sin que se especifique la instalación de ningún servicio de red.

Para una mejor comprensión en la instalación se utilizó como entorno base a “Servidor con GUI”, esto significa que se instalará el sistema con entorno gráfico para mayor facilidad de uso. Para usuarios avanzados se recomienda utilizar el tipo de instalación “Minimal”, el que está basado en consola de comandos sin entorno gráfico.

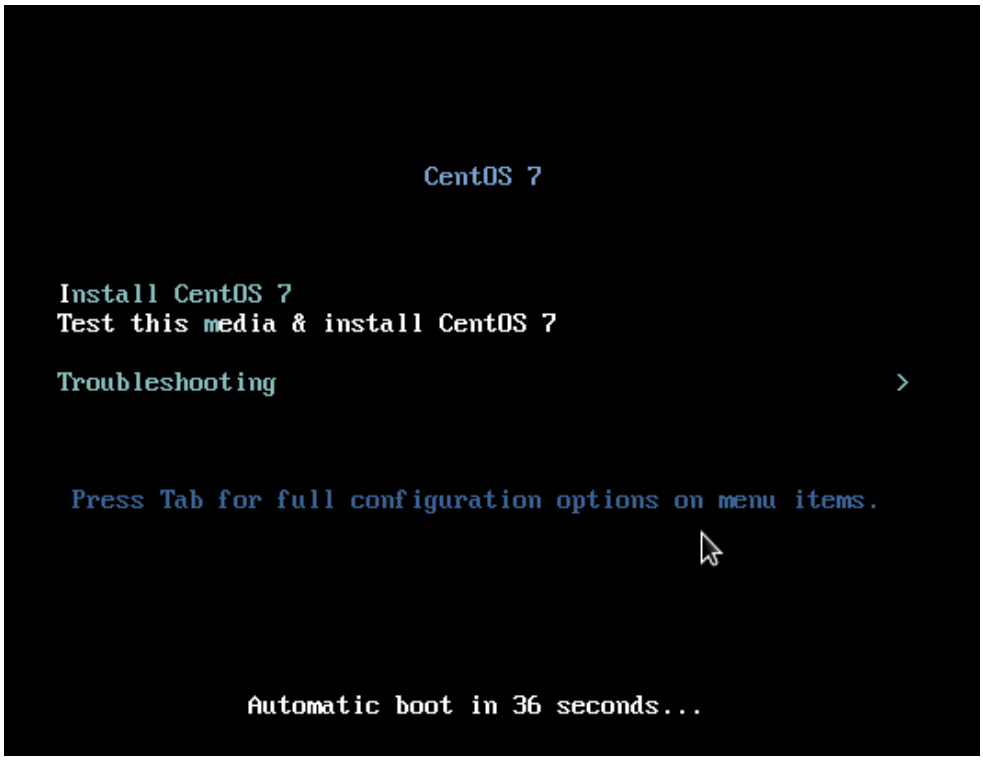
3. Proceso de Instalación

El proceso de instalación comienza con el arranque del equipo utilizando el ISO descargado desde cualquier servidor espejo de CentOS, en nuestro caso lo obtuvimos desde el repositorio del CEDIA: http://mirror.cedia.org.ec/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1503-01.iso. La imagen se la puede quemar en un DVD o se puede grabar en una USB-FLASH.

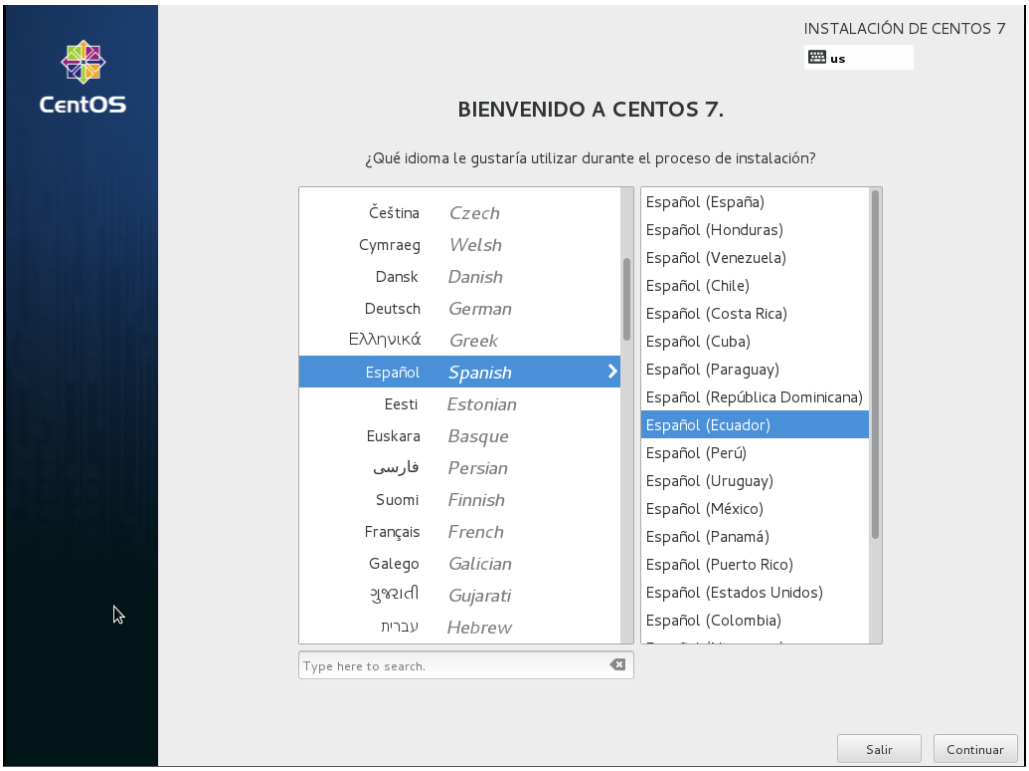
Una vez que tenemos nuestro medio de instalación, procedemos a configurar en el BIOS del equipo, para que el servidor arranque desde el medio elegido (DVD ROM o USB-FLASH). Grabamos los cambios del BIOS e iniciamos la máquina. Una vez cargada la ISO tendremos la pantalla con las opciones del instalador, elegimos la primera opción “Install CentOS 7”.

El instalador de CentOS se denomina “Anaconda”, el cual comienza por un chequeo del CD, DVD, USB-FLASH u otro medio, que tarda varios minutos. Si estamos seguros de que

el medio de instalación no tiene errores, podemos presionar la tecla “Esc” para saltar este paso.



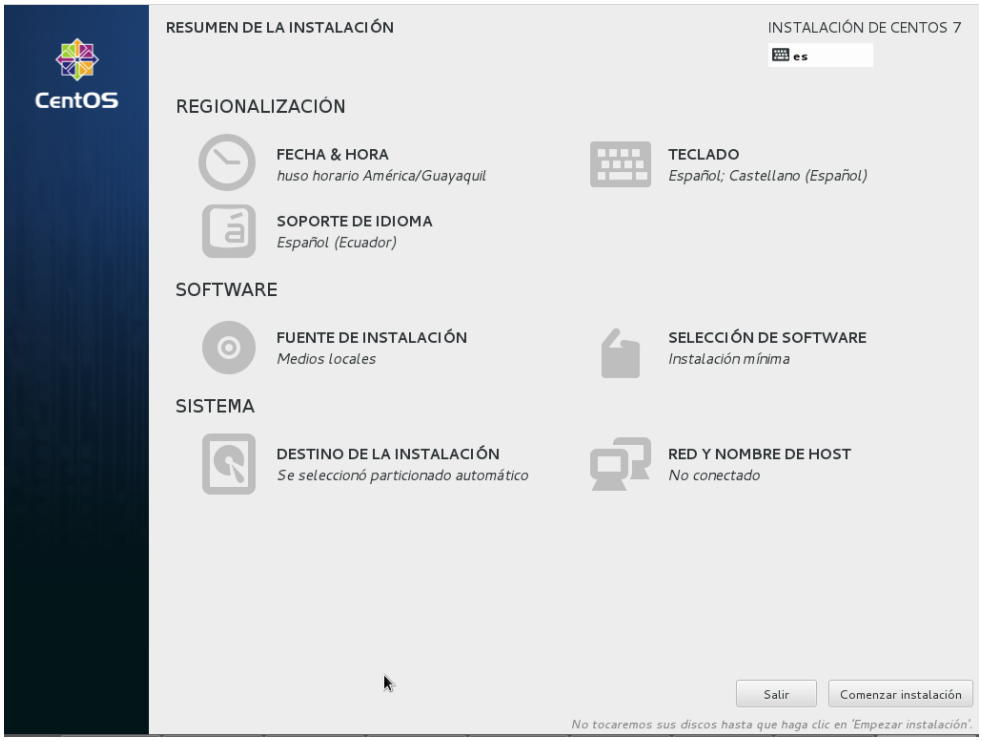
La primera pantalla presenta la selección del idioma que se desea utilizar para el proceso de instalación, también el idioma del teclado.



Es fundamental no obviar este paso, pues posteriormente debemos determinar contraseñas, las cuales pueden contener caracteres especiales y la precisión de las mismas depende de la distribución del teclado seleccionado.

Una vez seleccionado el idioma, le damos clic en “Continuar”, el instalador nos presenta una vista general de configuración con las siguientes opciones:

- Fecha y Hora
- Teclado
- Soporte de Idioma
- Fuente de Instalación
- Selección de Software
- Destino de la Instalación
- Red y Nombre del Host



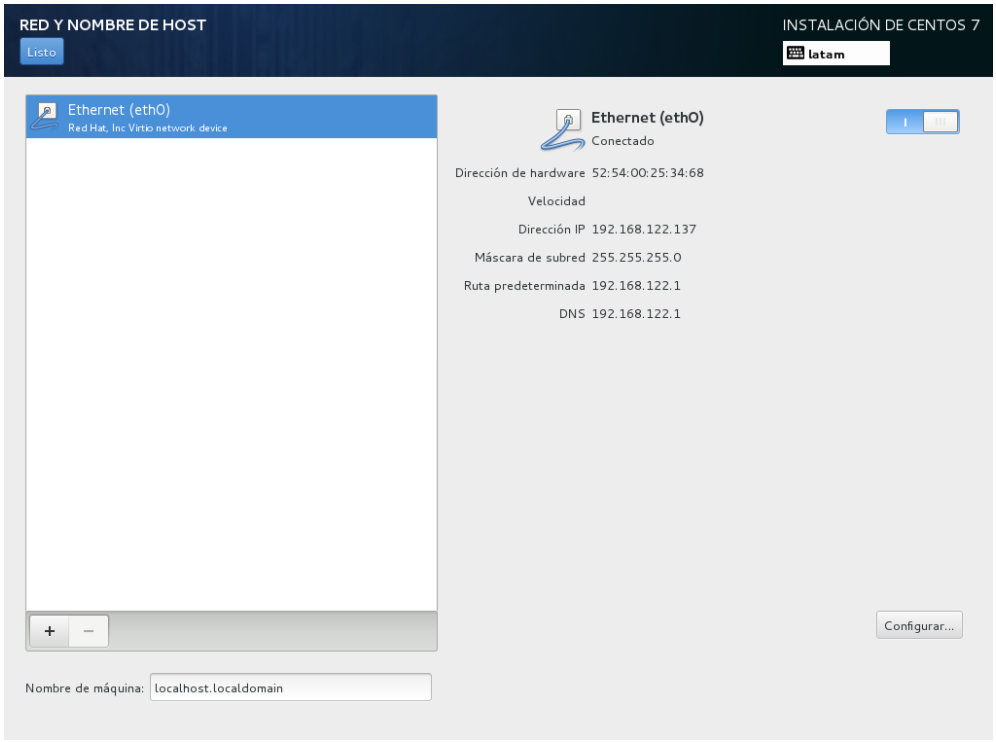
Las secciones de “Soporte de Idioma” y “Teclado” estarán preseleccionadas según lo elegido en paso anterior, sin embargo debemos diferenciar que son dos cosas distintas: La selección del idioma y distribución del teclado en esta sección es para el sistema, en cambio el del paso anterior determina el idioma y distribución de teclado para este proceso de instalación.

Luego de seleccionado el idioma, se recomienda configurar la red, en el caso de que el equipo esté conectado al Internet. Debemos elegir la opción “Red y Nombre de Host”; si tenemos un servidor DHCP, encendemos la red.

En esta pantalla también tenemos la opción de configurar manualmente los parámetros, para ello necesitamos la siguiente información:

- Dirección IP (IP Address)
- Máscara de Subred (Netmask)
- Puerta de Enlace (Gateway)
- Servidores de DNS (Al menos 2)

El tener acceso a la Internet, permite posteriormente configurar la fecha y hora mediante el uso de un servidor NTP.

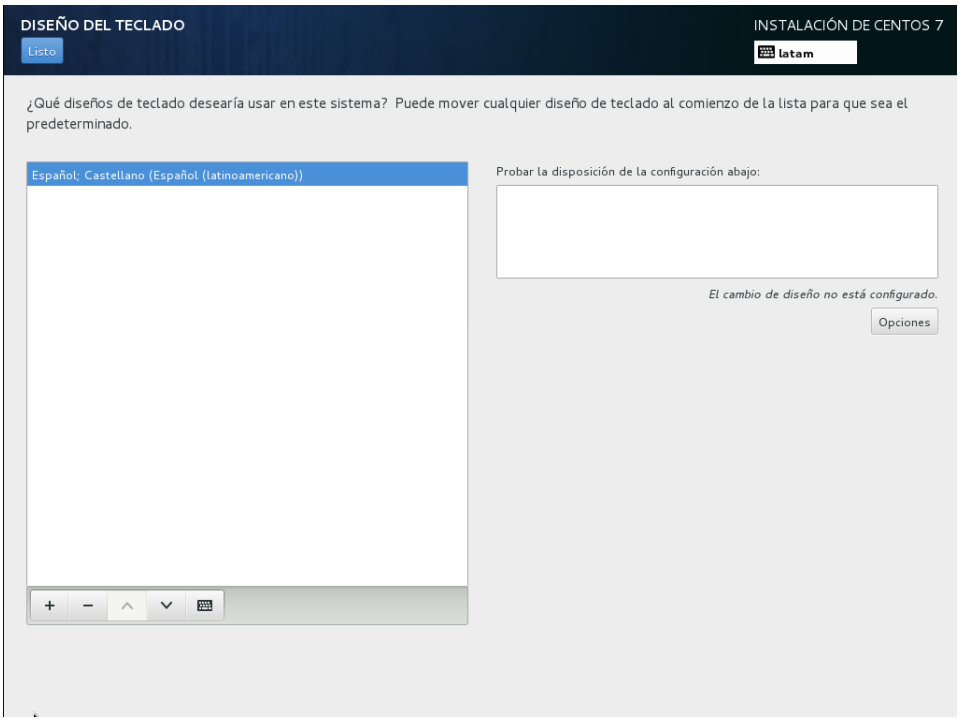


En esta sección también debemos indicar el nombre del equipo, en caso de que tengan registrado un dominio, pueden utilizarlo para determinar el nombre del servidor. Por ejemplo, si el equipo es para un servidor de correo, se puede asignar el nombre “mail.dominio.com”, para un servidor web, puede ser “www.dominio.com”.

No existe problema si ingresamos cualquier nombre de máquina, sin embargo recomendamos que esté acorde al uso del servidor.

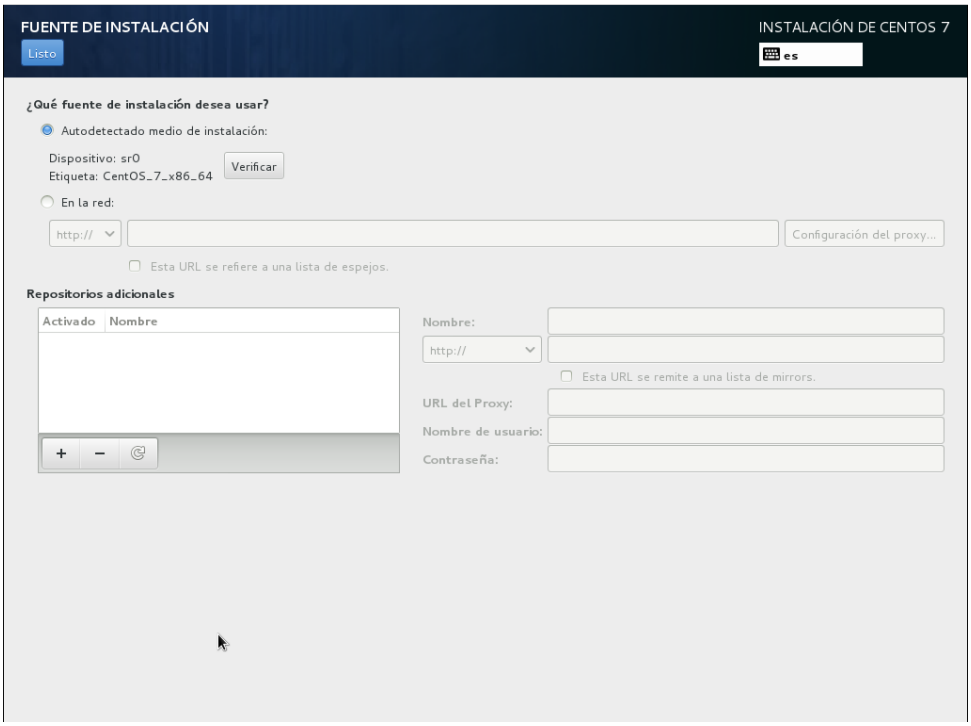
En la sección “Fecha y Hora” determinamos la zona horaria y la fecha y hora. Si estamos conectados al Internet, podemos activar la opción “Hora de red” para el uso de un servidor NTP. En nuestro caso la región es “America” (sin tilde), ciudad es “Guayaquil”. No existe otra ciudad del Ecuador a excepción de Galápagos con una hora menos. Le damos clic en el botón “Listo”.

En la sección “Diseño del Teclado” podemos cambiar la distribución determinando el idioma del teclado. Por defecto estará seleccionado el elegido en la primera pantalla del instalador. Le damos clic en el botón “Listo”.



En la sección “Fuente de Instalación” debemos seleccionar desde donde se copiarán los archivos para la instalación. Por defecto estará el propio CD/DVD/USB-FLASH, lo podemos dejar así.

Le damos clic en el botón “Listo”



Si contamos con un servidor de instalación bajo los protocolos httpd, ftp o nfs, podremos escoger la fuente remota. Cuando se desea realizar instalaciones masivas es recomendable instalar un servidor de instalación, el cual tiene la imagen completa de CentOS y es consumida por algún protocolo de red.

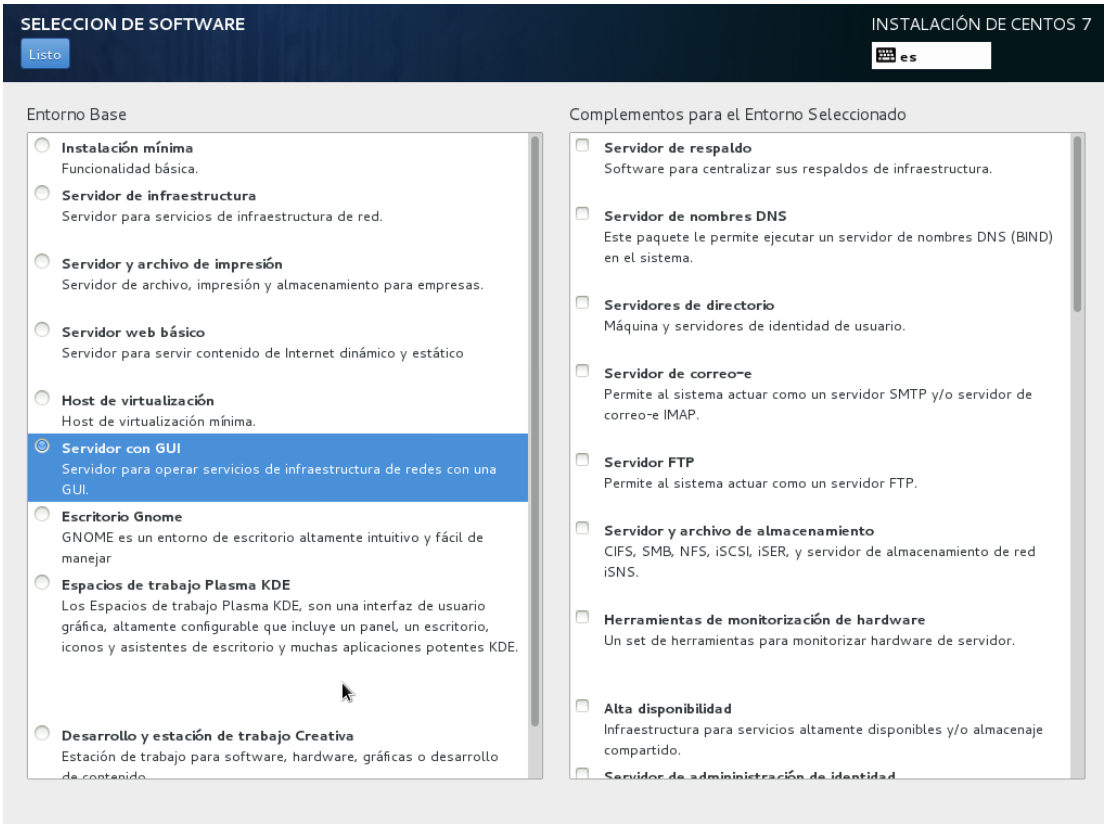
También se puede generar instalaciones desatendidas, mediante el uso de plantillas de instalación llamada kickstart.

En la sección “Selección de Software” podemos elegir que paquetes de programas serán instalados, las opciones son:

- **Instalación mínima.** Instala lo necesario sin interfaz gráfica (recomendado).
- **Servidor de infraestructura.** Instala los paquetes base más algunos servicios de red.
- **Servidor y archivo de impresión.** Instala los paquetes base más servidores de archivo e impresión.
- **Servidor Web básico.** Instala los paquetes base más el servidor web apache.
- **Host de virtualización.** Instala el servidor base y los paquetes para virtualización.

- **Servidor con GUI.** Instala los paquetes base más la interfaz gráfica.
- **Escritorio Gnome.** Instala los paquetes base más la interfaz gráfica, con el entorno de escritorio GNOME.
- **Espacios de trabajo Plasma KDE.** Instala los paquetes base más la interfaz gráfica, con el entorno de escritorio KDE.
- **Desarrollo y estación de trabajo creativa.** Instala los paquetes base más el software para desarrollo y herramientas gráficas.

Cada opción tiene el detalle de los paquetes a instalar en la parte derecha de la pantalla, pues así, Anaconda permite especificar el software que deseamos cargar al sistema operativo.



Para usuarios avanzados, recomendamos seleccionar “Instalación mínima”, debemos recordar que este tipo de instalación no incluye interfaz gráfica. Para la elaboración de esta guía utilizamos la opción “Servidor con GUI”. Le damos clic en el botón “Listo”.

En la sección “Destino de la Instalación” elegimos el disco duro destino. Abajo en “Otras opciones de almacenamiento” seleccionamos “Voy a configurar las particiones”. Le damos clic en el botón “Listo”.

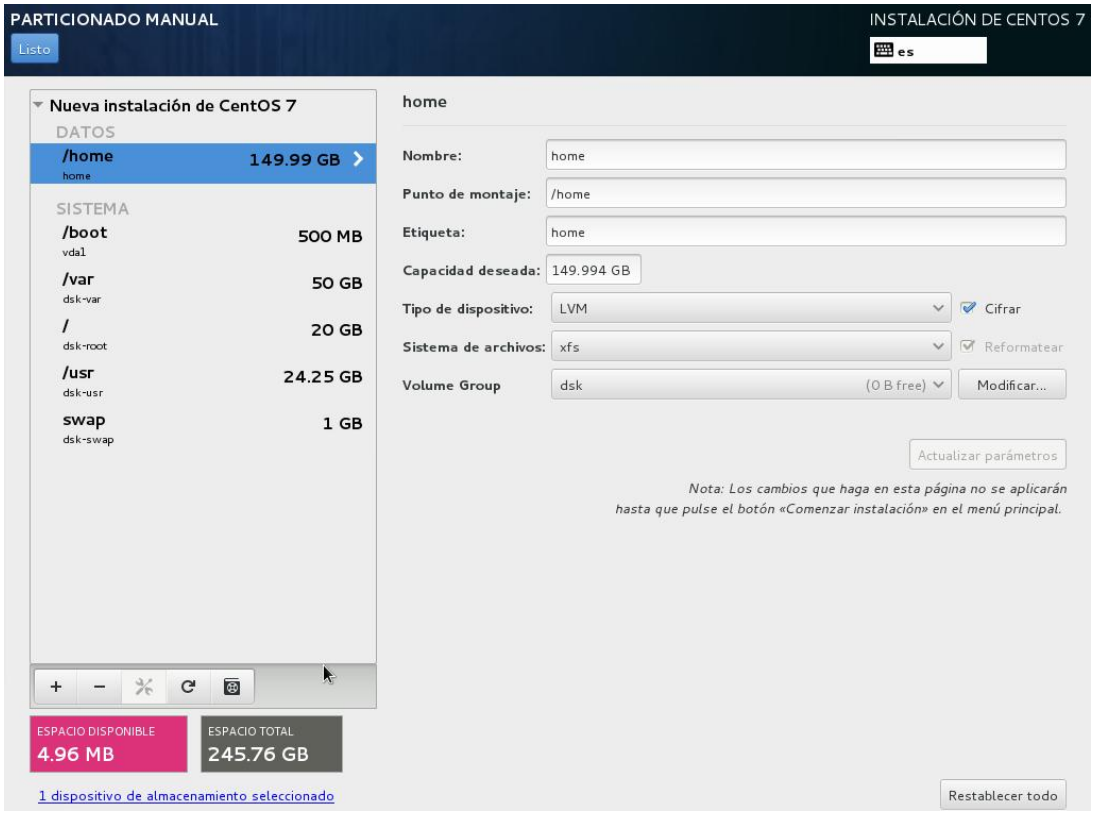
Aparece una pantalla para crear las particiones manualmente. La distribución de particiones depende de dos aspectos fundamentales:

1. **Espacio del disco.** Cuál es el tamaño que disponemos para la instalación.
2. **El propósito del servidor.** No es lo mismo instalar un servidor de base de datos que un servidor de archivos o correo. La diferencia está en la carga de información a guardar en las particiones. Por ejemplo, si instalamos un servidor de base de datos, la carga de información estará en la partición “/var”; en cambio si instalamos un servidor de archivos, la carga estará en la partición /home.

Bajo estos dos parámetros debemos crear un diseño de particiones, recomendamos al menos crear las siguientes:

- **/boot.** Es la partición donde se almacena las imágenes del kernel y lo necesario para el arranque del sistema.
- **/var.** Se almacenan datos variables, como registros del sistema, bases de datos, buzones de correo electrónico.
- **/home.** Guarda la información de los usuarios.
- **/usr.** Se usa para almacenar fundamentalmente los programas, comandos, etcétera.
- **/ .** Es la partición raíz donde se guarda toda la información, excepto las detalladas en las otras particiones.
- **Swap.** Es la memoria virtual.

La distribución de particiones en un disco de 240G, se otorgó la mayor carga de información a la partición home.



Citaremos algunas consideraciones adicionales:

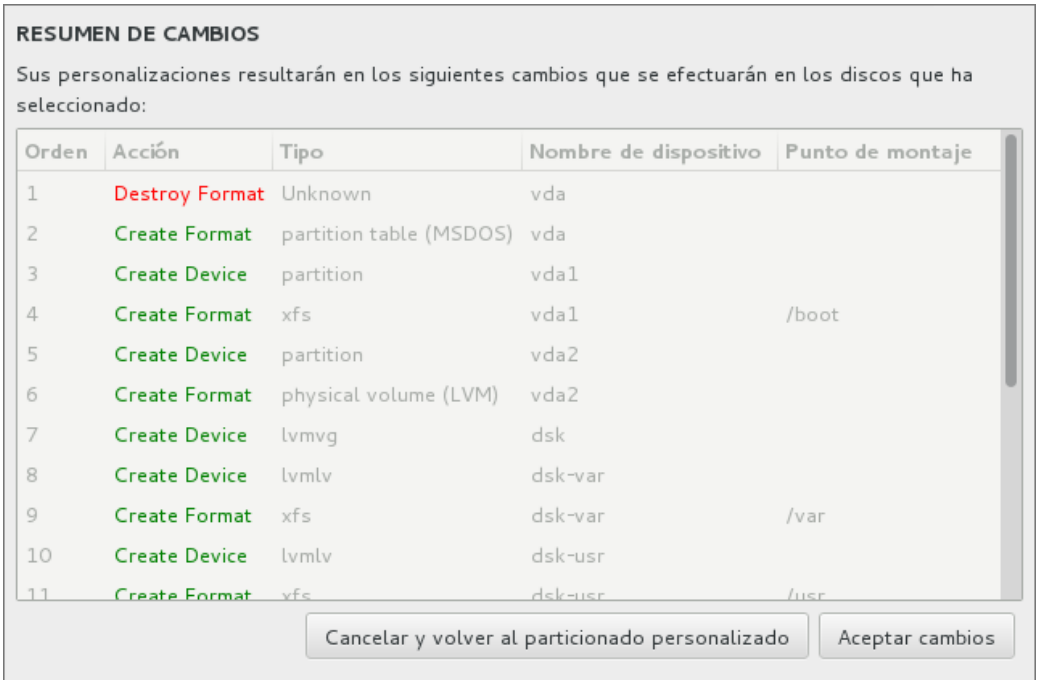
- La partición /boot no debería ser mayor a 500MB.

- La partición para la swap se la calcula en relación a la memoria RAM. Cuando la RAM es menor a 1GB, la swap debe ser el doble. Cuando RAM es mayor a 1GB la swap debe ser la mitad de la memoria RAM sin superar los 2GB.

Para proteger la información que se guarde en una partición se recomienda cifrar, no es necesarlas a todas, algunas no contienen datos específicos. Nuestra recomendación es cifrar la partición /var y /home.

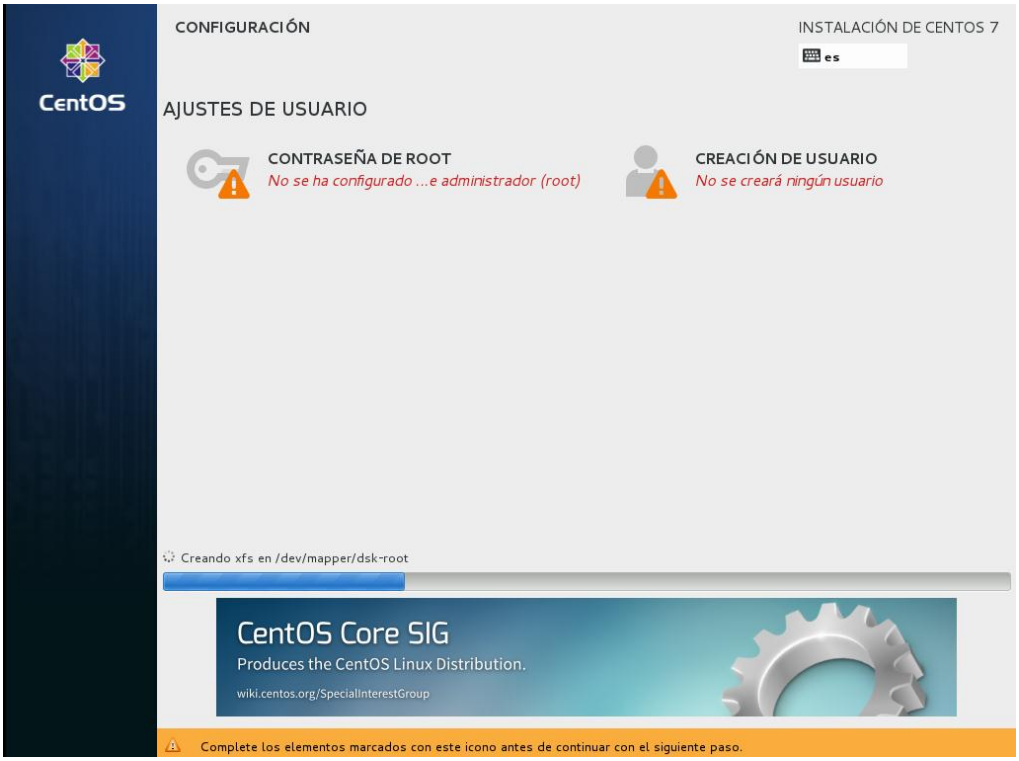
Por cada partición que elijamos cifrar, el instalador nos solicitará determinar una contraseña de cifrado.

Al finalizar la configuración de particiones le damos clic en el botón de “Listo”, aparecerá una pantalla con el resumen de cambios a ejecutar en el disco. Debemos revisar la información y dar clic en el botón “Aceptar cambios”.



Una vez configuradas todas las secciones, le damos clic en “Comenzar Instalación”. El instalador iniciará con la copia de archivos al disco, mientras este proceso se ejecuta tenemos dos secciones adicionales a configurar:

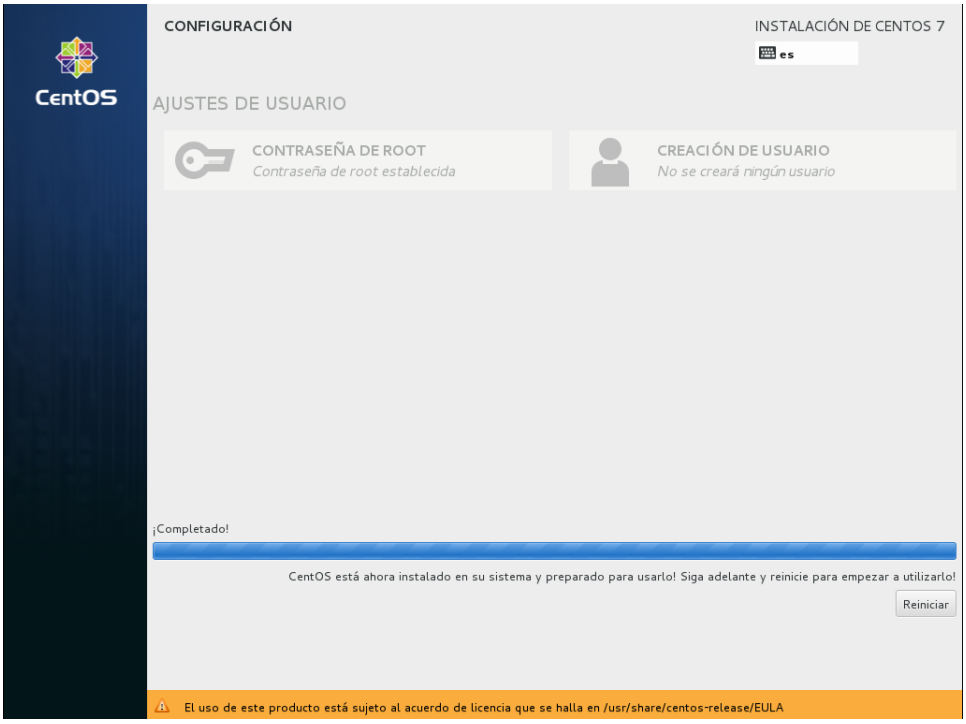
- Contraseña de ROOT
- Creación de Usuarios



En la sección “Contraseña de Root” debemos determinar la clave que debe ser segura. El instalador cuenta con un sistema de valoración de contraseña, es recomendable ingresar una clave robusta de al menos 10 caracteres combinados entre letras mayúsculas, minúsculas, números y caracteres especiales.

Luego de configurar la contraseña de root le damos clic en el botón “Listo”. El tiempo de instalación toma varios minutos, dependiendo del medio utilizado y la velocidad del disco duro.

Una vez finalizado el proceso de instalación aparecerá el botón “Reiniciar”, le damos clic. El equipo se reiniciará, podemos extraer el medio de instalación, así garantizamos el arranque del equipo desde el disco duro.



ANEXO D: Documento Guía – Aseguramiento de Linux CentOS 7

1. Objetivo

Describir los procesos a realizar para asegurar (endurecer) a Linux CentOS 7.

2. Consideraciones

El proceso descrito en la presente guía de instalación, está diseñado para sistemas Linux Red Hat Enterprise 7 o equivalente clon CentOS 7.

La presente guía describe los procesos a seguir para endurecer el sistema operativo base, este documento no incluye el aseguramiento de servicios específicos.

3. Proceso de Aseguramiento

La seguridad de un servidor implica realizar un sin número de procesos para minimizar los riesgos a los que está expuesto el equipo. La presente guía analiza algunos aspectos fundamentales que debemos aplicar a nuestro servidor, para asegurarlo, estos son:

1. Consideraciones del BIOS.
2. Contraseña del gestor de arranque GRUB2.
3. Actualización del sistema.
4. Instalación cortafuegos (Firewall).
5. Consideraciones SELinux.
6. Deshabilitar los servicios innecesarios.
7. Endurecer el sistema de archivos.
8. Instalar escáner de vulnerabilidades.
9. Instalar IDS/IPS.
10. Consideraciones de las cuentas de usuario.
11. Deshabilitar el acceso remoto para el usuario root

3.1. Consideraciones del BIOS

Cuando un atacante tiene acceso físico a un equipo, la seguridad está seriamente amenazada, éste puede realizar varias acciones para afectar al sistema. Es recomendable que el servidor se encuentre en un cuarto adecuado con las seguridades necesarias, para evitar el acceso a personal no autorizado que puede hacer mal uso del equipo.

Cuando hablamos de seguridad, siempre debemos pensar en el peor escenario y tratar de minimizar las opciones que tengan los atacantes para ejecutar algún daño en el equipo. La primera acción es asegurar y configurar adecuadamente el BIOS.

El BIOS es el primer programa que se ejecuta al momento que arranca el computador, su función principal es verificar el hardware del equipo y cargar el sistema operativo llamando al gestor de arranque (GRUB2).

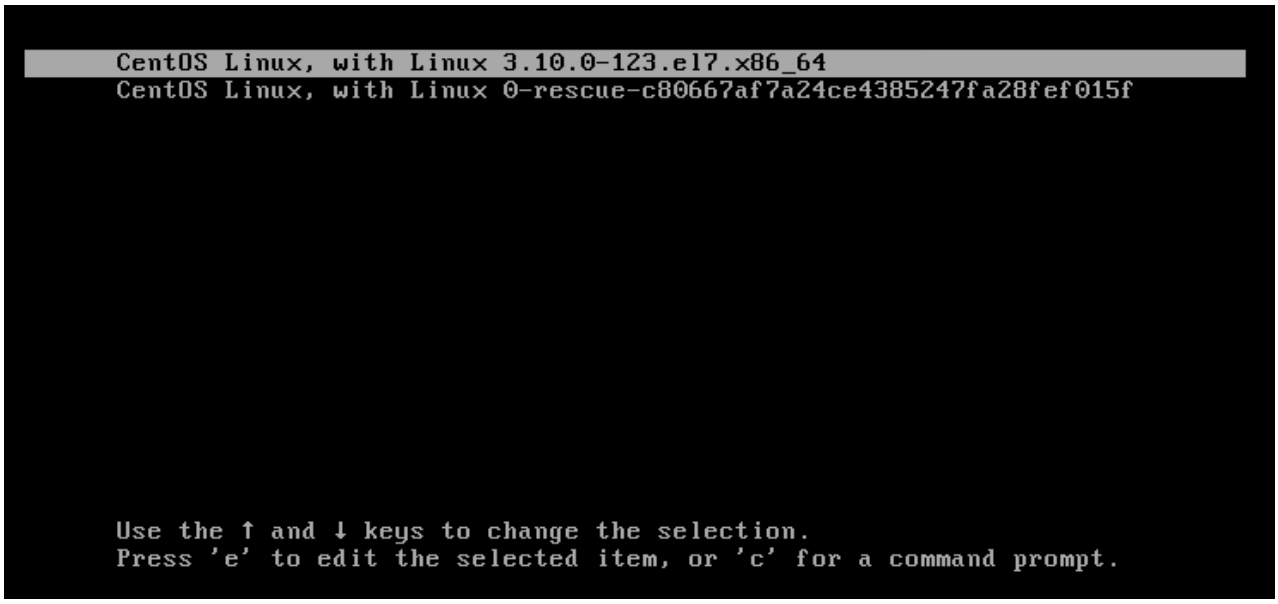
En la actualidad el BIOS tiene una serie de opciones que pueden ayudar a la seguridad, a continuación señalamos algunas:

- Permitir el arranque solamente desde el disco duro (Deshabilitar el arranque desde medios ópticos y externos).
- Si lo admite, activar la protección contra virus.
- Establecer la contraseña del BIOS.

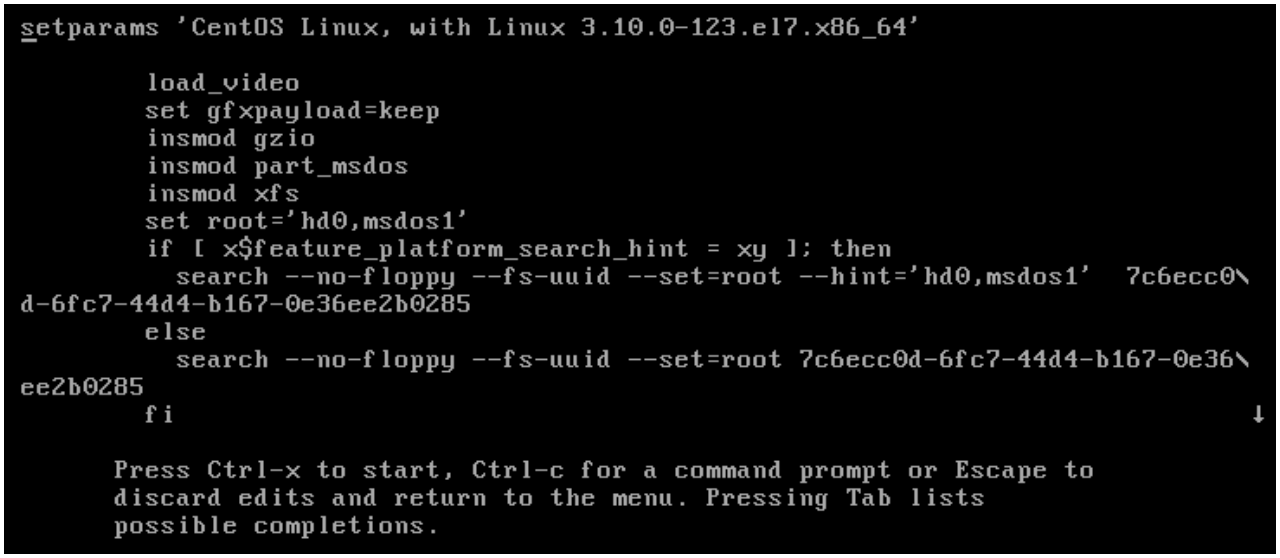
3.2. Contraseña del gestor de arranque GRUB2.

GRUB (GNU GRand Unified Bootloader) es el gestor de arranque utilizado por CentOS, permite iniciar el sistema operativo. Este gestor puede controlar varios kernel, incluso de otras distribuciones o sistemas operativos.

Al prender el equipo, luego de que carga el BIOS, este ejecuta el gestor de arranque, el cual presenta un menú para que el usuario seleccione el kernel con el que quiere iniciar el equipo.



Como podemos visualizar en la Figura 36, en la parte de abajo de la pantalla tenemos la opción ´e´ para editar los parámetros del kernel. Si un usuario no autorizado tiene la opción de editar los parámetros, este puede iniciar el sistema con opciones que le permitan alterar el correcto funcionamiento del equipo o que le faciliten cambiar la contraseña del super usuario root, sin conocer previamente la misma.



Para evitar que usuarios no autorizados tengan acceso para editar los parámetros del kernel, podemos proteger al gestor de arranque con una contraseña, a continuación detallamos el proceso para determinar la clave del GRUB.

Para mayor seguridad debemos utilizar una contraseña cifrada, para ello ejecutamos el siguiente comando:

```
[root@pruebas ~]# grub2-mkpasswd-pbkdf2
Introduzca la contraseña:
Reintroduzca la contraseña:
El hash PBKDF2 de su contraseña es grub.pbkdf2.sha512.10000.951B940C16BC2A8DCDA59CF2A14AAEEB524D5DDE5B26FFFAE84F726B9E4E476D1905913771ADFF096A2277EFD8EF65F7297B6A05A303DD49A2EBEA098AD21F1F.2697F0246B34957ACB46A6020054DBEBCDD1898AF9C751AC0B19F5C329A6706FB0F27050558689A9879CF8CEADEA6246B914AFD117C472B7BF10B987D9DDD910
[root@localhost ~]#
```

El comando ***grub2-mkpasswd-pbkdf2*** presenta en pantalla la contraseña cifrada, debemos copiar la clave y editar el archivo **/etc/grub.d/10_linux.**

```
[root@pruebas ~]# vi /etc/grub.d/10_linux
```

Al final del fichero debemos insertar el siguiente código:

```
cat << EOF
set superusers="admin"
password_pbkdf2 admin grub.pbkdf2.sha512.10000.951B940C16BC2A8DCDA59CF2A14AAEEB524D5DDE5B26FFFAE84F726B9E4E476D1905913771ADFF096A2277EFD8EF65F7297B6A05A303DD49A2EBEA098AD21F1F.2697F0246B34957ACB46A6020054DBEBCDD1898AF9C751AC0B19F5C329A6706FB0F27050558689A9879CF8CEADEA6246B914AFD117C472B7BF10B987D9DDD910
EOF
```

Dicho código contiene la contraseña cifrada generada por el comando grub2-mkpasswd-pbkdf2, la segunda y tercera línea indican que queremos usar al usuario con nombre “admin”. No es un usuario del sistema, puede ser cualquier nombre. Grabamos el archivo.

Para que los cambios surtan efecto debemos generar nuevamente el archivo de configuración del GRUB2, para ello ejecutamos lo siguiente:

```
[root@pruebas ~]# grub2-mkconfig -o /boot/grub2/grub.cfg
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-3.10.0-123.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-123.el7.x86_64.img
Warning: Please don't use old title `CentOS Linux, with Linux 3.10.0-123.el7.x86_64' for GRUB_DEFAULT, use `Advanced options for CentOS Linux>CentOS Linux, with Linux 3.10.0-123.el7.x86_64' (for versions before 2.00) or `gnulinux-advanced-42db7f2a-2163-42d8-a9f4-044519ce4994>gnulinux-3.10.0-123.el7.x86_64-advanced-42db7f2a-2163-42d8-a9f4-044519ce4994' (for 2.00 or later)
Found linux image: /boot/vmlinuz-0-rescue-c80667af7a24ce4385247fa28fef015f
Found initrd image: /boot/initramfs-0-rescue-c80667af7a24ce4385247fa28fef015f.img
[root@localhost ~]#
```

3.3. Actualización del sistema.

Una característica fundamental de RHEL/CentOS es que brinda soporte por 10 años, esto quiere decir que tienen la obligación de proporcionar actualizaciones de los paquetes por todo el tiempo de soporte.

Las actualizaciones no solo se refieren al aumentar o mejorar un software, un gran porcentaje de las mismas tienden a corregir problemas de seguridad. Un servidor actualizado aumenta enormemente la protección del sistema operativo.

Para actualizar el sistema debemos abrir una consola de comandos y ejecutar lo siguiente:

```
[root@localhost ~]# yum -y update
```

```
Complementos cargados:fastestmirror, langpacks
base                                    | 3.6 kB     00:00
extras                                  | 3.4 kB     00:00
updates                                 | 3.4 kB     00:00
updates/7/x86_64/primary_db             | 3.9 MB   00:04
Loading mirror speeds from cached hostfile
 * base: mirror.espoch.edu.ec
 * extras: mirror.espoch.edu.ec
 * updates: mirror.espoch.edu.ec
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete NetworkManager.x86_64 1:0.9.9.1-13.git20140326.4dba720.el7 debe ser obsoleto
---> Paquete NetworkManager.x86_64 1:1.0.0-16.git20150121.b4ea599c.el7_1 debe ser obsoleto
……
```

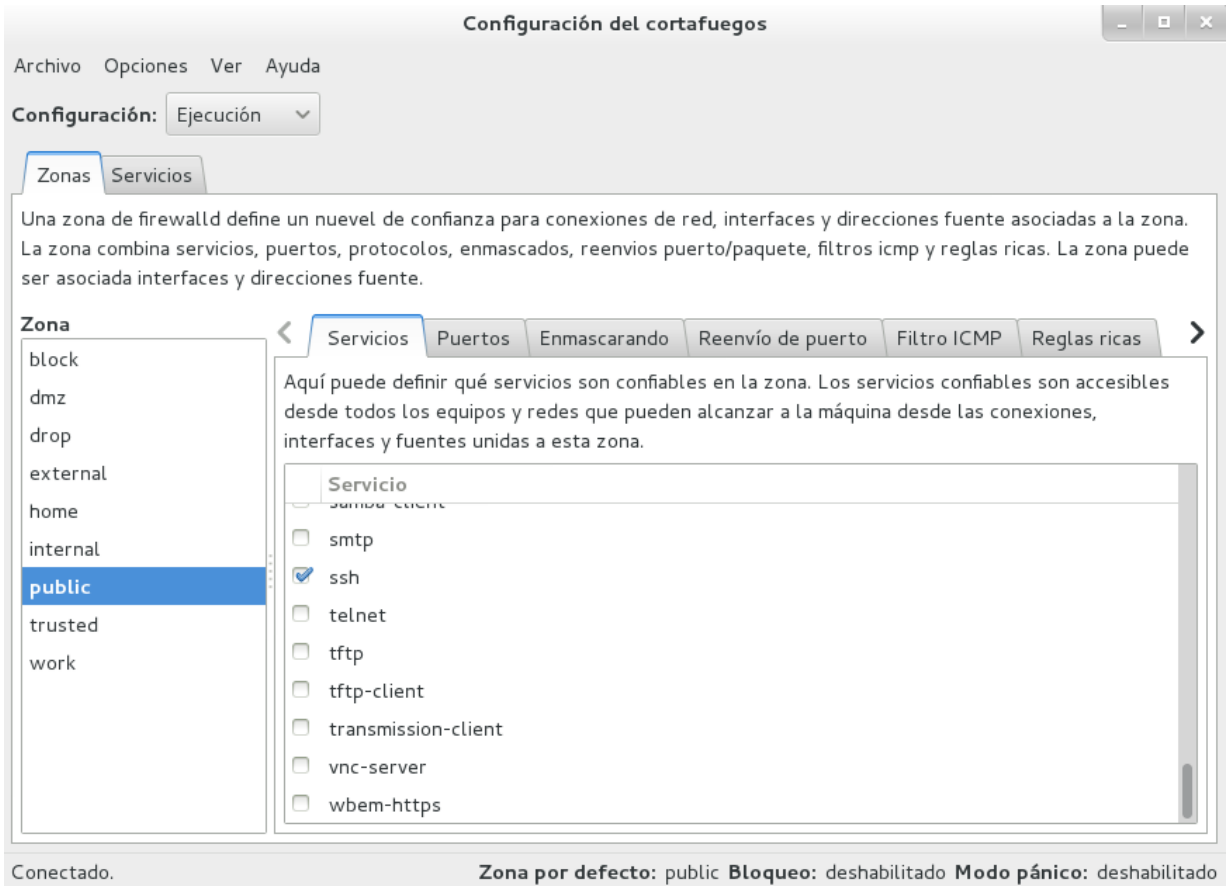
Las actualizaciones se las debe programar para que se ejecuten en horarios, donde el servidor no tenga mucha carga de trabajo; con el objetivo de que esta acción importante no influya en el normal desempeño del equipo. Como es lógico, el proceso de actualización consume recursos de red y del sistema en general.

3.4. Instalación cortafuegos (Firewall).

CentOS 7 provee un servicio llamado ***firewalld,*** el cual arranca al iniciar el servidor y se lo puede administrar mediante el entorno gráfico o por consola.

En el caso de que no tengamos entorno gráfico, existe el comando "***firewall-cmd***", el que permite configurar mediante consola; para mostrar el manual del comando ejecutamos lo siguiente:

```
[root@localhost system]# man firewall-cmd
```



La configuración bajo consola de comandos es compleja, en el caso de que requieran información de cómo hacerlo, pueden visitar la siguiente dirección de Internet:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Using_Firewalls.html

Si tenemos cargada la interfaz gráfica, el trabajo de configuración del firewall se facilita enormemente. Para ejecutar el programa de configuración, debemos entrar en: Aplicaciones→Varios→Cortafuego.

En el caso de que no encontremos el programa lo debemos instalar ejecutando lo siguiente:

```
[root@localhost ~]# yum -y install firewall-config.noarch
```

Podemos ejecutar el programa desde la consola de comandos, así:

```
[root@localhost ~]# firewall-config
```

El programa es bastante intuitivo y permite desde una configuración básica hasta personalizar reglas de iptables para asegurar nuestro sistema.

Una vez configurado, para verificar que está corriendo el servicio y se aplican las reglas, podemos ejecutar lo siguiente:

```
[root@localhost ~]# systemctl status firewalld
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)
   Active: active (running) since mié 2015-09-16 23:56:29 ECT; 5min ago
 Main PID: 10152 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─10152 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

sep 16 23:56:29 localhost.localdomain systemd[1]: Started firewalld - dynamic...
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost ~]#
```

Revisando las reglas de filtrado:

```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
INPUT_direct  all  --  anywhere             anywhere
INPUT_ZONES_SOURCE  all  --  anywhere             anywhere
INPUT_ZONES  all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
```

```
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
FORWARD_direct  all  --  anywhere             anywhere
FORWARD_IN_ZONES_SOURCE  all  --  anywhere             anywhere
FORWARD_IN_ZONES  all  --  anywhere             anywhere
FORWARD_OUT_ZONES_SOURCE  all  --  anywhere             anywhere
FORWARD_OUT_ZONES  all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
OUTPUT_direct  all  --  anywhere             anywhere

Chain FORWARD_IN_ZONES (1 references)
target     prot opt source               destination
FWDI_public  all  --  anywhere             anywhere             [goto]
FWDI_public  all  --  anywhere             anywhere             [goto]

Chain FORWARD_IN_ZONES_SOURCE (1 references)
target     prot opt source               destination

Chain FORWARD_OUT_ZONES (1 references)
target     prot opt source               destination
FWDO_public  all  --  anywhere             anywhere             [goto]
```

```
FWDO_public  all  --  anywhere            anywhere            [goto]

Chain FORWARD_OUT_ZONES_SOURCE (1 references)
target     prot opt source               destination

Chain FORWARD_direct (1 references)
target     prot opt source               destination

Chain FWDI_public (2 references)
target     prot opt source               destination
FWDI_public_log  all  --  anywhere            anywhere
FWDI_public_deny  all  --  anywhere            anywhere
FWDI_public_allow  all  --  anywhere            anywhere

Chain FWDI_public_allow (1 references)
target     prot opt source               destination

Chain FWDI_public_deny (1 references)
target     prot opt source               destination

Chain FWDI_public_log (1 references)
target     prot opt source               destination

Chain FWDO_public (2 references)
target     prot opt source               destination
FWDO_public_log  all  --  anywhere            anywhere
```

```
FWDO_public_deny  all  --  anywhere            anywhere
FWDO_public_allow  all  --  anywhere           anywhere

Chain FWDO_public_allow (1 references)
target     prot opt source               destination

Chain FWDO_public_deny (1 references)
target     prot opt source               destination

Chain FWDO_public_log (1 references)
target     prot opt source               destination

Chain INPUT_ZONES (1 references)
target     prot opt source               destination
IN_public  all  --  anywhere             anywhere          [goto]
IN_public  all  --  anywhere             anywhere          [goto]

Chain INPUT_ZONES_SOURCE (1 references)
target     prot opt source               destination

Chain INPUT_direct (1 references)
target     prot opt source               destination

Chain IN_public (2 references)
target     prot opt source               destination
IN_public_log  all  --  anywhere            anywhere
```

```
IN_public_deny  all  --  anywhere            anywhere

IN_public_allow  all  --  anywhere           anywhere


Chain IN_public_allow (1 references)

target     prot opt source               destination

ACCEPT     tcp  --  anywhere            anywhere            tcp dpt:ssh ctstate NEW


Chain IN_public_deny (1 references)

target     prot opt source               destination


Chain IN_public_log (1 references)

target     prot opt source               destination

LOG        tcp  --  192.168.0.0/24       anywhere            tcp dpt:ndmp ctstate NEW LOG
level error prefix "err"


Chain OUTPUT_direct (1 references)

target     prot opt source               destination

[root@localhost ~]#
```

Si no se esté ejecutando el servicio, tendremos la siguiente salida:

```
[root@localhost ~]# iptables -L

Chain INPUT (policy ACCEPT)

target     prot opt source               destination


Chain FORWARD (policy ACCEPT)

target     prot opt source               destination
```

```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]#
```

En este caso, el servidor está desprotegido al no ejecutarse ninguna regla para el filtrado de paquetes. Para poder gestionar el servicio, tenemos las siguientes opciones:

- Parar el servicio: # *systemctl stop firewalld*
- Arrancar el servicio: # *systemctl start firewalld*
- Reiniciar el servicio: # *systemctl restart firewalld*
- Verificar el estado del servicio: # *systemctl status firewalld*

Existen otras opciones de firewall que no son proporcionadas por la distribución, sin embargo pueden brindar mayor flexibilidad al momento de implementar el cortafuegos. En el caso de que deseemos instalar unos cortafuegos diferentes a firewalld, debemos asegurarnos en quitar y deshabilitar este servicio; para ello ejecutamos lo siguiente:

```
[root@localhost ~]# systemctl stop firewalld
[root@localhost ~]# systemctl disable firewalld
```

El primer comando, como ya lo indicamos, detiene la ejecución del servicio, el segundo comando deshabilita al demonio, para que este no arranque cuando reiniciemos el equipo.

Finalmente, enlistaremos las opciones recomendadas de firewall, que se pueden instalar en CentOS 7:

- APF
- Rc-firewall
- Shortwall
- CSF

3.5. Consideraciones SELinux.

SELinux (Security Enhanced Linux), es un sistema parte del kernel, encargado de controlar si los procesos tienen o no acceso para realizar una operación dentro del Linux.

El archivo principal de configuración se encuentra en ***/etc/selinux/config***, el que tiene el siguiente contenido:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

SELinux puede configurarse en tres estados: enforcing, permissive y disabled. Por defecto está en enforcing. El comando para determinar el estado de SELinux es ***getenforce***, para desactivar el SELinux podemos utilizar el comando ***setenforce 0***, sin embargo si el equipo se reinicia, mantendrá el valor determinado en el archivo de configuración.

A continuación la salida del comando getenforce:

```
[root@localhost ~]# getenforce
Enforcing
```

Otro comando que presenta información más detallada del SELinux es sestatus, con la siguiente salida:

```
[root@localhost ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
[root@localhost ~]#
```

Se recomienda tener habilitado a SELinux; en el caso de que al instalar un servicio tenga problemas, se debe revisar la documentación de configuración SELinux, para el uso correcto de cada servicio.

3.6. Deshabilitar los servicios innecesarios.

El tener corriendo servicios del sistema sin usarlos, ocasiona consumo innecesario de recursos y puede convertirse en un problema de seguridad. Es recomendable que quitemos los servicios que no estamos utilizando.

Lo primero que debemos hacer es enlistar todos los servicios que tiene el sistema operativo, para ello ejecutamos lo siguiente:

```
[root@localhost ~]# systemctl list-units | grep .service
abrt-ccpp.service               loaded active exited    Install ABRT coredump hook
abrt-oops.service               loaded active running   ABRT kernel log watcher
abrt-xorg.service               loaded active running   ABRT Xorg log watcher
abrtd.service                   loaded active running   ABRT Automated Bug Reporting Tool
accounts-daemon.service         loaded active running   Accounts Service
```

```
  alsa-state.service                loaded active running   Manage Sound Card State (restore
and store)
  atd.service                       loaded active running   Job spooling tools
  auditd.service                    loaded active running   Security Auditing Service
  avahi-daemon.service              loaded active running   Avahi mDNS/DNS-SD Stack
  bluetooth.service                 loaded active running   Bluetooth service
  chronyd.service                   loaded active running   NTP client/server
  colord.service                    loaded active running   Manage, Install and Generate Color
Profiles
  crond.service                     loaded active running   Command Scheduler
  cups.service                      loaded active running   CUPS Printing Service
  dbus.service                      loaded active running   D-Bus System Message Bus
  firewalld.service                 loaded active running   firewalld - dynamic firewall daemon
  firstboot-graphical.service       loaded failed failed    firstboot configuration program
  gdm.service                       loaded active running   GNOME Display Manager
  iprdump.service                   loaded active running   LSB: Start the ipr dump daemon
  iprinit.service                   loaded active running   LSB: Start the ipr init daemon
  iprupdate.service                 loaded active running   LSB: Start the iprupdate utility
  irqbalance.service                loaded active running   irqbalance daemon
  kdump.service                     loaded failed failed    Crash recovery kernel arming
  kmod-static-nodes.service         loaded active exited    Create list of required static device
nodes...
  ksm.service                       loaded active exited    Kernel Samepage Merging
  ksmtuned.service                  loaded active running   Kernel Samepage Merging
  libstoragemgmt.service            loaded active running   libstoragemgmt plug-in server daemon
  libvirtd.service                  loaded active running   Virtualization daemon
  lvm2-lvmetad.service              loaded active running   LVM2 metadata daemon
```

```
  lvm2-monitor.service          loaded active exited    Monitoring of LVM2 mirrors, ….
  lvm2-pvscan@252:2.service  loaded active exited    LVM2 PV scan on device 252:2
  ModemManager.service        loaded active running   Modem Manager
  network.service               loaded active exited    LSB: Bring up/down networking
  NetworkManager.service      loaded active running   Network Manager
  nfs-lock.service              loaded active running   NFS file locking service.
  polkit.service                loaded active running   Authorization Manager
  postfix.service               loaded active running   Postfix Mail Transport Agent
  qemu-guest-agent.service      loaded active running   QEMU Guest Agent
  rhel-dmesg.service            loaded active exited    Dump dmesg to /var/log/dmesg
  rhel-import-state.service       loaded active exited    Import network configuration ...
  rhel-loadmodules.service      loaded active exited    Load legacy module configuration
  rhel-readonly.service         loaded active exited    Configure read-only root support
  rngd.service                    loaded failed failed    Hardware RNG Entropy Gatherer
Daemon
  rpcbind.service               loaded active running   RPC bind service
  rsyslog.service               loaded active running   System Logging Service
  rtkit-daemon.service            loaded active running   RealtimeKit Scheduling Policy
Service
  smartd.service                loaded active running   Self Monitoring and Reporting ...
  spice-vdagentd.service        loaded active running   Agent daemon for Spice guests
  sshd.service                  loaded active running   OpenSSH server daemon
  sysstat.service               loaded active exited    Resets System Activity Logs
  systemd-ask-password-wall.service   loaded active running   Forward Password
Requests to Wall
  systemd-fsck-root.service         loaded active exited    File System Check on Root
Device
```

```
  systemd-hostnamed.service              loaded active running   Hostname Service
  systemd-journald.service               loaded active running   Journal Service
  systemd-logind.service                 loaded active running   Login Service
  systemd-random-seed.service            loaded active exited    Load/Save Random Seed
  systemd-remount-fs.service             loaded active exited    Remount Root and Kernel
...
  systemd-sysctl.service                 loaded active exited    Apply Kernel Variables
  systemd-tmpfiles-setup-dev.service     loaded active exited    Create static device nodes
in /dev
  systemd-tmpfiles-setup.service         loaded active exited    Create Volatile Files and
Directories
  systemd-udev-settle.service            loaded active exited    udev Wait for Complete
Device...
  systemd-udev-trigger.service           loaded active exited    udev Coldplug all Devices
  systemd-udevd.service                  loaded active running   udev Kernel Device
Manager
  systemd-update-utmp.service            loaded active exited    Update UTMP about
System...
  systemd-user-sessions.service          loaded active exited    Permit User Sessions
  systemd-vconsole-setup.service         loaded active exited    Setup Virtual Console
  tuned.service                          loaded active running   Dynamic System Tuning
Daemon
  udisks2.service                        loaded active running   Disk Manager
  upower.service                         loaded active running   Daemon for power
management
  [root@localhost ~]#
```

Existen algunos servicios que normalmente están corriendo en el sistema, sin embargo no tienen un uso práctico. Debemos identificarlos para detener su ejecución y posteriormente

deshabilitar el arranque al inicio del sistema. Proporcionamos una lista de servicios que habitualmente no deberían correr en el equipo:

- **alsa-state.service.** Servicio para el manejo de la tarjeta de sonido.
- **atd.service.** Servicio para tareas programadas (Poco usado).
- **bluetooth.service.** Servicio que administra dispositivos bluetooth.
- **crond.service.** Servicio de tareas programadas.
- **cups.service.** Servicio para administración de impresión.
- **libvirtd.service.** Servicio para el manejo de virtualización.
- **ModenManager.service.** Servicio para el manejo de módem.
- **postfix.service.** Servicio de correo electrónico cargado por defecto.

A continuación (como ejemplo) para deshabilitar el servicio de bluetooth, debemos ejecutar el siguiente comando:

```
[root@localhost ~]# systemctl disable bluetooth.service
rm '/etc/systemd/system/dbus-org.bluez.service'
rm '/etc/systemd/system/bluetooth.target.wants/bluetooth.service'
[root@localhost ~]#
```

3.7. Endurecer el sistema de archivos

Uno de los objetivos fundamentales de crear varias particiones de disco, es poder asignar algunas propiedades que pueden ayudar enormemente a la seguridad de un servidor. Se sugiere configurar al sistema de archivos con las opciones detalladas en la siguiente tabla:

Partición	Opciones
/	defaults,noatime,nosuid,noexec,nodev
/boot	defaults,noatime,nosuid,noexec,nodev
/home	defaults,noatime,nosuid,noexec,nodev
/usr	defaults,noatime,nosuid,nodev,ro

/var	defaults,noatime,nosuid,noexec,nodev

Tabla 1: Opciones recomendadas para sistemas de archivos

Linux permite montar las particiones de disco con algunas opciones especiales que pueden evitar problemas de seguridad, por ejemplo:

En la partición /var se guardan archivos de tamaño variable, como: logs, base de datos, correos electrónicos, etcétera. En esta no es necesario que se almacenen archivos ejecutables, por esta razón, podemos proteger a nivel de sistema de archivos, para que este impida la ejecución de ficheros en esta partición.

A continuación detallamos las opciones configuradas para las particiones anteriormente descritas:

- **noatime.** Evita la escritura para guardar la fecha de acceso a un archivo.
- **noexec.** Restringe la ejecución de archivos (programas) dentro de la partición.
- **nosuid.** No permite que los permisos especiales suid/sgid surtan efecto.
- **nodev.** Impide el acceso a dispositivos.
- **ro.** El sistema de archivos se monta solo de lectura.

Para aplicar estas configuraciones, debemos editar el archivo /***etc/fstab***, a continuación un ejemplo de cómo podría quedar dicho fichero:

```
#
# /etc/fstab
# Created by anaconda on Wed Sep 16 23:16:08 2015
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/dsk-root    /                xfs     defaults,noatime,nosuid,noexec,nodev        1
1
/dev/sda1               /boot            xfs     defaults,noatime,nosuid,noexec,nodev        1
0
```

```
/dev/mapper/home        /home           xfs     defaults,noatime,nosuid,noexec,nodev    1
2
/dev/mapper/dsk-usr     /usr            xfs     defaults,noatime,nosuid,nodev,ro        1
2
/dev/mapper/dsk-var     /var            xfs     defaults,noatime,nosuid,noexec,nodev    1
2
/dev/mapper/dsk-swap    swap            swap    defaults                                0
0
```

3.8. Instalar escáner de vulnerabilidades

Es recomendable instalar un sistema para el escaneo de vulnerabilidades. En la presente guía utilizaremos a Nessus.

Podemos analizar las características y opciones que brinda Nessus en la siguiente dirección web http://www.tenable.com/products/nessus-vulnerability-scanner.

Esta herramienta ofrece un archivo RPM para su instalación directa en CentOS 7, debemos descargarnos desde la siguiente dirección:

http://www.tenable.com/products/nessus/select-your-operating-system#tos.

Escogemos la opción Linux→ Red Hat ES 7 (64-bit) / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel). Nos pedirá aceptar la licencia y posteriormente se descargará el archivo RPM. El sitio de Nessus nos entrega un código MD5 para verificar que el archivo se encuentre íntegro, así comprobamos que tenemos una copia exacta; ejecutamos el siguiente comando:

```
[root@localhost ~]# cd Descargas/
[root@localhost Descargas]# md5sum Nessus-6.4.3-es7.x86_64.rpm
b6fc0cac871b39e7c7b7b0129aebaa6c  Nessus-6.4.3-es7.x86_64.rpm
[root@localhost Descargas]#
```

Si el código entregado es igual al proporcionado en la página, procedemos a instalar en nuestro sistema, para ello ejecutamos:

[root@localhost Descargas]# yum -y install Nessus-6.4.3-es7.x86_64.rpm

Complementos cargados:fastestmirror, langpacks

Examinando Nessus-6.4.3-es7.x86_64.rpm: Nessus-6.4.3-es7.x86_64

Marcando Nessus-6.4.3-es7.x86_64.rpm para ser instalado

Resolviendo dependencias

--> Ejecutando prueba de transacción

---> Paquete Nessus.x86_64 0:6.4.3-es7 debe ser instalado

--> Resolución de dependencias finalizada

base/7/x86_64 | 3.6 kB 00:00:00

extras/7/x86_64 | 3.4 kB 00:00:00

updates/7/x86_64 | 3.4 kB 00:00:00

Dependencias resueltas

==========

Package Arquitectura Versión Repositorio Tamaño

==========

Instalando:

Nessus x86_64 6.4.3-es7 /Nessus-6.4.3-es7.x86_64 34 M

Resumen de la transacción

==========

Instalar 1 Paquete

Tamaño total: 34 M

```
Tamaño instalado: 34 M

Downloading packages:

Running transaction check

Running transaction test

Transaction test succeeded

Running transaction

  Instalando    : Nessus-6.4.3-es7.x86_64                                  1/1

Unpacking Nessus Core Components...

nessusd (Nessus) 6.4.3 [build M20035] for Linux

Copyright (C) 1998 - 2015 Tenable Network Security, Inc


Processing the Nessus plugins...

[##########################################################]


All plugins loaded (1sec)

 - You can start Nessus by typing /bin/systemctl start nessusd.service

 - Then go to https://localhost.localdomain:8834/ to configure your scanner


  Comprobando   : Nessus-6.4.3-es7.x86_64                                  1/1


Instalado:

  Nessus.x86_64 0:6.4.3-es7


¡Listo!

[root@localhost Descargas]#
```

Las líneas resaltadas nos indican cómo debemos iniciar el servicio, ejecutamos lo siguiente:

[root@localhost Descargas]# systemctl start nessusd.service

Verificamos que esté levantado el servicio:

[root@localhost Descargas]# systemctl status nessusd.service

nessusd.service - The Nessus Vulnerability Scanner

Loaded: loaded (/usr/lib/systemd/system/nessusd.service; enabled)

Active: active (running) since vie 2015-09-18 00:48:21 ECT; 7s ago

Main PID: 5233 (nessus-service)

CGroup: /system.slice/nessusd.service

├─5233 /opt/nessus/sbin/nessus-service -q

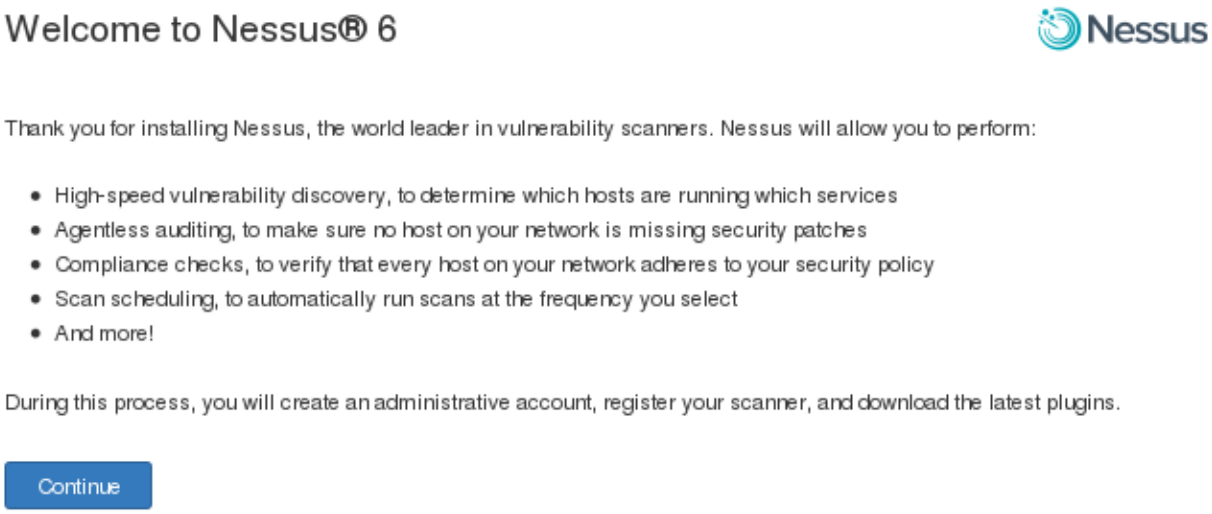
└─5234 nessusd -q

sep 18 00:48:21 localhost.localdomain systemd[1]: Started The Nessus Vulnerability Scanner.

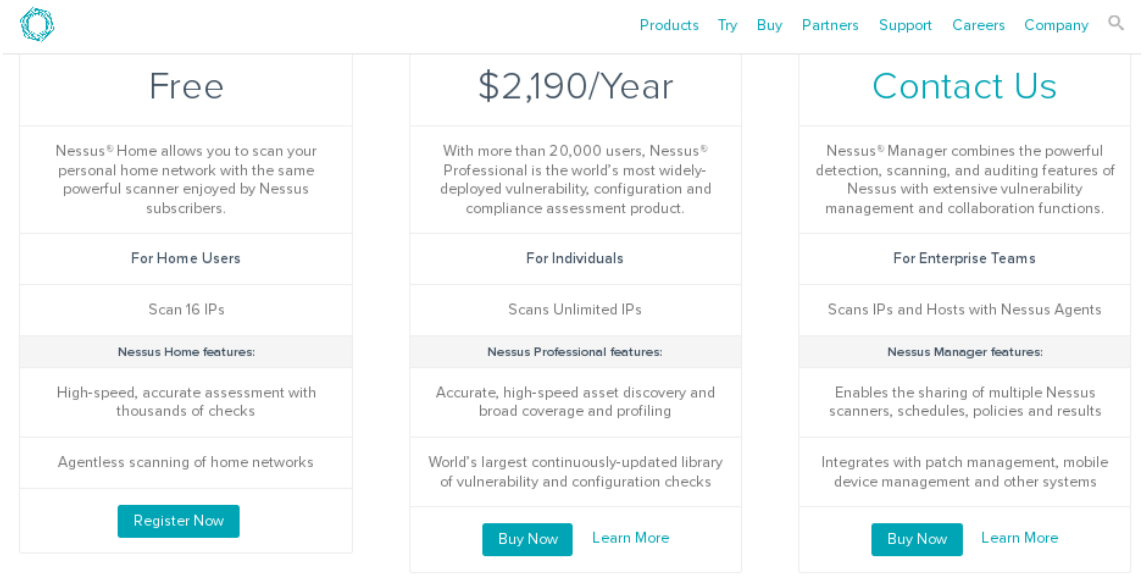
Configuramos para que arranque el servicio cuando inicie el equipo.

[root@localhost Descargas]# systemctl enable nessusd.service

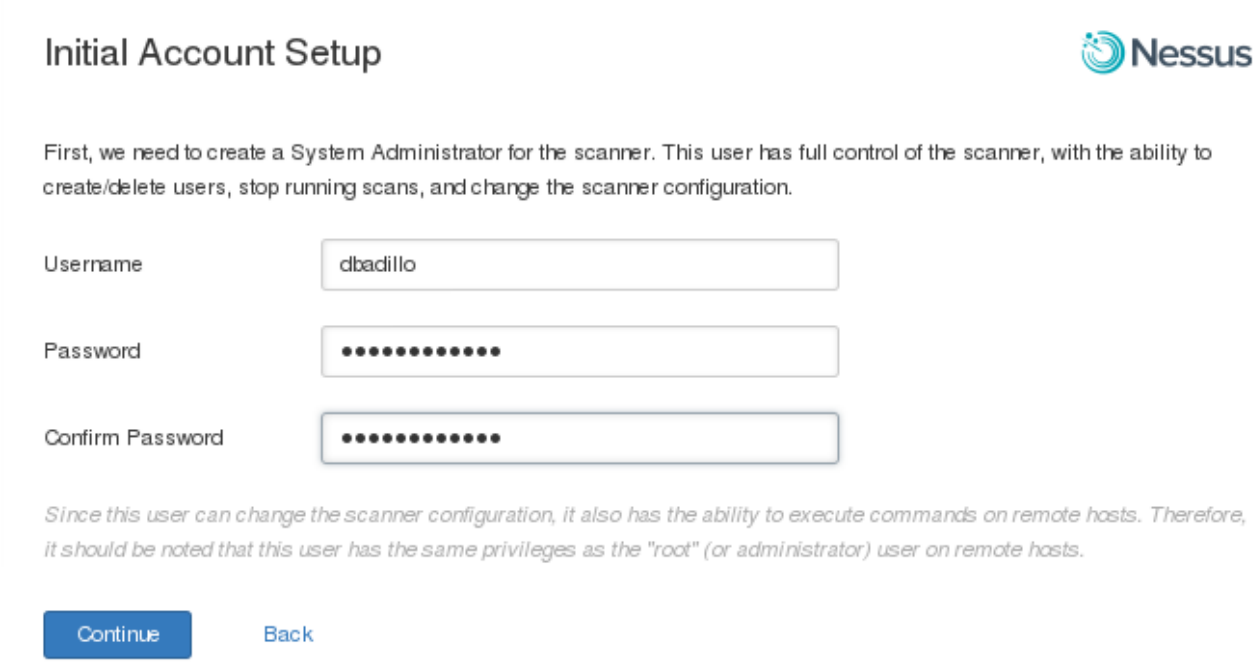
Desde un navegador abrimos la dirección **https://localhost.localdomain:8834/ ,** aparece la pantalla de bienvenida a Nessus.



Le damos clic en “Continue” y tendremos la pantalla para ingresar los datos de la cuenta.

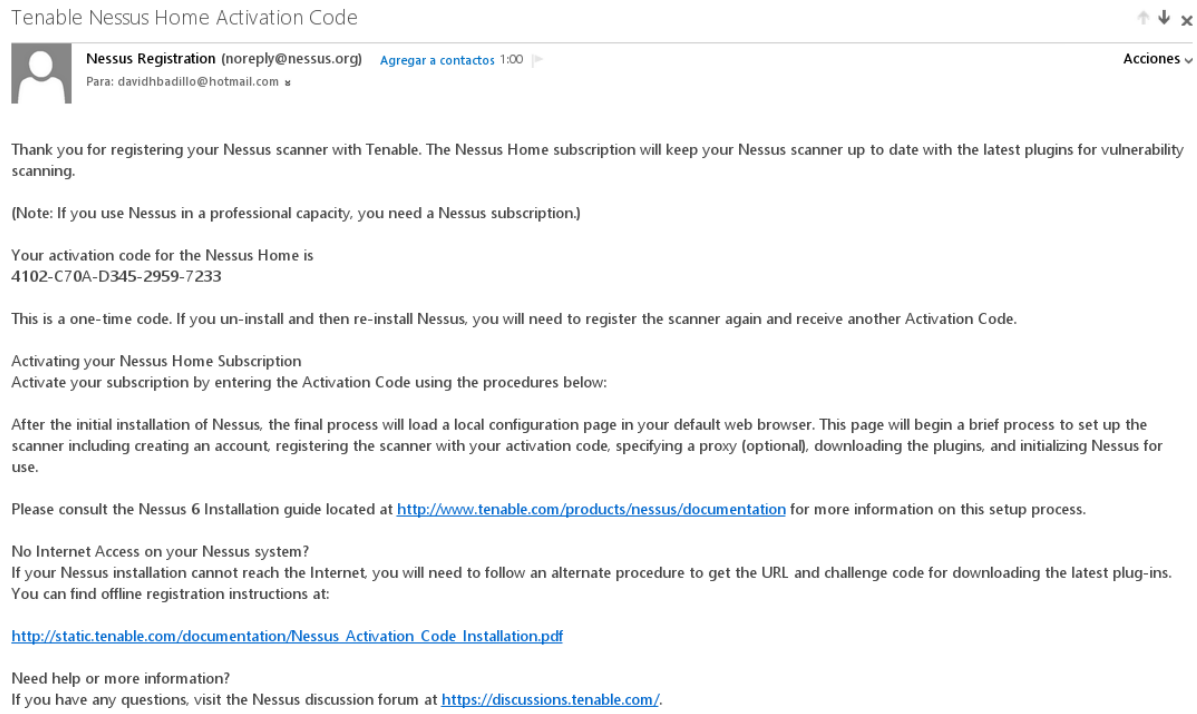


Damos clic en “Continue” para seguir; la siguiente pantalla nos pedirá registrarnos en el sitio Web, tenemos varias alternativas, entre ellas seleccionamos el registro gratuito “Free”, dándole clic en el botón “Register Now”.



A continuación tenemos el formulario para el registro, llenamos los datos indicados y le damos clic en “Register”.

Una vez registrados, Nessus nos enviará un correo electrónico con la clave de activación para ingresar al sistema instalado.



Tenable Nessus Home Activation Code

Nessus Registration (noreply@nessus.org) Agregar a contactos 1:00 Acciones

Para: davidhbadillo@hotmail.com

Thank you for registering your Nessus scanner with Tenable. The Nessus Home subscription will keep your Nessus scanner up to date with the latest plugins for vulnerability scanning.

(Note: If you use Nessus in a professional capacity, you need a Nessus subscription.)

Your activation code for the Nessus Home is
4102-C70A-D345-2959-7233

This is a one-time code. If you un-install and then re-install Nessus, you will need to register the scanner again and receive another Activation Code.

Activating your Nessus Home Subscription
Activate your subscription by entering the Activation Code using the procedures below:

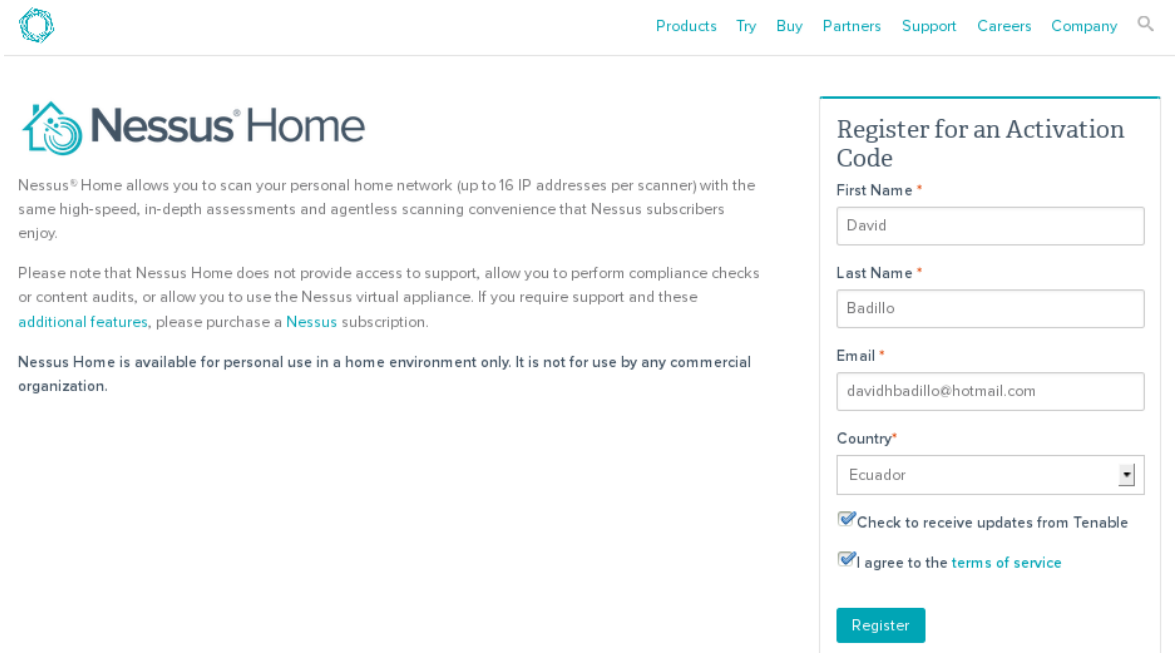
After the initial installation of Nessus, the final process will load a local configuration page in your default web browser. This page will begin a brief process to set up the scanner including creating an account, registering the scanner with your activation code, specifying a proxy (optional), downloading the plugins, and initializing Nessus for use.

Please consult the Nessus 6 Installation guide located at http://www.tenable.com/products/nessus/documentation for more information on this setup process.

No Internet Access on your Nessus system?
If your Nessus installation cannot reach the Internet, you will need to follow an alternate procedure to get the URL and challenge code for downloading the latest plug-ins. You can find offline registration instructions at:

http://static.tenable.com/documentation/Nessus_Activation_Code_Installation.pdf

Need help or more information?
If you have any questions, visit the Nessus discussion forum at https://discussions.tenable.com/.



Products Try Buy Partners Support Careers Company

Nessus® Home

Nessus® Home allows you to scan your personal home network (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Home does not provide access to support, allow you to perform compliance checks or content audits, or allow you to use the Nessus virtual appliance. If you require support and these additional features, please purchase a Nessus subscription.

Nessus Home is available for personal use in a home environment only. It is not for use by any commercial organization.

Register for an Activation Code

First Name *

David

Last Name *

Badillo

Email *

davidhbadillo@hotmail.com

Country*

Ecuador

Check to receive updates from Tenable

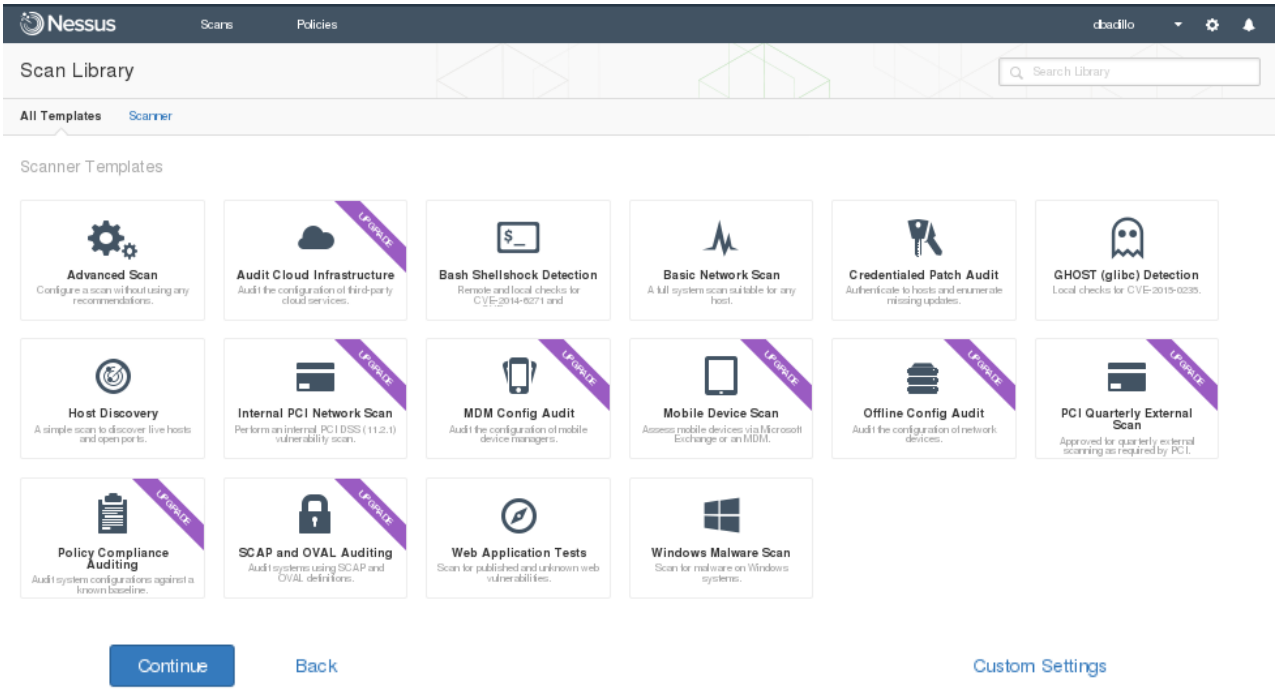
I agree to the terms of service

Register

Regresamos a la página de inicio de Nessus y copiamos el código de activación recibida en el correo electrónico; ingresamos en el campo “Activation Code”, le damos clic en el botón “Continue”, para seguir con el proceso de configuración. (Ver Figura 43)

Luego de varios minutos en el que Nessus procede a instalar algunos componentes adicionales, tendremos la pantalla para ingresar al sistema. (Ver Figura 44).

Una vez dentro de Nessus tendremos la pantalla principal, la cual ofrece algunas opciones para proteger a nuestro equipo. Como recomendación podemos seleccionar la opción “Advanced Scan”, para realizar un escaneo de vulnerabilidades en nuestro servidor.



3.9. Instalar IDS/IPS

Es de mucha importancia instalar un sistema IDS/IPS para detectar y prevenir intrusiones a nuestro servidor. En nuestro caso elegimos instalar Snort por su gran uso en sistemas Linux.

Para instalar podemos seguir las recomendaciones indicadas en el sitio de snort: https://www.snort.org/#get-started

En dicha dirección de Internet, tenemos la opción para bajar los instaladores o cargarlos directamente como lo haremos en esta guía.

Para cargar esta herramienta, primero debemos instalar el paquete daq, para ello ejecutamos lo siguiente:

```
[root@localhost ~]# yum install https://www.snort.org/downloads/snort/daq-2.0.6-1.centos7.x86_64.rpm
Complementos cargados:fastestmirror, langpacks
daq-2.0.6-1.centos7.x86_64.rpm                    | 147 kB     00:00
Examinando /var/tmp/yum-root-ujfL9k/daq-2.0.6-1.centos7.x86_64.rpm: daq-2.0.6-1.x86_64
Marcando /var/tmp/yum-root-ujfL9k/daq-2.0.6-1.centos7.x86_64.rpm para ser instalado
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete daq.x86_64 0:2.0.6-1 debe ser instalado
--> Resolución de dependencias finalizada

Dependencias resueltas

================================================================
 Package   Arquitectura Versión        Repositorio              Tamaño
================================================================
Instalando:
```

```
 daq       x86_64       2.0.6-1         /daq-2.0.6-1.centos7.x86_64       649 k


Resumen de la transacción

================================================================
Instalar  1 Paquete


Tamaño total: 649 k
Tamaño instalado: 649 k
Is this ok [y/d/N]: y
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Instalando    : daq-2.0.6-1.x86_64                                1/1
  Comprobando   : daq-2.0.6-1.x86_64                                1/1


Instalado:
  daq.x86_64 0:2.0.6-1


¡Listo!
[root@localhost ~]#
```

Luego instalamos Snort, ejecutando lo siguiente:

```
[root@localhost ~]# yum install https://www.snort.org/downloads/snort/snort-2.9.7.5-1.centos7.x86_64.rpm
```

```
Complementos cargados:fastestmirror, langpacks
snort-2.9.7.5-1.centos7.x86_64.rpm                    | 4.2 MB     00:02
Examinando /var/tmp/yum-root-ujfL9k/snort-2.9.7.5-1.centos7.x86_64.rpm: 1:snort-2.9.7.5-1.x86_64
Marcando /var/tmp/yum-root-ujfL9k/snort-2.9.7.5-1.centos7.x86_64.rpm para ser instalado
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete snort.x86_64 1:2.9.7.5-1 debe ser instalado
--> Resolución de dependencias finalizada

Dependencias resueltas

================================================================
 Package   Arquitectura
                  Versión         Repositorio                    Tamaño
================================================================
Instalando:
 snort     x86_64     1:2.9.7.5-1     /snort-2.9.7.5-1.centos7.x86_64      17 M

Resumen de la transacción
================================================================
Instalar  1 Paquete

Tamaño total: 17 M
Tamaño instalado: 17 M
Is this ok [y/d/N]: y
```

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Instalando    : 1:snort-2.9.7.5-1.x86_64                    1/1
  Comprobando   : 1:snort-2.9.7.5-1.x86_64                    1/1

Instalado:
  snort.x86_64 1:2.9.7.5-1

¡Listo!
[root@localhost ~]#
```

El manejo de esta herramienta está basado en reglas y toda la información sobre el uso de snort, lo pueden encontrar en la siguiente dirección de Internet: https://www.snort.org/documents

3.10. Consideraciones de las cuentas de usuario

Uno de los problemas de seguridad importantes que suelen presentarse en un servidor, están relacionados con las cuentas de usuario, por esta razón, debemos tomar las siguientes consideraciones:

1. Se deben crear las cuentas estrictamente necesarias.
2. Asignar contraseñas seguras, con al menos 8 caracteres de combinación entre: mayúsculas, minúsculas, números y caracteres especiales.
3. Desactivar/eliminar las contraseñas que no estén en uso.
4. Crear cuentas de usuario sin acceso a consola, ejecutando el siguiente comando: #**adduser *usuario* -s /sbin/nologin**

5. Realizar cambios periódicos de contraseñas.
6. Búsqueda de contraseñas débiles (Nessus o John).

3.11. Deshabilitar el acceso remoto para el usuario root

El usuario root puede hacer prácticamente cualquier cosa dentro del sistema, por esta razón como lo señalamos en la guía de instalación, debemos protegerla con una contraseña segura.

Se recomienda deshabilitar el acceso remoto directamente con este usuario. Para bloquear el acceso remoto debemos editar el archivo de configuración del servicio SSH, ejecutando lo siguiente:

```
[root@localhost ~]# vim /etc/ssh/sshd_config
```

Buscamos la línea donde está el parámetro PermitRootLogin:

```
#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
```

Descomentamos la línea y la dejamos de la siguiente manera:

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
```

Guardamos los cambios en el archivo de configuración y reiniciamos el servicio SSH.

```
[root@localhost ~]# systemctl restart sshd.service
```

Para poder administrar el servidor de manera remota, debemos ingresar al sistema utilizando una cuenta de usuario común; una vez dentro, nos cambiarnos a la cuenta de super administrador, ejecutando el comando:

```
# su –
```

4. Recomendaciones

A continuación detallamos algunas recomendaciones que debe tomar en cuenta un administrador del sistema Linux:

- La seguridad de un sistema no es un proyecto, es una forma de vida para el administrador.
- Se debe elaborar un documento con las políticas de uso.
- Educar a los usuarios finales sobre temas de seguridad.
- El administrador del servidor, siempre debe estar al día en temas de seguridad; debe capacitarse permanentemente.
- Implementar un sistema de respaldos de la información y documentarlo.
- Preparar un documento que contenga el plan de contingencia.
- La seguridad de un servidor, no representa la seguridad de toda la red.
- Monitorear constantemente el comportamiento del sistema.
- El administrador debe inscribirse a listas de correo como: RedIRIS (listserv@listserv.rediris.es), sec-linux(majordomo@ls.cica.es), bugtraq-es(LISTSERV@LISTS.SECURITYFOCUS.COM), etcétera; la información manejada en dichas listas, puede ser de gran utilidad para prevenir eventos.