Visita nuestro sitio SoloLinux.es

MAGAZINE SOLO LINUX

N° 09

Tu revista, la revista de tod@s

OCTUBRE 2019

Preguntas a un **Sysadmin**

Instalar **BlueMail** en Linux

Ubuntu 19.10 Eoan Ermine
Listo para su descarga

Liberar espacio en el disco ocupado por **Snap**

Desactivar la combinación de teclas **Ctrl + Alt + Del**

HTML vs **XML**

MANUALES, SCRIPTS, SOFTWARE, HARDWARE, DISTROS LINUX, SEGURIDAD, REDES Y MUCHO MAS EN LA WEB...

EDITORIAL

Revista digital de distribución gratuita.

SOLOLINUX MAGAZINE
Año 0. Número 09.
OCTUBRE 2019.
Sitio WEB

Edición:
Adrián A. A.
adrian@sololinux.es

Redacción y administrador web:
Sergio G. B.
info@sololinux.es
www.sololinux.es

Marketing digital:
@HeavenlyRainbow

Agradecimientos:
A todos los colaboradores de la revista, y a todas las personas que apoyan este proyecto.

Contacto:
adrian@sololinux.es

Aquí estamos de nuevo, hoy os quiero presentar el **número 9** de la revista digital **SOLOLINUX**.

Igual que en el número anterior nos gustaría animar a todos nuestros lectores para que nos envíen sus **opiniones sobre el Software Libre o sobre GNU/Linux**, pueden enviarlo a adrian@sololinux.es, con ello queremos proponer que cada mes se publicada una o varias de esas opiniones sobre lo mencionado en la nueva sección de la revista OPINIÓN DEL LECTOR. **Queremos saber la opinión de todos**. Se intentara incluir el máximo de opiniones en cada numero, pero si no sale la tuya este mes no desesperes, al siguiente podría tener un hueco en la revista. **ANÍMENSE Y ENVÍEN SUS OPINIONES.** Gracias.

Al igual que lo anteriormente mencionado, nos gustaría promover un espacio en la revista sobre los eventos de Software Libre y GNU/Linux en todo el mundo. Los organizadores de estos eventos pueden ponerse en contacto con migo a través de correo electrónico, adrian@sololinux.es

Sin mas **quiero agradecer a todos** los que hacéis posible que esta revista siga adelante.
Personalmente agradezco a Sergio todo su trabajo en la multitud de artículos que realiza a lo largo del mes para que esta revista pueda tener suficiente información mes a mes.

Gracias a TOD@S
Compartan esta revista en sus redes sociales o web.

Revista digital **SOLOLINUX MAGAZINE**. Tu revista, la revista de todos.

Adrián A. A.

PUBLICIDAD

Quieres poner publicidad en la revista, ahora puedes hacerlo de forma muy simple, llegando a todo el mundo con esta revista digital de software libre y GNU/Linux en ESPAÑOL

CON SOLOLINUX MULTIPLICARAS TUS CLIENTES

Para mayor información escribe un email a: adrian@sololinux.es

LA PUBLICIDAD DE LA REVISTA…
Aprende Linux en: www.linuxadistancia.com (Publicidad)
Compra tu ordenador con Linux en: www.vantpc.es (Publicidad)

COLABORA

Quieres colaborar en la revista.
Para mayor información escribe un email a: adrian@sololinux.es

La **Revista SOLOLINUX**, se distribuye gratuitamente en forma digital para todo el mundo que quiere disfrutar de ella. Si quieres imprimirla es cosa tuya.

Esta revista es de **distribución gratuita**, si lo consideras oportuno puedes ponerle precio.
Tu también puedes ayudar, contamos con la posibilidad de hacer donaciones para la REVISTA, de manera muy simple a través de **PAYPAL**

AYUDANOS A SEGUIR CRECIENDO

PayPal™
Apoyo con una donación

SoloLinux

VANT

INSTITUTO LINUX

CONTENIDO

NUESTROS NÚMEROS

Download Revista digital – Magazine SoloLinux Nº1

Download Revista digital – Magazine SoloLinux Nº2

Download Revista digital – Magazine SoloLinux Nº3

Download Revista digital – Magazine SoloLinux Nº4

Download Revista digital – Magazine SoloLinux Nº5

Download Revista digital – Magazine SoloLinux Nº6

Download Revista digital – Magazine SoloLinux Nº7

Download Revista digital – Magazine SoloLinux Nº8

En **Sololinux.es** seguimos creciendo gracias a nuestros lectores, puedes colaborar con el simple gesto de compartir nuestros artículos en otros sitios web, foros y redes sociales.
Si te perdiste algún número aquí tienes todos.

@vantpc vant.pc vantpc_es t.me/vantpc

VANT

#somoslinuxeros

EN NOVIEMBRE, CADA SEMANA...

OFERTAS MONSTRUOSAS

NOVIEMBRE comienza con HALLOWEEN
y casi finaliza en BLACK FRIDAY

Este mes, cada semana tendremos una oferta especial VANT.

Entérate cada semana en www.vantpc.es y en nuestras redes sociales

linux inside

la gama más completa de ordenadores linuxeros

descúbrenos en www.vantpc.es

Preguntas a un Sysadmin

Ya tratamos las funciones principales de un **Sysadmin** (administrador de sistemas) en un articulo anterior de nuestra Web, En este articulo veremos otro aspecto sobre su vida cotidiana, las consultas. Es común, incluso llega a ser agotador que un **sysadmin** reciba cientos de consultas, pueden ser de sus compañeros de oficina, de relaciones personales, amigos, etc…

Que levante la mano quien nunca hizo una pregunta a alguien con más conocimientos que el (por lo menos aparentemente), nadie verdad, pues imagínate que te relacionas con un buen **sysadmin**, y te quieres introducir en ese mundo. Lo vas a bombardear a preguntas, seguro, ja.

Hoy hacemos una recopilación de las consultas más frecuentes que recibe un **sysadmin**, unas son simples, otras no tanto. Comenzamos, no sin antes recordar un articulo donde se exponían **los scripts más comunes para un sysadmin**.

Preguntas a un Sysadmin

1.- ¿Como forzar la ejecución de fsck al reiniciar el sistema?
Para ejecutar fsck de manera forzada en un sistema de archivos (en el próximo reinicio), en el sistema de archivos creamos un nuevo archivo que se llamara "**forcefsck**". Supongamos que queremos ejecutar fsck en el /home.

```
cd /home ; touch forcefsck ; reboot
```

2.- ¿Cambiar la fecha de caducidad de la contraseña de una cuenta, sin modificar la contraseña?
Usando el comando "**chage**" podemos prolongar la fecha de vencimiento sin ningún problema. La sintaxis es la siguiente…

```
chage -d yy-mm-dd Usuario
```

3.- Verificar la última vez que se escaneó un sistema de archivos.
Con la herramienta **tune2fs**, podemos averiguar cuándo se realizó por ultima vez un análisis del sistema de archivos en busca de errores. Su sintaxis es la siguiente.

```
tune2fs -l <Device_Name> | grep 'Last checked'
```

4.- ¿Qué es Kdump y por qué es tan necesario?
Kdump es una herramienta del propio Kernel, que captura los volcados de memoria cuando se produce un fallo grave, o un **Kernel panic**. Su beneficio es que puedes analizar esos archivos, y localizar la causa.

5.- ¿Qué aplicación se utiliza para analizar los volcado de memoria (o el vmcore) en CentOS?
La aplicación para poder analizar los volcados es **crash**.

6.- ¿Como instalar todas actualizaciones y parches del sistema, en un servidor CentOS, excepto el kernel?
En este caso tan solo debes utilizar el parámetro **exclude** de yum o dnf.

```
yum update –exclude=kernel*
```

7.- ¿Como puedo saber si mi servidor es virtual o físico?
Para poder identificar y salir de dudas, nos ayudamos de **dmidecode**.

```
dmidecode -t system | grep 'Product Name'
```

8.- ¿Qué es el automounter y por qué es tan necesario?
Automounter es un servicio del sistema que se utiliza para montar un sistema de archivos (ya sea local o remoto), al acceder al dispositivo. Cuando el sistema de archivos está inactivo, el servicio (**autofs**) desmontará automáticamente el sistema de archivos. El beneficio de los **autofs** es que el sistema no necesita montar el sistema de archivos continuamente, solo montará cuando sea necesario.

9.- ¿Como verificar si el ultimo comando se ejecuta correctamente, o no?
Es muy fácil, por ejemplo del **comando ls**.

```
ls -l /var/
echo $?
```

10.- ¿Como puedo forzar a un usuario a cambiar su contraseña?
Ayudándonos del comando «chage», lo que haremos es caducar la password del usuario. Así, cada vez que inicie sesión en el sistema recibirá el siguiente aviso, "Su contraseña ha caducado. Debe cambiar su contraseña ahora e iniciar sesión de nuevo".

```
chage -d 0 Usuario
```

11.- ¿Como obtener información sobre un paquete rpm con yum?
En nuestro ejemplo sobre postfix.

```
yum history package postfix
```

12.- ¿Como modificar el nombre del host de manera permanente en CentOS?
Ya tratamos este tema de manera más extensa en otro articulo, de todas maneras es tan simple como ejecutar lo siguiente:

```
hostnamectl set-hostname Nuevo-hostname
```

13.- ¿Como saber que módulos del kernel están instalados?
El comando **lsmod** te dará un completo listado.

```
lsmod
```

14.- ¿Como puedo comprobar la I/O en linux?
Existen multitud de herramientas, pero sin dudarlo las más utilizadas son las siguientes (ejecútalas tal cual en tu sistema):

```
sar

iostat

vmstat
```

15.- ¿Para que sirven "/etc/lvm/backup" y "/etc/lvm/archive"?
Cuando creamos o actualizamos una partición basada en lvm, la copia de seguridad de los metadatos se guarda en "**/etc/ lvm/backup**", los nuevos metadatos se almacenan en "**/etc/lvm/archive**". Como ves son archivos importantes, ademas si tienes algún problema con el comando **vgcfgrestore** puedes restaurar los metadatos del volumen.

16.- ¿Como listar las tablas de enrutamiento en linux?
Para enumerar las tablas tenemos dos comandos ideales, son:

```
netstat -nr

#y

route -n
```

17.- ¿Como puedo modificar el puerto SSH predeterminado en linux?
Este tema también lo tratamos en profundidad en un articulo anterior, de todas maneras es así de fácil…

```
nano /etc/ssh/sshd_config
```

Edita donde pone «**22**», guarda el archivo y cierra el editor. No te olvides de conceder permisos al nuevo puerto.

18.- ¿Como puedo ver las marcas de tiempo en linux?
En la mayoría de distribuciones linux puedes utilizar el comando dmesg (mensajes de diagnostico), con su correspondiente parámetro.

```
dmesg -T
```

19.- ¿Como puedo saber la marca (fabricante) y el modelo de un servidor o estación de trabajo?
Con el comando **dmidecode**, podemos averiguar la marca y el modelo del servidor.

```
dmidecode -t system
```

20.- ¿Como identificar la bios del sistema?
Para esto, también nos ayudamos del comando **demidecode**.

```
dmidecode -t bios
```

21.- ¿Como extender un grupo de volúmenes ya creado?
Lo primero que tenemos que hacer es crear el volumen físico (pv) en el nuevo disco (sin formato), en este caso **/dev/sdb**.

```
pvcreate /dev/sdb
```

Ahora ejecutamos **vgextend**.

```
vgextend nombre-del-grupo-volumen /dev/sdb
```

Esta es la ultima de la serie de preguntas a un sysadmin más comunes, evidentemente son muchas más, pero he seleccionado las que considero más útiles para los usuarios en general.

Agregar espacio de intercambio en Debian 10

Un **espacio de intercambio**, también conocido como **swap**, es una porción única y exclusiva en el disco que se utiliza como memoria, cuando la RAM física está llena. Me explico, cuando un sistema Linux se queda sin RAM, toma el espacio de intercambio y mueve a el, los datos de la Ram que en ese momento están inactivos, pero se van a utilizar.

El espacio de intercambio se puede crear de dos maneras diferentes, en una podemos crear una partición dedicada, y en otra se crea un archivo que se utiliza como espacio de intercambio.

En este caso crearemos un archivo de intercambio, ¿por que archivo y no partición?, tu duda tiene fácil respuesta. La mayoría de proveedores de **VPS** no ofrecen **swap**, y si lo hacen es ínfima, ademas el método del archivo también es valido para ampliar tu espacio de intercambio (swap) sin tener que modificar las particiones físicas, algo que agradecen los usuarios más noveles.

Este método es valido para cualquier sistema linux, incluidos los domésticos.

En este articulo, centramos los pasos a seguir en **Debian 10**, pero es valido para la gran mayoría de distribuciones linux. Como ejemplo crearemos un espacio de 1GB, tu puedes modificar el valor según tus necesidades.

Agregar espacio de intercambio (swap)

Comenzamos creando el archivo al cual le indicamos que su valor será 1GB.

```
sudo fallocate -l 1G /swapfile
```

Normalmente «fallocate» esta instalado de manera predeterminada, aun así, también tienes la opción de crear el archivo con…

```
sudo dd if=/dev/zero of=/swapfile bs=1024 count=1048576
```

Bien, una vez creado el archivo modificas los permisos.

```
sudo chmod 600 /swapfile
```

Ahora creamos el espacio de intercambio.

```
sudo mkswap /swapfile
```

Lo activamos / habilitamos con «swapon».

```
sudo swapon /swapfile
```

Ahora mismo ya tienes tu swap creada y funcionando, pero claro, los cambios no son permanentes y al reiniciar el sistema desaparecerá el espacio de intercambio.

Para que las modificaciones sean permanentes debes editar el «fstab», veras que fácil.

```
sudo nano /etc/fstab
```

Copia y pega lo siguiente:

```
/swapfile   swap swap defaults 0 0
```

Guarda el archivo y cierra el editor.

Puedes verificar que tienes un nuevo espacio de intercambio con el siguiente comando.

```
sudo free –h
```

Eliminar el espacio de intercambio

El método anteriormente descrito funciona, y muy bien incluso en maquinas antiguas, pero si por algún motivo quieres eliminar el espacio de intercambio, también te explico como hacerlo.

Lo primero desactiva / deshabilita el archivo.

```
sudo swapoff –v /swapfile
```

Accede a fstab.

```
sudo nano /etc/fstab
```

y borra la linea que insertamos antes.

```
/swapfile   swap swap defaults 0 0
```

Guarda el archivo, y cierra el editor.
Para terminar, solo falta borrar el archivo.

```
sudo rm /swapfile
```

Instalar Node.js y NPM en CentOS 8

Nodejs es un entorno de tiempo de ejecución **JavaScript**, que permite a los desarrolladores crear aplicaciones y sitios web dinámicos, de forma altamente optimizada.

Node.js viene con el administrador de paquetes **NPM**, que facilita la tarea de publicar y compartir el código haciendo uso de las **bibliotecas Node.js**. En este tutorial, veremos cómo instalarlo en el nuevo **CentOS 8**.

Instalar Node.js y NPM en CentOS 8

Comenzamos instalando las herramientas de desarrollo necesarias para la aplicación.

```
sudo dnf groupinstall "Development Tools"
```

También puedes ejecutar **yum**, ahora mismo **dnf** es el predeterminado pero **yum** sigue estando disponible.

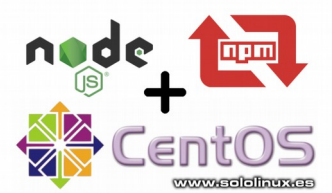
```
sudo yum groupinstall "Development Tools"
```

Actualizamos el sistema.

```
sudo dnf install update
```

Para instalar **Node.js y NPM en CentOS 8**, no es necesario agregar ningún repositorio, como en versiones anteriores. Lo tenemos **disponible en el repositorio oficial AppStream de CentOS 8**. Por tanto, lo primero que hacemos es buscar y ver cuál es la versión que tenemos disponible para instalar.

```
sudo dnf module list nodejs
```



Veremos un resultado similar a:

```
sololinux # dnf module list nodejs
Last metadata expiration check: 0:01:38 ago on Wed 03 Oct 2019 02:26:20 AM EDT.
CentOS-8 – AppStream
Name Stream Profiles Summary
nodejs 10 [d] common [d], development, minimal, s2i Javascript runtimeHint: [d]efault, [e]nabled, [x]disabled, [i]nstalled
```

Según podemos comprobar, el resultado anterior nos dice que la versión actual disponible es la **NodeJS 10.x**, que ademas es una LTS (largo plazo), así que una vez concluidas las comprobaciones, vamos a **instalar Node.js y NPM en CentOS 8**, con diferentes perfiles, concretamente con tres.

- Perfil normal
- Perfil desarrollador
- Perfil minimal

Para instalar la aplicación con el perfil normal (común / habitual), ejecuta lo siguiente:

```
sudo dnf module install nodejs
o
sudo dnf install @nodejs
```

El siguiente perfil es altamente recomendado para desarrolladores, ya que carga las bibliotecas para crear los módulos y más, ejecuta el comando…

```
sudo dnf module install nodejs/development
o
sudo yum module install nodejs/development
```

Por ultimo tenemos el denominado perfil mínimo.

```
sudo dnf module install nodejs/minimal
o
sudo yum module install nodejs/minimal
```

Bueno, ya tenemos instalada la herramienta. Verificamos.

En este paso vamos a verificar la versión instalada de Node.js y NPM, así como la carpeta donde se han instalado.

```
node-v
```

ejemplo de salida…
v10.14.1

```
npm -v
```

ejemplo de salida…
v6.4.1

```
which node
```

ejemplo de salida…
/usr/bin/node

```
which npm
```

ejemplo de salida…
/usr/bin/npm

Crear un USB Live persistente de Ubuntu

Una **USB persistente**, en un pendrive en el cual se ha creado una imagen ISO (de un sistema operativo) bootable, pero con la salvedad de que las modificaciones que hagamos serán guardadas en el mismo.

Explicado más sencillo, es como si fuera un S.O. portátil.

En este articulo crearemos una **Usb Live persistente** de la distribución **Ubuntu**, ademas… tan solo con un comando, ya veras que fácil es.

Crear un USB Live persistente

Existen otras alternativas, pero nosotros vamos a utilizar la herramienta **mkusb**. **Mkusb** es una de las aplicaciones más poderosas en linux a la hora de grabar una ISO en linux, y de la cual ya estamos preparando un articulo más extenso, incluyendo como trabajar con ella de manera gráfica.

Mkusb no viene de forma predeterminada en **Ubuntu**, así que lo primero que hacemos es agregar su repositorio «ppa».

```
sudo add-apt-repository ppa:mkusb/ppa
```

Actualizamos el sistema.

```
apt update
```

La instalación es bastante sencilla, tan solo debes ejecutar lo siguiente…

```
sudo apt install mkusb
```

Pero te recomiendo que agregues sus añadidos para una mejor experiencia de usuario, ejecuta lo siguiente:

```
sudo apt install mkusb mkusb-nox usb-pack-efi
```

Puedes verificar la aplicación.

```
mkusb -v
```

Ejemplo de salida correcta…

```
sololinux ~ # mkusb -v
mkusb-dus: dus 12.3.2
mkusb-11: mkusb 11.2.2
mkusb-nox: mkusb-nox 11.1.9
mkusb-bas: mkusb version 7.4.3
sololinux ~ #
```

Una vez instalado, su ejecución es tan simple como…

```
sudo mkusb /home/usuario/mi.iso.iso p
```

OJO!!!, inserta la ruta correcta de la ISO, no lo olvides.

Espera pacientemente a que concluya el proceso, y voila, ya tienes tu USB persistente. Enhorabuena.

Actualizar el kernel de Ubuntu con un click

Todo evoluciona, y como no podía ser menos, las distribuciones y herramienta linux también. En un pasado no muy lejano, si querías actualizar, cambiar, degradar, el **kernel** de linux, al final teníamos que compilarlo.

Hoy en día ya no es necesario, las actualizaciones se realizan de manera automática y normalmente no hay ningún problema. Como comentamos anteriormente, todo evoluciona, y con la herramienta **Ukuu** (**Ubuntu Kernel Update Utility**) ya es lo máximo.

¿Te imaginas una aplicación que te ofrezca de una manera simple y segura, instalar cualquier kernel compatible con tu sistema?.

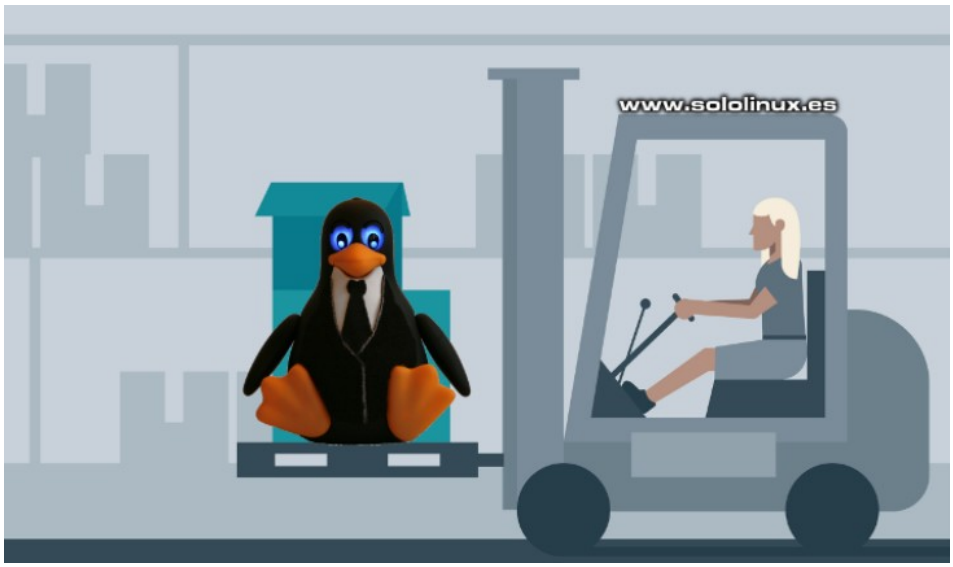
La aplicación existe, y se llama Ukku.

Ukuu descarga los kernels directamente desde **kernel.ubuntu.com**, por tanto no hay error posible. Te indico que como es evidente no solo es compatible con Ubuntu, también con todos sus derivados como **Linux Mint, Elementary OS**, y muchos más.

Principales características de **Ukuu**:

- Obtiene los núcleos desde **kernel.ubuntu.com**
- Muestra una notificación cuando hay una actualización del kernel disponible
- Descarga e instala las actualizaciones automáticamente
- Eliminar y purgar los kernel obsoletos
- Ver el registro de cambios del kernel
- Establece el tiempo de espera en el menú del GRUB

Es una herramienta muy interesante, así que vamos a probarla en nuestro sistema.



Actualizar el kernel de Ubuntu y derivados

Antes de comenzar debes asegurarte de la versión kernel instalada (por si acaso).

```
uname -r
```

En nuestro caso es…
4.15.0-58-generic

Continuamos actualizando el sistema.

```
sudo apt update && sudo apt dist-upgrade
```

Ahora agregamos el repositorio de Ukuu.

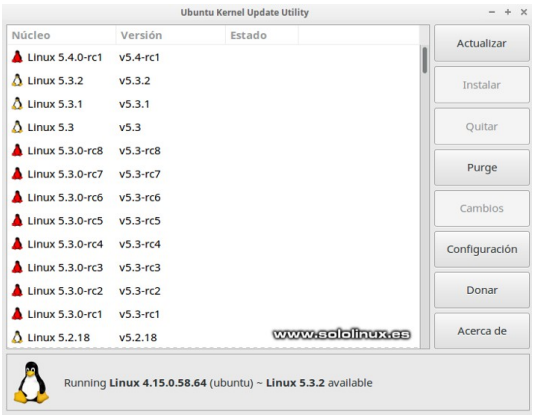
```
sudo add-apt-repository ppa:teejee2008/ppa
```

Instalamos la herramienta.

```
sudo apt update
sudo apt install ukuu
```

Una vez concluya la instalación lo ejecutamos. Puedes encontrar Ukuu en tu menú de aplicaciones, normalmente en sistema.

Al iniciar la herramienta se actualizara la base de datos, y nos aparecen los kernel.



OJO!!!, los kernel con el **Tux** de color rojo son versiones inestables, para que no aparezcan abres la configuración y marcas la opción «Ocultar versiones inestables y RC».
Para instalar un nuevo kernel tan solo debes pulsar sobre uno, y hacer click en instalar. Mi recomendación es que tengas habilitada la aplicación y ella te indicara la versión actualizada más apropiada para tu sistema (con una notificación en pantalla).

Instalar el cliente de Outlook 365 en Linux

Microsoft Outlook es una plataforma de comunicaciones propietaria de **Microsoft** que nos permite conectar y mantener organizado el correo electrónico, calendario y contactos desde la misma aplicación.

Microsoft Outlook se integra con Office 365.

A diferencia de los que «consumen» **Windows** y **Android**, los usuarios de Linux no tienen una aplicación oficial de escritorio (lógico). No pasa nada, gracias a **Julian Alarcon** tenemos **Prospect Mail**, un excelente **cliente de Outlook** no oficial para nuestro Linux.

Prospect Mail es un cliente no oficial de **Microsoft Outlook** para Linux. Lo que hace esta aplicación es envolver Outlook como si fuera un software independiente, para lograrlo utiliza **Electron**.

Algunas de las caracteristicas de Prospect Mail:

- Outlook OWA MS Office 365 online desde una aplicación de escritorio.
- Maximizar / minimizar.
- Bandeja de entrada, salida.
- Notificación del sistema al recibir comunicaciones.

En este articulo vemos como instalar el cliente de **Outlook 365** en **Linux**, gracias a Prospect Mail.

Instalar el cliente de Outlook 365 en Linux

La instalación es sencilla, usamos snap, si no recuerdas como instalar spnap, clic aquí.

Instalar Prospect Mail con Snap

Fácil, fácil, tan solo debes ejecutar el siguiente comando…

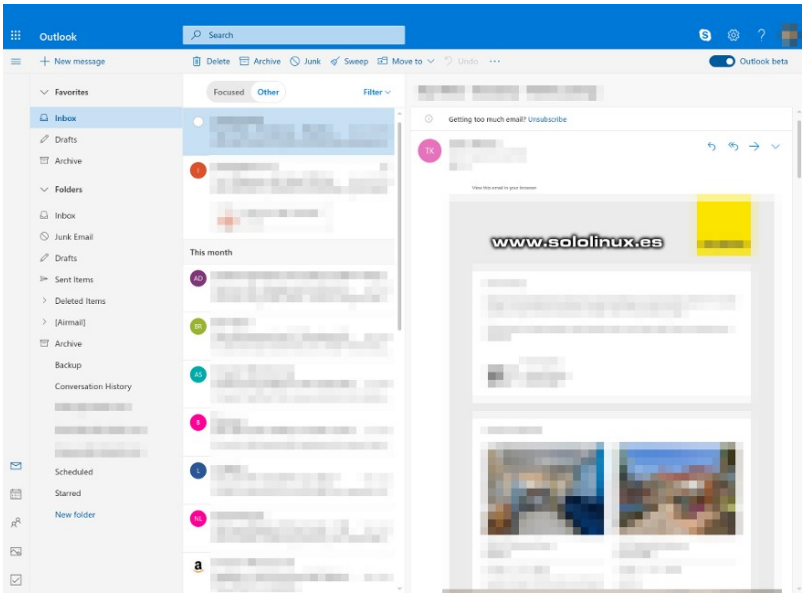
```
sudo snap install prospect-mail
```

Una vez instalado, abres la aplicación desde el menú de tu distribución linux.

Inserta tus credenciales.

Pantalla principal de Outlook 365 en linux.

Ya puedes comenzar a enviar y recibir correos desde la aplicación de escritorio en linux.



Instalar LAMP en Arch Linux y derivados

El paquete **LAMP** (Linux, Apache, MySQL/MariaDB, PHP) es el más común a la hora de montar un servidor web. En este articulo veremos cómo instalar LAMP en un servidor **Arch Linux**.

No debes preocuparte por las versiones que se instalaran, como **Arch** es una distribución Linux de lanzamiento constante, siempre instalara las ultimas versiones de PHP, Apache, y MariaDB.

Comenzamos…

Instalar LAMP en Arch Linux y derivados

Lo primero que debemos hacer es actualizar Arch Linux.

```
sudo pacman -Syu
```

Instalar Apache

Una vez tengamos nuestro servidor actualizado, instalamos **Apache**.

```
sudo pacman -Syu apache
```

Ahora editamos los recursos en el archivo de configuración de **Apache**, «httpd-default.conf». Te recomiendo que primero hagas una copia de seguridad con el siguiente comando.

```
cp /etc/httpd/conf/extra/httpd-mpm.conf ~/httpd-mpm.conf.backup
```

Abrimos el archivo con nuestro editor preferido, en nuestro caso utilizamos nano.

```
nano /etc/httpd/conf/extra/httpd-mpm.conf
```

Modifica los valores según tus necesidades. Si tienes un VPS, un buen Ejemplo es…

```
<IfModule mpm_prefork_module>
        StartServers 4
        MinSpareServers 20
        MaxSpareServers 40
        MaxRequestWorkers 200
        MaxConnectionsPerChild 4500
</IfModule>
```

Guarda el archivo, y cierra el editor. Te recomiendo que des-habilites KeepAlive, pero es tu decisión.

```
nano /etc/httpd/conf/extra/httpd-default.conf
```

Ejemplo…

```
KeepAlive Off
```

Solo nos falta habilitar el inicio automático de Apache con el sistema.

```
sudo systemctl enable httpd.service
```

Configurar el Virtual Host

Abrimos el archivo de configuración.

```
nano /etc/httpd/conf/httpd.conf
```

Debemos definir la raíz predeterminada. Busca la linea…

```
DocumentRoot "/srv/http"
```

y la editas como…

```
DocumentRoot "/srv/http/default"
```

En el mismo archivo buscamos otra linea más.

```
#Include conf/extra/httpd-vhosts.conf
```

la descomentas.

```
Include conf/extra/httpd-vhosts.conf
```

Guarda el archivo y cierra el editor.

Configuramos un host virtual (con tus datos reales).

```
nano /etc/httpd/conf/extra/httpd-vhosts.conf
```

Ejemplo de configuración…

```
<VirtualHost *:80>
        ServerAdmin webmaster@ejemplo.com
        ServerName ejemplo.com
        ServerAlias www.ejemplo.com
        DocumentRoot /srv/http/ejemplo.com/public_html/
        ErrorLog /srv/http/ejemplo.com/logs/error.log
            CustomLog  /srv/http/ejemplo.com/logs/access.log
combined
                    <Directory />
                        Order deny,allow
                        Allow from all
                    </Directory>
</VirtualHost>
```

Guarda el archivo y cierra el editor.

Creamos los directorios (carpetas) a los que hace referencia el Virtualhost (no te olvides de insertar tu dominio real).

```
sudo mkdir -p /srv/http/default

sudo mkdir -p /srv/http/ejemplo.com/public_html

sudo mkdir -p /srv/http/ejemplo.com/logs
```

Iniciamos el servicio Apache.

```
sudo systemctl start httpd.service
```

Instalar MariaDB en Arch Linux

Por defecto, Arch Linux instala el motor de base de datos MariaDB.

```
sudo pacman -Syu mariadb mariadb-clients libmariadbclient
```

```
sudo mysql_install_db --user=mysql --basedir=/usr --
datadir=/var/lib/mysql
```

Arrancamos MariaDB, y habilitamos su inicio con el sistema.

```
sudo systemctl start mysqld.service

sudo systemctl enable mysqld.service
```

No te olvides de asegurar la instalación de MariaDB.

```
mysql_secure_installation
```

- Enter current password for root (enter for none): Pulsa enter
- Set root password? [Y/n]: Y
- New password: Enter password
- Re-enter new password: Repeat password
- Remove anonymous users? [Y/n]: Y
- Disallow root login remotely? [Y/n]: Y
- Remove test database and access to it? [Y/n]: Y
- Reload privilege tables now? [Y/n]: Y

La instalación de MariaDB a concluido, ya podemos crear nuestra primera base de datos.

Accedemos a la consola MySQL. La password es la del usuario root.

```
mysql -u root -p
```

Creamos la base de datos «MiWeb».

```
CREATE DATABASE MiWeb;
```

El usuario y la password.

```
GRANT ALL ON webdata.* TO 'tu-usuario' IDENTIFIED
BY 'tu-password';
```

Para salir de la consola escribe lo siguiente.

```
quit
```

Instalar PHP en Arch Linux

Para finalizar la instalación de **LAMP en Arch**, nos falta instalar PHP.

```
sudo pacman -Syu php php-apache
```

Una vez concluya la instalación de PHP, editamos el archivo **php.ini**.

```
nano /etc/php/php.ini
```

El **php.ini** debe ser personalizado, pues depende de tu sitio web. Un buen comienzo es configurar el archivo para que obtenga los mensajes de error y registros, ademas de mejorar el rendimiento del servidor.

```
nano /etc/php/php.ini
```

Vemos un ejemplo de lineas a modificar en un VPS.

```
–error_reporting = E_COMPILE_ERROR|E_RECOVERABLE_ERROR|E_ERROR|E_CORE_ERROR
–log_errors = On
–error_log = /var/log/php/error.log
–max_input_time = 30
–extension=mysql.so
```

Creamos la carpeta donde se guardaran los registros, y concedemos permisos al usuario de Apache.

```
sudo mkdir /var/log/php

sudo chown http /var/log/php
```

Habilitamos el modulo PHP en Apache, insertando las siguientes lineas en su sección correspondiente.

```
nano /etc/httpd/conf/httpd.conf
```

```
# Dynamic Shared Object (DSO) Support
LoadModule php7_module modules/libphp7.so
AddHandler php7-script php

# Supplemental configuration
# PHP 7
Include conf/extra/php7_module.conf

# Located in the <IfModule mime_module>
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
```

Sin salir del archivo, busca la linea que te indico a continuación y la comentas.

```
LoadModule mpm_event_module modules/mod_mpm_event.so
```

Justo después de la anterior, copia y pega la que te indico a continuación.

```
LoadModule mpm_prefork_module modules/mod_mpm_prefork.so
```

Ejemplo…

```
#LoadModule mpm_event_module modules/mod_mpm_event.so
LoadModule mpm_prefork_module modules/mod_mpm_prefork.so
```

Guarda el archivo y cierra el editor.

Para finalizar reiniciamos Apache y el sistema.

```
sudo systemctl restart httpd.service
```

```
sudo systemctl reboot
```

Instalar PHP 7.3 en CentOS 8 y derivados

PHP es uno de los lenguajes de programación más utilizados, es de código abierto y especialmente desarrollado para aplicaciones o sitios web. Creado por **Rasmus Lerdorf**, este lenguaje se integra a la perfección con HTM para crear sitios web dinámicos.

En CentOS 8, RHEL 8 y derivados, de manera predeterminada viene PHP 7.2. En este articulo vemos como actualizar a PHP 7.3.

Nota: Puedes utilizar **dnf** o **yum**, nosotros en este caso seguiremos usando **yum**.

Instalar PHP 7.3 en CentOS 8 y derivados
Antes de comenzar debemos instalar los repositorios **Epel** y **Remi**.

Repositorio Epel:

```
rpm -Uvh https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

Repositorio Remi:

```
yum install -y https://rpms.remirepo.net/enterprise/remi-release-8.rpm
```

Ejemplo de salida…

```
Last metadata expiration check: 0:00:04 ago on Thu 08 Oct 2019 03:20:07 AM UTC.
remi-release-8.rpm                                              14 kB/s |  21 kB     00:01
Dependencies resolved.
================================================================================
 Package              Arch          Version                Repository       Size
================================================================================
Installing:
 remi-release         noarch        8.0-3.el8.remi         @commandline     21 k

Transaction Summary
================================================================================
Install  1 Package

Total size: 21 k
Installed size: 19 k
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Installing       : remi-release-8.0-3.el8.remi.noarch                     1/1
  Verifying        : remi-release-8.0-3.el8.remi.noarch                     1/1

Installed:
  remi-release-8.0-3.el8.remi.noarch

Complete!
```

Puedes listar los PHP instalables con el siguiente comando:

```
yum module list php
```

Habilitamos el **remi-7.3**, e instalamos **PHP 7.3**.

```
yum module enable php: remi-7.3 -y
```

```
yum install -y php php-cli php-common
```

Verificamos la versión instalada.

```
PHP 7.3.10 (cli) (built: Sep 24 2019 09:20:18) ( NTS )
Copyright (c) 1997-2018 The PHP Group
Zend Engine v3.3.10, Copyright (c) 1998-2018 Zend Technologies
    with Zend OPcache v7.3.10, Copyright (c) 1999-2018, by Zend Technologies
```

Instalar PHP-FPM y otras extensiones
Para instalar php-fpm, ejecuta lo siguiente:

```
yum install -y php-fpm
```

Extensión para soporte MySQL.

```
yum install -y php-mysqlnd
```

Para el buen funcionamiento de un sitio web basado en WordPress, te recomiendo instalar las siguientes extensiones.

```
yum install -y php-dom php-simplexml php-ssh2 php-xml php-xmlreader php-curl php-date php-exif php-filter php-ftp php-gd php-hash php-iconv php-json php-libxml php-pecl-imagick php-mbstring php-mysqlnd php-openssl php-pcre php-posix php-sockets php-spl php-tokenizer php-zlib
```

Para el buen funcionamiento de un sitio web basado en Joomla, te recomiendo instalar las siguientes extensiones.

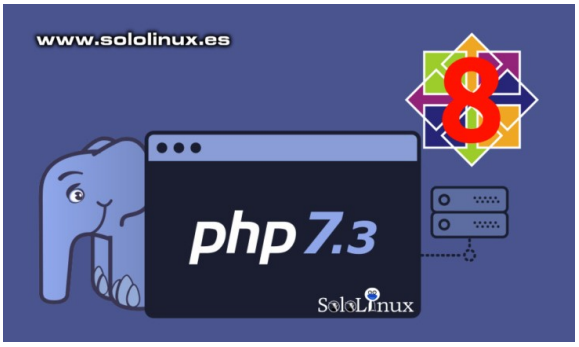
```
yum install -y php-mysqlnd php-zlib php-xml php-pear php-json php-mcrypt php-pecl-imagick
```

Para el buen funcionamiento de un sitio web basado en Drupal, te recomiendo instalar las siguientes extensiones.

```
yum install -y php-mysqlnd php-date php-dom php-filter php-gd php-hash php-json php-pcre php-pdo php-session php-simplexml php-spl php-tokenizer php-xml
```

Una vez concluida la actualización reinicia el sistema.

```
reboot
```



Instalar Netstat en CentOS 8 y derivados

Netstat es una utilidad en línea de comandos que nos ofrece información de las conexiones de red entrantes y salientes. Con este comando no solo visualizamos las conexiones de nuestro sistema, también las estadísticas de cada interfaz, las tablas de enrutamiento, conexiones ofuscadas, etc…

Sorprendentemente, **CentOS 8** no viene con la herramienta **Netstat** instalada de forma predeterminada, pero si que la encontramos en los repositorios oficiales. Por suerte que disponer de ella es una tarea sencilla.

A modo didáctico, antes de **instalar Netstat** podemos averiguar que paquete la contiene, y el repositorio que ofrece la aplicación. Ejecuta el siguiente comando:

```
yum whatprovides netstat
```

Ejemplo de salida…

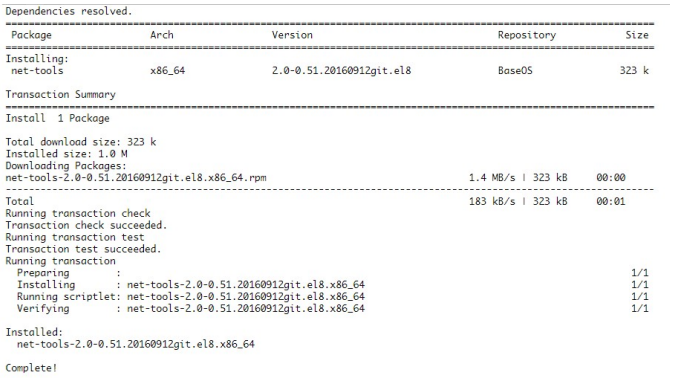
```
CentOS-8 – AppStream                    1.2 MB/s | 5.6 MB 00:04
CentOS-8 – Base                         1.5 MB/s | 5.3 MB 00:03
CentOS-8 – Extras                       567 B/s | 2.1 kB 00:03
Elasticsearch repository for 7.x packages
                                        754 kB/s | 3.4 MB 00:04
Extra Packages for Enterprise Linux 8 – x86_64
                                        515 kB/s | 2.0 MB 00:03

Last metadata expiration check: 0:00:01 ago on Wed 25 Sep 2019 06:26:50 AM EDT.
net-tools-2.0-0.51.20160912git.el8.i686 : Basic networking tools
Repo : BaseOS
Matched from:
Filename : /usr/bin/netstat

net-tools-2.0-0.51.20160912git.el8.x86_64 : Basic networking tools
Repo : BaseOS
Matched from:
Filename : /usr/bin/netstat
```

Como podemos ver en el ejemplo, el paquete «net-tools» contiene **Netstat**.

Instalar Netstat en CentOS 8
Puedes utilizar «**yum**» o «**dnf**», las dos opciones son aceptadas.

```
yum -y install net-tools
```

Ejemplo de instalación…



```
Dependencies resolved.
================================================================================
 Package              Arch          Version                    Repository   Size
================================================================================
Installing:
 net-tools            x86_64        2.0-0.51.20160912git.el8   BaseOS      323 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 323 k
Installed size: 1.0 M
Downloading Packages:
net-tools-2.0-0.51.20160912git.el8.x86_64.rpm  1.4 MB/s | 323 kB     00:00
--------------------------------------------------------------------------------
Total                                          183 kB/s | 323 kB     00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Installing       : net-tools-2.0-0.51.20160912git.el8.x86_64              1/1
  Running scriptlet: net-tools-2.0-0.51.20160912git.el8.x86_64              1/1
  Verifying        : net-tools-2.0-0.51.20160912git.el8.x86_64              1/1

Installed:
  net-tools-2.0-0.51.20160912git.el8.x86_64

Complete!
```

Ya la tienes instalada, así de fácil. Si quieres saber más sobre el comando Netstat te recomiendo que revises un articulo anterior al respecto.

Personalizar la terminal de Linux

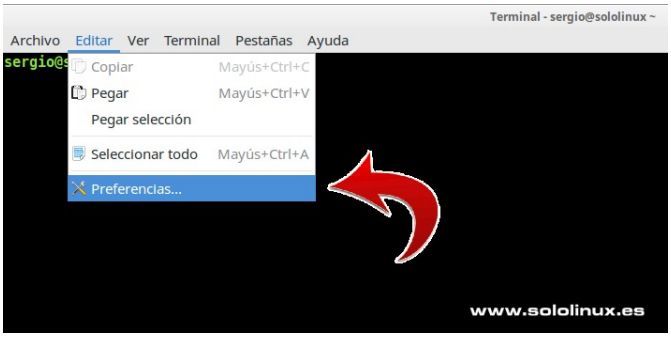
La terminal de cualquier distribución de GNU / Linux, o mejor dicho el emulador de terminal. Es la herramienta por excelencia con la que puedes controlar, manipular, y administrar tu sistema o incluso una compleja estructura en red.

Al iniciar el emulador de terminal solo aparece un mensaje con el nombre del host y el usuario. A pesar de su aspecto visual un tanto simple, ha mejorado enormemente a lo largo de los años. Los más veteranos en este mundillo saben perfectamente de que hablo, pues hoy en día, los emuladores de terminal son estéticamente agradables, ademas se integran perfectamente en los entornos de escritorio de la mayoría de **distribuciones Linux**.

En este articulo, vamos a explicar cómo puedes personalizar el aspecto de la **Terminal** (consola) en tu distribución preferida. Para escribir este articulo hemos tomado como ejemplo el **Terminal de XFCE**, pero el proceso es similar en otros emuladores.

Personalizar la terminal de Linux

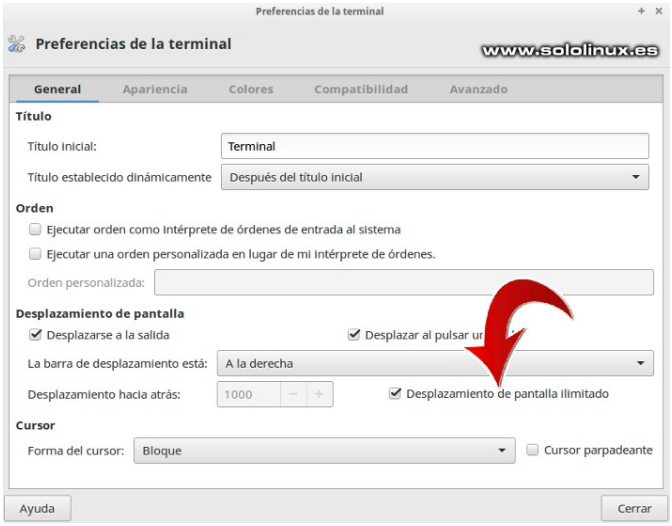
En el menú del emulador pulsamos en editar, en el desplegable hacemos clic en «**Preferencias**».



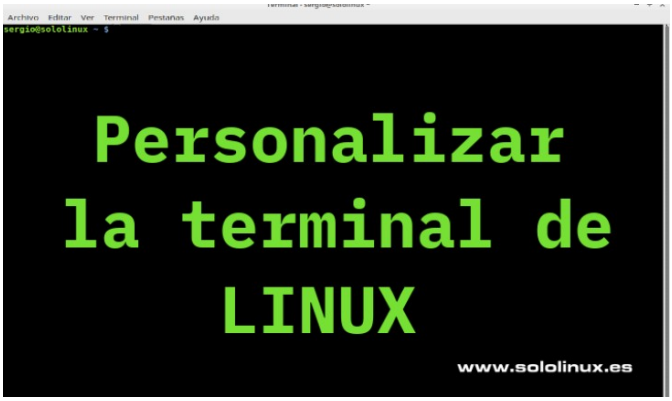
Se abre una nueva pantalla en la que veras las siguientes opciones (en otros emuladores puede variar algún nombre, pero básicamente es lo mismo):

- General
- Apariencia
- Colores
- Compatibilidad
- Avanzado

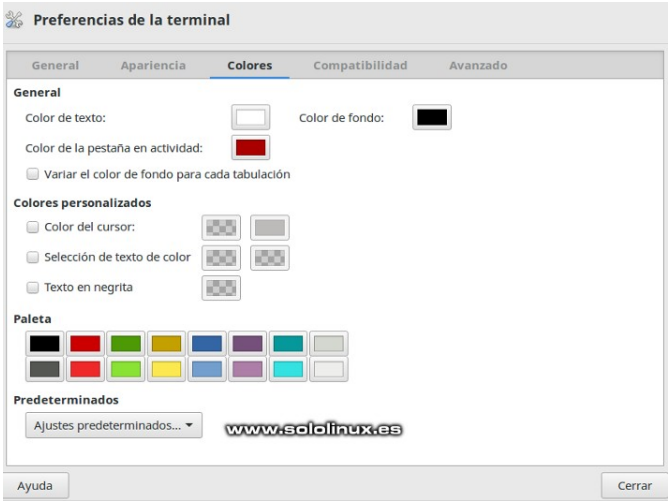
La opción general no tiene ningún misterio, la imagen inferior se explica por si sola. Únicamente me gustaría darte un consejo, normalmente la pestaña de **Desplazamiento de pantalla ilimitado** viene desmarcada, haz clic en ella. Al activar esa opción podremos revisar absolutamente todo lo que hacemos en la terminal, siempre que no la cierres evidentemente.



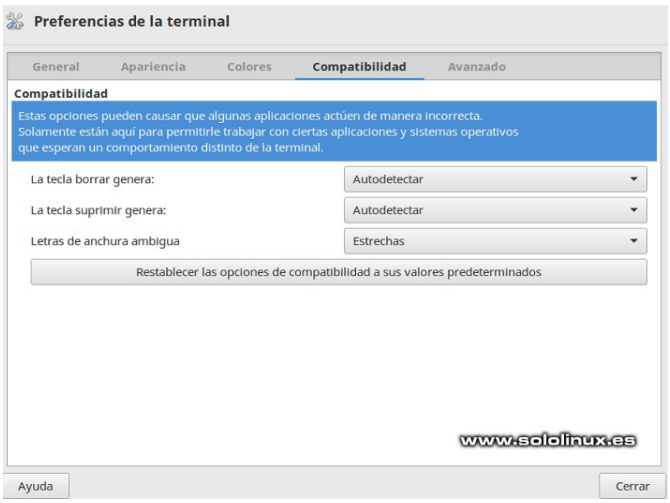
La siguiente opción es el menú «Apariencia», donde podrás seleccionar el tipo de letra, su tamaño, y varias cosas más. A tener en cuenta que puedes modificar la Geometria de la Terminal (su tamaño depende de ti), pero donde si quiero hacer incapie es en el fondo, por dios, no lo puedo entender. Cada día veo más y más distribuciones que aplican fondos semitransparente a sus emuladores de terminal predeterminados, si vas a escribir un comando al día da igual, pero si quieres trabajar en el… tu vista agredecera un color solido.



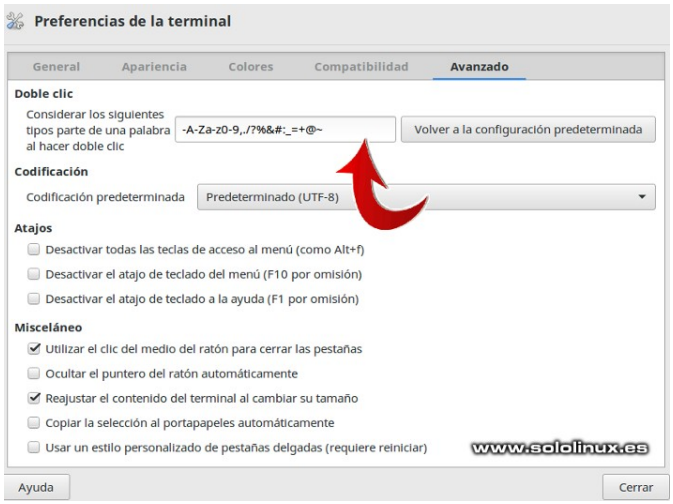
La siguiente opción de las preferencias de la terminal, es Colores. Aquí tenemos poco que decir, es tu decisión. Para gustos colores, jeje.



En la opción Compatibilidad puedes seleccionar la función de unas teclas determinadas. Puede provocar alguna incompatibilidad con alguna otra aplicación externa, así que si no es imprescindible déjalas como están.



Llegamos al final, la opción Avanzado. Aquí puedes habilitar o deshabilitar atajos de teclado, y alguan opción más que te puede ser de utilidad. También existe la lista de caracteres (puedes agregar más) que se consideran como parte de una palabra al hacer doble clic en ellos. A no ser que sea imprescindible, no recomiendo modificar nada de esta opción.



Llegamos al final, tan solo falta cerrar la pantalla de preferencias y salir de la Terminal. Al iniciar de nuevo el emulador tendrás todas las modificaciones habilitadas.

Ejecutar Ubuntu en Windows Subsystem for Linux

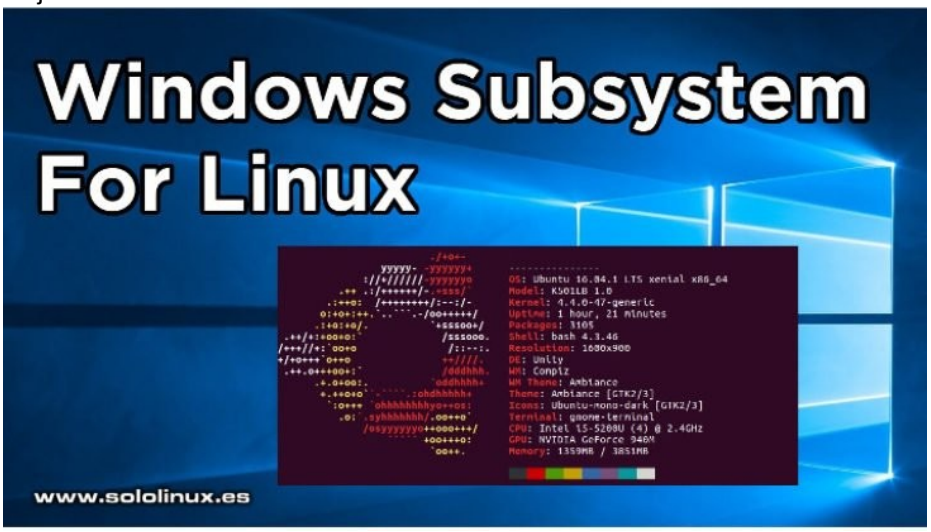
Windows Subsystem for Linux, más conocido como **WSL**, es una capa de compatibilidad diseñada por **Microsoft** que permite a sus usuarios instalar distribuciones Linux, y ejecutar de forma nativa los binarios de Linux en sistemas **Windows 10 y Windows Server 2019**.

Para poder utilizar **WSL**, los usuarios de **windows** deben iniciar sesión en su estación de trabajo Windows 10 o en el servidor Windows 2019. En este articulo, se toma como ejemplo **Windows 10**.

En otoño de 2018, Windows 10 envió junto a sus (masivas) actualizaciones la herramienta **Windows Subsystem for Linux**, por lo que solo necesitas habilitar esta característica que es opcional.

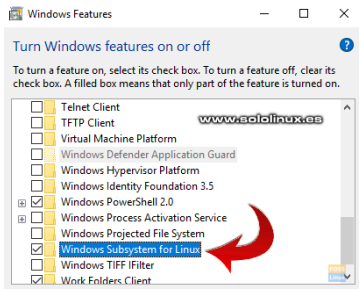
Antes de comenzar asegúrate que tu versión es **Windows 10 build 14393** o superior, si no es así, debes actualizar tu Windows. Recuerda que **WSL** solo es compatible con sistema de 64bits.

En este articulo vemos como **habilitar WSL**, y ejecutar Ubuntu en Windows. Vamos a ello.



Ejecutar Ubuntu en Windows Subsystem for Linux

Para habilitar WSL, haces clic en **Inicio de Windows** y busca Características de Windows . Busca **activar o desactivar características de Windows**, y selecciona **Windows Subsystem for Linux**.

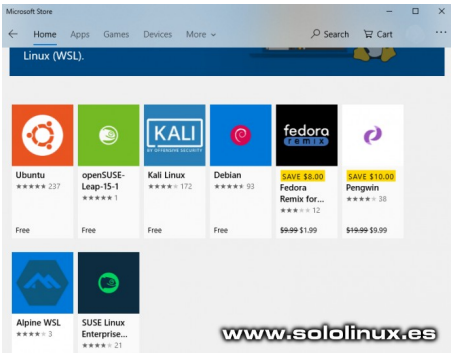


Pulsa en aceptar, y esperas pacientemente a que concluya la instalación. Al terminar te pedirá reiniciar el sistema, acepta.

Bien, ya instalamos la aplicación y reiniciado el sistema. Ahora desde tu navegador web favorito accede a la siguiente url:

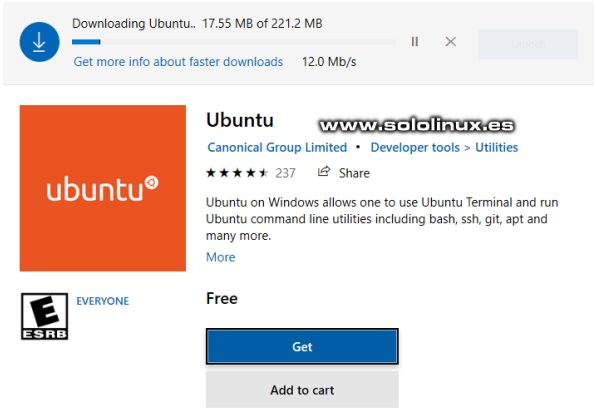
https://aka.ms/wslstore

Debes aceptar para permitir que Windows inicie **Microsoft Store**.



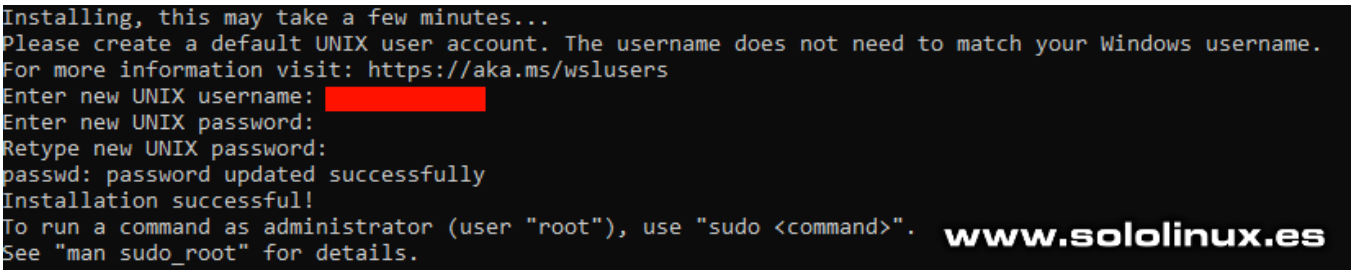
Como puedes ver aparecen varias distribuciones linux, en este articulo y a modo de ejemplo instalaremos Ubuntu, así que la seleccionas con doble clic.

Iniciamos la descarga de **Ubuntu** desde **Microsoft Store**.



Cuando termine la descarga, pulsa en iniciar la instalación.

Una vez concluya la instalación te pedirá que ingreses un usuario y password para linux.



Al igual que en cualquier instalación normal, lo primero que debes hacer es actualizar tu sistema.

```
sudo apt update
```

Ya tienes Ubuntu instalado en **Windows Subsystem for Linux**.

Como punto final dos detalles importantes, la instalación de nuestro linux la tenemos en:

C:\Users\tu-usuario\AppData\Local

Para acceder de nuevo a la consola de **Ubuntu**, haces clic en inicio de sesión y pulsas en «Ejecutar» o «Run». Escribe **cmd** para acceder a la consola.

Una vez estés en la terminal, tan solo debes insertar la palabra **bash**, y pulsar la tecla **Enter**.

Instalar BlueMail en Linux

BlueMail es una plataforma de comunicaciones que nos permite conectar de forma segura y organizada con nuestro correo electrónico, calendario y contactos, desde una potente aplicación.

Tiene una poderosa y bonita interfaz con una excelente experiencia de usuario, puedes enviar notificaciones y paquetes de **email** a través de múltiples **cuentas de correo** (se permite utilizar diferentes proveedores). Destacamos que **BlueMail** no tiene publicidad, y nos lanza notificaciones de escritorio. Realmente es una alternativa decente para sistemas Linux.

Independientemente de que seas una gran o pequeña empresa, **BlueMail** cumplirá con tus expectativas ya que dispone de versiones de escritorio, y también para dispositivos móviles. En este articulo veremos como instalar la aplicación de manera simple.

Instalar BlueMail en Linux

La forma más rápida de instalar BlueMail, es a traves de SNAP. Si no recuerdas como instalar snap revisa este articulo.

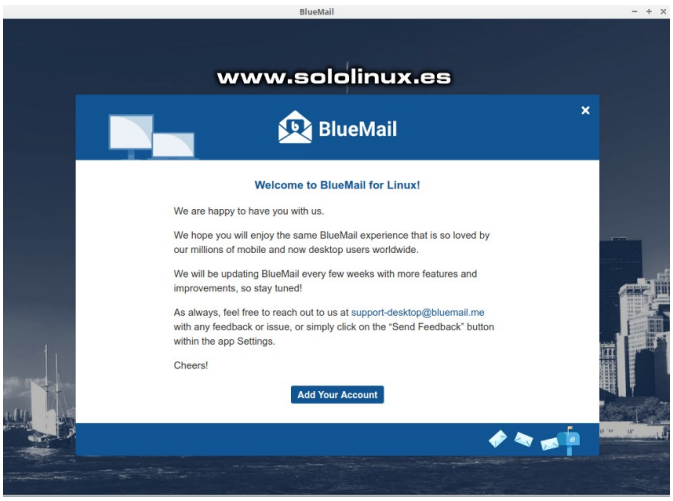
Para instalar la aplicación ejecuta lo siguiente:

```
sudo snap install bluemail
```

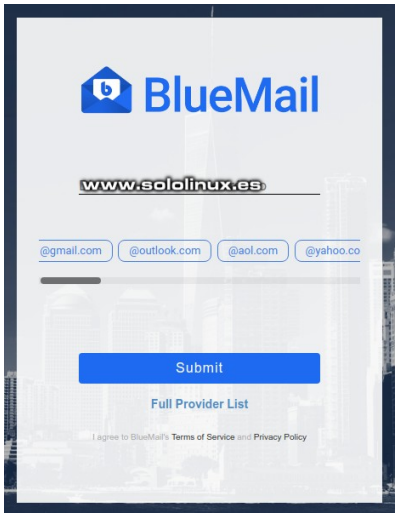
Una vez concluya la instalación busca el lanzador en el menú de aplicaciones y haces clic en el. OJO!!!, se puede dar algún caso en el cual no aparece el lanzador en el menú, entonces desde la terminal (consola) ejecutamos…

```
bluemail
```

Al iniciar por primera vez nos aparece la pantalla de bienvenida. Pulsamos en «ADD YOUR ACCOUNT» (agregar cuenta).

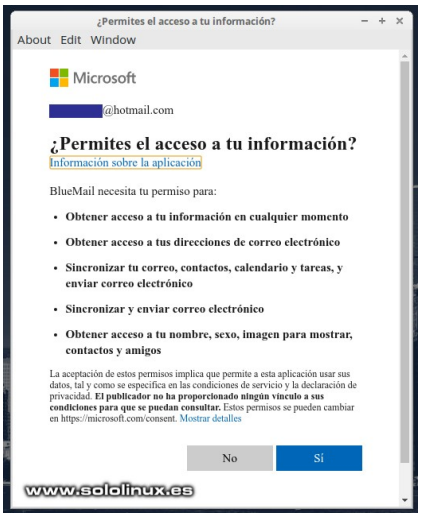


Agregamos nuestro email.

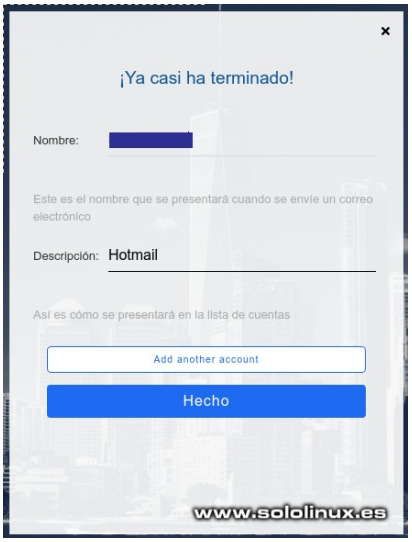


Insertamos la password de la cuenta de correo.

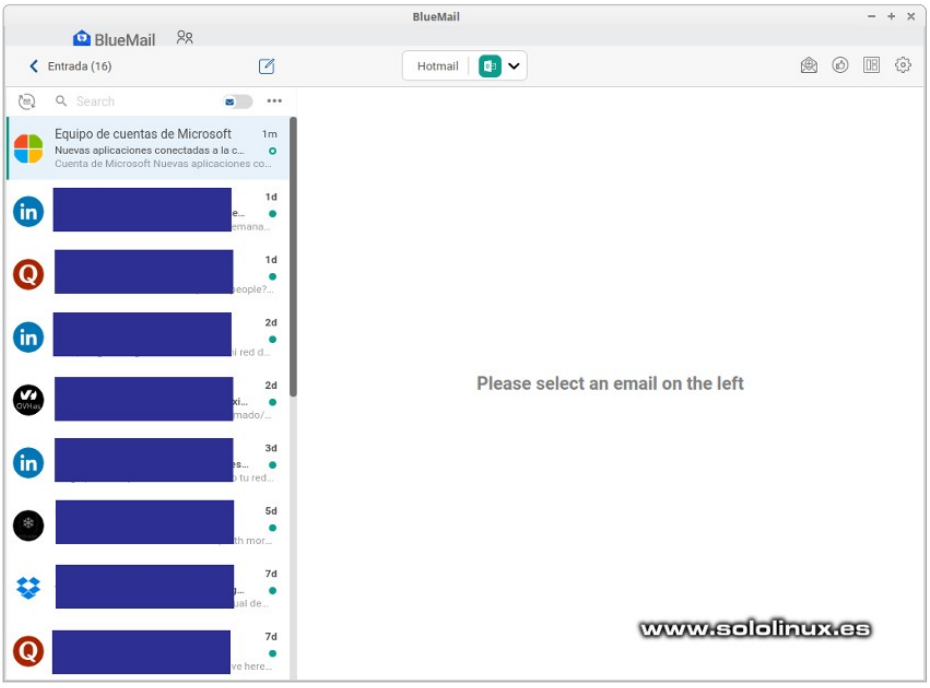
Dependiendo de tu proveedor de correo debes conceder los permisos pertinentes.



A modo informativo, **BlueMail** te permite configurar el nombre y la descripción de la cuenta de correo.



Al pulsar en «Hecho», accedemos automáticamente a nuestra cuenta de correo electrónico a través de BlueMail.



Felicidades, ya tienes la aplicación instalada y funcionando correctamente.

Reiniciar Ubuntu desde linea de comandos

Los sistemas basados en **Ubuntu** o **Debian** son fáciles de usar, confiables, y con una excelente experiencia de usuario. Ademas, existe una extensa colección de software que puedes instalar y ejecutar de manera gratuita, desde juegos hasta software de productividad para empresas o usuarios domésticos.

Hoy en día, no es necesario adquirir grandes conocimientos sobre el uso de la **terminal** (consola), sin embargo un entendimiento mínimo te puede sacar de algún apuro. De la misma forma que aprendes a utilizar una **distribución linux**, también deberías (por lo menos) comprender «el porqué» y «el cómo» de los principales comandos en Linux.

Si tuviéramos que elegir solo un comando indispensable, es evidente que sería uno que nos ayudara a reiniciar el sistema. Es importante aprender correctamente como reiniciar nuestro sistema, independientemente que sea un pc de escritorio, portátil, o servidor. Te aseguro que algún día lo necesitaras.

A continuación, aprenderás a **reiniciar Ubuntu** o cualquier otra distribución linux desde la línea de comandos.

Reiniciar Ubuntu desde linea de comandos

Veremos tres opciones que nos permiten reiniciar nuestro sistema. Recalcamos que son alternativas que **funcionan en todas las distribuciones linux más populares**, no solo en Ubuntu, Debian, y derivados.

- **systemctl**
- **shutdown**
- **reboot**

Reiniciar con Systemctl

Aunque tiene sus detractores, prácticamente la totalidad de distribuciones modernas utilizan systemctl para administrar sus tareas (cambiar el nombre del host, la zona horaria, etc…), por este motivo debe ser nuestra primera opción. Es tan sencillo como ejecutar lo siguiente…

```
sudo systemctl reboot
```

Dependiendo del uso, es posible que los clientes que estén conectados a tu sistema reciban una notificación indicando que el sistema se cierra, ya!!!. Si no quieres que aparezca ningún mensaje, reiniciamos de la siguiente forma.

```
sudo systemctl --no-wall reboot
```

Si por el contrario quieres personalizar una notificación al reiniciar, en el ejemplo lanzamos un mensaje de Sistema en Mantenimiento.

```
sudo systemctl --message="System Maintenance" reboot
```

Reiniciar con shutdown

Antes de la extensión masiva de **systemctl**, el comando para apagar o reiniciar el sistema era **shutdown**. Esta formula sigue siendo valida, ademas tiene unas características muy interesantes. Para reiniciar nuestro sistema ejecutamos el comando…

```
sudo shutdown -r
```

Si no has modificado su configuración, el sistema se reiniciara aproximadamente en un minuto. Pero observa el detalle, si quieres que se reinicie, por ejemplo en 10 minutos la sintaxis es…

```
sudo shutdown -r +10
```

Aun hay más, mira que interesante. Si quieres programar el reinicio, por ejemplo a las 12,15 am.

```
sudo shutdown -r 12:15
```

Debes saber que también es posible anular el reinicio programado, mira que fácil.

```
sudo shutdown -c "Canceling scheduled reboot"
```

Realmente estamos ante un comando muy interesante.

Reiniciar con reboot
Tal vez el comando reboot sea el más conocido, pero no por ello es el mejor. La verdad es que no sería la primera vez que un servidor remoto se queda colgado al usar este comando base. Aun así, al igual que los anteriores te puede sacar de algún apuro.

Dos maneras de utilizar el comando reboot.

```
sudo reboot
```

también puedes ejecutar…

```
sudo /sbin/reboot
```

Con este ultimo comando damos por concluido este articulo, recuerda usarlos con precaución.

Debes actualizar WhatsApp para evitar problemas.

Hace unos meses alertamos de la distribución de **malware** a través de imágenes alojadas en servidores seguros como los de **Google**, puedes leer la noticia aquí.

Estaba claro que tarde o temprano saltaría alguna alarma, y así es. El **Instituto Nacional de Ciberseguridad (INCIBE)** que pertenece al **Gobierno de España**, ha emitido una alerta sobre una vulnerabilidad que facilita a un hacker la tarea de secuestrar un **smartphone** y manejarlo de forma remota.

La vulnerabilidad fue localizada en **WhatsApp**, concretamente en las versiones anteriores a la 2.19.244 de Android, que a través de un código malicioso insertado en imágenes con extensión .gif abren la puerta para que un **hacker** se apodere de nuestro sistema **android**.

Recordemos que los **gifs** son un formato de imagen en movimiento muy popular, que se encuentra integrado en servicios de mensajería como **WhatsApp** o **Telegram**, y en redes sociales como **Twitter**.

Debes actualizar WhatsApp para evitar problemas.

La cuestión también afecta a la **galería de imágenes** de los smartphones, y ten presente que la gran mayoría reproducen los gif de manera automática. El error que permite secuestrar nuestro dispositivo, está localizado en las librerías relacionadas con la aplicación que reproduce los archivos de forma automática.

Al visualizar la imagen en movimiento, se ejecuta el código maligno, y se instala la aplicación que permite el acceso a nuestra información personal, así como el control remoto total del dispositivo.

Actualizar WhatsApp

Por suerte, la solución al fallo de seguridad es sencilla, tan solo debes actualizar la aplicación. Puedes actualizar WhatsApp desde tu Play Store, o accediendo a la pagina web de la aplicación.

- Google Play Store de WhatsApp
- Sitio web oficial de WhatsApp

Desactivar la combinación de teclas Ctrl + Alt + Del

Ctrl + Alt + Del, es una combinación de teclas que nos permite reiniciar nuestro sistema. A veces es muy útil, pero ojo, no sería el primer servidor que se reinicia por un error humano con esta **combinación de teclas**.

Para evitar situaciones desagradables, debes saber que es muy sencillo anular este atajo de teclado. El método que te propongo es valido en **CentOS, Rhel, Fedora, OpenSuse**, y muchas más.

Desactivar Ctrl + Alt + Del

Lo primero que hacemos es revisar el archivo «/etc/inittab» para verificar si es posible, ejecuta lo siguiente:

```
cat /etc/inittab
```

Ejemplo de salida…

```
[root@host ~]# cat /etc/inittab
# inittab is no longer used when using systemd.
#
# ADDING CONFIGURATION HERE WILL HAVE NO EFFECT ON YOUR SYSTEM.
#
# Ctrl-Alt-Delete is handled by /usr/lib/systemd/system/ctrl-alt-del.target
#
# systemd uses 'targets' instead of runlevels. By default, there are two main targets:
#
# multi-user.target: analogous to runlevel 3
# graphical.target: analogous to runlevel 5
#
# To view current default target, run:
# systemctl get-default
#
# To set a default target, run:
# systemctl set-default TARGET.target
```

Como puedes ver en el ejemplo ya no es posible desactivar la combinación de teclas en este archivo, en versiones antiguas si.

Para deshabilitar la combinación de teclas copia y pega lo siguiente…

```
systemctl mask ctrl-alt-del.target
```

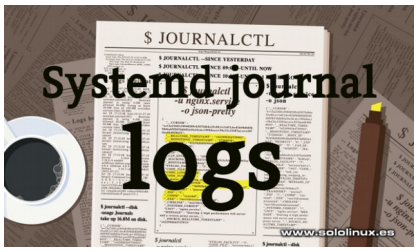
Ejemplo de salida valido…

```
[root@host ~]# systemctl mask ctrl-alt-del.target
Created symlink from /etc/systemd/system/ctrl-alt-del.target to /dev/null.
[root@host ~]#
```

Ya lo tienes, se acabo el peligro.

Cómo borrar los registros Systemd Journal Logs

Systemd tiene su propio sistema de registro conocido como **Systemd Journal Logs**, que proporciona una gestión centralizada de los registros del núcleo y también de los procesos de usuario.



El servicio encargado de recopilar y almacenar los datos es «systemd-journald». Estos datos de registro se almacenan en **/run/log/journal/MACHINE-ID/** si no son permanentes (se borran al reiniciar el sistema), y en **/var/log/journal/MACHINE-ID** si se guardan en el disco duro.

Como es lógico, dependiendo de la configuración de tu **sistema linux** estos registros pueden ocupar un espacio considerable en el disco. En este artículo veremos cómo borrar los archivos de registro de **Systemd Journal Logs**.

Cómo borrar los registros Systemd Journal Logs

Antes de ver como borrar los archivos, es interesante averiguar cuanto espacio están ocupando. Ejecuta el siguiente comando para visualizar la suma de los archivos guardados y activos.

```
journalctl --disk-usage
```

Ejemplo de salida…

```
[root@host ~]# journalctl –disk-usage
Archived and active journals take up 344.0M on disk.
[root@host ~]#
```

En el ejemplo anterior no ocupan mucho espacio, el motivo es porque la rotación es diaria. En sistemas con la rotación por defecto (normalmente 30 días), el espacio ocupado puede ser de varios digas (incluso decenas), y es evidente que eso tampoco es bueno, puede producir una degradación del rendimiento del disco.

Para borrar todos los archivos, incluyendo los que están activos actualmente, copia, pega, y ejecuta los dos comandos que te indico.

```
sudo journalctl --rotate
```

```
sudo journalctl --vacuum-time=1s
```

Explicamos la secuencia:

- **rotate**: El demonio borra todos los archivos actualmente activos.
- **vacuum-time=1s**: Se eliminan todos los archivos guardados en el registro con una antigüedad de más de un segundo. También se admiten otros tiempos, por ejemplo: **2m** (dos minutos), **5h** (cinco horas), **3weeks** (tres semanas), **5months** (cinco meses).

En vez de «–vacuum-time», puedes utilizar «–vacuum-size». Con size puedes establecer el borrado por tamaño de los archivos en vez de por tiempo. Por ejemplo…

```
sudo journalctl --vacuum-size=200M
```

Otro detalle que debes conocer… en las ultimas versiones de systemd puedes fusionar las dos opciones, rotate y vacuum. Observa…

```
sudo journalctl --rotate --vacuum-time=5m
```

```
sudo journalctl --rotate --vacuum-size=75M
```

Todo lo que hemos visto anteriormente es para borrar de forma manual (bajo demanda), si quieres automatizar el proceso puedes editar el archivo de configuración journald.conf.

```
nano /etc/systemd/journald.conf
```

Aparece algo similar a:

```
# This file is part of systemd.
#
# systemd is free software; you can redistribute it and/or modify it
# under the terms of the GNU Lesser General Public License as published by
# the Free Software Foundation; either version 2.1 of the License, or
# (at your option) any later version.
#
# Entries in this file show the compile time defaults.
# You can change settings by editing this file.
# Defaults can be restored by simply deleting this file.
#
# See journald.conf(5) for details.

[Journal]
#Storage=auto
#Compress=yes
#Seal=yes
#SplitMode=uid
#SyncIntervalSec=5m
#RateLimitInterval=30s
#RateLimitBurst=1000
#SystemMaxUse=
#SystemKeepFree=
#SystemMaxFileSize=
#RuntimeMaxUse=
#RuntimeKeepFree=
#RuntimeMaxFileSize=
#MaxRetentionSec=
#MaxFileSec=1month
#ForwardToSyslog=yes
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
#MaxLevelConsole=info
#MaxLevelWall=emerg
#LineMax=48K
```

Configura el archivo según tus necesidades (recuerda descomentar las lineas a utilizar), guarda el archivo, cierra el editor y **reinicia el sistema**.

Liberar espacio en el disco ocupado por Snap

Vaya sorpresa tuve el otro día, ufff. Revisando mi disco duro me di cuenta de que tenia ocupado demasiado espacio, la leche pensé, no puede ser, no puede ser.

Indagando, me di cuenta que el problema provenía del directorio **/var/lib/snapd/snaps/,** como puede ser, no lo entiendo. Resulta que al actualizar las aplicaciones de **snap**, no se eliminan los paquetes que previamente estaban instalados, no señor, no.

De manera predeterminada, el sistema almacena 3 versiones de las aplicaciones, en serio, no me lo podía creer. Cada herramienta que tengas instalada de **snap** y vayas actualizando, guardara las tres ultimas versiones con el consecuente consumo de espacio ocupado en el disco de forma innecesaria.

Liberar espacio en el disco ocupado por Snap

Buscando una solución encontré un comando para que no guardara tantas revisiones, lo deje en solo dos (se admite entre dos y veinte) con el siguiente comando.

```
sudo snap set system refresh.retain=2
```

Puedes visualizar el contenido restante en la carpeta después de reiniciar el sistema.

```
cd /var/lib/snapd/snaps
```

```
dir
```

Lo anterior puede ser una solución factible para muchos, para mi no.

Quiero borrar todas las revisiones que no se usan.

Vale… nos ponemos a ello que para eso tenemos bash. Veras que fácil.

```
nano borrar-snaps.sh
```

Copia y pega lo siguiente:

```
#!/bin/bash
# Borrar revisiones snaps
set -eu

snap list --all | awk '/disabled/{print $1, $3}' |
    while read snapname revision; do
        snap remove "$snapname" --revision="$revision"
    Done
```

Guarda el archivo y cierra el editor.

Le concedemos los permisos correspondientes.

```
chmod +x borrar-snaps.sh
```

Ejecutamos el script.

```
sudo ./borrar-snaps.sh
```

Ejemplo…

```
$ sudo ./remove-old-snaps
atom (revision 223) removed
atom (revision 222) removed
bitwarden (revision 15) removed
bitwarden (revision 16) removed
chromium (revision 607) removed
chromium (revision 660) removed
core (revision 6531) removed
core (revision 6405) removed
gallery-dl (revision 36) removed
gallery-dl (revision 167) removed
gimp (revision 110) removed
gimp (revision 113) removed
```

Ya tenemos borrado lo sobrante, felicidades.

Actualizar Plesk Onyx a Plesk Obsidian

Hace pocos días fue lanzada la nueva versión del afamado panel de control web, **Plesk**.

Denominada como **Plesk Obsidian** viene con grandes mejoras, especialmente en temas de experiencia de usuario y de seguridad, ademas destacamos que han integrado el monitor **Grafana** y **PHP Composer**. Puedes saber más sobre el tema en la pagina oficial de Obsidian.

Actualizar Plesk Onyx a Plesk Obsidian, no siempre esta disponible desde la zona de actualizaciones de tu panel Plesk. Por ello en este articulo veremos como subir de versión sin ningún riesgo y de forma segura, utilizando la **terminal** de nuestro linux.

Actualizar Plesk Onyx a Plesk Obsidian
Antes de comenzar te recomiendo que hagas backups y los descargues a tu sistema (por si acaso). Ahora es tan fácil como ejecutar el siguiente comando:

```
/usr/local/psa/admin/autoinstaller
```

En la pantalla que te aparece debes pulsar la tecla «F» en mayúsculas dos veces.

```
El asistente de instalación y actualización de Plesk le guiará por el
proceso de instalación o actualización.
========================================================================

------ IMPORTANTE ------

* La instalación de producto(s) sólo debería efectuarse en servidores limpios.

* Antes de instalar o actualizar Plesk, cree un backup de sus datos.

* El uso de este asistente supone la aceptación de los términos y condiciones
  descritos en http://www.plesk.com/legal/terms/ así como de los del contrato
  de licencia del usuario final de Plesk.

Acciones disponibles:
(F) Adelante
(Q) Cancelar la instalación
                                                        www.sololinux.es
Seleccione una acción [F/q]: F
Introduzca uno de los caracteres de la leyenda que puede ver arriba [F/q]: F
```

Ahora te pide que indiques una acción o un numero, debes seleccionar Plesk Obsidian que en nuestro caso es el numero 2.

Una vez modificado a la nueva versión de Plesk, pulsamos la tecla «F» para comenzar la actualización.

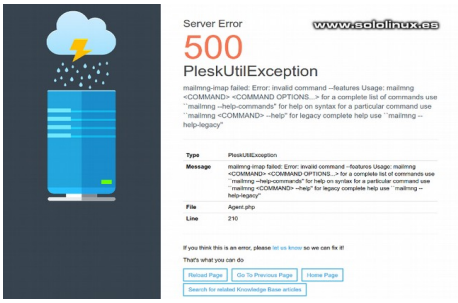
```
Seleccione los productos que desea instalar y sus versiones
========================================================================

Hay disponibles las siguientes versiones del producto:

1. [*] Plesk
  2. (*) Plesk Obsidian 18.0.19
  3. ( ) Plesk Onyx 17.8.11 (Stable) (currently installed)

Acciones disponibles:
(F) Adelante
(B) Volver
(Q) Cancelar la instalación
(S) Mostrar la configuración avanzada

Seleccione una acción o un número [F/b/q/s/1-3]: F          www.sololinux.es

Tiene la versión del producto Plesk 17.8.11 instalada. ¿Desea actualizarla? [Y/n]:
```

El nuevo Plesk necesita descargar paquetes esenciales de Obsidian, pulsa «F» en mayúsculas para continuar.

Ejemplo…

```
Preparando su sistema para la instalación del producto
========================================
========================

En su sistema no se han encontrado 7 paquetes
imprescindibles para
el correcto funcionamiento del producto.

Para instalar el producto es necesario
actualizar 52 paquetes.

Tiene 8 paquetes instalados que serán
eliminados.Acciones disponibles:
(F) Adelante
(B) Volver
(Q) Cancelar la instalación
(S) Mostrar la lista de paquetes

Seleccione una acción [F/b/q/s]:
```

Una vez comienza la actualización es posible que salte un error 500 al intentar acceder al panel de control, tranquilo los sitios web siguen online.



La actualización es bastante rápida, pero claro… todo depende de tu sistema. Al concluir el upgrade to Plesk Obsidian aparece un mensaje indicando que todo es correcto.

Ejemplo…
Upgrade is finished

Congratulations!

The upgrade has been finished. Plesk is now running on your server.

Use the username 'admin' to log in. To log in as 'admin', use the 'plesk login' command.
You can also log in as 'root' using your 'root' password.

Use the 'plesk' command to manage the server. Run 'plesk help' for more info.

Use the following commands to start and stop the Plesk web interface:
'service psa start' and 'service psa stop' respectively.

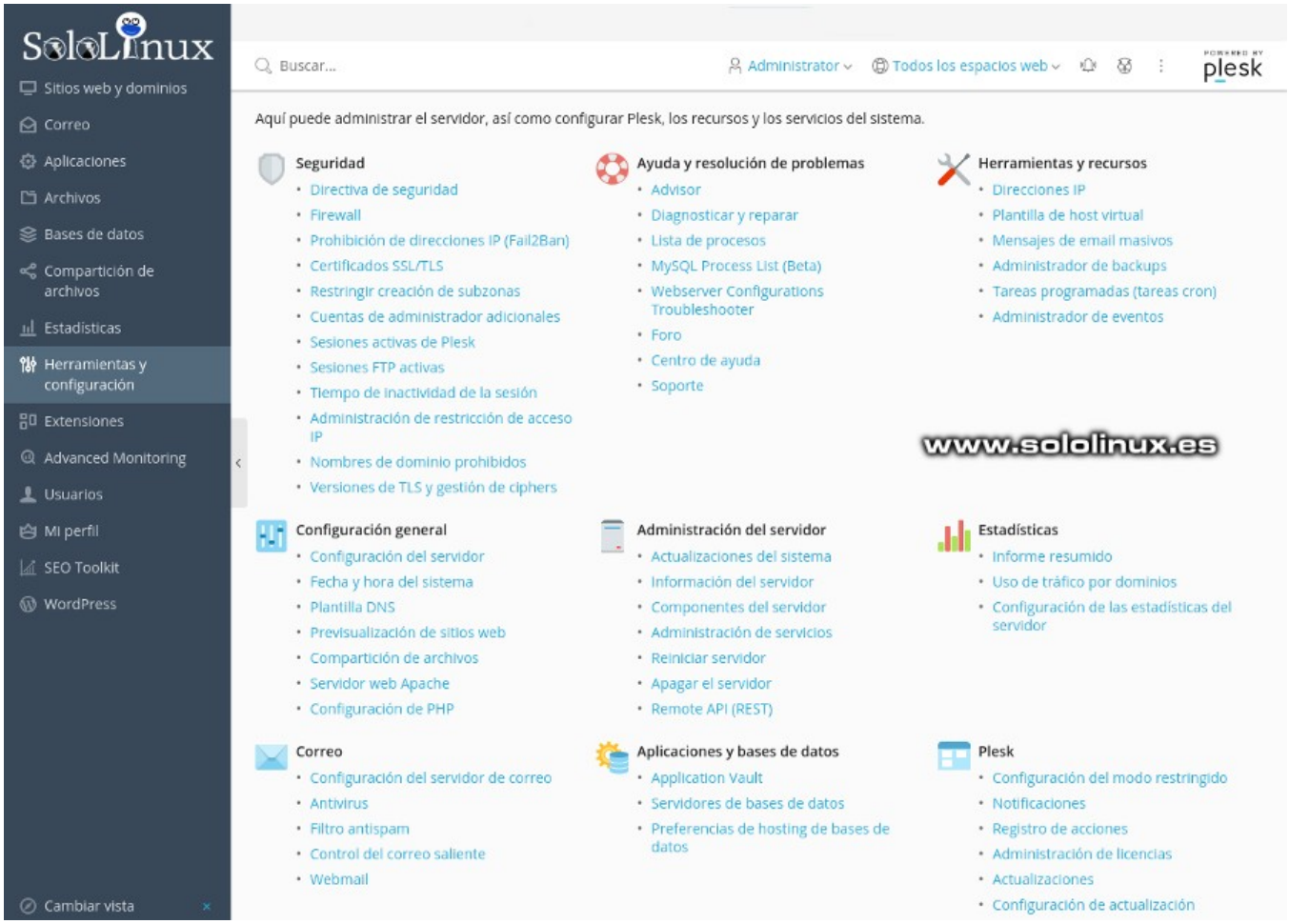
Los cambios se han aplicado correctamente.

Es recomendable que actualices el sistema y lo reinicies.

```
yum update
```

```
reboot
```

Ya tienes tu **Plesk Onyx** actualizado a **Plesk Obsidian**, felicidades.



Instalar Fail2ban en CentOS, Fedora, y derivados

Fail2ban es la herramienta de prevención de intrusiones por excelencia. De código abierto y totalmente configurable es la más utilizada en servidores y sistemas en red a nivel mundial.

Su forma de operar es bastante simple, ya que tan solo escanea los archivos de registro buscando direcciones IP con síntomas maliciosos, por ejemplo demasiados errores al introducir la contraseña.

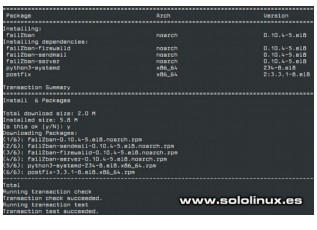
Al detectar un dirección ip que incumple con su configuración, automáticamente actualiza las reglas del **firewall** (normalmente **iptables** o **nftables**) de manera que sea rechazada. Por defecto, ya viene con filtros preconfigurados para los servicios más comunes, incluido **sshd**.

En este artículo, vemos cómo instalar y configurar **fail2ban** en nuestro servidor o VPS. En este articulo usamos como plataforma un **CentOS 8 minimal** que hemos instalado con **netinstall**.

Instalar Fail2ban en CentOS o Fedora

El paquete fail2ban no está en los repositorios oficiales pero si en el repositorio EPEL, así que lo habilitamos.

```
dnf install epel-release
o
yum install epel-release
```



Ahora instalamos Fail2ban.

```
dnf install fail2ban
o
yum install fail2ban
```

Configurar Fail2ban

Bien, una vez instalado vamos a **configurar fail2ban.** Los archivos de configuración los puedes localizar en **/etc/fail2ban/**, y los filtros en **/etc/fail2ban/filter.d/**. También tenemos el archivo de configuración general en **/etc/fail2ban/jail.conf,** pero no te recomiendo que pierdas el tiempo con el, mejor filtro por filtro ya que cada servicio requiere de su propia seguridad.

Lo que te recomiendo encarecidamente es crear un archivo llamado **jail.local**, y definir o configurar los filtros que necesites. Por ejemplo:

```
nano /etc/fail2ban/jail.local
```

Ejemplo de jails de un servidor web en producción.

```
[DEFAULT]
ignoreip = 127.0.0.1/8
destemail = webmaster@midominio.es
bantime = 21600
maxretry = 2
findtime = 600

[apache]
maxretry = 4
enabled = true
logpath = /var/www/vhosts/system/*/logs/error_log
/var/log/httpd/*error_log
action = iptables-multiport[name=apache, port=»http,https,7080,7081"]

[a[apache-badbot]em>
enabled = true
action = iptables-multiport[n[name=BadBots,
port=»http,https,7080,7081"]em>
logpath = /var/www/vhosts/system/*/logs/*access*log
/var/log/httpd/*access_log

[dov[dovecot]>
enabled = true
action = iptables-multiport[nam[name=»plesk-dovecot»,
port=»imap,imap3,imaps,pop3,pop3s,4190"]>

[postf[postfix]/span>
enabled = true
action = iptables-multiport[name=[name=»plesk-postfix»,
port=»smtp,smtps,submission»]/span>

[proft[proftpd]/span>
maxretry = 1
enabled = true
action = iptables-multiport[name=[name=»plesk-proftpd», port=»ftp,ftp-
data,ftps,ftps-data»]/span>

[round[roundcube]/span>
enabled = true
action = iptables-multiport[name=[name=»roundcube»,
port=»http,https,7080,7081"]/span>

[wordpre[wordpress]pan>
enabled = true
logpath = /var/www/vhosts/system/*/logs/*access*log
/var/log/httpd/*access_log
action = iptables-multiport[name=»[name=»plesk-wordpress»,
port=»http,https,7080,7081"]pan>

[ssh][ssh]n>
enabled = true
action = iptables[name=SSH,[name=SSH, port=ssh, protocol=tcp]n>
```

Guarda el archivo y cierra el editor.

Iniciamos fail2ban y lo habilitamos para que inicie con el sistema.

```
systemctl start fail2ban

systemctl enable fail2ban
```

```
systemctl status fail2ban
```

```
fail2ban-client status ssh
```

Cambiar de usuario desde la terminal

Si eres un usuario recién llegado al mundo **Linux**, tal vez no sepas que existen muchas formas de **cambiar de usuario** en la sesión actual.

Es evidente que la forma más conocida de cambiar de user, es a través de la interfaz gráfica del **entorno de escritorio**. Personalmente te digo, que es mucho más rápido y seguro ejecutar esta acción desde la terminal, ya veras que fácil, observa.

Cambiar de usuario desde la terminal

Para cambiar rápidamente de usuario utilizamos «su».

```
su usuario
```

Ejemplo…
#su sergio
Password:
[sergio@sololinux juan ~]#

OJO!!!, si observas con atención el ejemplo, podrás comprobar que el usuario «sergio» a heredado las variables de entorno de la cuenta del anterior usuario, en el ejemplo «juan». Puedes verificarlo con el siguiente comando:

```
echo $USERNAME
```

Realmente no debería existir ningún problema grave, pero bueno, nosotros queremos aprender a trabajar de manera correcta.

Para cambiar de usuario creando un nuevo entorno, debemos separar la orden del nombre con un guion y espacios.

```
su - usuario
```

Ejemplo…
#su – sergio
Password:
[sergio@sololinux ~]#

Ahora si que cambiamos de usuario correctamente, con su propio entorno.

Instalar Grafana en CentOS 8

Grafana, es una de las mejores herramientas para **monitorizar** servidores que puedes encontrar, tiene unas propiedades únicas para ser de **código abierto**.

No pienses que estamos ante una herramienta común, no no, de eso nada. Solo te digo que gigantes como **eBay, Paypal** o el mismo **RedHat**, utilizan **Grafana** para monitorear sus servidores. Es una herramienta imprescindible si quieres controlar tus servidores de manera robusta y escalable.

Como ya comentamos en un articulo anterior, el nuevo panel de control web, **Plesk Obsidian**, lo integra de serie en sus instalaciones. Es muy, muy bueno.

Grafana tiene otra interesante particularidad, nos permite optar por vincularlo con bases de datos de series temporales como InfluxDB o Prometheus, o con bases de datos relacionales como MySQL, MariaDB o PostgreSQL.

Instalar Grafana en CentOS 8 o CentOS 7

Comenzamos actualizando el servidor.

```
sudo yum update
```

Agregamos el repositorio de Grafana.

```
nano /etc/yum.repos.d/grafana.repo
```

Copia y pega lo siguiente:

```
[grafana]
name=grafana
baseurl=https://packages.grafana.com/oss/rpm
repo_gpgcheck=1
enabled=1
gpgcheck=1
gpgkey=https://packages.grafana.com/gpg.key
sslverify=1
sslcacert=/etc/pki/tls/certs/ca-bundle.crt
```

Guarda el archivo, cierra el editor, y actualiza el sistema.

```
sudo yum update
```

Instalamos Grafana.

```
sudo yum install grafana
```

Una vez concluya la instalación, puedes comprobar el servicio con sus rutas.

```
cat /usr/lib/systemd/system/grafana-server.service
```

Ejemplo…

```
[Unit]
Description=Grafana instance
Documentation=http://docs.grafana.org
Wants=network-online.target
After=network-online.target
After=postgresql.service mariadb.service mysqld.service

[Service]
EnvironmentFile=/etc/sysconfig/grafana-server
User=grafana
Group=grafana
Type=notify
Restart=on-failure
WorkingDirectory=/usr/share/grafana
RuntimeDirectory=grafana
RuntimeDirectoryMode=0750
ExecStart=/usr/sbin/grafana-server \
                                        –config=${CONF_FILE} \
                                        –pidfile=${PID_FILE_DIR}/grafana-
server.pid \
                                        –packaging=rpm \
                                        cfg:default.paths.logs=${LOG_DIR} \
                                        cfg:default.paths.data=${DATA_DIR} \
                                        cfg:default.paths.plugins=$
{PLUGINS_DIR} \
                                        cfg:default.paths.provisioning=$
{PROVISIONING_CFG_DIR}

LimitNOFILE=10000
TimeoutStopSec=20

[Install]
WantedBy=multi-user.target
```

Según nos indica el ejemplo anterior…

- Los binarios de Grafana están en /usr/sbin/grafana-server.
- El archivo que define las variables de entorno las podemos encontrar en /etc/sysconfig/grafana-server.
- El archivo de configuración es a través de la variable CONF_FILE.
- El PID del archivo lo determina la variable PID_FILE_DIR.
- Las rutas del registro, datos, complementos, y más… también están indicadas por las variables.

Puedes ver las variables en: etc/sysconfig/grafana-server

Ejemplo…

```
GRAFANA_USER=grafana

GRAFANA_GROUP=grafana

GRAFANA_HOME=/usr/share/grafana

LOG_DIR=/var/log/grafana

DATA_DIR=/var/lib/grafana

MAX_OPEN_FILES=10000

CONF_DIR=/etc/grafana

CONF_FILE=/etc/grafana/grafana.ini

RESTART_ON_UPGRADE=true

PLUGINS_DIR=/var/lib/grafana/plugins

PROVISIONING_CFG_DIR=/etc/grafana/provisioning

# Only used on systemd systems
PID_FILE_DIR=/var/run/grafana
```

Puedes ver en el ejemplo anterior, que al instalar Grafana ya se creo un usuario (grafana).

Vale, continuamos…

Iniciamos Grafana y verificamos el servicio.

```
sudo systemctl start grafana-server
```

```
sudo systemctl status grafana-server
```

Felicidades, ya tiene a Grafana corriendo en tu sistema. No te olvides de abrir el puerto correspondiente.

```
sudo firewall-cmd --add-port=3000/tcp --permanent
```

```
sudo firewall-cmd --reload
```

Interfaz de usuario de Grafana

El puerto por defecto de Grafana es el «3000», por tanto desde tu navegador web favorito puedes acceder así…

http://ip-del-servidor:3000/
http://localhost:3000/

Nos aparece la pantalla de inicio de sesión, por defecto el usuario y la contraseña es «admin».

La aplicación te pide que modifiques la contraseña por defecto.

Accedemos a la pantalla predeterminada por defecto de Grafana.

La url de inicio de sesión en Grafana es la siguiente:

http://ip-del-servidor:3000/signup
http://localhost:3000/signup

Si tu eres el sysadmin, y no quieres que nadie más tenga acceso, algo recomendable (ni intentar registrarse), sigue los pasos que te indico a continuación.

Editamos el archivo «grafana.ini».

```
sudo nano /etc/grafana/grafana.ini
```

Busca la siguiente linea…

```
[users]
# disable user signup / registration
;allow_sign_up = true
```

La modificas a false.

```
[users]
# disable user signup / registration
;allow_sign_up = false
```

Guarda el archivo y cierras el editor.

Para concluir reiniciamos Grafana.

```
sudo systemctl restart grafana-server
```

En un próximo articulo aprenderemos a crear nuestro primer tablero, síguenos.

Ubuntu 19.10 Eoan Ermine Listo para su descarga

Canonical ha lanzado oficialmente la ultima versión estable de **Ubuntu**. Conocido como **Ubuntu 19.10 Eoan Ermine**, nos encontramos con una versión que viene con bastantes características novedosas.

Seis meses después de su anterior lanzamiento, el nuevo **Ubuntu 19.10** conocido como **Eoan Ermine**, es la versión número 31 de **Ubuntu Linux**, uno de los sistemas operativos de código abierto más populares del mundo. Con esta versión, se celebran los quince años desde que la primera versión vio la luz.

Al no ser una versión LTS su muerte ya tiene fecha, julio de 2020.

Vemos algunas de sus características principales, así como su pagina oficial de descarga.

Ubuntu 19.10 Eoan Ermine

Ubuntu 19.10 incluye los controladores propietarios de Nvidia integrados (por fin), notaras una gran mejora en el rendimiento, y velocidad en los juegos, otro tema interesante es que ahora se ofrece soporte para el último estándar de seguridad **WPA3 Wi-Fi**. Podrás compartir mediante **DLNA**, ya que viene habilitado por defecto.

En cuanto al software, **Ubuntu 19.10** actualiza su entorno de escritorio a GNOME 3.34 con nuevas variantes de su tema **Yaru**. El navegador web **Chromium** esta instalado por defecto, ademas de **Mozilla Firefox 69**, la suite ofimática **LibreOffice 6.3**, el cliente de correo **Thunderbird 68**, así como el sistema de sonido **PulseAudio 13.0**.

El nuevo kernel Linux 5.3, ofrece soporte para GPU AMD Navi, pantallas ARM Komeda, Intel Speed Select en servidores Xeon, procesadores Zhaoxin x86 de estaciones de trabajo, así como nuevos chips ARM, y LZ4. **Initramfs** también es la compresión predeterminada (en todas las arquitecturas) para que el sistema inicie más rápido. El compilador del sistema GCC fue reforzado para mayor seguridad.

Se han actualizado las herramientas y aplicaciones GCC (GNU Compiler Collection) 9.2.1, Glibc (GNU C Library) 2.30, Python 3.7.5, OpenJDK 11, Perl 5.28.1, Rustc 1.37, Ruby 2.5.5, PHP 7.3.8, y Golang 1.12.10. AArch64 y POWER también se han mejorado para permitir un soporte de compilación cruzada en arquitecturas ARM, RISCV64 y S390X. Si hablamos de un servidor, Ubuntu 19.10 integra QEMU 4.0, libvirt 5.6, dpdk 18.11.2, Open vSwitch 2.12, MySQL 8.0, OpenStack Train, así como cloud-init y curtin 19.2.

Mejoras específicas para los sistemas IBM Z y LinuxONE, y una nueva imagen de invitado optimizada para KVM amd64 qcow2, ademas de ISO Live server para ppc64el y arm64. Por último, pero no menos importante, Ubuntu 19.10 viene con imágenes preinstaladas de 32 bits y 64 bits para los Raspberry Pi compatibles con el ultimo SBC de Raspberry Pi 4, y la mayoria de sabores de Raspberry Pi.

Puedes descargar la nueva versión desde su pagina oficial.

Chequear la versión instalada de Ubuntu, Debian y derivados

Es algo común que nos olvidemos de la versión del sistema que estamos usando, tranquilo en este articulo veremos una cuantas opciones para que lo puedas identificar de manera exacta.

Existen variadas formas de identificar tu sistema, tal vez alguna te de error dependiendo de tu sistema, pero están probadas en **Ubuntu, Debian, y Linux Mint**. Los ejemplos que aportamos en este articulo están creados sobre un **Linux Mint Sylvia**.

Chequear la versión instalada de Ubuntu y derivados

La primera opción a tener en cuenta es lsb_release.

```
lsb_release -a
```

Ejemplo de salida…

```
sololinux ~ # lsb_release -a
No LSB modules are available.
Distributor ID: LinuxMint
Description: Linux Mint 18.3 Sylvia
Release: 18.3
Codename: sylvia
sololinux ~ #
```

Seguimos con «issue» que no aportara tanta información, pero justo lo que necesitamos.

```
cat /etc/issue
```

Ejemplo de salida…

```
sololinux ~ # cat /etc/issue
Linux Mint 18.3 Sylvia \n \l
sololinux ~ #
```

Ahora la comprobamos con os-release.

```
cat /etc/os-release
```

Ejemplo de salida…

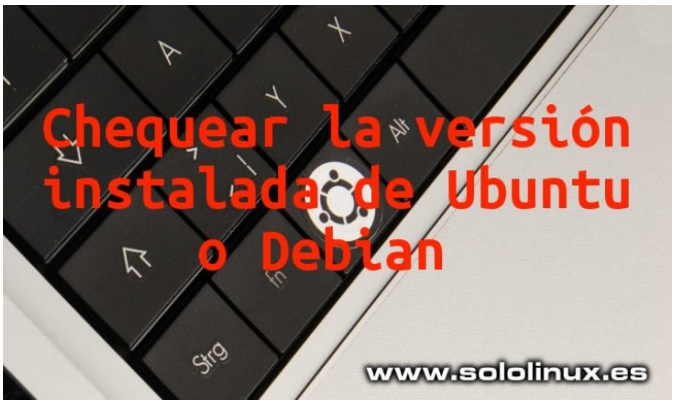
```
sololinux ~ # cat /etc/os-release
NAME=»Linux Mint»
VERSION=»18.3 (Sylvia)»
ID=linuxmint
ID_LIKE=ubuntu
PRETTY_NAME=»Linux Mint 18.3″
VERSION_ID=»18.3″
HOME_URL=»http://www.linuxmint.com/»
SUPPORT_URL=»http://forums.linuxmint.com/»
BUG_REPORT_URL=»http://bugs.launchpad.net/
linuxmint/»
VERSION_CODENAME=sylvia
UBUNTU_CODENAME=xenial
sololinux ~ #
```

Es evidente que como ultima opción no podía faltar hostname.

```
hostnamectl
```

Ejemplo de salida…

```
sololinux ~ # hostnamectl
Static hostname: Pruebas-web
Icon name: computer-desktop
Chassis: desktop
Machine ID: 0a2058fc54c649ada1c67c1b7f870152
Boot ID: 2d4c2377a259482da488a2af967975b6
Operating System: Linux Mint 18.3
Kernel: Linux 4.15.18-041518-generic
Architecture: x86-64
sololinux ~ #
```



HTML vs XML

HTML, son las siglas de HyperText Markup Language, que es el lenguaje más común para definir la estructura de una página web. Se compone de varios elementos HTML y a su vez de diversas etiquetas HTML con su contenido.

Es un lenguaje hipertexto, por lo tanto nos permite crear cadenas de enlaces. La versión más moderna de HTML es HTML5, pero ojo, debemos tener en cuenta que al ser estático puede ignorar pequeños errores en su programación. No es necesario cerrar las etiquetas para su funcionamiento.

Vemos un ejemplo sencillo de HTML:

```
<!DOCTYPE html>
<html lang="es">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<title>HTML de SoloLinux</title>
</head>
<body>
<h1 style="text-align: center;color:#db133a;">HTML</h1>
<h3 style="text-align: center;">Documento HTML de SoloLinux.</h3>
</body>
</html>
```

El anterior código lo vemos en pantalla como…

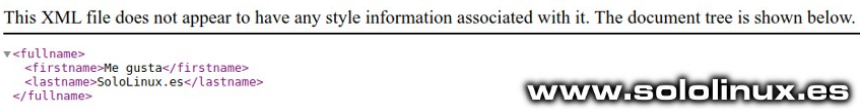
XML

XML quiere decir eXtensible Markup Language, y es un lenguaje creado para la función de transferir datos y no para estructurarlos. Es dinámico y nos informa de todos los errores, al contrario de HTML son necesarias las etiquetas de cierre. Realmente, es un formato de datos textuales con soporte de Unicode para idiomas humanos. La versión actual de XML es XML1.1.

Vemos un ejemplo sencillo de XML:

```
<?xml version="1.0" encoding="UTF-8"?>
<fullname>
<firstname>Me gusta</firstname>
<lastname>SoloLinux.es</lastname>
</fullname>
```

En pantalla lo vemos así…



Como podemos comprobar en la anterior imagen, los datos están sin estructurar. Al estructurarlos la cosa cambia, ejemplo…

Me gusta SoloLinux.es

Analizamos las diferencias entre uno y otro.

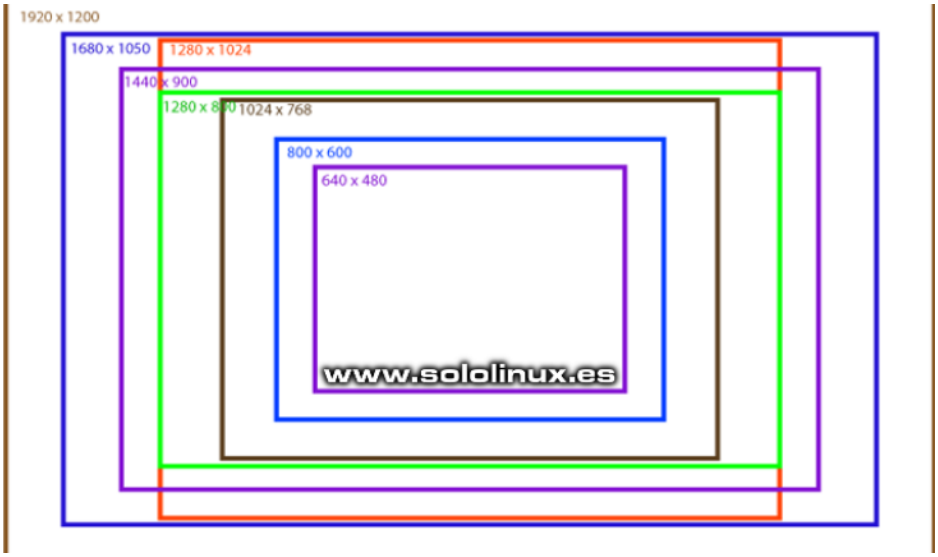
HTML vs XML

HTML	XML
HTML (HyperText Markup Language), es un lenguaje utilizado para describir la estructura de una página web. Se compone de varios elementos HTML que se componen de etiquetas HTML y su contenido.	XML (lenguaje de marcado extensible), es un lenguaje utilizado para transferir datos y no para estructurarlos.
HTML es estático porque se usa para mostrar datos.	XML es dinámico y se usa para transferir datos.
Es un lenguaje de presentación.	No es un lenguaje de presentación.
No es necesario usar una etiqueta de cierre.	Es obligatorio usar una etiqueta de cierre.
Las etiquetas predefinidas como , , , etc... están presentes en HTML.	Puedes definir tus propias etiquetas.
HTML no conserva los espacios en blanco.	XML imprime los espacios en blanco.
HTML no distingue entre mayúsculas y minúsculas.	XML si que distingue entre mayúsculas y minúsculas.

Cambiar la resolución del monitor desde la terminal

El uso de la **Terminal**, nos ayuda a que muchas tareas cotidianas se ejecuten de manera más eficiente, e incluso más rápidas. Todo tiene su explicación, ademas evidente, las herramientas en línea de comandos utilizan muchísimos menos recursos que si las ejecutamos de forma gráfica (**GUI**).

En este articulo aprenderás a modificar la resolución de tu monitor de forma sencilla y rápida (desde la terminal o consola).



Cambiar la resolución del monitor desde la terminal

En un articulo anterior ya hablamos de la herramienta **Xrandr** (complemento de **Xorg**), recordemos que es una interfaz en línea de comandos para la extensión **RandR**, que entre otras cosas nos permite configurar dinámicamente las salidas de la pantalla. Todo ello sin tener que modificar ninguna configuración específica de xorg.conf.

Esta utilidad está instalada por defecto en todas las **distribuciones linux** que usan «XORG», en nuestro ejemplo trabajamos sobre un sistema **Ubuntu 18.04**.

Vemos dos maneras de cambiar el tamaño de pantalla:

- **Relación de aspecto.**
- **Por resolución de pixels.**

Por aspecto:

```
xrandr --size [size-index]
```

Ejemplo…
xrandr –size 4:3

Por pixels:

```
xrandr --size [widthxheight]
```

Ejemplo…
xrandr –size 1280×1024

Como puedes comprobar es fácil modificar la resolución de tu monitor desde la terminal. Si quieres puedes verificar el tamaño actual en:

http://whatismyscreenresolution.net/

Bloquear ataques DDos con Fail2ban

Bloquear ataques DDos (**ataque de denegación de servicio**) a gran escala, no es tarea sencilla, por no decir imposible. Para lograrlo deberíamos contar con una tremenda estructura tanto a nivel de red como de hardware, que lograra redireccionar las peticiones malignas.

Estos ataques a gran escala no suelen dirigirse a pequeños sitos web, sus victimas son grandes empresas o corporaciones. Aun así, nadie esta libre de recibir un ataque **ddos** a menor escala, y claro… lo mejor es prevenir.

Fail2ban es una excelente herramienta contra intrusiones, y aunque no está especialmente diseñada para bloquear ataques ddos, si que nos puede ayudar. En este articulo vemos como configurar correctamente Fail2ban para tal efecto.

Bloquear ataques DDos con Fail2ban

Si recuerdas el articulo anterior, las **reglas de Fali2ban** se basan en **jails** (jaulas). Así que nos aseguramos que tenemos en **/etc/fail2ban/jail.local** el **jail ssh** bien configurado.

```
[ssh-ddos]
enabled  = true
port     = ssh
filter   = sshd-ddos
logpath  = /var/log/auth.log
maxretry = 3
```

Pero claro… normalmente un **ataque ddos** no se dirige a **ssh**, atacan a **http** (**apache**). Tenemos un problema, de manera predeterminada **Fail2ban** no viene con ninguna regla para proteger Apache. No te preocupes Fail2ban nos permite crear nuestro jail personalizado.

Copia y pega lo siguiente:

```
[http-get-dos]
enabled = true
port = http,https
filter = http-get-dos
logpath = /var/log/apache*/*access.log
maxretry = 300
findtime = 300
bantime = 600
action = iptables[name=HTTP, port=http, protocol=tcp]
```

Guarda el archivo y cierra el editor.

Ahora necesitamos establecer el nuevo filtro http-get-dos.

```
cd /etc/fail2ban/filter.d
```

Creamos el archivo filtro.

```
sudo nano http-get-dos.conf
```

Copia y pega lo siguiente:

```
# Fail2Ban configuration filter httpd
#
#
[Definition]
# Option: failregex
# Note: This regex will match any GET entry in your logs, so basically all valid and not valid entries are a match.
# You should set up in the jail.conf file, the maxretry and findtime carefully in order to avoid false positives.
failregex = ^<HOST> -.*"(GET|POST).*
# Option: ignoreregex
# Notes.: regex to ignore. If this regex matches, the line is ignored.
# Values: TEXT
#
ignoreregex =
```

Guarda el archivo y cierra el editor.

Necesitamos reiniciar fail2ban.

```
sudo service fail2ban restart
```

Como ultimo apunte puedes verificar que fail2ban esta trabajando de manera correcta.

```
cat /var/log/fail2ban.log
```

Ejemplo de salida correcta:

```
[root@host ~]# cat /var/log/fail2ban.log
2019-10-20 03:29:03,830 fail2ban.server [3623]: INFO rollover performed on /var/log/fail2ban.log
2019-10-20 03:31:35,249 fail2ban.filter [3623]: INFO [proftpd] Found 115.226.132.151 – 2019-10-20 03:31:35
2019-10-20 03:31:35,600 fail2ban.actions [3623]: NOTICE [proftpd] Ban 115.226.132.151
2019-10-20 03:33:50,927 fail2ban.filter [3623]: INFO [ssh] Found 106.12.109.188 – 2019-10-20 03:33:50
2019-10-20 03:33:53,636 fail2ban.filter [3623]: INFO [ssh] Found 106.12.109.188 – 2019-10-20 03:33:53
2019-10-20 03:33:54,329 fail2ban.actions [3623]: NOTICE [ssh] Ban 106.12.109.188
2019-10-20 03:33:54,340 fail2ban.filter [3623]: INFO [apache] Found 106.12.109.188 – 2019-10-20 03:33:54
```

Sudo vs Su

Al igual que en otros menesteres, en Linux, también disponemos de diferentes formas de realizar una misma tarea.

En este articulo hablamos de sudo y su, dado que son comandos que intercambiamos inconscientemente, pero cuyo objetivo real es totalmente diferente en uno y otro. Lo comprobamos.

Sudo vs Su

Comando su

El **comando su** nos permite cambiar de usuario durante una sesión o inicio de sesión. Si lo invocamos sin insertar ningún nombre de usuario, su valor predeterminado es convertirse en el superusuario (**root**) del sistema.

Como utilizar su.

Con nuestro nombre heredamos las variables de entorno:

```
su sergio
```

El argumento «–» se utiliza para iniciar sesión desde otro usuario con un nuevo entorno, sin heredar nada.

```
su - sergio
```

Ahora vemos la diferencia con el usuario root, con ejemplos.

```
su
```

Ejemplo de salida…

```
sergio@sololinux ~ $ su
Contraseña:
sololinux sergio #
```

Como puedes ver en el ejemplo anterior, hemos iniciado como superusuario en el entorno del usuario “sergio”. Ahora lo hacemos con un nuevo entorno aplicando el guion.

```
su -
```

Ejemplo de salida…

```
sergio@sololinux ~ $ su –
Contraseña:
sololinux ~ #
```

Comando sudo

A diferencia de «su», sudo concede acceso temporal, para que usuarios sin privilegios puedan realizar algunas tareas de administración sin tener que declarar la password del root.

Por ejemplo, si queremos instalar gimp siendo un usuario, ejecutamos lo siguiente (en Ubuntu):

```
sudo apt install gimp
```

En el ejemplo anterior nos solicita nuestra contraseña, y ejecuta la instalación, si tuviéramos permisos de superusuario bastaría con:

```
apt install gimp
```

Como puedes ver, ambos comando son capaces de lograr el mismo objetivo pero con formulas diferentes. Depende de ti, del escenario donde estés, y de los conocimientos que tengas el utilizar uno o otro. Si no estas completamente seguro de lo que haces, no conviene trabajar como root. Por otro lado, si eres un usuario experto es mucho más cómodo operar como superusuario, pero ojo, ten cuidado.

La cuenta root de Ubuntu y derivados está deshabilitada por defecto, si quieres habilitar el root en Ubuntu, revisa este anterior articulo.

Alternativas a Photoshop de código abierto

Adobe Photoshop es una aplicación propietaria disponible para **Windows y macOS**. Sin lugar a dudas, debo reconocer que es de lo mejor que puedes encontrar en edición y diseño de imágenes.

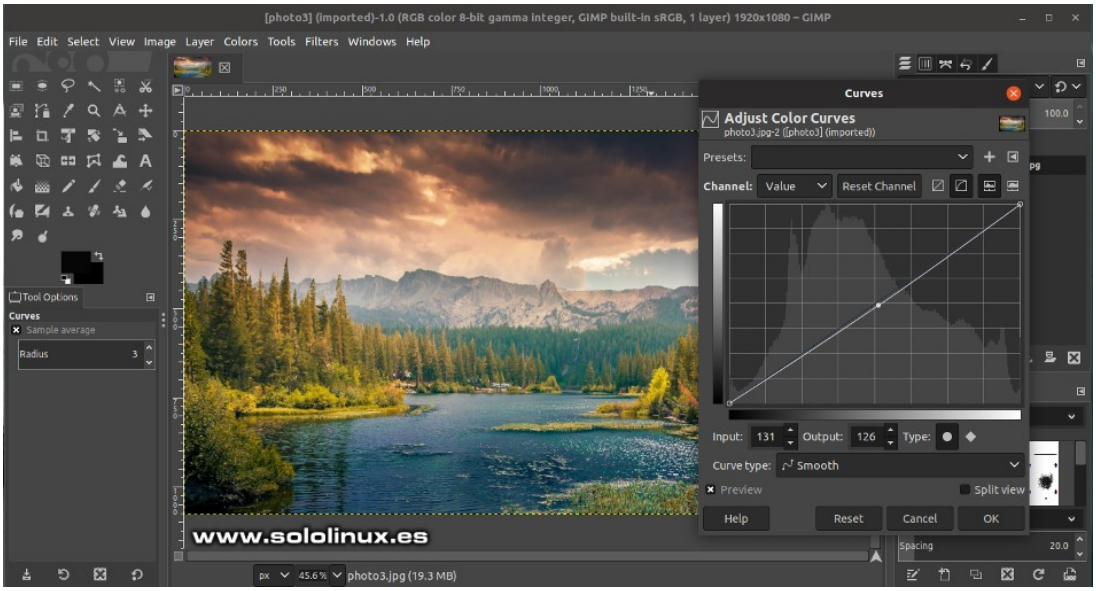
Photoshop no es solo un completo editor de fotografías e imágenes, es mucho más. Lo utilizan fotógrafos profesionales, artistas digitales, editores diversos, y expertos en otras materias relacionadas con el diseño.

Lamentablemente, en **linux** no tenemos muchas opciones disponibles como **alternativa a Photoshop**. Aun así, en este artículo, nombramos algunas de las mejores **alternativas a Photoshop** de código abierto (gratis) disponibles para nuestro sistema.

El software alternativo no tiene todas las características de **Photoshop**, pero puedes lograr el mismo objetivo combinando varias. Antes de comenzar el articulo, debes saber que **Wine** soporta Photoshop pero la experiencia de usuario es pésima, no te lo recomiendo.

Alternativas a Photoshop

Gimp



Sin importar cuán básica o avanzada sea la tarea, en **sololinux.es** siempre utilizamos **Gimp**. Esta herramienta es la que más se asemeja a un reemplazo real de **Photoshop en Linux**.

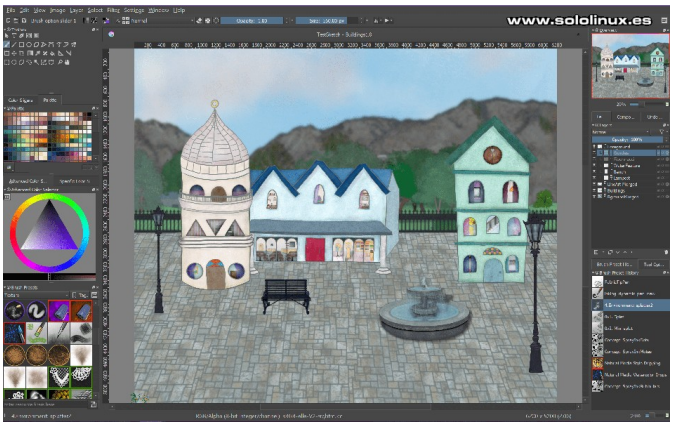
Tiene todas las características necesarias para la edición de imágenes, incluyendo el soporte de gestión de capas. Destacamos que es muy fácil de usar, ademas cuenta con un completo **manual oficial** y buenos **tutoriales**. Altamente recomendado.

Características principales:

- Interfaz personalizable.
- Retoque digital.
- Mejora de fotos.
- Gran soporte de hardware, incluyendo tabletas sensibles, MIDI, etc.
- Soporta la mayoría de formatos de imagen.
- Excelente gestión de capas.

Puedes visitar su pagina oficial aquí, pero suele venir preinstalado en la mayoría de distribuciones linux.

Krita



Estamos ante una espectacular herramienta **open source**, diseñada para crear dibujos digitales (pintura). Con su soporte de gestión de capas, y las herramientas de transformación que contiene, con **Krita** podrás diseñar y editar imágenes ya creadas.

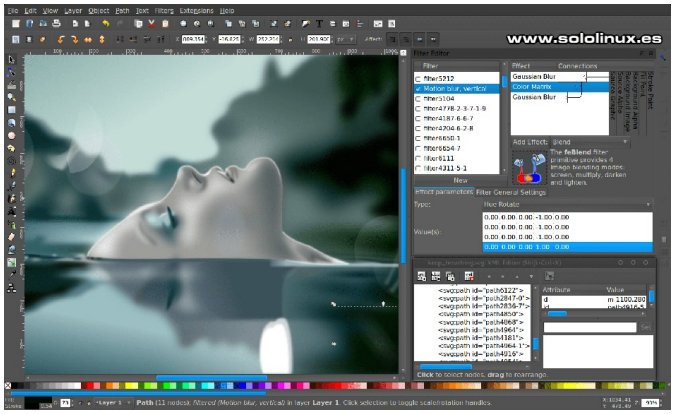
De todas maneras te indico que su fuerte no es la edición, sino la creación. Si lo tuyo es dibujar, Krita es tu aplicación.

Características principales:

- Soporte de gestión de capas.
- Herramientas de transformación.
- Gran variedad de pinceles y herramientas de dibujo.

Normalmente la encontraras en los repositorios de tu distribución linux, también puedes visitar su pagina oficial de descargas.

Inkscape



La aplicación **Inkscape**, es un editor de gráficos vectoriales de código abierto muy popular incluso entre los profesionales del sector. Ofrece herramientas de diseño flexibles que te ayudan a crear autenticas obras de arte. En realidad es una **alternativa a Illustrator**, lo incluimos en este articulo por sus funciones compatibles como **alternativa a Photoshop**.

Características principales:

- Herramientas para la creación de objetos.
- Soporte de gestión de capas.
- Herramientas para editar imágenes.
- Selector de color (RGB, HSL, CMYK, rueda de color, CMS).

Soporta los formatos de archivo más conocidos. Al igual que los recursos oficiales de GIMP, los **tutoriales de Inkscape** también son muy buenos. Normalmente la encontraras en los repositorios oficiales de tu distribución linux, como alternativa puedes visitar su pagina oficial de descargas.

Darktable

Existen otras aplicaciones, pero sin duda la mejor herramienta de procesado fotográfico en **formato raw** (negativo digital) open source, es **Darktable**.

Darktable permite gestionar los negativos digitales en una base de datos, verlos a través de una mesa de luz con zoom incluido, ademas de editar y mejorar las imágenes en bruto.

Características principales:

- Desarrollar las imágenes RAW.
- Muchos formatos de imagen admitidos.
- Viene con varios módulos para editar la imagen incluyendo operadores de mezcla.

Al igual que las aplicaciones mencionadas en este articulo, Darktable la encontraras en los repositorios oficiales de tu sistema linux. Si tienes alguna duda visita su pagina oficial donde explica como instalar Darktable.

En este articulo no hemos hablado de todas las herramientas disponibles, pero si de las más importantes. Si las juntas todas no tienes nada que envidiar a **Photoshop**, todo lo contrario.

MX Linux 19 – Novedades y descarga

Ya tenemos lista para su descarga la distribución linux MX Linux 19.

Es evidente que hablamos de la gran revolución del 2019, puedes leer aquí mi opinión al respecto. Como ya comentamos anteriormente es una gran distro, y hoy después de su lanzamiento oficial hablamos del mismo.

MX Linux 19 – Novedades

La instalación de **MX Linux** fue muy fácil, y en contra de la opinión de otros compañeros considero que cuenta con uno de los instaladores más sencillos y a la vez completos que puedes encontrar.

En el instalador destaca por encima de todo la adición o eliminación de servicios que no te interesan, por ejemplo: no tengo impresora y no quiero ningún servicio ligado a la impresión… Basta con desactivar ese servicio antes de que se instale y nos llene el sistema de dependencias inútiles (inútiles en nuestro caso). Este detalle me parece muy útil.

Tenemos disponibles multitud de opciones de configuración y personalización durante el proceso de instalación, insisto que este instalador me parece un gran acierto. Es verdad que a nivel visual no es una belleza, y que más da, yo quiero que funcione rápido y seguro, los muñecos y animaciones que bailan a ritmo de salsa, solo entorpecen un funcionamiento estable.

Las actualizaciones de MX-Linux 19 son brutales, vemos algunos ejemplos.

- XFCE – 4.14
- GIMP – 2.10.12
- MESA – 18.3.6
- Kernel – 4.19.5
- Firefox – 68
- VLC – 3.0.8
- Clementine – 1.3.1
- Thunderbird – 60.8.0
- LibreOffice – 6.1.5 (incluyendo actualizaciones de seguridad)
- etc…

MX Linux 19 – Descargas

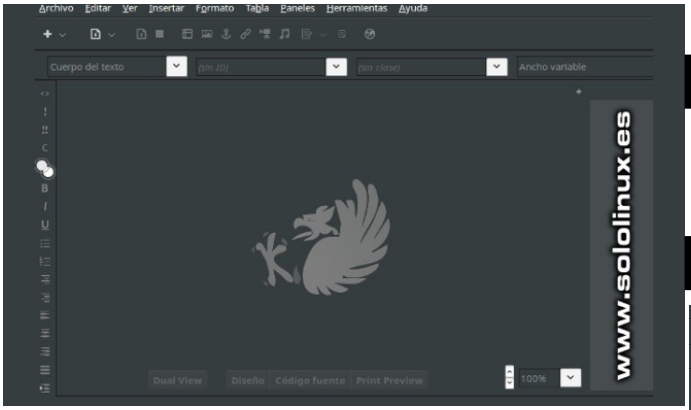
Aun así, sigo discutiendo con multitud de usuarios que piensan que es una distribución linux enfocada a hardware obsoleto. Me canso, la verdad es que me canso que repetir que los orígenes de **MX Linux** estaban orientados a maquinas con pocos recursos, pero eso ya no es así.

Señores… yo no necesito el pesado **gimp 2.10,** quiero el Gimp 2.8 que soluciona todos mis problemas. y MX no me permite migrar (es un ejemplo). A pesar de mis vanas reclamaciones estamos ante una distro linux de escándalo.

Puedes descargar MX desde:

- Forma directa.
- Por torrent.

Instalar BlueGriffon WYSIWYG Content Editor en Ubuntu



BlueGriffon es un editor **WYSIWYG** de páginas web gratuito. También esta disponible una versión de pago con algún componente adicional. Está basado en el motor de renderizado **Gecko** de **Firefox**.

Esta excelente aplicación, es utilizada por los desarrolladores de sitios web. Es una buena alternativa al famoso **Adobe Dreamweaver de Windows**.

BlueGriffon tiene sus orígenes en Daniel Glazman, que desarrollo **NVU** con múltiples lenguajes de programación, como Java, C ++, C y GPL 2.0. Es una herramienta ligera y portable, ademas esta disponible para Linux, Microsoft Windows, y MacOS.

Destaca por ser compatible con diferentes formatos web como HTML 4, HTML 5, XHTML 1.0, XHTML 1.1, y con la mayoría de lenguajes de programación. Te aseguro que si la pruebas no la abandonaras jamas, es un gran producto, y una tremenda ayuda independientemente de tus conocimientos como desarrollador web.

Lamentablemente las ultimas versiones no disponen de paquetes rpm, solo deb. De todas formas, al final del articulo pondré unos enlaces con paquetes rpm que algunas distribuciones compilaron por su cuenta. Nosotros vamos a **instalar Bluegriffon en Ubuntu 18.04 y Ubuntu 16.04 (incluyendo sus derivados)**.

Instalar BlueGriffon en Ubuntu

En Ubuntu 18.04 y derivados.

Actualizamos el sistema.

```
sudo apt update
```

Descarga la ultima versión de BlueGriffon estable.

```
wget http://bluegriffon.org/freshmeat/3.1/bluegriffon-3.1.Ubuntu18.04-x86_64.deb
```

Instalamos BlueGriffon con dpkg,

```
sudo dpkg -i bluegriffon-3.1.Ubuntu18.04-x86_64.deb
```

Al concluir la instalación, puedes iniciar Bluegriffon desde el icono del menú de aplicaciones, o desde la terminal de tu linux.

```
bluegriffon
```

En Ubuntu 16.04 y derivados.

La ultima versión de **BlueGriffon** no es compatible con Ubuntu 16.04 o derivados. Si lo intentas recibirás un error similar a:

XPCOMGlueLoad error for file /opt/bluegriffon/liblgpllibs.so: /lib/x86_64-linux-gnu/libm.so.6: version `GLIBC_2.27' not found (required by /opt/bluegriffon/liblgpllibs.so)

Lamentablemente por un tema de librerías (supongo que GTK), no es posible instalar la ultima versión estable, Bluegriffon 3.1. Instalamos la anterior, Bluegriffon 3.0.1, que al igual que la ultima tambien funciona estupendamente.

Actualizamos el sistema.

```
sudo apt update
```

Descargamos Bluegriffon 3.0.1.

```
wget http://bluegriffon.org/freshmeat/3.0.1/bluegriffon-3.0.1.Ubuntu16.04-x86_64.deb
```

Instalamos BlueGriffon.

```
sudo dpkg -i bluegriffon-3.0.1.Ubuntu16.04-x86_64.deb
```

Al concluir la instalación, puedes iniciar Bluegriffon desde el icono del menú de aplicaciones, o desde la terminal de tu linux.

```
bluegriffon
```

Paquetes BlueGriffon rpm
No existen muchas distribuciones rpm que hayan compilado BlueGriffon, pero por ejemplo la de Mageia 7 no debería dar ningún problema en otras distribuciones linux. Puedes descargar el paquete desde aquí.

Como alternativa puedes descargar la aplicación en código fuente y compilarla tu mismo. Ademas por si te interesa otra versión… están todas.

- Descargar BlueGriffon

Como proteger la privacidad de tu Smartphone

En la actualidad, prácticamente todo el mundo es propietario de un Smartphone con el que acceden de forma constante a Internet. Si bien la tecnología brinda muchas ventajas y ofrece un mundo de posibilidades, también presenta ciertos riesgos, que a menudo nos pasan desapercibidos. Existen miles de fuentes maliciosas que pueden acceder a los dispositivos móviles y robar información; si no estás preparado, te conviertes en su victima al instante.

Quienes buscan robar información
La información es valiosa. Cualquier tipo de datos se considera útil en el mundo digital. Cada usuario en su Smartphone tiene una gran cantidad de información importante, que a su vez, puede resultar atractiva para los amigos de lo ajeno. En primer lugar nos encontramos con los hackers, que son aquellas personas que tienen las capacidades y conocimientos suficientes como para ingresar en dispositivos ajenos y sustraer información sensible. También tenemos sitios web malignos, que con técnicas de engaño pueden obtener los datos de los usuarios. Incluso debes tener cuidado de amigos y familiares. Muchas veces son los conocidos más cercanos quienes buscan espiar un smartphone ajeno, sobretodo para acceder a las conversaciones de whatsapp, hackear Instagram o las redes sociales.

Proteger la privacidad de tu Smartphone
Técnicas para proteger el celular (smartphone)
Existen ciertas prácticas y consejos que puede seguir cualquier persona para proteger al máximo posible su smartphone (celular), y así frenar a posibles intrusos. Algunas de ellas son:

- Usar antivirus: Es clave el uso de un antivirus, que se encargará del cuidado del dispositivo. Constantemente estará en funcionamiento, analizando y buscando cualquier tipo de actividad sospechosa o archivos maliciosos.
- Descargar aplicaciones de las tiendas oficiales: Las tiendas oficiales (Google Play en Android y Apple Store en iOS) son la única fuente fiable para descargar aplicaciones. Tienen sus propios controles de seguridad, que nos garantiza que las aplicaciones que se ofrecen son seguras y están limpias.
- Vigilar los permisos que se otorgan: Para su correcto funcionamiento, las aplicaciones necesitan ciertos permisos por parte del usuario. Sin embargo, en algunas ocasiones se piden permisos de mas, que no son necesarios para nada. Es importante prestar atención y observar qué permisos se están otorgando y cuales hay que rechazar.
- Usar el bloqueo de pantalla: Los celulares actuales ofrecen distintas herramientas para el bloqueo de pantalla, y hay que usar al menos uno. Entre ellos se puede optar por un PIN, un patrón de desbloqueo, una contraseña o incluso la huella digital del dedo. De esta forma, se evita que cualquier persona pueda ingresar libremente al dispositivo, ya sea por robo, o simplemente por curiosidad de alguna persona allegada.

Situaciones que se deben evitar
Además de tomar medidas para proteger la privacidad, también hay ciertas situaciones o actividades que pueden resultar peligrosas y que conviene evitar por los posibles riesgos.

Es importante no utilizar siempre la misma contraseña (password). Si lo haces corres un gran riesgo, ya que si un hacker o usuario malintencionado obtiene una sola contraseña, tendrá acceso total a tus dispositivos, por lo tanto tu privacidad queda en entredicho. Por otra parte, hay que evitar sitios web sospechosos o de baja calidad. Muchas veces, existen únicamente con el objetivo de sustraer información de los usuarios. Por último, no prestar el celular (o smartphone) a personas desconocidas, e incluso en ocasiones, tampoco a conocidos o familiares. Siempre existe la posibilidad de que intenten instalar una aplicación espía y así tener acceso a toda nuestra información personal.

Los mejores enrutadores WIFI

En este artículo, vamos a ver algunos de los mejores enrutadores WiFi disponibles hoy en día. En los tiempos modernos que corren, cada vez tenemos más complementos electrónicos a nuestro alrededor, y como es evidente si algo no puede faltar es un enrutador wifi (tambien llamado router).

Si hablamos de componentes informáticos domésticos, el enrutador se ha convertido en uno de los más importantes, ya que nos permite conectar casi cualquier dispositivo electrónico que tengamos a la Web. Hablamos de un dispositivo indispensable, y que por velocidad y seguridad debe ser de calidad. Por desgracia, los aparatos que regalan, o comercializan a bajo coste las compañías que nos proveen internet son una autentica castaña, más malos imposible.

Por ese motivo, los expertos recomiendan adquirir un hardware de calidad, y eso es lo que vemos en este articulo, algunos de los mejores enrutadores que puedes encontrar en cualquier comercio que se precie.

Los mejores enrutadores WIFI

Asus RT-AC68U Dual-band Wireless-AC1900 Gigabit Router

El **Asus RT-AC68U** es uno de los enrutadores más potentes disponibles en la actualidad, ya que está repleto de características que los usuarios domésticos y las empresas encontrarán útiles. El Asus RT-AC68U emplea la última tecnología, por lo que ofrece una conexión Wi-Fi rápida junto a los últimos estándares de Wi-Fi. No solo está diseñado para un uso regular, sino también para un rendimiento de alta gama. Está creado para usuarios exigentes, si buscas un **enrutador** Wi-Fi de alta calidad, no lo dudes.

Cuanta con un potente **procesador** de doble núcleo a 800MHz, y es compatible con el chip Wi-Fi que puede alcanzar velocidades de 1.3Gbps (en frecuencia de 5Ghz). En la banda de 2.4GHz, admite hasta 600Mbps que tampoco esta nada mal. No es el dispositivo más económico (alrededor de 125€), pero si es una excelente opción.

Pagina oficial del Asus RT AC68U

Linksys EA4500 Media Stream N900

El EA4500 es conocido por su excelente rendimiento, similar a los routers de alta gama. La solución Cisco Connect Cloud, integrada en el enrutador, es una característica que lo distinque del resto. Si lo que quieres es un enrutador fácil de administrar, este es muy bueno. Debemos indicar que ya lleva unos años en el mercado y no es fácil encontrarlo, pero sigue siendo muy bueno.

El EA4500 es similar al Linksys E4200 v2, incluso tiene el mismo diseño elegante. Su rendimiento está a la altura de los mejores con soporte para 450Mbps en las bandas de 2.4GHz y 5GHz. También monta un procesador que trabaja rápido en redes y se permite utilizar con un disco duro USB. Destacamos que admite hasta cincuenta clientes, algo fuera de lo común en en esta gama de enrutadores. En cuanto al diseño, puede parecerse a cualquier otro enrutador, pero es muy potente y puede hacer mucho.

Pagina oficial de Linksys EA4500

Asus RT-AC66U 802.11ac

Llega el turno del Asus RT-AC66U, que funciona de manera increíble bien en la banda de 5Ghz, y por sus características está destinado a negocios y hogares. Este enrutador está recomendado si buscas uno que sea compatible con el estándar Wi-Fi 802.11ac.

Actualmente es uno de los enrutadores más rápidos con soporte 802.11ac que podemos encontrar. Sus puertos USB soportan todo tipo de impresoras, y dispositivos de almacenamiento externo. Destacamos el servicio AiCloud, útil para almacenar y administrar archivos. Las características generales están a la altura de los mejores.

Pagina oficial del Asus RT-AC66U

D-Link DIR-868L Wireless AC1750 Dual Band Gigabit Cloud

El D-Link DIR-868L tiene un diseño que llama la atención, pero sin olvidar de sus muchas características excelentes. Como es habitual en el fabricante, su administración es sencilla pero a la vez poderosa.

Es compatible con los estándares 802.11ac y 802.1n, por lo que no tendremos ningún problema. Soporta velocidades de hasta 450Mbps. No es el más rápido de este articulo, pero si de los más confiables.

Pagina oficial del D-Link DIR-868L

Asus RT-N66U Dark Knight Double 450Mbps

El conjunto de características del Asus RT-N66U Dark Knight es uno de los mejores de los más potentes de su gama. Destacamos que puede funcionar como servidor VPN, y el gran alcance de su red WIFI. Una buena opción para una pequeña oficina o vivienda.

Tiene muchas características, pero si hablamos de facilidad de uso, te aseguro que puede ser manejado por casi cualquier persona. La configuración, en particular, es muy fácil e intuitiva.

Pagina oficial del Asus RT-N66U Dark Knight

D-Link DIR-857 HD Media Router 3000

Como punto y final, no nos podíamos olvidar del enrutador D-Link DIR-857 HD Media Router 3000, un router de alta gama que ofrece una buena velocidad en el rango de 5Ghz. Sus características también son de máxima categoría, e incluso trae de manera predeterminada algunas características impresionantes, como VoIP y QoS para juegos y transmisión de medios.

Hay muchos enrutadores disponibles en el mercado, pero este se distingue porque sus aplicaciones añadidas son realmente útiles para cualquier usuario, no solo para expertos o profesionales.

Pagina oficial del D-Link DIR-857 HD Media Router 3000

Estos son los mejores enrutadores WiFi disponibles en la actualidad, sé que no están todos, pero si los más destacados. Soy consciente que algunos diréis que faltan otras marcas, siii, ya lo se, otras marcas alternativas como por ejemplo TP-Link, o MikroTic pueden ofrecer un rendimiento similar a los tratados en el articulo, lo se, pero el problema de las marcas alternativas son los materiales usados en su fabricación, por ejemplo de las carcasas. Otras alternativas son buenas por dentro, los del articulo son buenos por dentro y por fuera.

Jugar al solitario en Ubuntu terminal

Todos hemos jugado alguna vez al solitario, todos. Estamos aburridos, esperamos que termine una tarea u otra, vamos a **jugar al solitario**, jaja.

En este articulo veremos como instalar el solitario desarrollado por **mpereira**, para la terminal linux. Lo único que necesitamos son las dependencias de **Ncurses**.

Jugar al solitario en Ubuntu terminal
Instalamos las dependencias necesarias en Ubuntu o derivados.

```
sudo apt-get install libncurses5-dev libncursesw5-dev
```

Ahora descargamos el juego tty-solitaire.

```
wget -O tty-solitaire-v1.1.0.tar.gz https://github.com/mpereira/tty-solitaire/archive/v1.1.0.tar.gz
```

Lo descomprimimos.

```
tar xvf tty-solitaire-v1.1.0.tar.gz
```

Accedamos al directorio del juego.

```
cd tty-solitaire-1.1.0
```

Compilamos con make.

```
make
```

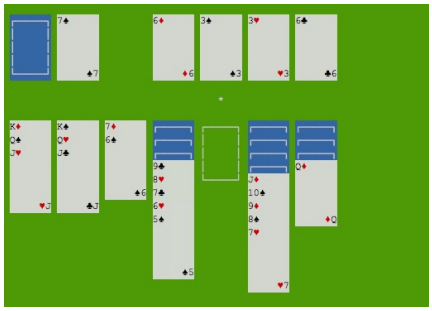
Solo nos falta instalar la aplicación.

```
sudo make install
```

Para lanzar el juego del solitario, ejecuta el siguiente comando:

```
ttysolitaire
```

Ya puedes comenzar tu partida, observa el ejemplo…



Su uso es bastante sencillo, puedes operar de forma habitual como si fuera en tu entorno de escritorio.

```
usage: ttysolitaire [-v|--version] [-h|--help] [-p|--passes=NUMBER]
-v, --version  Show version
-h, --help     Show this message
-p, --passes   Number of passes through the deck
```

Qué es y cómo funciona Tor

Si quieres proteger tu privacidad en línea, debes conocer Tor. En este artículo, hablaremos sobre qué es Tor, quién lo usa, y el porqué. A partir de ahí, veremos exactamente cómo funciona Tor, cómo nos ofrece anonimato y las limitaciones del servicio.

Qué es Tor
Tor se comenzó a desarrollar en la década de los 90, cuando los investigadores del US Naval Research Laboratory crearon el «enrutamiento cebolla«. Esta formula de enrutar hace posible transferir mensajes a través de una red de manera anónima. El truco es que utiliza múltiples capas de cifrado, que se despegan una por una (como si peláramos una cebolla) a medida que el mensaje pasa a través de los múltiples nodos de la red.

En 2004, se lanzó la segunda generación de Tor . En 2006, los desarrolladores que trabajaban en Tor fundaron el Proyecto Tor y aceptaron el compromiso de mantener Tor.

Tor, se basa en una red de miles de computadoras en todo el mundo que implementa el enrutamiento cebolla. En su origen fue diseñado para proteger las comunicaciones online de la Agencia de Inteligencia de EE. UU., hoy en día presta servicio a millones de usuarios, militares, gubernamentales y civiles, independientemente del país donde se encuentren.

Quién usa Tor
Todo el mundo que quiera o necesite proteger su privacidad en internet. Algunos ejemplos:

- Ciudadanos y periodistas de países con graves deficiencias democráticas que necesitan lanzar información al resto del mundo.
- Servicios de noticias, como el New York Times y The Guardian que usan el programa Secure Drop.
- La policía lo usa para casi todo, desde líneas de información anónimas, hasta seguimientos de sitios web y operaciones encubiertas.
- Activistas de derechos humanos, desde personas, hasta organizaciones.
- Empresas que necesitan comunicaciones privadas.
- Agencias gubernamentales y militares que necesitan comunicaciones seguras.
- Cualquier persona que quiera o necesite que sus actividades online sean privadas.

El proyecto Tor ofrece un sitio donde podrás ver estadísticas de su uso por apartados.
- Estadísticas de Tor

Como protege Tor nuestra privacidad
El equipo de Tor lanzo un vídeo (subtitulado en español), donde lo explica de manera amena y hasta divertida.

https://youtu.be/JWII85UlzKw

Es legal utilizar Tor?
Lo usan gobiernos y agencias de todo el mundo, por tanto puedes utilizarlo sin consecuencias en cualquier país del mundo.

Pero ojo!!!, puedes usar Tor de manera segura y legal, pero el simple hecho de que lo estés utilizando puede atraer la atención de algunas agencias de seguridad. Si un servicio detecta que te estas anonimizando puede pensar que algo tienes que ocultar, tal vez sea peor el remedio que la enfermedad.

Cómo funciona Tor
Los conceptos básicos de cómo funciona Tor es algo sencillo, entenderlo en profundidad no tanto.

Cuando visitas un sitio web (sin usar Tor), tu maquina se conecta directamente al servidor donde se aloja el sitio web. El problema es que el sitio puede ver todo tipo de información sobre ti, tu dirección IP, el sistema operativo instalado, el navegador web que estás utilizando y más. Con esta información es posible rastrear lo que haces online, incluso llegar a identificarte.

Cuando usas Tor para visitar una web, las cosas cambian. La conexión entre tu maquina y el servidor del sitio web pasa a través de tres servidores aleatorios de la red Tor. Cada servidor por el que pasas solo conoce de donde vienes y adonde vas, por tanto ningún servidor de la red conoce la ruta completa.

Como resultado, no hay forma de identificarlo en función de la conexión entre tu PC y el sitio web. Así se logra que tu conexión sea anónima.

Ten en cuenta que al visitar un sitio web sin usar Tor, tu maquina establece una conexión directa con el servidor, no lo olvides.

Más allá de lo dicho, el navegador web comparte automáticamente todo tipo de información con el sitio que visitas. Esto incluye datos como quién es tu proveedor de Internet, qué sistema operativo utilizas, el modo de visualización de vídeo, incluso el nivel de la batería si haces uno de un dispositivo portátil. Para evitar esto puedes utilizar el navegador Tor.

Tor Browser
El navegador Tor se conecta a un punto de entrada aleatorio (Guard Relay) de la red Tor, y negocia una conexión encriptada con Guard Relay. Los datos enviados de esta conexión se cifran con claves para que solo nuestro navegador y Guard Relay puedan descifrarlos.

Después se negocia otra conexión, esta vez desde Guard Relay a otro servidor de la red Tor, a la que llamamos Middle Relay. Para esta conexión, crea otro conjunto de claves que son utilizadas por Guard Relay y Middle Relay.

Por ultimo, el navegador negocia una tercera conexión. Entre el relé medio y un relé de salida. Se generan unas claves que se utilizarán para cifrar y descifrar los datos que pasan a lo largo de la conexión entre el relé medio y el relé de salida.

Los datos que pasan de nuestro navegador a Internet se cifran tres veces.

- Primero: se cifra utilizando las claves para la conexión entre el Relé de salida y el Relé medio.
- Segundo: se cifra con las claves para la conexión entre el relé medio y el relé de guardia.
- Tercero: se encripta con las claves para la conexión entre Guard Relay y el navegador.

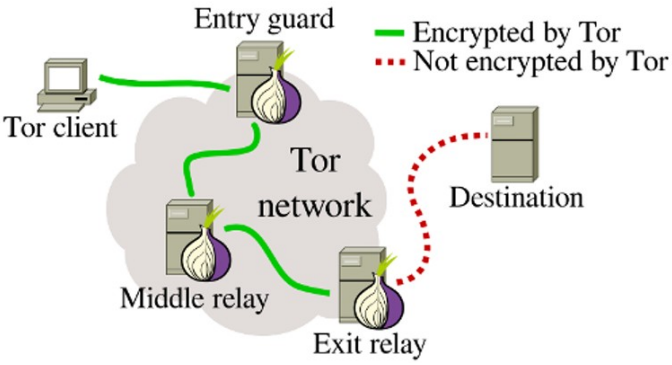
Cómo descodifica los datos
El navegador envía los datos codificados por triplicado al Guard Relay. Este elimina la capa más externa de encriptación. Dos capas de cifrado aún protegen los datos. El resultado es que Guard Relay solo conoce de dónde vienen los datos y a qué Middle Relay debe enviarlos.

El relé de guardia envía los datos doblemente codificados al relé medio. Middle Relay elimina la siguiente capa de cifrado. Una capa de cifrado aún protege los datos. El resultado es que Guard Relay solo conoce de dónde vienen los datos y a qué Middle Relay debe enviarlos.

La retransmisión media envía de nuevo los datos codificados individualmente a la salida. El relé de salida elimina la ultima capa de cifrado. Los datos ahora desprotegidos. El relé de salida puede ver los datos originales, pero desconoce que estos datos se originaron en nuestro navegador. Lo único que sabe es de donde vienen y a que sitio web debe enviarlos.

El sitio web recibe los datos del relé de salida. El sitio web piensa que los datos se originaron en el relé. No tiene forma de saber que los datos se originaron en tu navegador.

Ningún nodo conoce la ruta completa, el trafico de datos es anónimo.



En este articulo hemos tratado de explicar Tor y sus entresijos, de la manera más simple que nos ha sido posible, cualquier duda que tengas escribe un comentario.

Tor vs VPN

Tor es una red de anonimato. que proporciona herramientas diseñadas para que puedas acceder a Internet de forma anónima. En una VPN, el proveedor siempre conoce tu dirección IP real y puede ver el tráfico de Internet desde su punto de salida.

Como explicamos en un articulo anterior, Tor, se enruta a través de varios nodos, cada uno de los cuales solo conoce las direcciones IP de origen y destino, de modo que nadie puede conocer la ruta completa del sitio web al que intentamos conectar. Por tanto la diferencia es clara y evidente, de todas maneras se permite el uso de una VPN con Tor, eso debe quedar claro.

Si lo pensamos fríamente, el propósito de Tor y el de un VPN, es el mismo, pero las diferencias son abismales. En este articulo las analizamos, Tor vs VPN.

Tor vs VPN

Como estamos hablando, el propósito de Tor es muy similar al de una VPN: mantener el anonimato de los usuarios en linea, y evitar los firewalls o cualquier otra traba en la conexión de destino.

De la misma manera que Tor, VPN, también puede ser utilizado para falsificar tu ubicación geográfica, sin embargo, la tecnología y modo de uso es muy diferente. Vemos las ventajas y desventajas de cada uno.

VPN

Ventajas de VPN

- Rápido: En general su uso es mucho más rápido que Tor.
- Modificar la ubicación real: La mayoría de los proveedores de VPN ofrecen servidores en varias ubicaciones en todo el mundo, por lo tanto es una tarea sencilla. Como la conexión es relativamente rápida es ideal para transmitir contenido multimedia geo-restringido.
- Compartir archivos P2P: Algunos proveedores lo prohíben, pero como norma general cualquier VPN que se precie ya está configurado para ello.

Desventajas de VPN

- Privacidad: El proveedor de VPN puede ver tu actividad en Internet, y en muchos países la ley exige que mantenga registros de la misma, y que deba entregarse a las autoridades bajo petición judicial. Las VPN son vulnerables a los análisis de servidores por parte de la policía. Es vital elegir un proveedor que no guarde registros, y cerciorarte de ello.
- Coste: Si quieres un VPN de verdad, tiene un coste, es económico, si, pero lo tiene.

Tor

Ventajas de Tor

- Rastreo: Muy difícil de rastrear.
- Red distribuida: Casi imposible de cerrar o atacar de forma importante.

Desventajas de Tor

- Muy lento: A causa de que sus datos son aleatorios, pasan por varios nodos circulando por todo el mundo. Esto entorpece una buena experiencia de usuario a la hora de navegar por internet, mejor utilizarlo en sitios puntuales.
- Compartir archivos P2P: El uso de BitTorrent sobre Tor es extremadamente lento, ademas ralentizas la red al resto de usuarios de Tor. No lo hagas por favor.
- Geolocalización: Si este es tu único propósito, no te recomiendo Tor, es lento, lento, hasta la desesperación. Para suplantaciones geográficas mejor un VPN.

Espero haber aclarado las dudas de muchos usuarios sobre Tor vs VPN. Cada herramienta es para lo que es, y aunque podríamos considerar ciertas similitudes en un mismo fin, no es correcto su uso.

Bug en PHP7 con NGINX y PHP-FPM

Descubierto un **nuevo bug en PHP7** que permite tomar el control de un servidor mediante código remoto. El exploit publicado convierte esta hazaña en algo trivial, por lo que es muy posible que esté siendo aprovechada por atacantes «in the wild».

La vulnerabilidad (**CVE-2019-11043**) es una ejecución de código remoto en PHP7, la nueva versión estable de PHP, y uno de los lenguajes de programación más extendidos en sitios web.

La vulnerabilidad **afecta a sitios que funcionan con el servidor web NGINX y PHP-FPM, centrándose en una configuración en concreto**, la cual es muy común encontrar en webs en producción. Se trata de algo muy sencillo de explotar con este exploit, los investigadores que localizaron la vulnerabilidad lo han publicado.

PHP-FPM es una alternativa a PHP FastCGI, capaz de gestionar mucho mejor sitios web de alto trafico, además ofrece un manejo avanzado de los procesos.

La vulnerabilidad principal es un error de *underflow memory corruption en «env_paht_info»* en el módulo PHP-FMP, que combinándose con otros errores permiten ejecutar código en servidores vulnerables de manera remota.

Andrew Danau descubrió la vulnerabilidad en una competición CTF (Capture The Flag), cuyo objetivo era resolver una serie de retos informáticos. El fallo se encontró a partir de un comportamiento extraño por parte del servidor al introducir un salto de línea codificado en la URL '%0A'. Al ver la extraña forma de proceder, Andrew, junto a otros dos investigadores, Emil Lerner y Omar Ganiev, descubrieron el fallo y crearon el exploit, cuya ejecución se realiza con una simple línea de comando.

Bug en PHP7 con NGINX y PHP-FPM

Un sitio web es vulnerable a la explotación si cumple las siguientes características:

- Utiliza NGINX y está configurado para reenviar las peticiones al procesador PHP-FPM.
- Está configurado 'fast_split_path_info' con una expresión regular que comience con '^' y termine con '$' (no contempla un salto de línea).
- La variable PATH_INFO esta definida con fastcgi_param.
- No hay comprobaciones como try_files $ uri = 404 o if (-f $ uri) que determinen si un archivo existe o no.

La configuración que se describe puede parecerse a la siguiente:

```
location ~ [^/]\.php(/|$) {
  ...
  fastcgi_split_path_info ^(.+?\.php)(/.*)$;
  fastcgi_param PATH_INFO       $fastcgi_path_info;
  fastcgi_pass   php:9000;
  ...
}
```

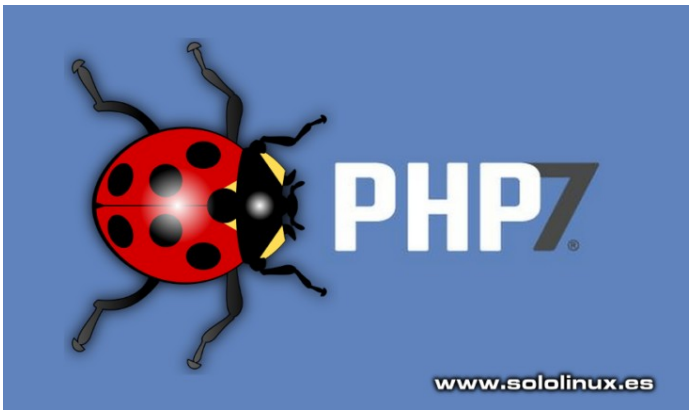
Se trata de una situación frecuente. Incluso algunos hosting utilizan esta configuración como parte de sus tutoriales sobre PHP-FPM. Muchos proveedores de hosting están avisando a sus clientes para que revisen sus servidores, y tomen las medidas necesarias.

Aquí tienes la solución.

Ya existe un parche para esta vulnerabilidad, pero han tardado casi un mes después de ser informados (al equipo de desarrolladores de PHP), y dado que el exploit ya está disponible, es probable que muchos atacantes estén escaneando Internet para encontrar sitios web vulnerables.

Este fallo ha sido catalogado como CVE-2019-11043, y se recomienda encarecidamente que los usuarios actualicen PHP a PHP 7.3.11 y PHP 7.2.24.

Visto en unaaldia.hispasec.com



Script bash: Backup remoto por FTP

Hoy vemos un sencillo script que nos ayudara a realizar un **backup remoto** por **FTP** de manera simple. Lo puedes usar en cualquier **servidor Linux** que necesite copias de seguridad, ya sea de los archivos, las carpetas del sistema, y de todas sus bases de datos MySQL o MariaDB.

El script utiliza **NcFTP** como cliente de **FTP**, debemos tenerlo instalado. Algunas de sus características más importantes: elimina las copias de seguridad anteriores los días que definamos, también envía un correo electrónico al **sysadmin** indicándole si el proceso fue un éxito, o si por el contrario se produjo algún error.

Backup remoto por FTP
Antes de comenzar, revisa atentamente las indicaciones:
Guarda el script en /bin/ftpbackup.sh y lo haces ejecutable.

```
chmod +x /bin/ftpbackup.sh
```

Recuerda que necesitas tener NCFTP instalado, por ejemplo:

```
sudo apt-get install ncftp
```

Por defecto el lunes se hace la copia de seguridad completa, puedes modificar estos valores en el script (de lo contrario se realizan copias de seguridad incrementales).
Por defecto se borran los backups con más de 30 días, puedes modificar la configuración según tus necesidades.
Creamos el Script bash.

```
nano /bin/ftpbackup.sh
```

Copia y pega el **código de la derecha**, pero OJO!!!, inserta tus datos reales, tal vez incluso debas modificar las rutas.

Guardas el archivo, y cierras el editor.

Lo puedes ejecutar con:

```
./ftpbackup.sh
o
bash ftpbackup.sh
```


```
#!/bin/bash
# File System Backups via FTP with MySQL Databases
##
# Guardar en /bin/ftpbackup.sh y hacer ejecutable
# chmod +x /bin/ftpbackup.sh

## Your System Settings ##

DIRS="/bin /etc /home /var/local /usr/local/bin /usr/lib /var/www"
BACKUP=/tmp/backup.$$
NOW=$(date +"%Y-%m-%d")
INCFILE="/root/tar-inc-backup.dat"
DAY=$(date +"%a")
FULLBACKUP="Mon"

## Your MySQL Settings ##

MUSER="root"
MPASS="tupassword"
MHOST="localhost"
MYSQL="$(which mysql)"
MYSQLDUMP="$(which mysqldump)"
GZIP="$(which gzip)"

## Your FTP server Settings ##

FTPD="//backup-directory-on-ftp-server"
FTPU="ftp-usuario"
FTPP="ftp-password"
FTPS="ftp.server.address"
NCFTP="$(which ncftpput)"

## Your Email Address ##

EMAILID="tuemail@tudominio.com"

## Backup our DPKG Software List ##

dpkg --get-selections > /etc/installed-software-dpkg.log

## Start the Backup for the file system ##

[ ! -d $BACKUP ] && mkdir -p $BACKUP || :

## Check if we want to make a full or incremental backup ##

if [ "$DAY" == "$FULLBACKUP" ]; then
  FTPD="//full-backups"
  FILE="MyServer-fs-full-$NOW.tar.gz"
  tar -zcvf $BACKUP/$FILE $DIRS
else
  i=$(date +"%Hh%Mm%Ss")
  FILE="MyServer-fs-incremental-$NOW-$i.tar.gz"
  tar -g $INCFILE -zcvf $BACKUP/$FILE $DIRS
fi

## Start the MySQL Database Backups ##
## Get all the MySQL databases names ##

DBS="$($MYSQL -u $MUSER -h $MHOST -p$MPASS -Bse 'show databases')"
for db in $DBS
do
 FILE=$BACKUP/mysql-$db.gz
 $MYSQLDUMP --single-transaction -u $MUSER -h $MHOST -p$MPASS $db | $GZIP -9
> $FILE
done


## Check the Date for Old Files on FTP to Delete ##

REMDATE=$(date --date="30 days ago" +%Y-%m-%d)

## Start the FTP backup using ncftp ##

ncftp -u"$FTPU" -p"$FTPP" $FTPS<<EOF
cd $FTPD
cd $REMDATE
rm -rf *.*
cd ..
rmdir $REMDATE
mkdir $FTPD
mkdir $FTPD/$NOW
cd $FTPD/$NOW
lcd $BACKUP
mput *
quit
EOF


## Find out if ftp backup failed or not ##

if [ "$?" == "0" ]; then
 rm -f $BACKUP/*
 mail  -s "MYSERVER - BACKUP SUCCESSFUL" "$EMAILID"
else
 T=/tmp/backup.fail
 echo "Date: $(date)">$T
 echo "Hostname: $(hostname)" >>$T
 echo "Backup failed" >>$T
 mail  -s "MYSERVER - BACKUP FAILED" "$EMAILID" <$T
 rm -f $T
fi
```

Script bash: Instalar y configurar Samba

Hoy en día, es común trabajar en una red donde se alternan máquinas con sistemas **Windows** y **Linux**, y como es lógico quieres intercambiar archivos entre las mismas.

Con la herramienta **Samba** es una tarea bastante sencilla. De esta aplicación destacamos que es **open source**, y nos permite acceder a los recursos compartidos, incluyendo archivos, carpetas, impresoras, etc.

Ya tratamos el tema de como instalar **Samba**, en varios artículos anteriores. Hoy vamos un poco más allá, lo que haremos es instalar y configurar **Samba** mediante un script bash.

Antes de comenzar debes asegurarte que los recursos compartidos, el servidor, y el sistema del cliente trabajan en la misma **subred IP**.

Instalar y configurar Samba
Creamos el script bash de instalación.

```
nano installsamba.sh
```

Copia y pega el siguiente código, pero antes debes revisarlo bien por si acaso es necesario modificar algún valor, o dato (por ejemplo la interfaz de red).

```
# !/bin/bash
#
# Samba Instalador

if [ "$EUID" -ne 0 ]
  then echo "Debes ejecutar el script como root. 'sudo $0'"
  exit
fi

apt install samba -y

hostname=`hostname`

cat > /etc/samba/smb.conf <<EOF
[global]
   workgroup = WORKGROUP
   #usershare allow guests = yes security=share security=user
   security = user
   guest account = nobody
   follow symlinks = yes
   wide links = no
   unix extensions = no
   lock directory = /var/cache/samba
   netbios name = $hostname
   follow symlinks = yes
   wide links = yes
   unix extensions = no
   log file = /dev/null
bind interfaces only = yes
#interfaces = eth0
#interfaces = 212.154.12.48 10.0.0.5
#encrypt passwords = no
#obey pam restrictions = yes
#pam password change = yes
#client plaintext auth = yes
#client ntlmv2 auth = no
[Root]
        comment = Root
        path = /
        read only = No
        #access based share enum = Yes
        browsable = yes
        valid user = root
EOF

pass=`< /dev/urandom tr -dc a-z | head -c${1:-5}`

echo "$pass
$pass" | smbpasswd -a root

service smbd restart
service nmbd restart

echo "Username : root
Password: $pass
"
```

Guarda el archivo, y cierra el editor.

Concedemos los permisos necesarios.

```
chmod +x installsamba.sh
```

Lo ejecutamos:

```
./installsamba.sh

o

bash installsamba.sh
```

Fedora 31 listo para su descarga

Fedora 31, la distribución Linux apoyada por **Red Hat**, acaba de lanzar su ultima versión. Viene con varias y actualizaciones en todas sus versiones, incluyendo la de servidor. Pensando en un futuro próximo, han abandonado **Python 2** y los núcleos de 32bits.

Debo aclarar que aunque la nueva versión no tiene su variante de 32bits, si que se conserva el soporte para aplicaciones con dependencias de 32 bits y del hardware heredado con controladores de 32 bits. Se requieren bibliotecas de 32 bits para una correcta compatibilidad con **WINE**, así como con algunas herramientas privativas, como pueden ser algunos juegos provistos a través de la plataforma **Steam**.

Fedora 31

Para los usuarios de **Fedora Desktop**, los cambios más importantes se aplican a la mejora del rendimiento de **Wayland** y **GNOME**, incluyendo una integración mejorada de **Qt** en GNOME a través de **Qt GNOME**, así como mejoras en el modo normal **GNOME Classic**. **Fedora 31 Xfce** incluye **Xfce 4.14**, con su migración a **GTK3**.

Fedora 31 mejora la velocidad de instalación a la hora de actualizar (se agradece), ya que los paquetes se comprimen con **zstd** en vez de **xz**. Esta actualización es transparente para los usuarios, ya que se maneja en el servidor de compilación. Además, rpm se actualiza a 4.15, y el administrador de paquetes yum 3 desaparece.

El soporte para AAC y los perfiles H.264 se incluyen listos para utilizar, así se evita el tener que instalar paquetes de terceros como RPMfusion para una correcta reproducción de medio.

Otras actualizaciones importantes de Fedora 31 son las bibliotecas y herramientas estándar: Mono 5.20, IBus 1.5.21, Erlang 22, Perl 5.30, Golang 1.13, Node.js 12.x, Gawk 5.0.1 y glibc 2.30, entre otros.

AVISO!!!. Los usuarios de **Docker** deben migrar a la herramienta **podman**, ya que Fedora 31 hace uso de **cgroups2**.

Como es normal, Fedora es compatible con la gran mayoría de sistemas actuales Intel o AMD de 64 bits, para el soporte completo de las GPU NVIDIA se necesitan paquetes de terceros.

Descargar Fedora 31

Puedes descargar Fedora desde los enlaces oficiales que proponemos.

- Fedora Desktop
- Fedora Server
- Fedora CoreOS
- Silverblue
- Fedora IoT

También puedes conseguir los paquetes adicionales que necesites, a través de RPMFusion.

- RPMFusion

Actualizar Fedora 30 a Fedora 31

Como hablamos en el anterior articulo, Fedora 31 ya está listo para su descarga. En este vemos como actualizar nuestro sistema Fedora 30 a Fedora 31, y obtener las últimas funciones y actualizaciones disponibles para esta gran distribución Linux.

Fedora Workstation tiene un método de actualización gráfica, pero la verdad es que no me gusta nada de nada. Actualizar una distribución desde GUI, solo puede acarrear problemas de diversa indole, mucho mejor desde la terminal. Así que vamos a ello.

Actualizar Fedora 30 a Fedora 31

Antes de comenzar el proceso de actualización, asegúrate de tener el último Fedora 30 (incluidas las herramientas). El paso anterior es muy importante, sobre todo si tiene instalado software modular. Ejecuta el siguiente comando.

```
sudo dnf upgrade --refresh
```

Una vez actualizado Fedora 30, te recomiendo que hagas un backup de tus datos más importantes.

Ahora instalamos el plugin system upgrade de Fedora.

```
sudo dnf install dnf-plugin-system-upgrade
```

Para comenzar con la actualización, ejecuta lo siguiente:

```
sudo dnf system-upgrade download --releasever=31
```

El comando anterior descargara todas las actualizaciones a nuestra máquina, y preparara el upgrade. Si tienes problemas al actualizar debido a dependencias rotas o paquetes inexistentes, agrega el indicador --allowerasing al comando anterior. Esto elimina los paquetes que están bloqueando la actualización del sistema.

Reiniciar y actualizar Fedora

Una vez que termine la descarga de la actualización, el sistema estará listo para reiniciarse. Para iniciar Fedora con el proceso de actualización, ejecuta el comando que te indico a continuación:

```
sudo dnf system-upgrade reboot
```

No te asustes, al reiniciar comenzara a operar de forma extraña, es normal. Se crea una nueva opción en la pantalla donde se selecciona el kernel de arranque, el sistema se reinicia con el núcleo actual instalado (el de Fedora 30), no te preocupes, es un proceso normal. Después de la pantalla del kernel, comienza el proceso de actualización.

¡Ahora relájate y se paciente!, puede tomar su tiempo. Al finalizar el proceso, reiniciara la maquina con tu flamante Fedora 31 instalado. Felicidades.

Problemas al actualizar Fedora

NOTA 1: No se permite actualizar saltando alguna versión, por ejemplo no es posible pasar de Fedora 29 a Fedora 31. En ese caso deberías actualizar primero a la versión 30, y después a la versión 31.

NOTA 2: Si persisten los problemas para actualizar pese a la solución indicada anteriormente, seguro que tienes algún repositorio de terceros instalado, debes deshabilitar estos repositorios mientras se actualiza.

Ubuntu vs Arch Linux

Arch Linux y Ubuntu son dos gigantes, si hablamos de distribuciones en el mundo Linux. Ambas tienen una legión de seguidores tremenda, entre las cuales se adoptan todo tipo de posturas, unas más radicales, y otras más suaves.

Estas dos distribuciones han generado una lista de distribuciones derivadas incontable, algunas tan buenas que incluso quitan protagonismo a la madre, por ejemplo: **Linux Mint** y **Manjaro**. Pero… ¿cual es mejor?, ¿es Ubuntu el rey de las distros linux?, ¿Arch es mucho mejor pero solo para usuarios con conocimientos?, la respuesta a las dos ultimas preguntas es sí.

En este articulo analizamos varios aspectos que las diferencian (algunos contundentes), con el fin que tu mismo puedas sacar tus propias conclusiones y selecciones la que más se adapte a tus necesidades y conocimientos. Vemos las siguientes características:

- **Instalación y configuración.**
- **Aplicaciones y herramientas.**
- **Multimedia.**
- **Personalización**.

Ubuntu vs Arch Linux

Instalación y configuración

Ubuntu ofrece un instalador gráfico, en **Arch** se debe instalar desde la terminal.

El instalador gráfico de **Ubuntu**, lo hace ideal tanto para usuarios no experimentados, como para los que si lo son pero no necesitan configurar cada aspecto del sistema. Puedes realizar cualquier modificación con un simple click, y lo más importante, no es necesario adquirir conocimientos técnicos avanzados. El proceso es muy rápido.

Arch Linux no viene con un instalador gráfico. Solo ofrece utilidades en línea de comandos para instalar un sistema **Arch Linux** desde cero. El resultado es un proceso mucho más abierto, pues permite personalizar y configurar a tu gusto tu nuevo sistema. **Arch** será lo que tu quieras que sea, pero ojo, es mucho más fácil cometer un error, ademas, crear un sistema como tu quieres puede llevar se tiempo.

Aplicaciones y herramientas

Arch al igual que **Ubuntu**, tienen inmensos repositorios de software. **Ubuntu**, es muy popular y eso provoca que está bien respaldado por aplicaciones de terceros. La gran mayoría de herramientas se programan para que funcionen en **Ubuntu**. Existen multitud de repositorios no oficiales en forma de PPA, en los que puedes encontrar de todo.

El software de **Ubuntu** suele ser bastante nuevo, pero no las ultimas versiones. Solo se lanza al publico en general cuando se considera muy estable.

Arch tiene un excelente sistema de empaquetado, ademas de ser muy simple. El **equipo de Arch**, se puede permitir el lujo de empaquetar las aplicaciones más rápido. Es raro que no encuentres lo que buscas en Arch Linux.

Si se da el caso que no encuentras lo que buscas en **Arch**, puedes recurrir a **Arch User Repository (AUR)** donde tienes de todo. AUR es realmente impresionante, permite a los usuarios empacar para Arch y almacenar los paquetes en un lugar unificado (así, está disponible para todos). Insisto en que AUR está repleto de todo tipo de aplicaciones y herramientas, incluyendo software del lado oscuro.

Multimedia
En multimedia y juegos son bastante parejos, cualquiera de los dos es una excelente opción.

Las dos distribuciones ofrecen las principales aplicaciones multimedia desde sus repositorios predeterminados. Extras y códecs, no falta de nada. Encontraras tu reproductor de música preferido, y si por algún caso no encuentras lo que buscas, puedes recurrir a AUR o PPA.

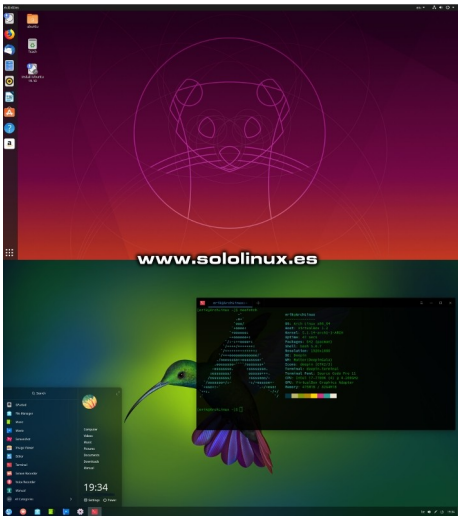
El juego no es muy diferente. Ubuntu es oficialmente compatible con Valve for Steam, pero Arch es una **distribución linux** tan simple de adaptar que Steam también funciona sin problemas. Los últimos controladores gráficos de NVIDIA y AMD también están soportados por las dos distros.

Personalización
Si solo hablamos de cambiar la apariencia del escritorio, tanto **Ubuntu** como **Arch Linux** tienen acceso a una amplia gama de escritorios. La facilidad de uso es la misma, el único problema, es que en Arch tienes que instalar tu mismo el entorno de escritorio con el que te sientas más cómodo.

Si solo comparamos la personalización del sistema en general, no hay ninguna duda, Arch es el ganador por goleada.

Al ofrecer un sistema **listo para usar**, Ubuntu se ve obligada a limitar la personalización. Los desarrolladores de Ubuntu trabajan para que todo lo incluido en su sistema funcione bien, incluyendo el resto de configuraciones. Ten cuidado al hacer alguna modificación importante, no sería la primera vez que alguien intenta configurar un componente en particular, y al final acaba por tener que reinstalar todo otra vez.

Arch es diferente, imagínate esas cajas llenas de piezas de plástico con las que los niños montan estructuras diversas, pues, eso es **Arch**. Puedes seleccionar las piezas que tu necesites, y juntarlas. **OJO!!!,** puedes construir un sistema operativo excelente, o una autentica porquería que ademas es inestable, jaja. Si eres hábil y cuentas con los conocimiento suficientes, puedes crear algo realmente magnífico y ademas único. Seras la envidia.



Conclusión final
En definitiva, ¿cual de los dos es mejor, Ubuntu vs Arch?. La verdad es que no puedo responder a eso, tengo mis preferencias desde hace años, y sería imparcial.

Es evidente que **Ubuntu** proporciona una mejor experiencia en usuarios noveles, lo instalas y funciona. Es muy completo y te ofrece todo lo que necesitas para comenzar.

Por otro lado, **Arch** te permite crear un sistema como tu quieres, o necesitas. Es extremadamente rápido, liviano y muy poderoso. Con Arch, nunca te quedarás atascado con una configuración que no hayas implementado tu mismo, pero recuerda que toda la responsabilidad de que funcione bien es tuya, y debes asumir ese riesgo.

La decisión final es tuya, suerte.

Que todas las url acaben en barra inclinada

Esto no es un articulo como los que escribimos habitualmente, tan solo es un pequeño truco. Puede parecer una tontería, pero es posible que alguna vez necesites que la url de una dirección termine en barra inclinada.

/

A veces por temas de seo, otras veces por obligar al cliente a que la escriba, en fin, por motivos diversos. Lo que debemos hacer para lograr que todas las url acaben en barra inclinada, es editar el archivo **.htaccess.** Copia y pega lo siguiente:

```
RewriteEngine On
RewriteBase /

RewriteCond %{REQUEST_URI} /+[^.]+$
RewriteRule ^(.+[^/])$ %{REQUEST_URI}/ [R=301,L]
```

Guarda el archivo, cierra el editor, y reinicias **Apache**. Si no recuerdas como reiniciar Apache, revisa este anterior articulo.

Instalar FreeOffice 2018 en Linux

FreeOffice es una **suite ofimática** gratuita (no open source) bastante completa, cuenta con un procesador de textos, una hoja de cálculo y una aplicación de presentaciones al estilo PowerPoint.

Es una buena **alternativa** a **Microsoft Office**, y es evidente que intenta ser la competencia directa de **LibreOffice**.

Ofrece un soporte completo para leer y escribir en todos los formatos de Microsoft Office (desde los más antiguos a los nuevos), como **DOCX, XLSX, PPTX, DOC, XLS y PPT**, así como con el inconfundible formato de **LibreOffice OpenDocument Text (ODT),** ademas es multiplataforma (Linux, MacOS, Windows).

En este articulo veremos como instalar **FreeOffice 2018** en nuestro linux, vale la pena probarlo, es un buen producto, pero no me voy engañar a mi mismo, yo sigo con LibreOffice.

Instalar FreeOffice 2018 en Linux

En este momento la ultima versión es la 2018-971, si tienes problemas puedes verificar su pagina oficial de descargas.

FreeOffice en Ubuntu, Debian, Linux Mint y derivados:

Descargamos la aplicación.

```
wget https://www.softmaker.net/down/softmaker-freeoffice-2018_971-01_amd64.deb
```

Instalamos FreeOffice 2018.

```
sudo dpkg -i softmaker-freeoffice-2018_971-01_amd64.deb

sudo apt-get install -f
```

FreeOffice ya está instalado, si quieres que la suite ofimática se actualice automáticamente, ejecuta lo siguiente:

```
sudo /usr/share/freeoffice2018/add_apt_repo.sh
```

FreeOffice en Fedora, OpenSuse, CentOS y derivados:

Descargamos la aplicación.

```
wget https://www.softmaker.net/down/softmaker-freeoffice-2018-971.x86_64.rpm
```

Importamos la key publica.

```
sudo rpm --import linux-repo-public.key
```

Instalamos FreeOffice 2018.

```
sudo rpm -ivh softmaker-freeoffice-2018_971-01_amd64.rpm
```

FreeOffice ya está instalado, si quieres que la suite ofimática se actualice automáticamente, ejecuta lo siguiente:

```
sudo /usr/share/freeoffice2018/add_rpm_repo.sh
```

Otras distribuciones linux:

Si utilizas Arch Linux o alguno de sus derivados tienes el paquete en AUR. De todas formas, mira que sencillo es instalar la suite desde su archivo comprimido.

```
wget https://www.softmaker.net/down/softmaker-freeoffice-971-amd64.tgz
```

Descomprime el archivo.

```
tar xvzf softmaker-freeoffice-2018-971-amd64.tgz
```

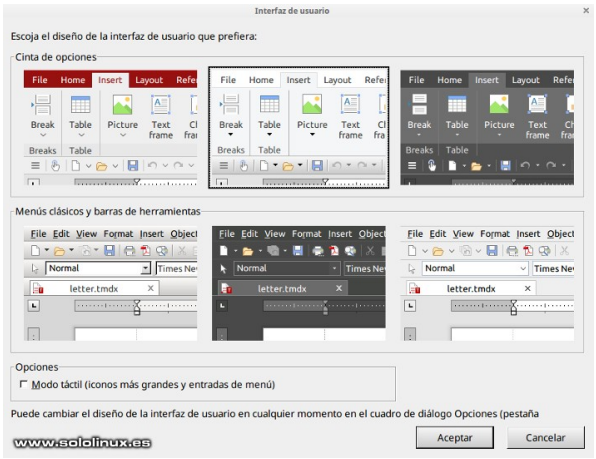
Ahora instala FreeOffice 2018.

```
sudo ./installfreeoffice
```

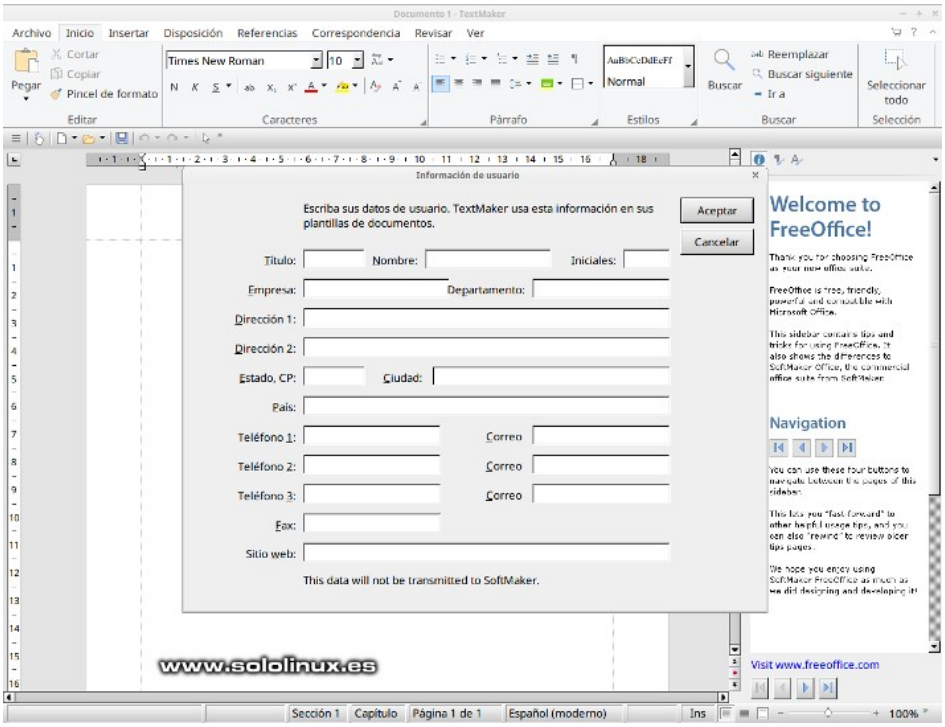
Suite instalada.

FreeOffice 2018

Al abrir por primera vez alguna herramienta de la suite ofimática, te ofrece las opciones visuales predeterminadas, selecciona una.



En este caso abrimos TextMaker.



Versión de FreeOffice 2018.

Visita nuestro sitio proximamente

MAGAZINE

SoloWordpress

Número XX

Todo sobre WordPress

MES / AÑO

SoloWordpress

NUMERO

PRÓXIMAMENTE

MANUALES

TRUCOS

CONSEJOS

PRÓXIMAMENTE

Manuales, consejos, trucos.