



Nº 0001

# fedora™ -LATAM magazine

Una revista para Latinoamericanos  
hecha por latinoamericanos

## Robotica Educativa

Fedora como sistema para la integración de conocimientos

## Trucos

Obtener contraseñas de redes Wifi desde Fedora.

Instalando KVM con QEMO, virtualiza!!

## Eventos

FUDcon LATAM en Santiago de Chile.

FISL11, Porto Alegre viste Fedora

 **conoce fedora<sup>f</sup>**

Te presentamos en exclusiva la primera entrevista oficial al nuevo Lider del Proyecto Fedora Internacional, Jared Smith.

Conoce sobre Jared y su nuevo rol a cargo de la estructura colaborativa más grande del mundo!



PUBLICIDAD

# Indice

## 3 Editorial

### 4 **Conoce Fedora:**

Jared Smith, nuevo Lider del Proyecto fedora Internacional

### 6 **Robotica Educativa:**

Fedora como sistema para la integracion de conocimientos

### **Trucos:**

7 Obtener contraseñas de redes Wifi desde Fedora

8 Parte I

Instalando KVM con QEMO, Virtualiza!!

### 9 **Eventos:**

10 FUDcon LATAM en Santiago

FISL11, Porto Alegre viste Fedora



conoce fedora



# Jared Smith

Nuevo líder del Proyecto Fedora Internacional

# PUBLICIDAD

# Robotica Educativa

## Fedora como sistema para la integracion de conocimientos

Uno de los principales objetivos de la Robótica Educativa es la generación de entornos de aprendizaje basados en la práctica real de los estudiantes. La idea es que los niños puedan concebir, desarrollar y poner en práctica diferentes tipos de robots que les permitan resolver algunos problemas y facilitar al mismo tiempo su aprendizaje.

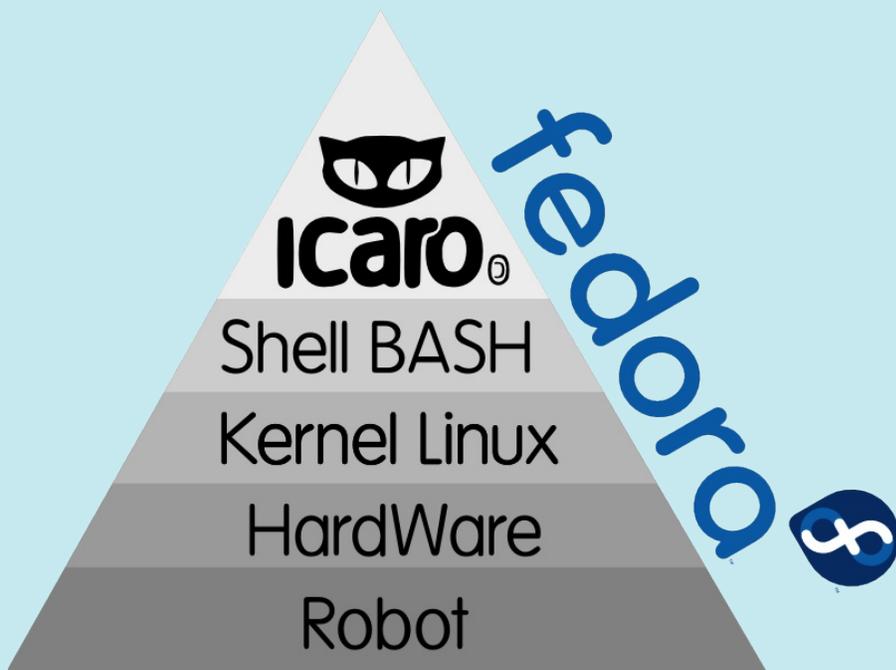
La Robótica Educativa, dado su carácter multidisciplinario y polivalente, constituye una actividad que permite abordar conocimientos complejos en torno a las nuevas tecnologías y partiendo de aportes provenientes de la electrónica, física, matemática e informática.

En particular, es posible enseñar las bases fundamentales de la lógica de sistemas computacionales mediante la creación de mecanismos autónomos electrónicos (robótico).

ICARO es un software desarrollado con la intención de acercar de una manera transparente, los fundamentos de la programación (iteración, repetición, recursividad, si condicionales) al usuario, aplicados a un contexto físico como

puede ser un robot o cualquier sistema de automatización.

Su funcionamiento se basa en escribir instrucciones en un archivo



**ICARO trabaja como un lenguaje de script a nivel de consola BASH**

ICARO se podría considerar como un Framework para trabajar con el puerto paralelo (lpt) de una manera sencilla.

de texto plano para que el software (que funciona como un intérprete) vaya leyendo línea por línea y enviando la información traducida al



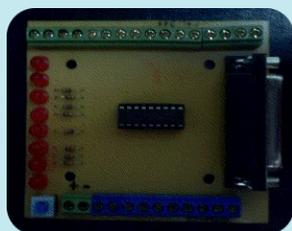
# Robotica Educativa

puerto paralelo, y mediante un hardware de protección eléctrico, poder encender/apagar distintos mecanismos electrónicos como motores, motores paso a paso, solenoides, servos etc etc.

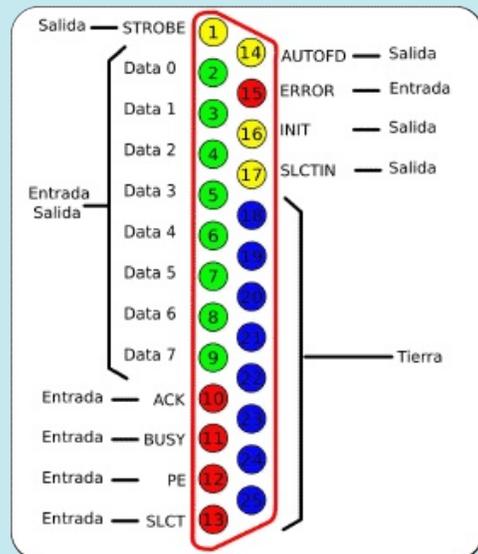
El puerto paralelo es una interfaz entre una computadora y un periférico cuya principal característica es que los bits de datos viajan juntos enviando un byte completo o más a la vez. Es decir, se implementa un cable o una vía física para cada bit de datos formando un bus. El puerto paralelo de una PC es ideal para ser usado como herramienta de control de motores, relés, LED's, etc. El mismo posee un bus de datos de 8 bits (Pin 2 a 9) y muchas señales de control, algunas de salida y otras de entrada que también pueden ser usadas fácilmente.

Basicamente la placa de control no es mas que una proteccion para evitar quemar el puerto paralelo y aumentar la tension de salida hasta 12 volt 1 amper, todo el peso del procesamiento esta en la computadora.

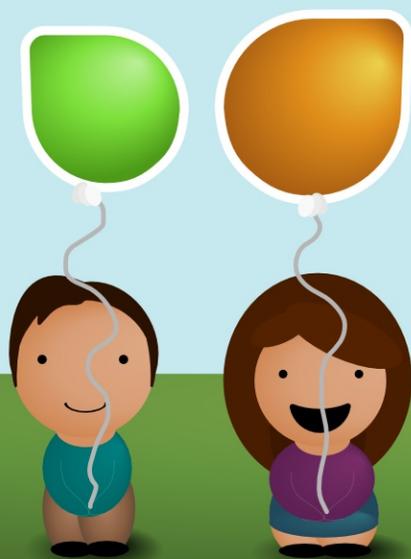
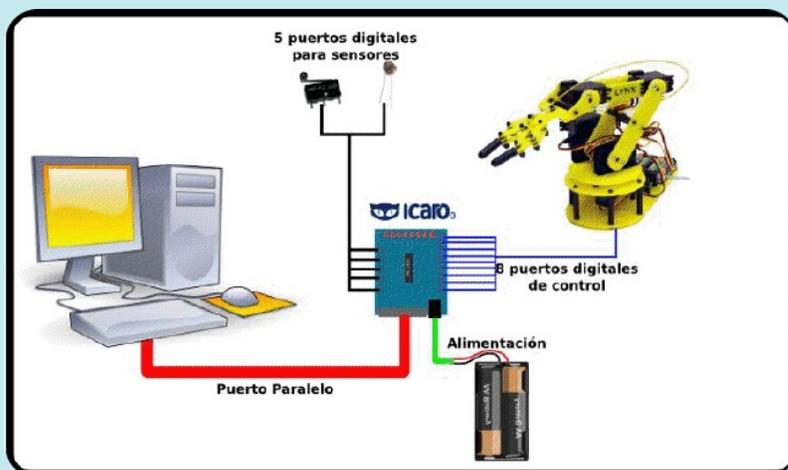
De esta forma, al hacer una placa sencilla (sin microprocesadores), se mantiene un costo bajo del componente, facilitando su adquisicion o armado por los colegios



La placa ICARO sirve como proteccion y para aumentar la tension de salida del puerto



Esquema de pines del conector DB25 del puerto paralelo



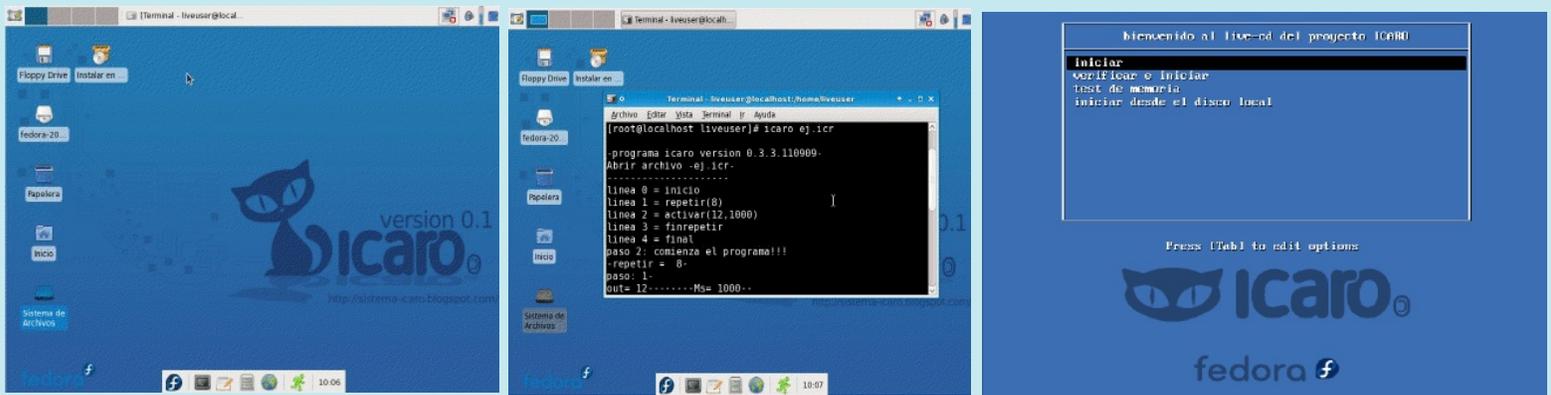
# Fedora como sistema para la integracion de conocimientos

## FEDORA LIVE-CD

Muchas veces migrar pcs de un colegio a una solucion de software libre puede ser problemático o hasta impracticable por varias razones (politicas escolares , costos de migracion etc.. ).

FEDORA es una distribucion linux que siempre tuvo la filosofia de estar a la vanguardia de los adelantos y actualizaciones de software y mantenerse como un sistema amigable para el usuario.

nivel inicial y medio. Estamos trabajando en conjunto con gente de la UCAB de venezuela, 2 colegios de Buenos Aires argentina y la comunidad FEDORA cordoba.



Para eso se desarrollo un live cd usando remix de la distribucion FEDORA 10. Este live-cd tiene instalado el software ICARO para poder usarlo directamente en cualquier PC con puerto paralelo.

Trae por defecto el gestor de ventanas liviano XFCE y programas especificos de electronica como el excelente software de diseño CAD/CAM KICAD otros mas.

Es una excelente distribucion para uso diario y facilita la migracion a software libre, a su vez la comunidad latinoamericana es muy activa y siempre estan dispuestos a ayudar.

ICARO actualmente esta enmarcado dentro del proyecto FEDORA Argentina, hace falta gente que quiera participar, sobre todo educadores que puedan montar una experiencia piloto en escuelas de

**Valentin Basel**  
Argentina  
[valentinbasel@fedoraproject.org](mailto:valentinbasel@fedoraproject.org)



## Contacto

[valentinbasel@fedoraproject.org](mailto:valentinbasel@fedoraproject.org)

<http://www.sistema-icaro.blogspot.com/>

# Trucos Fedora:

Quien decía que desde nuestra distro (Fedora 12 Constantine) instalado, no podrías conseguir las contraseñas de la wifi que detecte nuestra PC o portátil, ahora ya no es necesario descargar algún LiveCD, como son los famosos y super buenos wifitray, backtrack, wifislax.

Solo es necesario instalar el paquete **Aircrack-ng** de aquellos programas dedicados a descifrar las contraseñas de alguna wifi. Para ello necesitamos cargar un terminal y loguearnos como usuario root.

NOTA: De ahora en adelante se usara con el usuario root.

Ejemplo:

**Aplicaciones -> Herramientas del sistema --> Terminal.**

Una vez cagado el terminal colocamos 'su', para cambiarnos de usuario, lo cual nos pedirá la contraseña del mismo (no se preocupen si no se ve lo que escribimos, es una buena forma de proteger nuestra privacidad). Una vez ya en modo root, pasamos a copiar lo siguiente: **yum -y install aircrack-ng**, listo eso es todo, es cosa de esperar la instalación del paquete.

```
hanx@Emolet: ~]$ su
Contraseña:
[root@Emolet hanx]#
```

Ya instalado, pasamos a probar como es que se encuentra nuestra wifi, para ello, en el terminal copiamos iwconfig, lo que hacemos, es ver en detalle nuestra tarjeta wifi.

```
hanx@Emolet:home/hanx
Archivo Editar Ver Terminal Ayuda
[hanx@Emolet ~]$ su
Contraseña:
[root@Emolet hanx]# iwconfig
lo        no wireless extensions.
eth0     no wireless extensions.
eth1     IEEE 802.11g  ESSID:"niko 833@hotmail..."
Mode:Managed  Frequency:2.412 GHz  Access Point: 00:C0:CA:1C:96:42
Bit Rate:5.5 Mb/s   Tx-Power=20 dBm   Sensitivity=8/9
Retry limit:7  RTS thr:off   Fragment thr:off
Encryption key:8837-1964-52   Security mode:open
Power Management:off
Link Quality=56/100  Signal level=-67 dBm  Noise level=-91 dBm
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:2  Invalid misc:1  Missed beacon:15
pan0    no wireless extensions.
virbr0  no wireless extensions.
```

**Nota: En este caso ya estoy conectado con al red la cual he probado toda esta teoría, por cierto dice tener mucha seguridad'.**

Como vemos, mi tarjeta esta con el nombre **eth1**, no olviden de ese nombre ya que les va ser de mucha utilidad, nos fijamos en el modo en que se encuentra nuestra tarjeta, por defecto la encontraremos en modo **Managed**.

Una vez que nos fijamos en el estado de nuestra tarjeta, debemos de ponerla a modo **Monitor**, y nos estaremos preguntando que es eso de modo Managed y Monitor, la respuesta son muy sencillas. Modo Managed, en este estado de la tarjeta se pone visible ante cualquier AP, Router, lo cual deja 'huella' cuando hace un 'movimiento', es el estado normal de toda tarjeta cuando realiza una conexión para una navegación; en cambio en Modo Monitor, la tarjeta esta en un estado invisible y captura todos los paquetes que se transmita por la wifi sin que el administrador se

de cuenta que alguien se a colgado de su red, esto tiene varias utilidades buenas y malas, ya que podemos ver todos los datos y mensajes que se transmitan, ver los usuarios que se encuentre conectados a la red y muchas cosas mas; muy interesante no?.

Ilustramos algunos conceptos para poder entrar mas en habiente, falta ahora lo mas importante, colocar a la tarjeta en modo monitor. Para

ello en el terminal colocarnos **airmon-ng start eth1**, con esto ponemos a nuestra tarjeta en modo monitor; pero si quisieras salir de ese modo, pues detenemos el proceso colocando **airmon-ng stop eth1**.

```
hanx@Emolet:home/hanx
Archivo Editar Ver Terminal Ayuda
pan0    no wireless extensions.
virbr0  no wireless extensions.
[root@Emolet hanx]# airmon-ng start eth1
Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working
after a short period of time, you may want to kill (some of)
these:
PID   Name
1075  NetworkManager
1086  wpa_supplicant
1095  avahi-daemon
1096  avahi-daemon

Interface  Chipset      Driver
-----
[root@Emolet hanx]# airmon-ng stop eth1

Interface  Chipset      Driver
-----
eth1       Intel 2200BG  ipw2200 (monitor mode disabled)
[root@Emolet hanx]#
```

En esta imagen vemos que ya activamos el estado monitor a mi tarjeta. Ahora veremos como lo desactivamos el estado.

# Obtener contraseñas de Redes Wifi usando Fedora

Una vez que nuestra tarjeta se encuentra en modo monitor, nos interesa saber cuantas son las redes wifi que nuestra tarjeta detecta para ello necesitamos realizar un escaneo, vamos al terminal y copiamos **airodump-ng eth1**, no olvidar que eth1 es el nombre de mi tarjeta, ustedes pondrán lo que le salga cuando ejecutan el comando iwconfig.

```
hans@emotet:~/hans$ airodump-ng eth1
CH 7 | Elapsed: 12 mins | 2010-03-10 21:21 | eth1 reset to monitor mode
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:0E:2E:92:88:93 -1 0 09 0 113 -1 WEP WEP <length: 0>
00:0E:2E:1F:98:E4 -65 187 0 0 13 11 WEP WEP <length: 7>
00:C0:CA:1C:96:42 -66 448 3055 0 1 54 WEP WEP SKA <length: 16>
00:AF:02:25:D9:E4 -79 63 0 0 11 54 WEP WEP PONCE <length: 0>
00:0E:2E:93:35:E4 -1 0 37 0 100 -1 WEP WEP <length: 0>
BSSID STATION PWR Rate Lost Packets Probes
00:C0:CA:1C:96:42 00:0E:2E:A6:0F:55 -1 5 0 0 166
00:C0:CA:1C:96:42 00:0E:2E:A6:0F:5C -1 11 0 0 736
00:C0:CA:1C:96:42 00:C0:CA:1C:81:66 -1 11 0 0 649
00:C0:CA:1C:96:42 00:C0:CA:17:9C:D0 -1 11 0 0 868
00:C0:CA:1C:96:42 00:0E:2E:80:00:6A -1 11 0 0 287
00:C0:CA:1C:96:42 00:C0:CA:1C:00:A0 -69 11 5 51 367
00:C0:CA:1C:96:42 00:C0:CA:1C:81:98 -81 11 5 0 296
00:C0:CA:1C:96:42 00:C0:CA:1C:83:48 -82 0 5 0 1
00:C0:CA:1C:96:42 00:C0:CA:1C:80:88 -1 11 0 0 21
00:C0:CA:1C:96:42 00:C0:CA:1C:92:00 -1 11 0 0 9
```

Como vemos, estamos realizando un escaneo de todas las redes wifi que detecto mi tarjeta, si nos fijamos, en la parte superior vemos CH 7, nos esta indicando el canal por el cual en este momento esta escaneando; seguido nos muestra el tiempo que llevamos realizando la operación, la fecha y hora, por ultimo el nombre de nuestra tarjeta y el estado.

En seguida vemos una linea de títulos como:

- \* **BSSID**, es la columna donde nos mostraran todas las MAC Address de las redes wifi que detecto. Dirección MAC del AP.
- \* **PWR**, nivel de señal reportado por la tarjeta. Su significado depende del controlador, pero conforme te acercas

al AP o a la estación la señal aumenta. Si PWR == -1, el controlador no soporta reportar el nivel de señal.

- \* **Beacons**, número de paquetes-anuncio enviados por el AP. Cada punto de acceso envía unos diez beacons por segundo al ritmo (rate) mínimo (1M), por lo que normalmente pueden ser recogidos desde muy lejos.
- \* **#Data**, número de paquetes de datos capturados (si es WEP, sólo cuenta IVs), incluyendo paquetes de datos de difusión general.
- \* **#/s**, número de paquetes de datos capturados por segundo calculando la media de los últimos 10 segundos.
- \* **CH**, número de canal (obtenido de los paquetes beacon). Nota: algunas veces se capturan paquetes de datos de otros canales aunque no se esté alternando entre canales debido a las interferencias de radiofrecuencia.
- \* **MB**, velocidad máxima soportada por el AP. Si MB = 11, entonces se trata de 802.11b, si MB = 22 entonces es 802.11g y velocidades mayores son 802.11n.

- \* **ENC**, algoritmo de encriptación en uso. OPN = sin encriptación, "WEP?" = WEP o mayor (no hay suficiente datos para distinguir entre WEP y WPA), WEP (sin la interrogación) indica WEP estática o dinámica, y WPA si TKIP o CCMP están presentes.

\* **CIPHER**, detector cipher. Puede ser CCMP, WRAP, TKIP, WEP, WEP40, o WEP104.

\* **AUTH**, nos esta indicando con que tipo identificación se encuentra la red;

\* **ESSID**, conocida como "SSID", puede estar vacía si el ocultamiento de SSID está activo. En este caso airodump tratará de recuperar el SSID de las respuestas a escaneos y las peticiones de asociación.

\* **STATION**, Dirección MAC de cada cliente asociado. En la captura de pantalla, vemos que se han detectado dos clientes (00:09:5B:EB:C5:2B y 00:02:2D:C1:5D:1F).

\* **Lost**, el número de paquetes perdidos en los últimos 10 segundos.

\* **Packets**, el número de paquetes de datos enviados por el cliente.

\* **Probes**, los ESSIDs a los cuales ha intentado conectarse el cliente.

En la 2da parte nos conectaremos a la red que escogimos para finalmente acceder.

Hans Cruz Buchelli  
Perú  
hans@fedoraproject.org