
# CARATULA

DEPARTAMENTO ELÉCTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN COMPUTACIÓN

AUTORES: CHALACÁN REYES JORGE VINICIO
REVELO YÉPEZ RUPERTO IVÁN

TEMA: CONFIGURACIÓN DE SEGURIDADES DE UN SERVIDOR LINUX

DIRECTOR: ING. RAUL CAJAS
CODIRECTOR: ING. NANCY JACHO

LATACUNGA, AGOSTO 2014

UNIVERSIDAD DE LA FUERZAS ARMADAS - ESPE

DEPARTAMENTO ELÉCTRICA Y ELECTRÓNICA

# CERTIFICADO

Ing. RAUL CAJAS

Ing. NANCY JACHO

**CERTIFICAN**

Que el trabajo titulado, Configuración de seguridades de un servidor Linux realizado por JORGE VINICIO CHALACÁN REYES y RUPERTO IVAN REVELO YEPÉZ, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas-ESPE.

Debido a la investigación realizada y su valioso contenido si recomiendo su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a JORGE V. CHALACÁN R. y RUPERTO I. REVELO YÉPEZ, que lo entregue al Ing. LUIS GUERRA, en su calidad de Director de la Carrera.

Latacunga, 20 de marzo del 2014

| | |
|---|---|
| ING. RAUL CAJAS | ING. NANCY JACHO |
| DIRECTOR | CODIRECTOR |

UNIVERSIDAD DE LA FUERZAS ARMADAS - ESPE

DEPARTAMENTO ELÉCTRICA Y ELECTRÓNICA

# DECLARACIÓN DE RESPONSABILIDAD

JORGE VINICIO CHALACÁN REYES

RUPERTO IVAN REVELO YÉPEZ

DECLARAMOS QUE:

El proyecto de grado denominado [Configuración de seguridades de un servidor Linux], ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan el pie de las páginas correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Latacunga, 20 de marzo del 2014

| | |
|---|---|
| JORGE V. CHALACÁN REYES | RUPERTO I. REVELO YÉPEZ |
| C.C. 0401440243 | C.C. 0401397229 |

UNIVERSIDAD DE LA FUERZAS ARMADAS - ESPE

DEPARTAMENTO ELÉCTRICA Y ELECTRÓNICA

# AUTORIZACIÓN

Nosotros, JORGE VINICIO CHALACÁN REYES y

RUPERTO IVAN REVELO YÉPEZ

Autorizamos a la Universidad de las Fuerzas Armadas-ESPE la publicación, en la biblioteca virtual de la Institución del trabajo, Configuración de seguridades de un servidor Linux, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Latacunga, 20 de marzo del 2014

_____ _____

JORGE V. CHALACÁN REYES

C.C. 0401440243

RUPERTO I. REVELO YÉPEZ

C.C. 0401397229

# DEDICATORIA

El presente trabajo de tesis está dedicado a **DIOS**, por darme la vida a través de mis queridos padres, mi **MADRE** quien con mucho cariño, amor y ejemplo ha hecho de mí, una persona con valores para poder desenvolverme como: **ESPOSO, PADRE Y PROFESIONAL**

A mi **ESPOSA**, que ha estado a mi lado dándome amor, confianza y apoyo incondicional para seguir adelante y poder cumplir otra etapa de mi vida.

A mis **HIJOS**, quienes son el motivo y la razón de seguir superándome día a día, para alcanzar mis más apreciados ideales de superación.

Son muchas las personas que han formado parte de mi vida profesional alas que me encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones.

# DEDICATORIA

A la institución que me acogió en su seno y me brindó la oportunidad de formarme como soldado y mejorar como ser humano

A mi **ESPOSA E HIJOS**, quienes constituyen el pilar fundamental de la familia, que con paciencia han sabido apoyar al esfuerzo desplegado para lograr el objetivo final en esta trayectoria de mi vida, quienes con sus rostros inocentes y puros, me han regalado parte de su tiempo para poder cumplir con este delicado e importante trabajo.

A mis **PADRES** por su apoyo incondicional que supieron guiarme por el camino del bien, para poder salir del grupo mayoritario de nuestro pueblo, que es el desconocimiento de la ciencia.

# AGRADECIMIENTO

Nos complace de sobre manera a través de este trabajo exteriorizar nuestro sincero agradecimiento a la Universidad de las Fuerzas Armadas-ESPE Sede Latacunga, y en ella a los distinguidos docentes quienes con su profesionalismo y ética puesto de manifiesto en las aulas, nos procuran sus cocimientos, para ser útiles a la sociedad.

A nuestros directores de tesis, quienes con su experiencia como docentes han sido la guía idónea, durante el proceso que ha llevado el realizar esta tesis, nos han brindado el tiempo necesario, como la información para que este anhelo llegue a ser felizmente culminada.

# ÍNDICE DE CONTENIDOS

# ÍNDICE DE GRÁFICOS

# RESUMEN

## SEGURIDAD DE UN SERVIDOR CENTOS

En todos los casos, el servidor de seguridad protege al equipo de ataques externos realizados mediante Internet que podrían suponer amenazas para su seguridad en Ia red, así como para los archivos del equipo. Entre el software de seguridad más conocidos se encuentran: El protocolo SSH, el Firewall y Proxy (integrado en el sistema operativo CentOS). Un Servidor de seguridad necesita una serie de instrucciones, un soporte lógico que ponga en funcionamiento los distintos elementos y consiga que trabajen en forma coordinada para realizar las funciones que se espera de ellos; CentOS es un sistema multiusuario, por lo tanto, se puede añadir, modificar, eliminar y en general administrar usuarios. Necesita de una política de permisos segura y planificada para mantener el sistema seguro. Un administrador de sistemas Linux debe prestar mucha atención y planificar dicha política de permisos para mantener su sistema seguro. CentOS permite la configuración del cortafuego en modo gráfico; De Fail2Ban que es un analizador que busca intentos fallidos de ingreso al servidor y bloque a las IP's de donde provienen estos intentos; La configuración SSH, que es un protocolo de ordenes seguras, permite transmitir la información de forma rápida y segura; Wireshark, es un analizador de protocolos, utilizado para realizar análisis y solucionar problemas en redes de comunicaciones.

Palabras Clave: Software de Seguridad, Servidor CentOS, Multiusuario, Protocolos Seguros, Sistema Operativo.

# ABSTRACT

## SECURITY OF SERVANT CENTOS

In all cases, the firewall protects the computer from external attacks carried out through the Internet that could pose security threats in the network, as well as computer files. Among the known security software are: SSH, Firewall and Proxy protocol (built into the CentOS operating system). A Firewall requires a series of instructions, software that operates the various elements and gets to work in a coordinated manner to perform the functions we expect of them. CentOS is a multiuser system, therefore, you can add, modify, delete and generally manage users. Need a safe and planned policy permits to keep the system safe. A Linux system administrator should pay close attention to the policy and planning permissions to keep your system secure. CentOS allows the firewall configuration in graphical mode ; De Fail2Ban which is a scanner that failed attempts to login to the server and block the IP's from which these attempts , SSH configuration is a protocol secure orders, allows information quickly and safely; Wireshark is a protocol analyzer , used for analyzing and solving problems in communication networks.

Keywords: Software Security, CentOS Server, Multi, Insurance Protocols Operating System

# CAPÍTULO I
# INTRODUCCIÓN

## 1.1 ANTECEDENTES

En la actualidad las empresas buscan seguridad para su información, eso conlleva a la instalación de un servidor de seguridad.

Un servidor de seguridad pueden aplicarse al software y al hardware, eso da más seguridad y confidencialidad la información de cualquier empresa o institución. En todos los casos, el servidor de seguridad protege al equipo de ataques externos realizados mediante Internet que podrían suponer amenazas para su seguridad, así como para los archivos del equipo.

## 1.2 PLANTEAMIENTO DEL PROBLEMA

La Dirección de Sistemas y Comunicaciones (DISICOM), como un ente principal de los sistemas y comunicaciones de la Fuerza Terrestre ha visto la necesidad de investigar la implementación de un servidor de seguridad en un sistema operativo Linux, esto permitirá proteger a usuarios frente a otros y protegerse a sí mismo, a fin de garantizar los servicios que presenta cada servidor.

Con la generalización de las conexiones a internet y el rápido desarrollo del software, la seguridad se está convirtiendo en un tema muy importante, ya que la red global es insegura por definición.

## 1.3 OBJETIVO GENERAL

Configurar las seguridades de un servidor CentOS, con la finalidad de mantener su información confiable y segura.

## 1.4 OBJETIVOS ESPECÍFICOS

- Analizar las seguridades que ofrece el Sistema Operativo CentOS.
- Configurar el sistema operativo CentOS como servidor de seguridad.
- Probar el servidor de seguridad para garantizar su funcionamiento.

# CAPÍTULO II
# MARCO TEÓRICO

## 2.1 LINUX

Entre algunos de los ejemplos de software de servidores de seguridad conocidos se encuentran: El protocolo SSH, el Firewall y Proxy (integrado en el sistema operativo CentOS).

El servidor de seguridad Linux permite configurar reglas para permitir o denegar el paso del tráfico de Internet. Si no ha configurado el servidor de seguridad con un conjunto de reglas propio, las prácticas de seguridad estándar determinarán que se aplique un conjunto de reglas predeterminado de denegación del servidor de seguridad.(1)

Mientras los datos estén almacenados en un soporte informático y vayan desde un sistema X a otro sistema Y a través de un medio físico, red, Internet, por ejemplo, puede pasar por ciertos puntos durante el camino proporcionando a otros usuarios la posibilidad de interceptarlos, e incluso alterar la información contenida, además algún usuario de su sistema puede modificar datos de forma maliciosa para hacer algo que nos pueda resultar perjudicial. Con el acceso masivo a Internet aumentado notablemente el número de potenciales atacantes, aquello nos ha llevado a que la seguridad de las redes sea la base fundamental, para mantener la información segura(2).

## 2.2 SEGURIDADES DEL SERVIDOR

La seguridad es un tema importante, sobre todo cuando el sistema actúa como un Servidor de seguridad, se debe saber claramente, que dependiendo del tipo y valor que tenga la información, mayor empeño tendrán los atacantes para ingresar al sistema.

Se debe tener activos los servicios justos y necesarios para cumplir con el objetivo del servidor de seguridad, teniendo en cuenta instalaciones innecesarias de aplicaciones, así por ejemplo para un servidor de seguridad no es vital que se le instale aplicaciones para tratamiento de gráficos ni suite ofimáticas, aparte de ser innecesarias consumen el valioso y escaso espacio en disco duro.

Lo que se debe considerar como puntos importantes en la instalación y configuración del servidor de seguridad es la actualización del sistema operativo con los parches/actualizaciones recomendadas por el fabricante, instalar el antivirus corporativo (sólo para servidores), Instalar las aplicaciones/programas adicionales para prestar los servicios indicados del servidor de seguridad e Instalar el cortafuegos adecuado al sistema (iptables en Linux).(3)

Otra opción es mantener el mínimo de puertos abiertos evitando así el ingreso de usuarios no deseados a nuestro equipo.

Para controlar remotamente el servidor de seguridad se puede ingresar por medio de un terminal SSH, es el nombre de un protocolo y del programa que lo implementa, sirve para acceder a máquinas remotas a través de una red, de esta forma se asegura que los datos viajan seguros.(4)

La aplicación PUTTY, es segura para la conexión entre los diferentes sistemas operativos CentOS y Windows, ya que PUTTY, es un cliente de red que soporta los protocolos SSH y sirve principalmente para iniciar una sesión remota con otra máquina o servidor. Es de licencia libre y por su sencillez es muy funcional y efectivo con el cual se puede conectar al servidor y administrarlo.(5)

Se debe considerar una configuración muy importante el uso del conocido FIREWALL o muro de fuego, este funciona entre las redes conectadas permitiendo o denegando las comunicaciones entre dichas

redes. También un firewall es considerado un filtro que controla el tráfico de varios protocolos que pasan por el para permitir o denegar algún servicio, el firewall examina la petición y dependiendo de este lo puede bloquear o permitirle el acceso. Un firewall puede ser un dispositivo de tipo Hardware o software que se instala entre la conexión a Internet y las redes conectadas en lugar que es muy necesario para tener una seguridad efectiva.(6)

## 2.3 SEGURIDAD Y FUNCIONALIDAD DE RED

Se debe tener en cuenta que existe una relación inversa entre seguridad y funcionalidad. Tiene que decidir dónde está el equilibrio entre la facilidad de uso de su sistema y su seguridad.

### 2.3.1 SEGURIDAD

La seguridad de las conexiones en red merecen una atención especial, el propio desarrollo tanto de Linux, como de la mayoría del software que lo acompaña, es de fuentes abiertas, por lo tanto se puede ver y estudiar el código, esto tiene la ventaja que la seguridad en Linux está siendo escrutado por muchas personas distintas que rápidamente detectan los fallos y los corrigen con una velocidad asombrosa, además comprendemos los mecanismos que se siguen en las conexiones en red, y mantenemos actualizados nuestros programas, podemos tener un nivel de seguridad y una funcionalidad aceptables. (7)

### 2.3.2 FUNCIONALIDAD

Las funcionalidades de red garantizan que tus aplicaciones tengan acceso a los recursos de red necesarios y que el usuario final reciba expectativas precisas en cuanto a su acceso.

El envío de datos en la red se puede solicitar desde un cliente a un servidor, o entre dispositivos que funcionan en una conexión, donde la relación se establece según el dispositivo de origen y de destino. Los

mensajes se intercambian entre los servicios de la capa de aplicación en cada dispositivo final de acuerdo con las especificaciones del protocolo para establecer y utilizar estas relaciones.(8)

## 2.4 TIPOS DE INTRUSOS

Intruso es una persona que intenta acceder a un sistema informático sin autorización utilizando los medios a su alcance, a menudo tienen intenciones, en encontrar información reservada.

La detección de intrusos, es una ciencia relativamente avanzada, por lo que existen muy pocos sistemas operativos que incluyan herramientas para la detección de estos atacantes.

Todos estos mecanismos forman los componentes individuales de la compleja arquitectura de seguridad CentOS.

Como por ejemplo las amenazas proceden de varios tipos de intrusos, y es útil tener en mente sus diferentes características cuando esté asegurando sus sistemas.

Los diferentes tipos de intrusos que se debería tener en cuenta, para prevenir y proteger la integridad de nuestro servidor son:

### 2.4.1 EL CURIOSO

Este tipo de intruso está interesado básicamente en qué tipo de sistema y datos posee.

### 2.4.2 EL MALICIOSO

Este tipo de intruso pretenderá, hacerle caer el sistema, modificar su página web o cualquier otra cosa que le cueste tiempo y dinero recuperar.

### 2.4.3 EL INTRUSO MUY PERSONALIZADO.

Este tipo de intruso trata de usar su sistema para ganar popularidad o mala fama. Puede usar su sistema para promocionar sus habilidades.

### 2.4.4 LA COMPETENCIA

Este tipo de intruso está interesado en los datos que tiene en el sistema. Puede ser alguien que piense que tiene algo que le puede interesar financieramente o de otra forma.

## 2.5 VULNERABILIDAD

Vulnerabilidad es la exposición latente a un riesgo que se puede encontrar en la red de trabajo, en el ingreso a la gran red como es el Internet y en muchos factores que afecten la integridad de la red.

Los riesgos han evolucionado y, ahora, las instituciones deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de accesos no autorizados a los sistemas, estas herramientas con la capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.(9)

Los requisitos de seguridad se pueden resumir en una serie de puntos ilustrativos:

### 2.5.1 DISPONIBILIDAD.

Consistente en mantener la información y los recursos de acuerdo con los requisitos de utilización que pretende la entidad que utiliza la red informática. La disponibilidad de la información pretende garantizar que no se limite el acceso autorizado a la información y el correcto funcionamiento de los recursos.

### 2.5.2 INTEGRIDAD.

La información que se almacena en los sistemas o que circula por las líneas de comunicación debe estar protegida contra la modificación no

autorizada. Se requiere que la información sólo pueda ser modificada por las entidades autorizadas.

### 2.5.3 AUTENTICIDAD.

La información que se almacena o circula por una red debe permanecer protegida ante falsificaciones. La autenticidad requiere mecanismos de identificación correctos, asegurando que las comunicaciones se realicen entre entidades legítimas.

### 2.5.4 CONFIDENCIALIDAD.

Evita la difusión no autorizada de la información. Requiere que la información sea accesible únicamente por las entidades autorizadas.

### 2.5.5 NO RECHAZO.

Establecer los mecanismos para que nadie pueda negar que haya realizado una determinada comunicación. En particular, en Linux tendremos que proteger ciertos ficheros que contienen información sobre los usuarios.

## 2.6 USAR CONTRASEÑAS FUERTES

El servidor se encuentra expuesto al mundo exterior, una de las primeras cosas que podrá notar serán los intentos de los hackers, tratando de acceder para adivinar su nombre de usuario/contraseña. Un hackers canjeará los puertos de tráfico y por defecto el puerto 22 (el puerto por defecto, por el cual SSH escucha), para encontrar máquinas que estén funcionando, y entonces intentar un ataque contra éstas.

Con contraseñas fuertes en su lugar, felizmente cualquier ataque será registrado y notificado antes de que pueda tener éxito. Si usted no está utilizando contraseñas fuertes, trate de escoger combinaciones que contengan:

- 8 Caracteres como mínimo
- Mezcle letras mayúsculas y minúsculas
- Mezcle letras y números
- Use caracteres no alfabéticos (ejemplo: !" £ $) (% ^ .)(10)

# CAPÍTULO III
# SISTEMA OPERATIVO

## 3.1 EL SISTEMA OPERATIVO CENTOS

Todos los componentes de un computador, aunque se encuentren correctamente conectados, no son capaces de realizar ninguna tarea por sí solos. Necesitan una serie de instrucciones, un soporte lógico que ponga en funcionamiento los distintos elementos y consiga que trabajen en forma coordinada para realizar las funciones que esperamos de ellos. Este tipo de programas se conocen como sistema operativo y son responsables del control de los dispositivos físicos, del proceso de almacenamiento o generación de la información y de la ejecución de las aplicaciones.

Varias de las tareas propias del sistema operativo deben ser supervisadas por el usuario. Para ello, proporciona la interfaz de usuario que permite acceder al control los dispositivos a través de la interacción con el sistema. En épocas anteriores los sistemas operativos ofrecían una interfaz de texto, sin embargo, en la actualidad es posible interactuar con el computador a través de una interfaz gráfica que permite una mejor facilidad de comunicación. El grafico 1, muestra la interacción entre el Sistema Operativo y el resto de las partes, es decir el usuario da una orden por medio de la aplicación o interfaz la cual será atendida por el sistema operativo que se encuentra controlando toda la parte de hardware y software para luego de ser procesada proporcionar un resultado al usuario.(11)


**Grafico1Interacción entre el SO con el resto de partes**

Fuente: http://es.wikipedia.org/wiki/Sistema_operativo

## 3.2 PRESENTACIÓN DEL S.O. CENTOS

CentOS es un sistema operativo gratuito, con código abierto, optimizado para Internet (utilizado por los piratas con mucha frecuencia).

La palabra CentOS, hace referencia a una cierta parte de Linux, que es precisamente su núcleo. Cabe indicar que Linux no es un sistema operativo completo como para ser instalado, los sistemas operativos que pueden ser instalados y utilizados por el usuario reciben el nombre de distribuciones tales como: CentOS, Conectiva, Debian, Fedora, Gentoo, Mandrake, RedHat, Slackware, SuSE, Turbo Linux.

CentOS tiene claras ventajas a causa de una gran activa y creciente comunidad de usuarios de soporte, actualizaciones de seguridad rápida mantenida por CentOS, dedicado equipo de desarrolladores, y el apoyo de respuesta rápida a través de la red.(12)

## 3.3 CENTOS COMO SISTEMA INDEPENDIENTE

Las fuentes del núcleo de Linux son abiertas. Cualquiera puede obtenerlas, analizarlas y modificarlas. Este modelo de desarrollo abierto, que siguen tanto CentOS como la mayoría de las aplicaciones que se ejecutan sobre él, conduce a altos niveles de seguridad, CentOS es conocido por su

alto nivel de estabilidad, que parte del propio núcleo del sistema operativo Linux.

Normalmente se necesita garantizar que el sistema permanezca en funcionamiento de forma adecuada, también garantizar que nadie pueda obtener o modificar una información que no tiene derecho legítimo, llegando a tener una buena planificación, ayuda bastante a conseguir los niveles de seguridad que se pretende alcanzar. Se debe determinar el nivel de amenaza quiere protegerse, qué riesgo está más propenso y vulnerable es su sistema. Se analiza el sistema para saber qué está protegido, saber qué valor tiene y quiénes tienen responsabilidad sobre sus datos y elementos.(13)

## 3.4 ADMINISTRACIÓN BÁSICA DE CENTOS

La seguridad de las redes se ha convertido en un fenómeno y no parece que los medios de comunicación tengan bastante información.

Este problema por la seguridad ha otorgado un interés especial a la seguridad en Internet y, por ende, a los administradores de sistemas.

### 3.4.1 LA IDEA BÁSICA

Todo el poder administrativo se otorga al root. Éste controla a los usuarios individuales, a los grupos y los archivos, y dicho control se ejerce, habitualmente, en una secuencia lógica.

Dos características muy peculiares lo diferencian del resto de sistemas que se encuentra en el mercado, la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia y el sistema viene acompañado del código fuente. El sistema lo forman el núcleo del sistema, más un gran número de programas / bibliotecas que hacen posible su utilización.(14)

## 3.5 INSTALACIÓN DEL SISTEMA OPERATIVO CENTOS

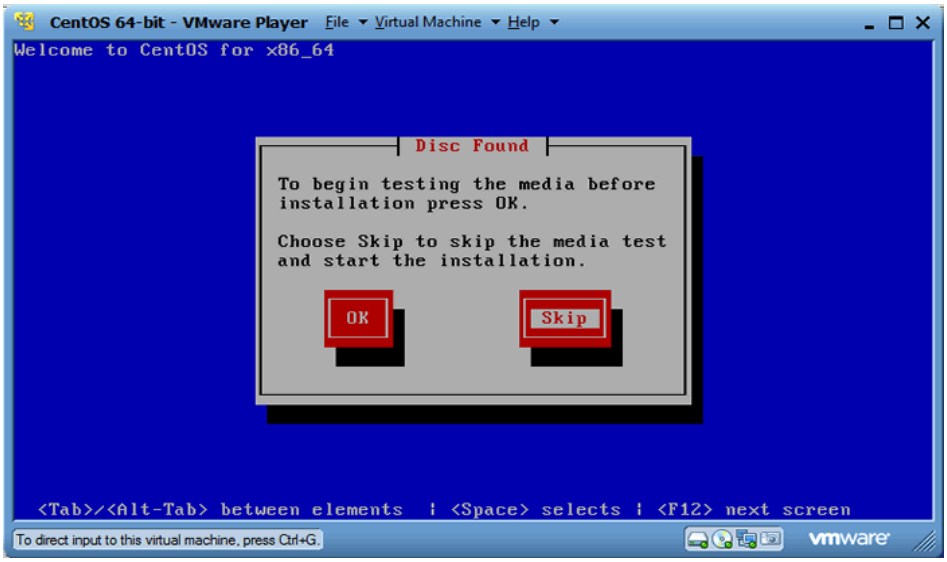
Existen varias opciones, para la instalación del Sistema Operativo CentOS, ya sea, descargando CentOS de la web, insertando disco o extrayendo el instalador de cualquier unidad de almacenamiento.

Las diferentes distribuciones de CentOS tienen distintas herramientas de instalación, algunas de estas herramientas de instalación especifican automáticamente qué servidores se activan durante el arranque, otras herramientas de instalación profundizan en los paquetes individuales, para poder seleccionar con total exactitud el software que se instala.

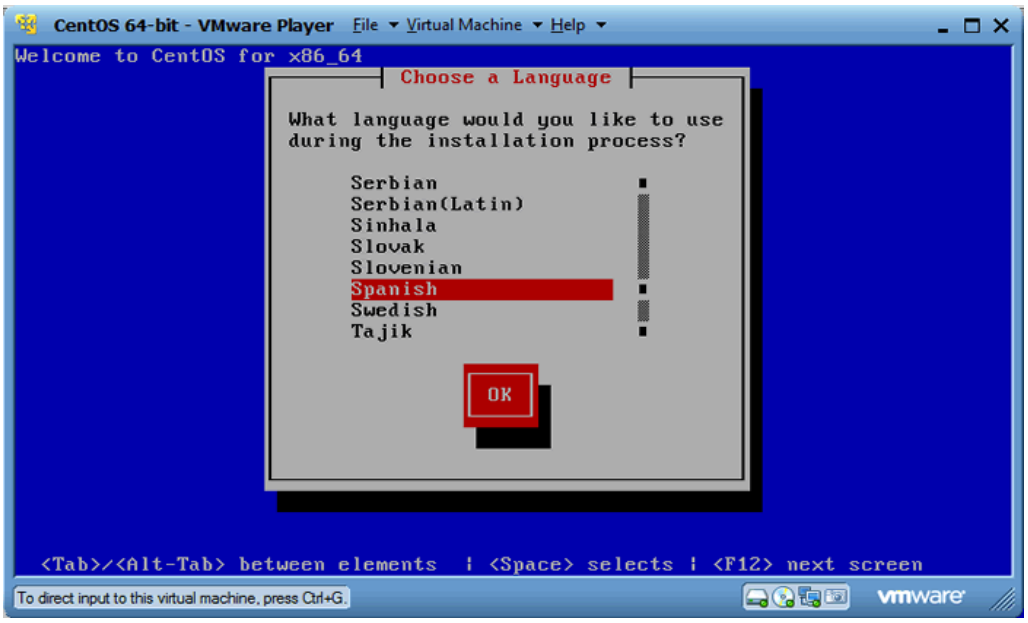
El Sistema Operativo CentOS se puede instalar ningún problema. Sólo tiene que tener conocimiento y utilizar ciertas prácticas de seguridad.

- Instalación del sistema Operativo CentOS, Insertado el dispositivo de instalación muestra a elegir la opción “si” del menú de selección, para iniciar la instalación, así como muestra la pantalla siguiente:

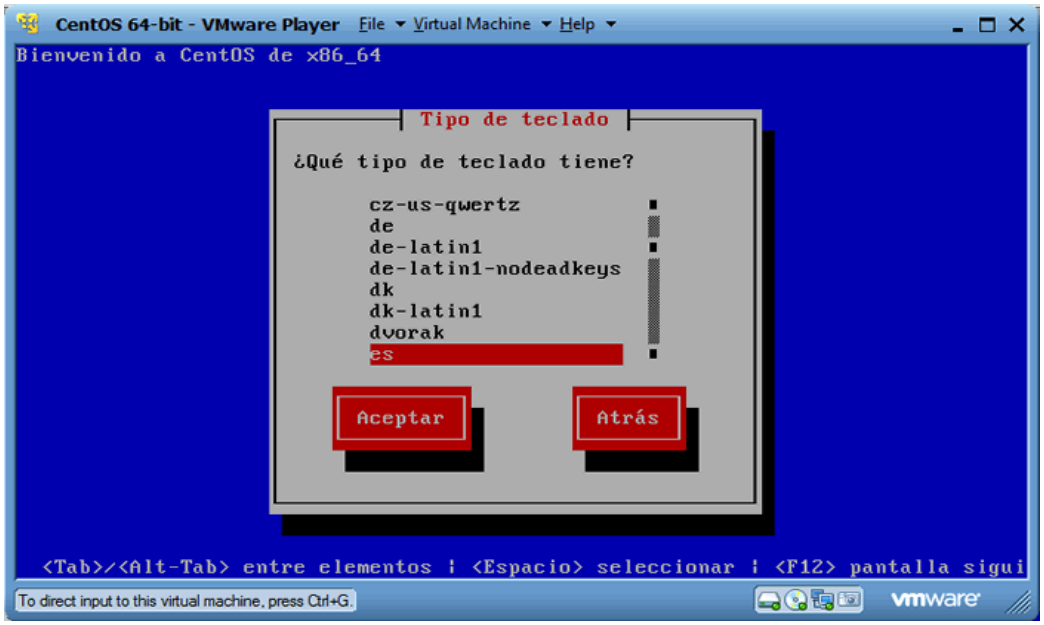
- Pedirá la verificación del medio que deseamos instalar (disco, memoria o imagen) que esté bien grabado y sin fallos: Es necesario verificar para no tener fallos posteriores en la instalación, para verificar el medio de instalación seleccionamos “OK”.



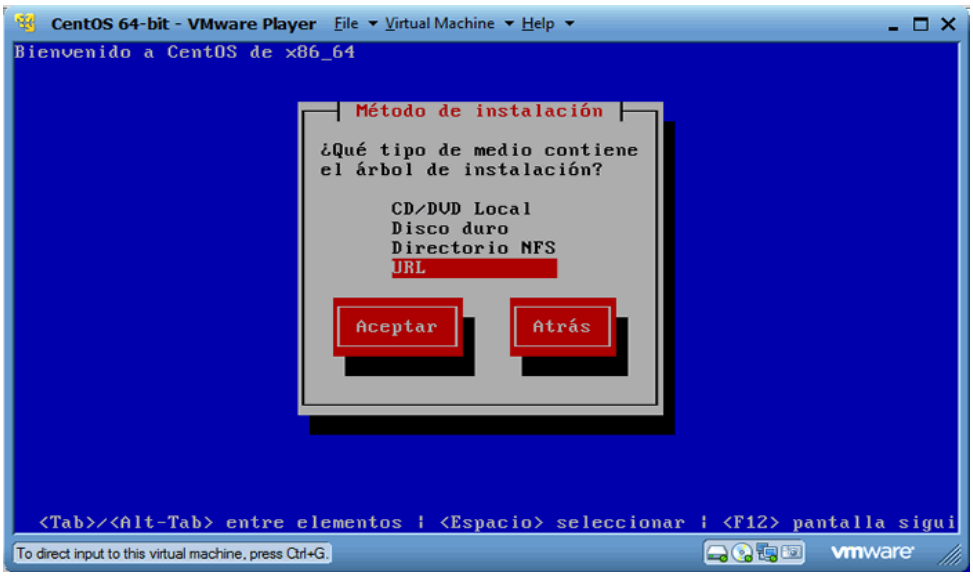
- Selección del idioma de instalación, en este caso español, clic en “OK”



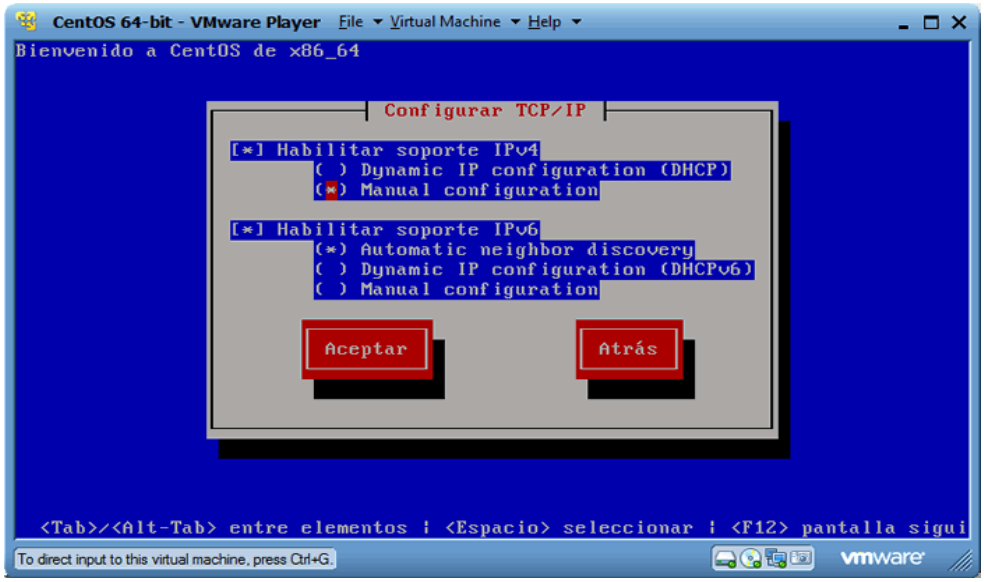

- Selección de la distribución del teclado:



- Elección del programa de instalación: CD/DVD, Disco Duro, Directorio NFS (compartir ficheros en Linux/UNIX), URL.  Clic en “URL”

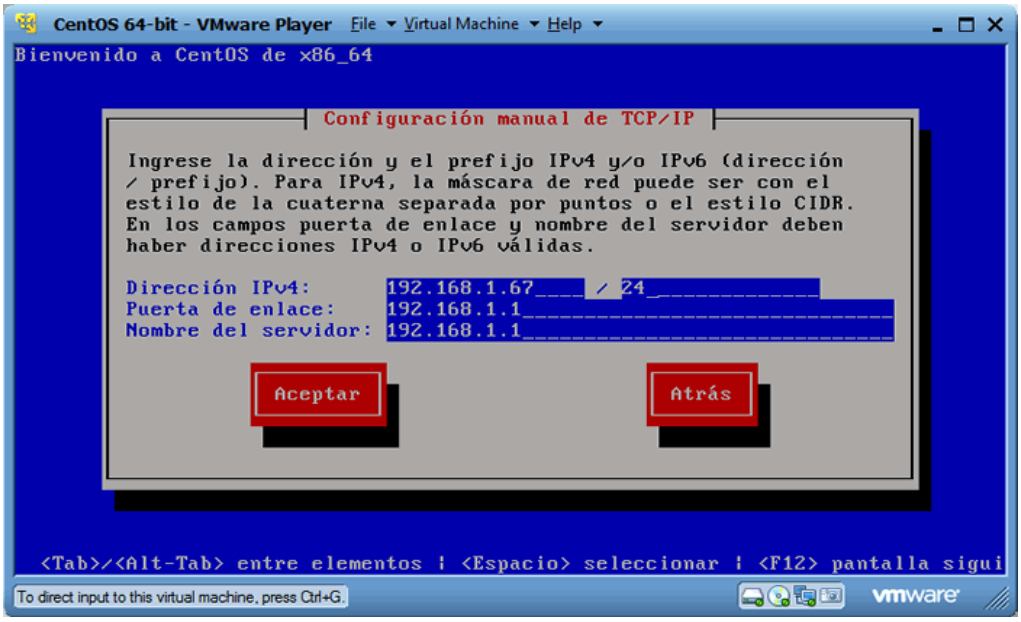



- Configurar la red para poder conectarse a un servidor y descargar los ficheros: en este caso configurar los parámetros de red de manera manual.

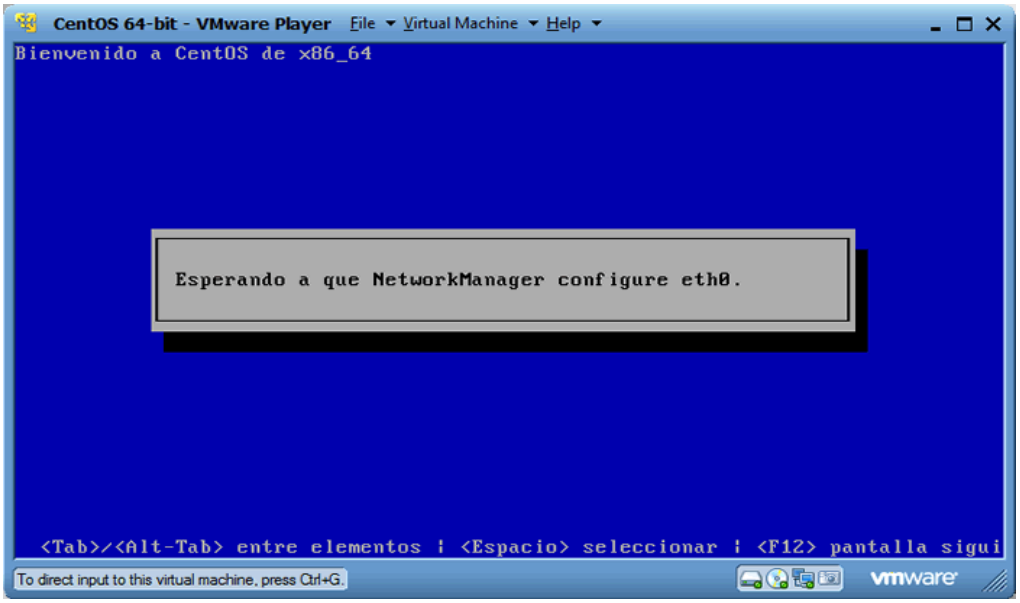


- Ingresar los datos de configuración de la red, en este caso, serán: Dirección IP = 192.168.1.67, Máscara = 255.255.255.0, Puerta de enlace = 192.168.1.1 y servidor DNS = 192.168.1.1.


- La máscara de red también puede introducirse en formato CIDR (notación /XX donde XX son los bits de la máscara de red):



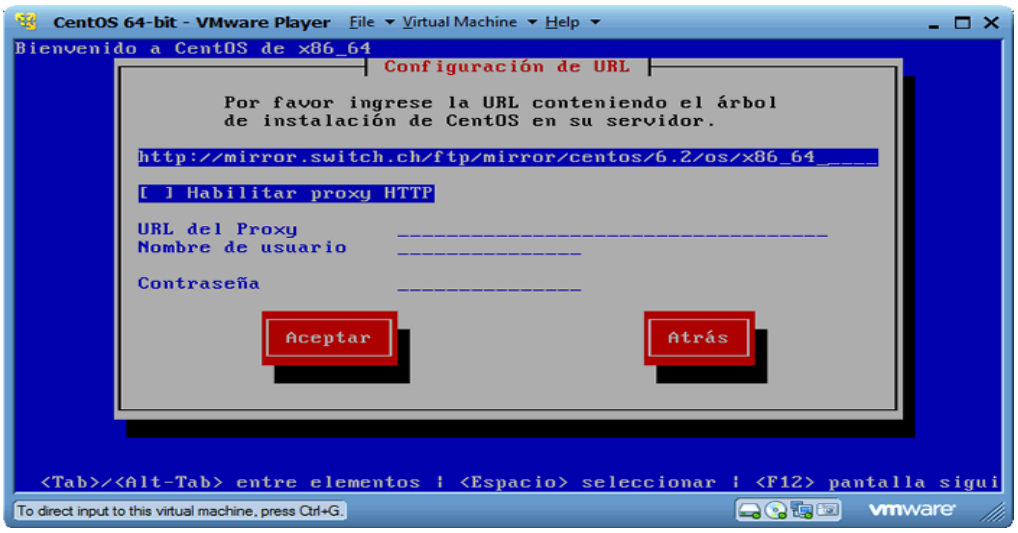
- El programa de instalación empieza a configurar la interfaz de red.



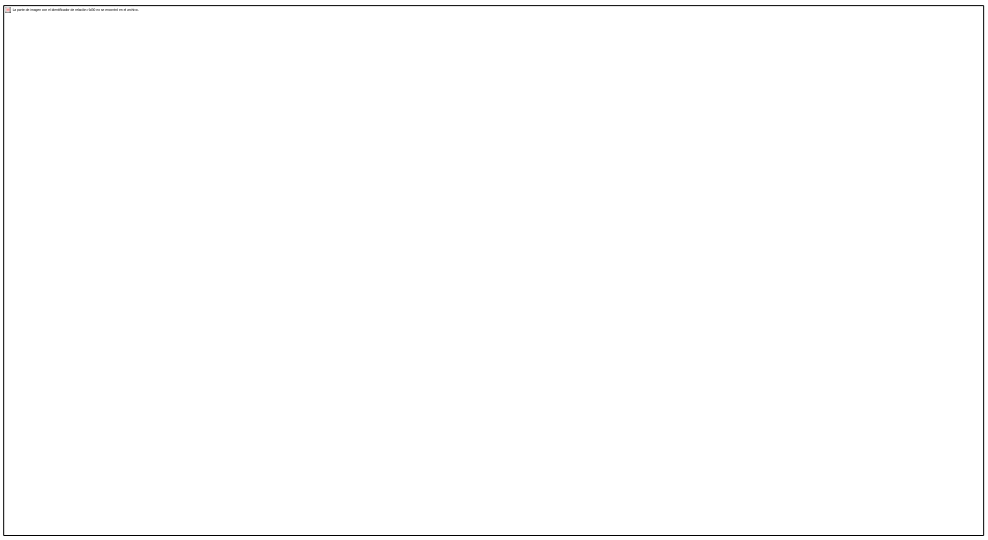

- Tomar nota de la ruta hacia el directorio "imagen" de un servidor, puede ser un servidor público o bien se puede descomprimir la ISO de instalación completa de CentOS en un servidor de la red local, y poner la ruta hacia el directorio "imagen" en dicho servidor. En este caso la ruta es:

  "http://mirror.switch.ch/ftp/mirror/centos/6.2/os/x86_64"

- Se escribe la ruta en la pantalla correspondiente, si hay que configurar los parámetros de un proxy, también se configuran aquí:



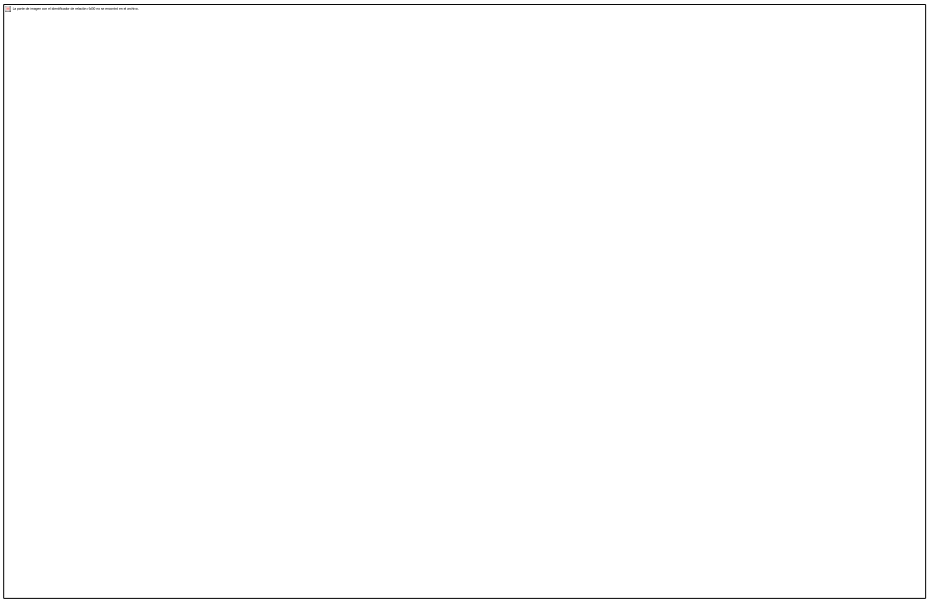

- El programa de instalación recupera los ficheros de instalación desde el servidor:



- Aparece la pantalla de instalación de CentOS:

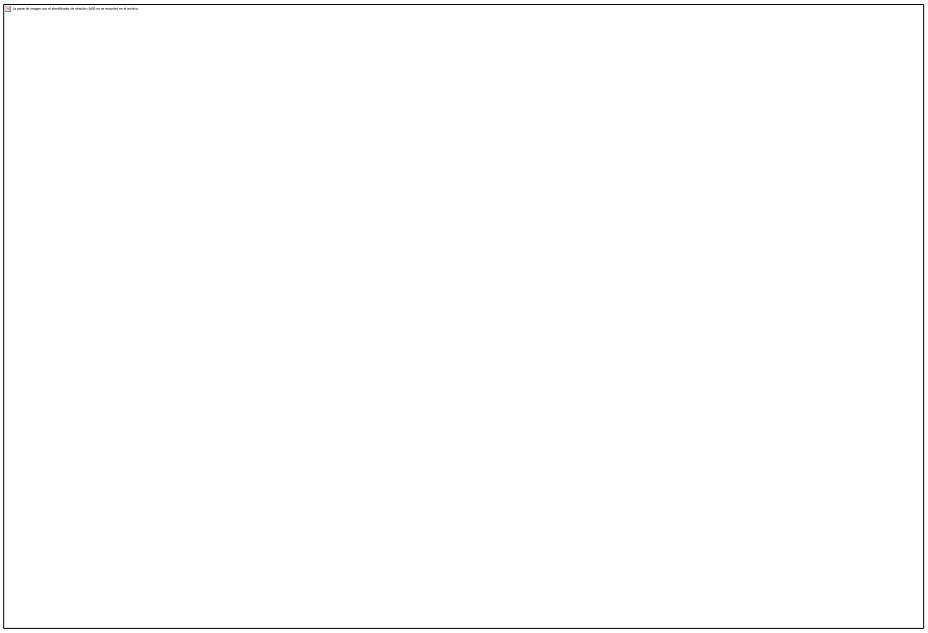
- Se elige el tipo de dispositivos de almacenamiento que tiene la máquina. y seguramente todos los que sean para experimentar, la opción a elegir será dispositivos básicos de almacenamiento:

- Pide eliminar los datos de la unidad para instalar CentOS:



- Digitar el nombre para el sistema en el cual se está instalando CentOS:

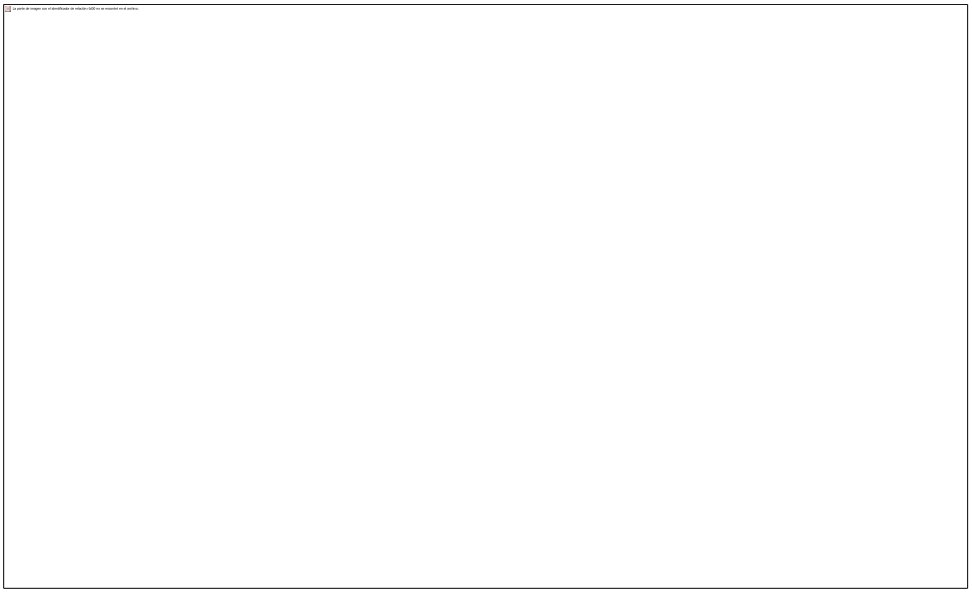
- Elegir la zona horaria: Guayaquil



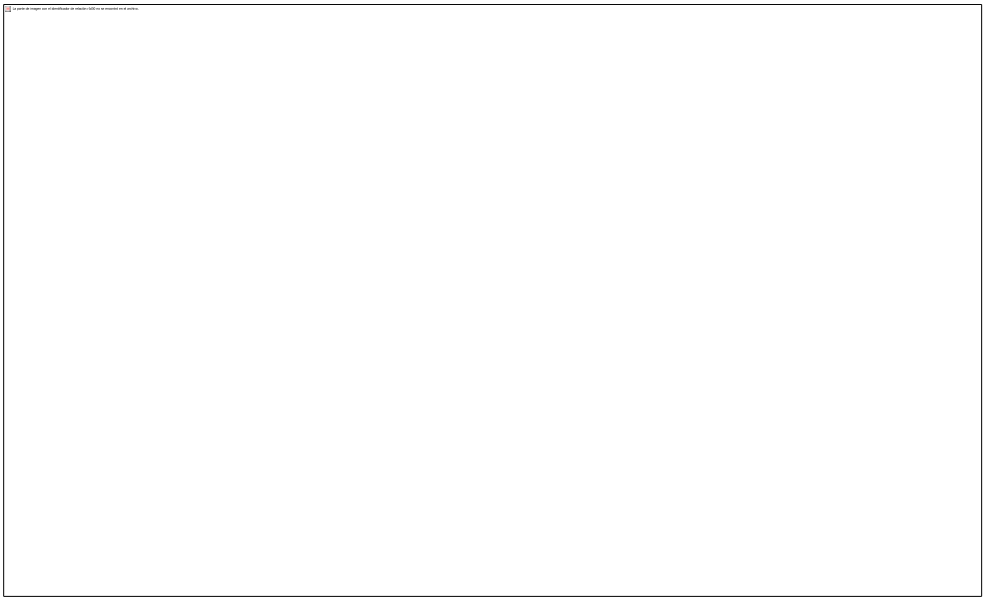
- Ingresar la contraseña del usuario "root" que será el que más privilegios tenga:

- Da opciones diferentes de partición en la unidad, elegir personalizar el esquema de particiones.

- Elegir desde la base, el espacio disponible para crear las particiones.



- Crear una partición estándar.



- Establecer el punto de montaje, tipo de sistema de ficheros, tamaño y otras opciones.

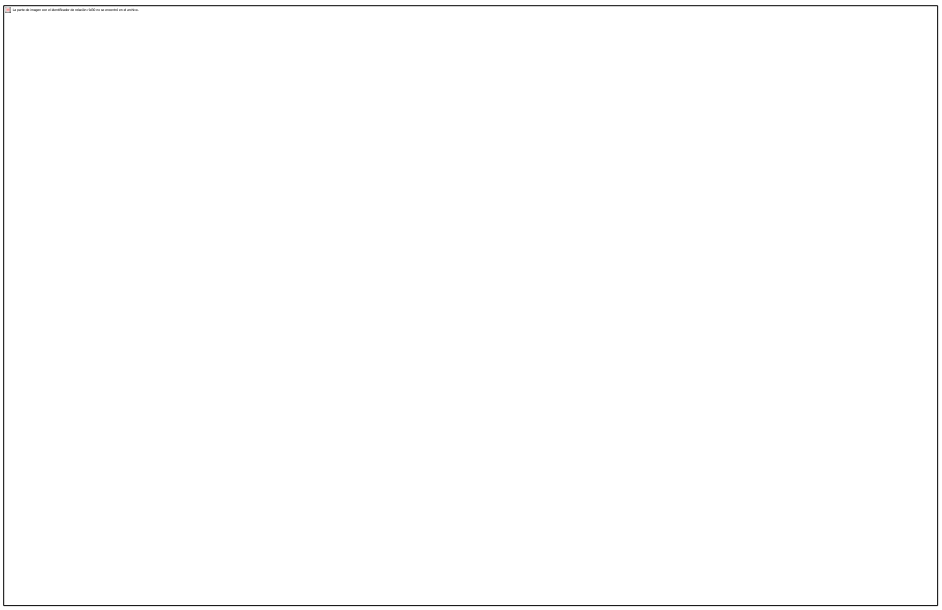
- Se crea la partición principal y de intercambio, donde se especifica la partición de intercambio en el menú desplegable de tipo de sistema de archivo.

- Informa que se formatea la partición y que se perderá los datos.

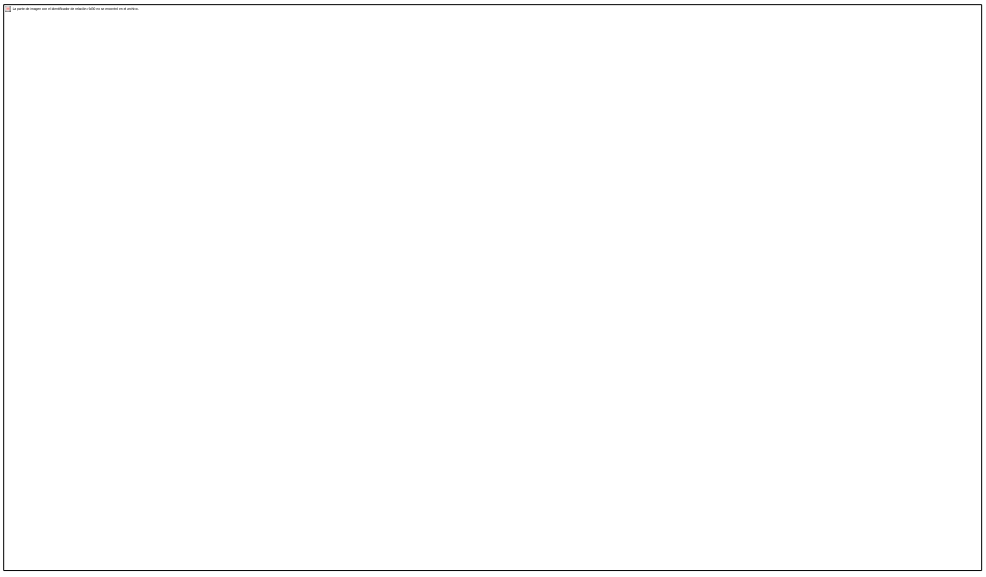
- Ya guardados los cambios se perderá cualquier dato que haya en la unidad.

- Formatea la unidad

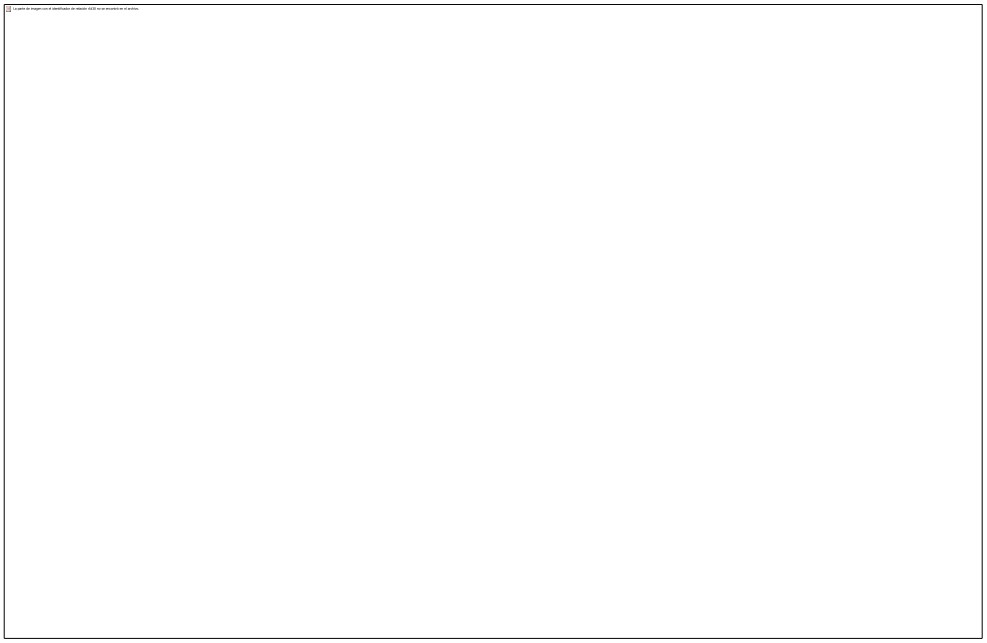
- Indica donde se instala el gestor de arranque y los sistemas operativos que aparecerán.



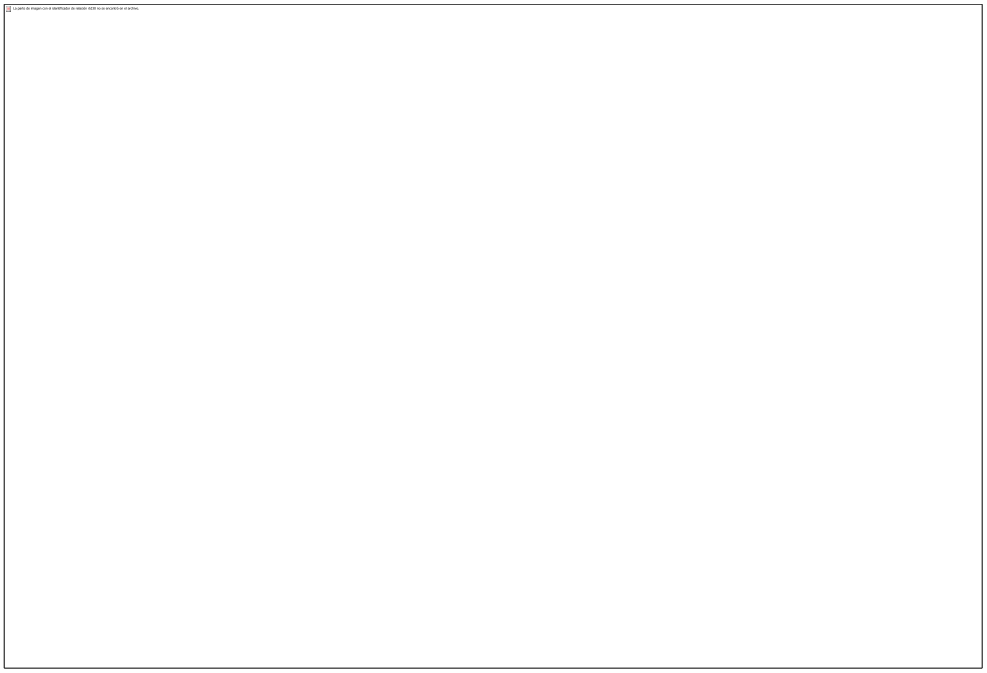
- Pide el tipo de instalación del equipo, elegir mínima para poder añadir después todo lo que quiera instalar.



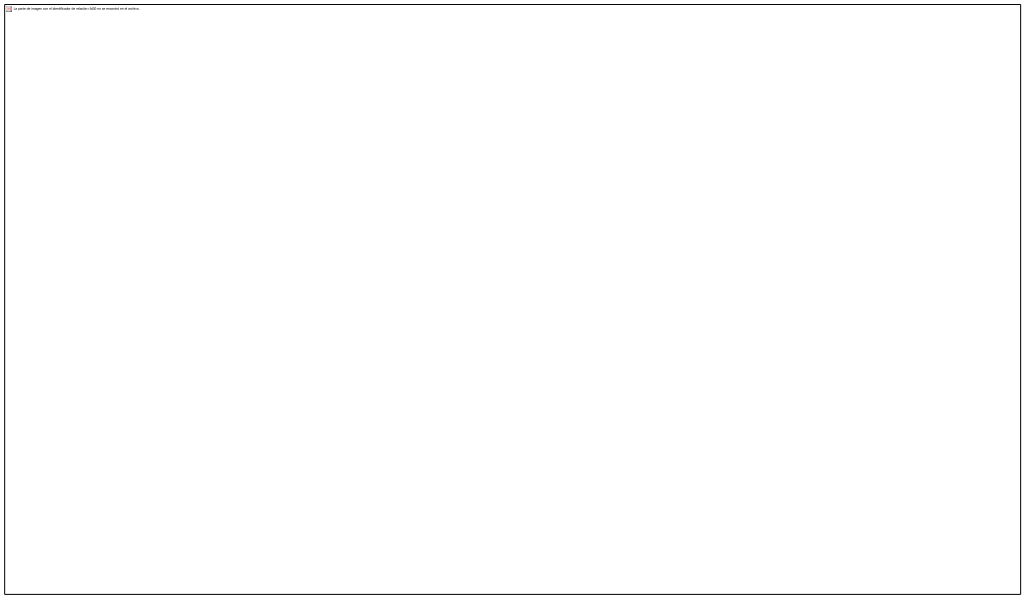
- Se inicia la instalación.



- Se copian los ficheros y se instala el gestor de arranque.

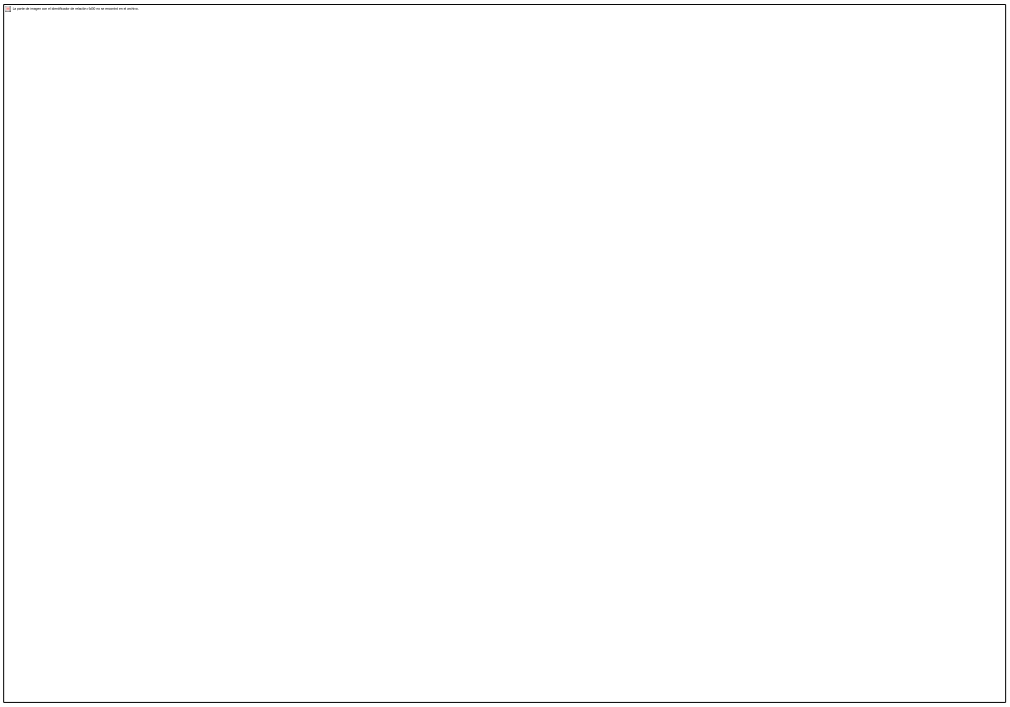


- Finaliza la instalación



- Arranca CentOS.

- Cagando el Sistema Operativo



- Aparece la pantalla de inicio de sesión

- Introducimos el usuario y contraseña para ingresar al sistema operativo CentOS.

# CAPÍTULO IV
# SEGURIDAD EN LINUX

## 4.1 SEGURIDAD EN EL ARRANQUE

Cuando se enciende la máquina, el sistema lo primero que pide es la identificación del usuario y su clave; si el usuario tiene autorización se ingresará la clave correcta, y podrá iniciar una sección para trabajar en el sistema, caso contrario no podrá tener acceso a ninguna aplicación, es recomendable cambiar periódicamente la clave de acceso.

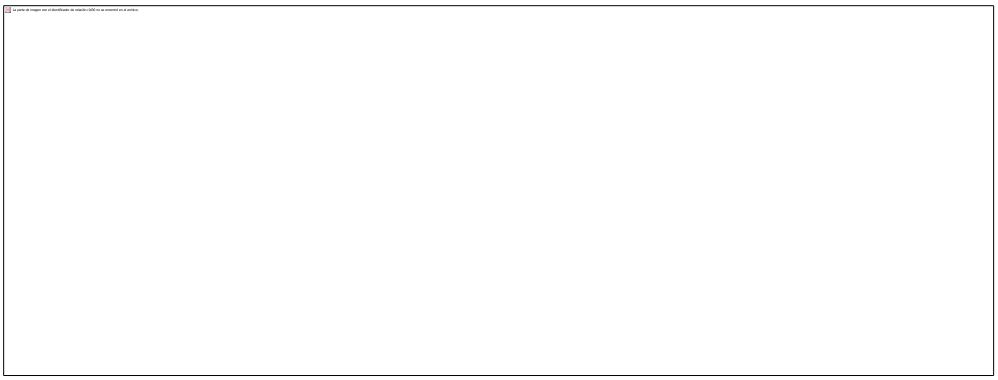
Se debe tener en cuenta que ningún sistema es realmente seguro frente a una persona que tenga grandes conocimientos en esta área, se debe tener en cuenta el tipo de personas que rodean el sitio o lugar donde se mantiene el servidor.

Se inicia la configuración del servidor de sus cuentas y usuarios que es considerada la configuración básica del sistema operativo, para su funcionamiento como servidor.

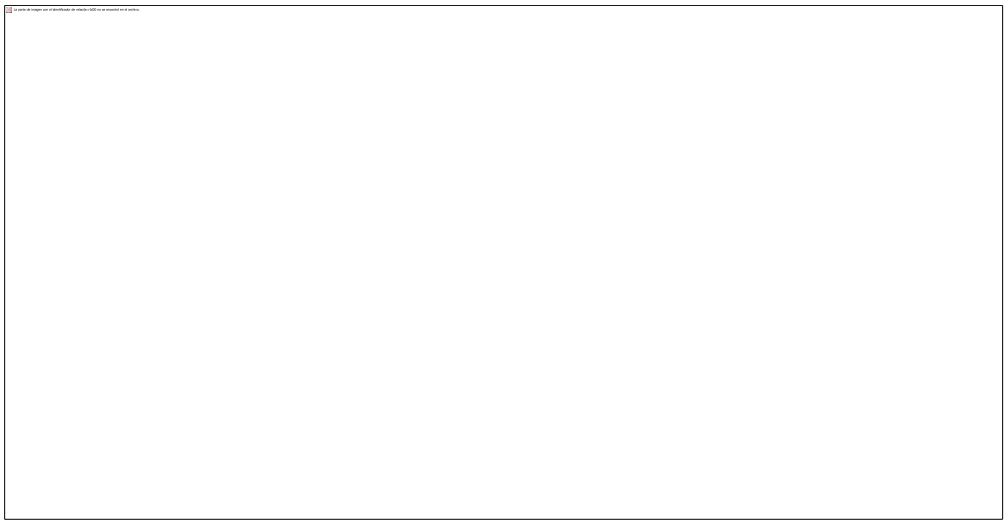
- Cuando inicia CentOS se interrumpe el inicio tecleando una vez cualquier cursor como lo muestra la imagen.

- Pulsa la tecla **e** y se ingresa a las opciones del kernel del SO.

- Se elige la segunda opción, nuevamente se ingresa **e** y se digita **Linux single**.



- Esto arroja nuevamente a la pantalla, pero ya editado el kernel por lo tanto se pulsa la tecla **b**.



- Con la tecla **b** en el paso anterior fue elegir la opción **boot** que inicia el sistema operativo, luego de esto aparece una opción **sh -3.2#** donde se coloca el comando **passwd** y el nombre del usuario a cambiar la contraseña del usuario<**root**>, luego da la opción ingresar la nueva contraseña con su confirmación.

- Asignación de contraseña y su confirmación para usuario <root>.

- Con el paso siguiente se crea el nuevo usuario junto con su password, y reinicio el S.O., con el comando **reboot**.

- Se puede iniciar al usuario **root** con la contraseña puesta anteriormente; este usuario es el principal, por lo tanto tiene acceso a todos los comandos.

## 4.2 CREANDO GRUPOS Y USUARIOS

Un usuario es un individuo particular que puede entrar en el sistema, un grupo es un conjunto de usuarios con acceso al sistema que comparten unas mismas características, de forma que nos es útil agruparlos para poder darles una serie de permisos especiales en el sistema. Un usuario debe pertenecer, al menos, a un grupo.

Es posible identificar tres tipos de usuarios en Linux:

- ***Usuario root***, también llamado súper usuario o administrador, es la única cuenta de usuario con privilegios sobre todo el sistema, tiene acceso total a todos los archivos y directorios con independencia de propietarios y permisos.

- ***Usuarios especiales***, se llaman también cuentas del sistema, no tiene todos los privilegios del usuario root, pero dependiendo de la cuenta asumen distintos privilegios de root.

- ***Usuarios normales***, se usan para usuarios individuales, cada usuario dispone de un directorio de trabajo, tienen solo privilegios completos en su directorio de trabajo.

Sólo root tiene permiso para manipular la información de los usuarios, darlos de alta, eliminarlos, etc. Para ello utiliza una serie de comandos:

- ***useradd:*** Añade un usuario al sistema.
- ***adduser:*** Añade un usuario a un grupo determinado.
- ***usermod:*** Con este podemos modificar la mayoría de los campos.

- ***chfn:*** Cambia la información personal del usuario.
- ***userdel:*** Elimina un usuario del sistema, borrando o guardando todos sus ficheros, según los parámetros que le pasemos.
- ***passwd:*** Para cambiar la contraseña del usuario, la información de expiración de la misma, o para bloquear o desbloquear una determinada cuenta.
- ***groupadd:*** Permite añadir un grupo al sistema.
- ***groupmod:*** Permite modificar la información de un determinado grupo.
- ***groupdel:*** Elimina un determinado grupo.
- ***gpasswd:*** Para cambiar la contraseña del grupo. (15)

En el ejemplo siguiente se crea un usuario ***"pepe"*** agregado al grupo de trabajo ***"cimse".***

**# *groupadd cimse***

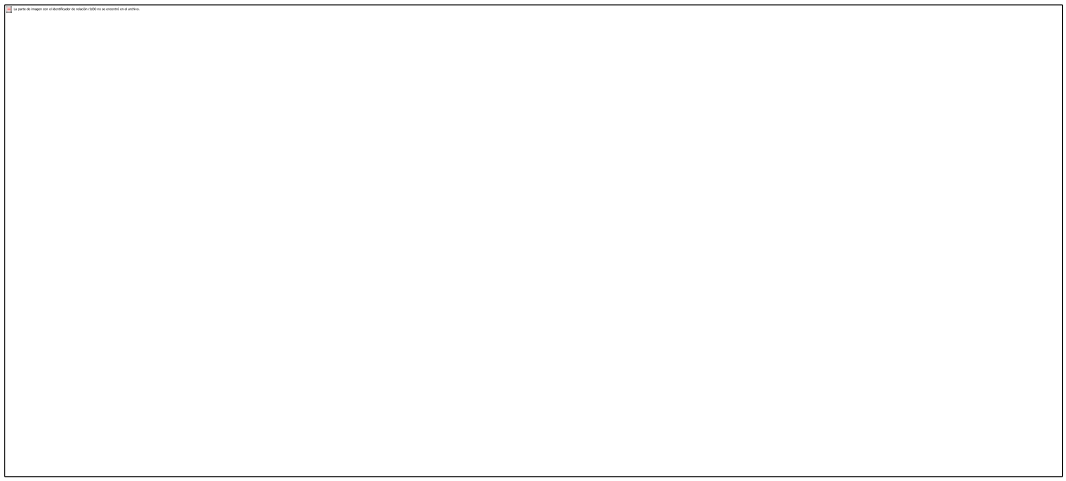
Donde ***groupadd***es el comando para crear el grupo con el nombre ***cimse***

**#*useradd pepe***

Donde***useradd***es el comando para crear el usuario ***pepe***

**#*gpasswd -a pepe cimse***

Donde ***gpasswd -a*** es el comando para asignar el usuario al grupo



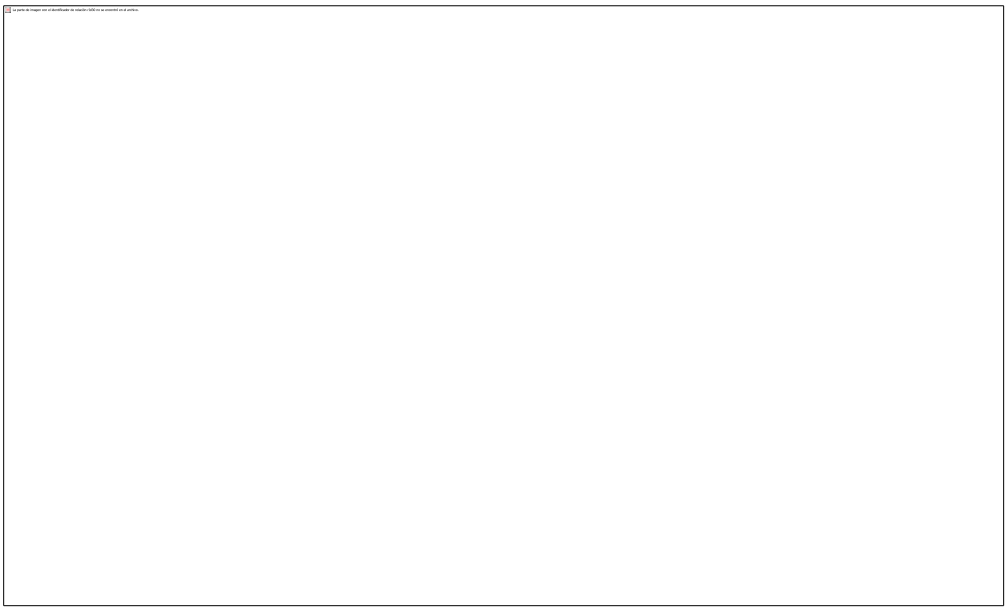
## 4.3 CREAR USUARIOSY GRUPOS EN FORMA GRÁFICA

CentOS es amigable en su entorno gráfico, facilita la creación de grupos y usuarios en una forma rápida y segura.

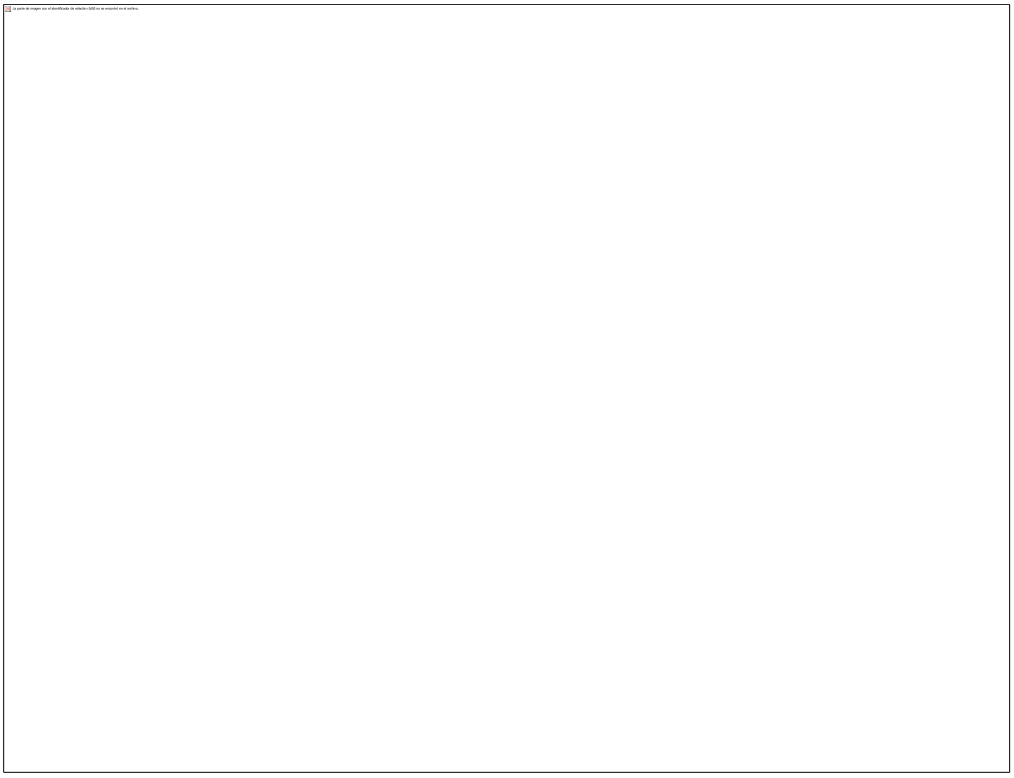
En la pantalla siguiente se muestra cómo crear grupos y usuarios en CentOS.

- Ingresar en ***sistema*** luego en ***administración*** y clic en ***usuarios y grupos.***

- La pantalla siguiente muestra los usuarios y grupos creados en el sistema, de igual forma se puede añadir usuario, añadir grupo, borrar usuarios y grupos.



- La pantalla siguiente muestra las preferencias que se puede dar a un usuario y grupo.



## 4.4 PERMISOS DE USUARIOS Y GRUPOS

CentOS es un sistema multiusuario, por lo tanto, se puede añadir, modificar, eliminar y en general administrar usuarios

Necesita de una política de permisos segura y planificada para mantener el sistema seguro. Un administrador de sistemas Linux debe prestar mucha atención y planificar dicha política de permisos para mantener su sistema seguro.

El ejemplo siguiente muestra cómo está estructurado los permisos de los usuarios y grupos.

**{T} {rwx} {rwx} {rwx} {N} {usuario} {grupo} {tamaño} {fecha de creación}{nombre}**

**1 2 3 4 5 6 7 8 9 10**

1- **{T}** En esta posición nos indica que tipo de archivo es:
**-** Si es un fichero normal
**D** Si es un directorio
**C** Especial de modo carácter (impresora...)
**P** Pipe
**L** Enlace simbólico
**2- {rwx}** Nos indica los permisos que tiene el propietario del archivo.
3- **{rwx}** Nos indica los permisos que tiene el grupo al que pertenece el archivo.
4- **{rwx}** Nos indica los permisos del resto de usuarios. (Otros)
5- **{N}** Es el número de archivos/directorios que contiene. Si es un fichero aparecerá 1, si se trata de un directorio aparecerá como mínimo 2 (los directorios '.' y '..' Más los que contenga).
6- **{usuario}** Indica el nombre del usuario al que pertenece el archivo o directorio.
7- **{grupo}** Indica el nombre del grupo al que pertenece el archivo o directorio.

8- **{tamaño}** Indica el tamaño.

9- **{fecha de creación}** Indica la fecha de creación.

10- **{nombre}** Indica su nombre.

Los grupos de permisos se agrupan de 3 en 3: **rwx**, donde (r) significa permiso de lectura, (w) permiso de escritura y (x) permisos de ejecución.

Por lo tanto un fichero con esta apariencia:

**rwx r-x ---**

Significa que tendrá permisos de lectura, escritura y ejecución para el propietario, permisos de lectura y ejecución para el grupo, y ningún permiso para el resto.

**rwxrwxrwx**

Significa que el propietario, el grupo y el resto, tendrá todos los permisos.

De igual forma CentOS brinda las seguridad en forma binaria: **rwx**, donde **r** tiene un valor de **4, w** un valor de **2** y **x** un valor de **1.**

**rwx = 7**

**rw- = 6**

**r-x = 5**

**r-- = 4**

**-wx = 3**

**-w- =2**

**--r = 1**

**--- = 0**

**Ejemplo:**

**-rwxr-xr-x 1 rootroot 3518 2006-09-19 14:38 pepe**

1- **{-}** Es un fichero normal

2-**{rwx}** El propietario tiene todos los permisos del archivo.

3- **{r-x}** Nos indica que el grupo tiene permisos de lectura y ejecución.

4- **{r-x}** El resto de usuarios tiene permisos de lectura y ejecución.

5- **{1}** Indica que es fichero.

6- **{root}** Nombre del usuario al que pertenece el archivo o directorio.

7- **{root}** Nombre del grupo al que pertenece el archivo o directorio.

8- **{3518}** Indica el tamaño.

9- **{2006-09-19 14:38 }** fecha de creación.

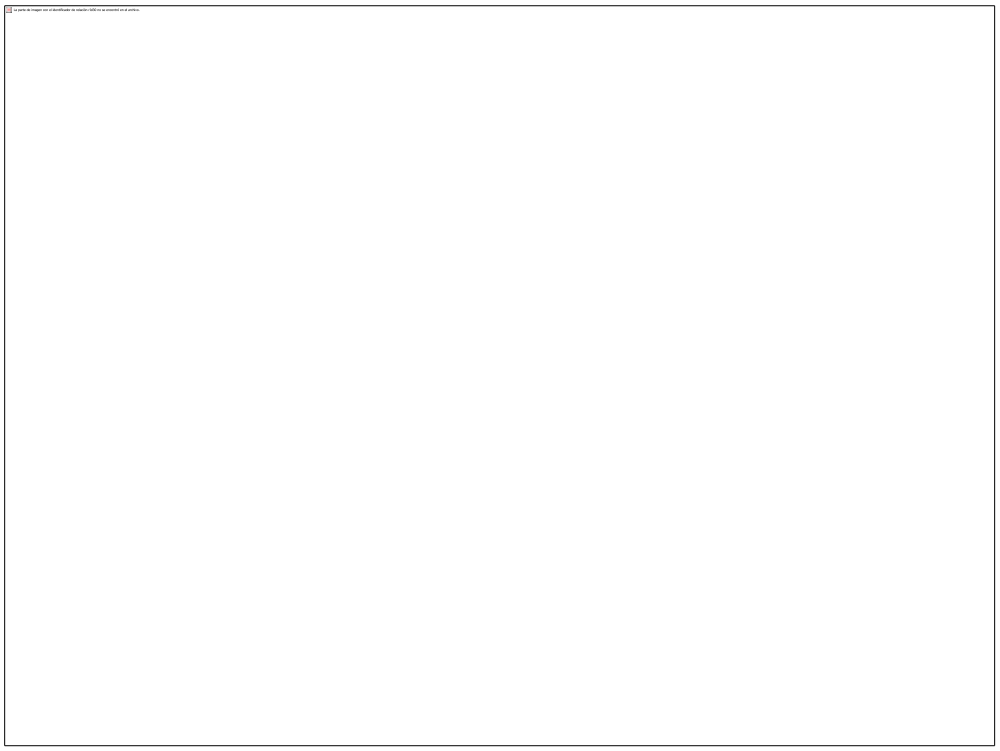
10- **{pepe}** Su nombre.(16)

## 4.5 PERMISOS DE ARCHIVOS EN EL MODO GRÁFICO.

CentOS dispone también de un ambiente gráfico, facilitando la creación de archivos y carpetas de una forma muy segura.

En la pantalla siguiente se muestra cómo crear archivos y carpetas de una forma rápida y segura.

- Se crea una carpeta con el nombre tesis, luego clic derecho en la carpeta, y escoge propiedades.



- Muestra la siguiente ventana donde se escoge la opción permisos.

- Aparece la pantalla siguiente, donde se escoge los permisos **propietario, grupo y otros.**

  **-Propietario:** se escoge el usuario donde pertenece la carpeta o archivo.

  **-En propietario acceso a carpeta:** selecciona según el permiso que se desea dar al usuario sea Crear y borrar archivos, solo listar archivos y acceder archivos.

  **-En propietario acceso a archivos:** selecciona según el permiso de los archivos solo lectura y escritura.

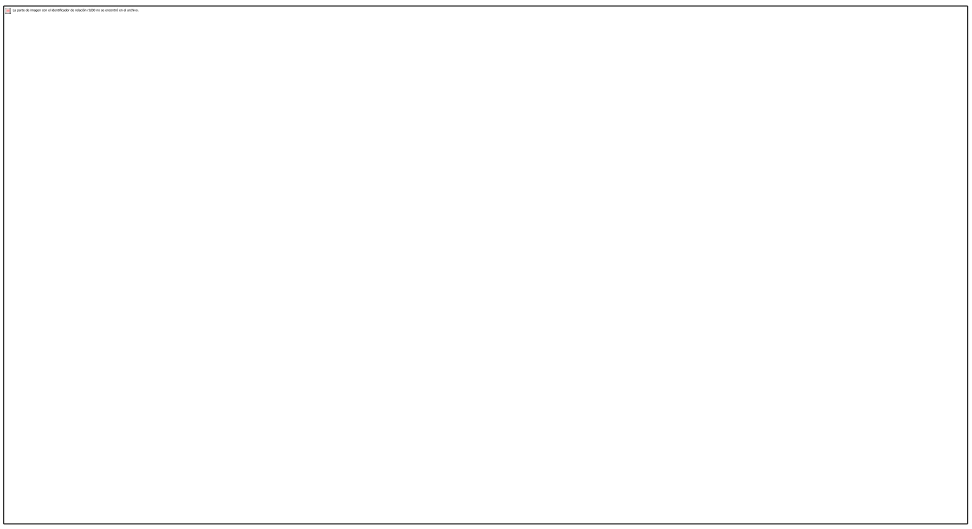
  **-En grupo:** se escoge el grupo donde se desea que pertenezca el documento.

  **-En grupo acceso a carpetas:** seleccionar según los permisos de seguridad: ***Ninguno*****, *Solo listar archivos, Acceder a archivos crear y borrar archivos.***

  **-Otros:** En acceso a carpetas se encuentra, ***Ninguno, Solo listar Archivos, Acceder a archivos, Crear y Borrar Archivos.***

**-En otros accesos a archivos**: Igual encontramos, *N**inguno, Solo lectura, Lectura Escritura.***

- Por último aparece la opción de **ejecución,** que permite ejecutar el archivo como un programa.



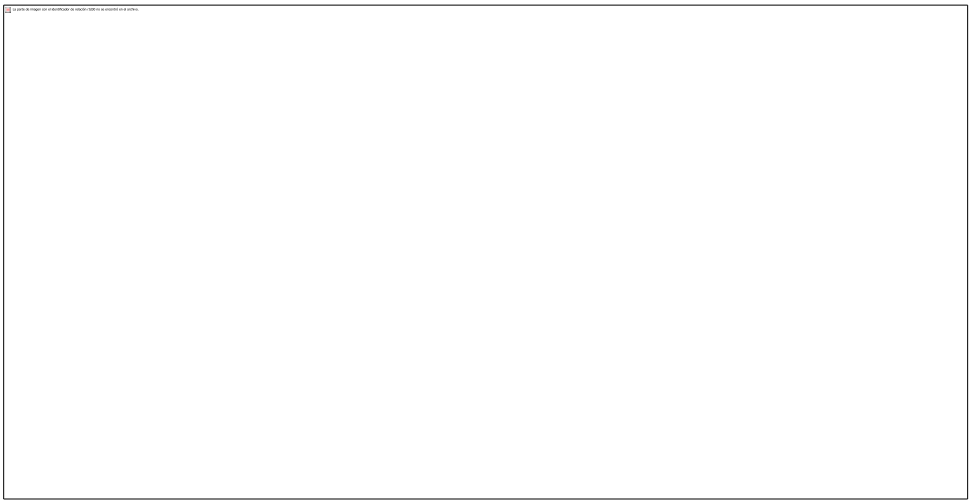
Con esta opción de permisos se puede mantener los documentos protegidos, para prevenir el mal uso de la información en los usuarios no deseados de la red.

## 4.6 FILEZILLA

FileZilla es un cliente FTP multiplataforma de código abierto y software libre, licenciado bajo la Licencia Pública General de Linux. Soporta el protocolo FTP.

Para el uso de sus archivos compartidos desde Windows se ha utilizado el programa **FileZilla** el cual nos permite acceder a los documentos de acuerdo a sus permisos asignados por el administrador, como muestra en las siguientes pantallas.

- Pantalla de conexión al servidor de archivos:



- Pantalla de trabajo de acuerdo a sus permisos:

## 4.7 FIREWALL EN CENTOS 6

Un cortafuego es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Cualquier computadora conectada directamente a una conexión del internet debe ejecutar un cortafuego para proteger contra la actividad desconocida.

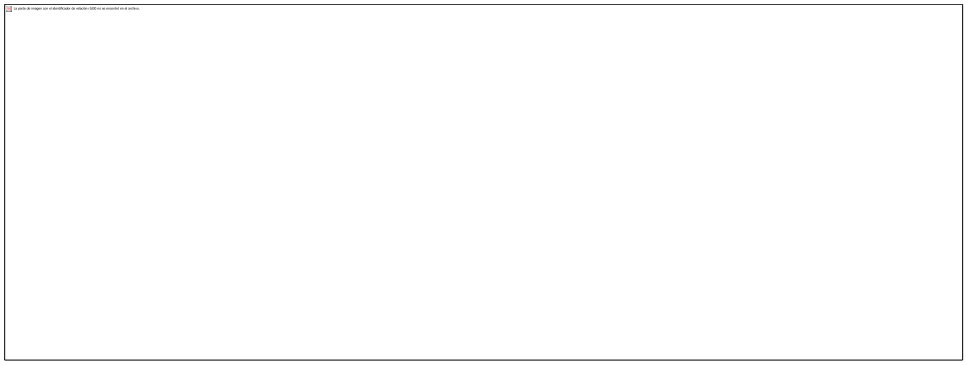
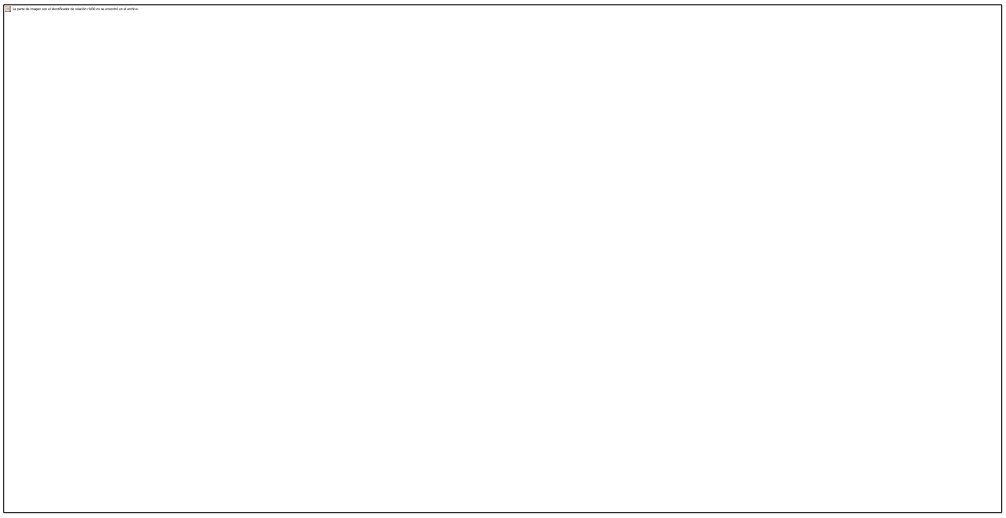


**Grafico2 Esquema de un Firewall**

http://s0.cyberciti.org/uploads/faq/2012/12/centos-firewall-shorewall.png

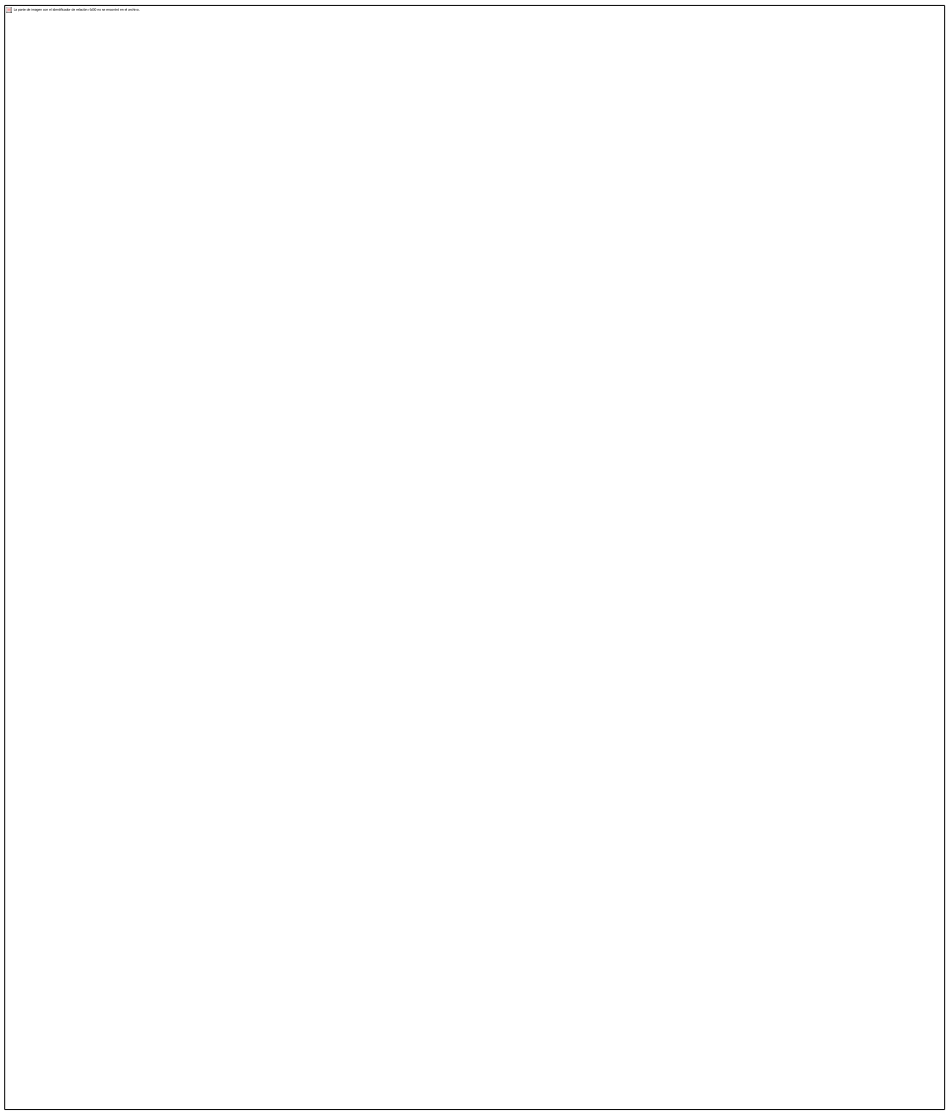
CentOS 6 se proporciona con la tecnología del cortafuego poderosa conocido como el iptables incorporado. Proporciona algunas herramientas que hacen la configuración del cortafuego fácil para el medio usuario. (17)

- CentOS, por su entorno gráfico es un sistema operativo muy amigable para el usuario, en la pantalla siguiente se muestra la forma de ingresar a la configuración del cortafuegos.



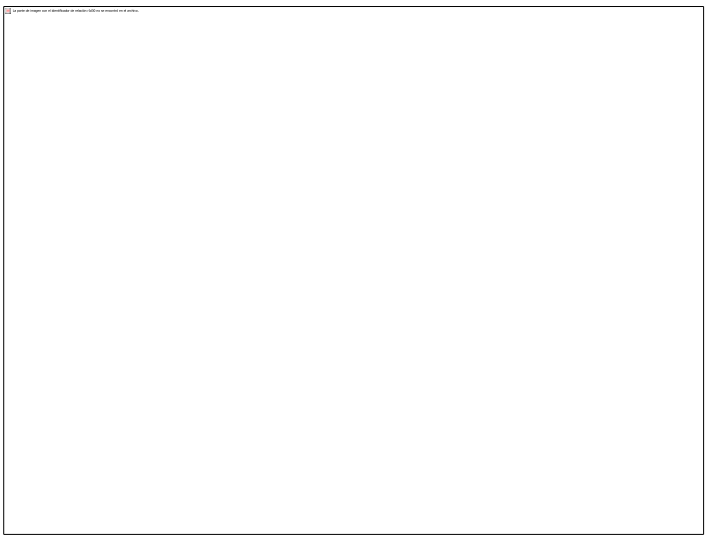
- En la pantalla siguiente se muestra las opciones de ***Habilitar y Deshabilitar*** el cortafuegos, donde la opción ***Habilitar***, es para dar protección al servidor.

- Clic en la opción ***Servicios Confiables*** donde se desplegara todos los servicios disponibles en el servidor, estos servicios serán accesibles desde todos los equipos que estén en la red, la pantalla siguiente muestra los servicios disponibles que se encuentran en CentOS.

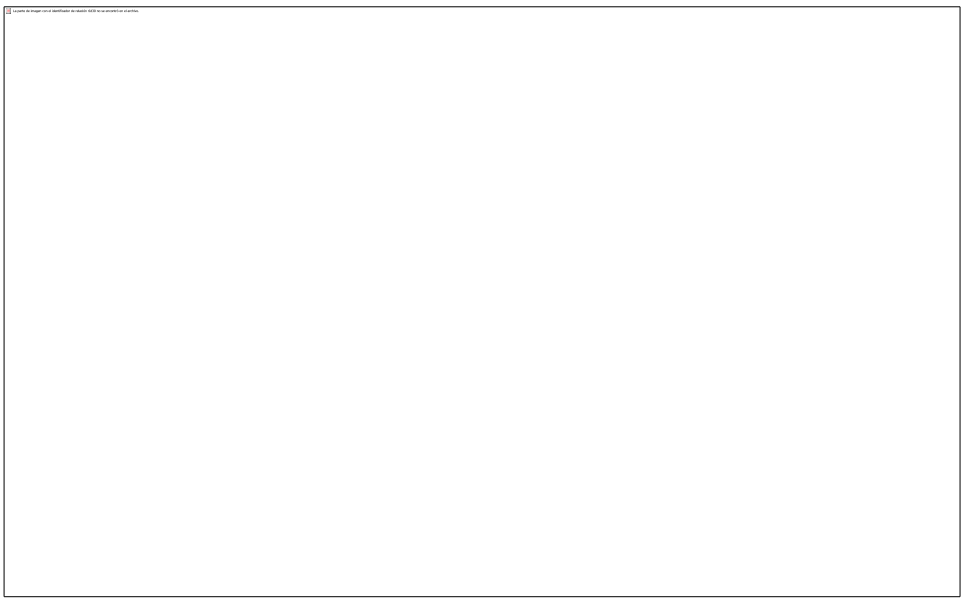


- La opción ***Otros Puertos***, es muy importante, se puede agregar puertos adicionales o rango de puertos que necesitan ser accesibles desde todos los equipos o redes, la pantalla siguiente muestra cómo se puede agregar otros puertos necesarios por el usuario, clic en otros puertos y luego en añadir.

Luego de hacer clic en ***añadir***, se muestra la siguiente pantalla donde muestra todos los puertos adicionales disponibles para el servidor.



- La opción ***Interfaces Confiables*** muestra todas las interfaces que deban tener acceso completo al sistema, la pantalla siguiente muestra las interfaces disponibles para el servidor.



- La opción ***Enmascarado,*** permite que la red local no sea visible, que se muestra el equipo como uno solo, la pantalla siguiente muestra las interfaces que dispone el cortafuegos para su configuración.

- La opción de ***Filtro ICMP*** (Protocolo de Control de Mensajería de Internet) se usa principalmente para enviar mensajes de errores entre computadoras en la red, por ejemplo los pedidos de ping y sus respuestas.

- La opción ***Archivos de reglas Personalizadas*** se usa para agregar reglas adicionales al cortafuego del servidor, la pantalla siguiente muestra todas las reglas disponibles.

## 4.8 SNIFFERS WIRESHARK

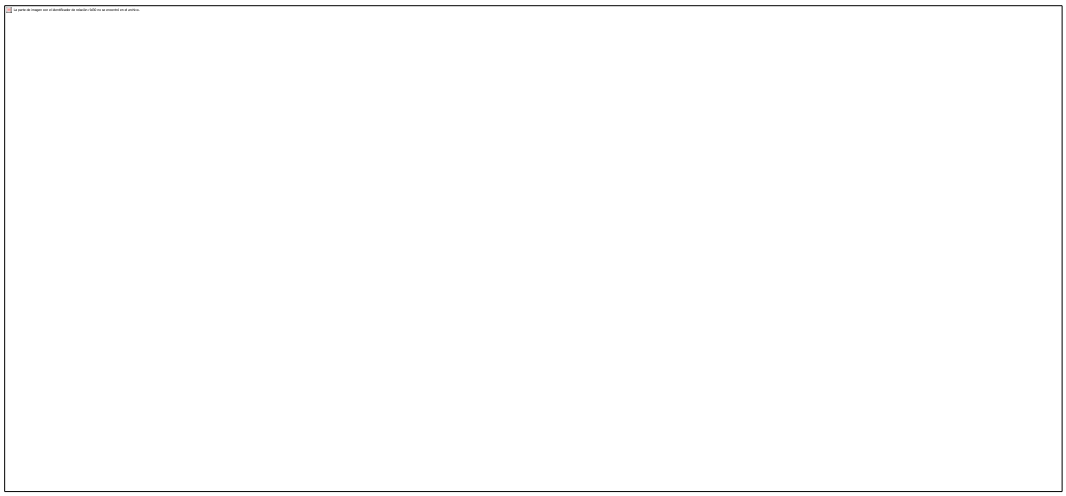
Wireshark, es un analizador de protocolos, utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, también se puede utilizar como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

La funcionalidad añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, esta herramienta permite ver el tráfico que pasa a través de una red Ethernet, aunque es compatible con algunas otras, estableciendo la configuración en modo promiscuo.

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete, incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.(18)

- Para instalar aplicación Wireshark se ejecuta el comando:
  **# yum install wireshark -gnome**
- Para iniciar Wireshark en modo grafico mediante consola se digita:
  **# Sudo Wireshark**

- En la siguiente pantalla se muestra la interfaz gráfica de Wireshark y su funcionamiento.



## 4.9 UTILIZANDO SSH EN EL SERVIDOR

SSH, es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. SSH se ha convertido en el estándar para el acceso remoto, remplazando al protocolo telnet. SSH ha hecho que los protocolos como telnet sean redundantes, en su mayoría, por el hecho de que la conexión es encriptado y las contraseñas no son enviadas en texto plano para que todos la puedan ver.

Por lo tanto este servicio convierte a su servidor como un equipo altamente protegido y libre de interrupciones por usuarios no deseados en red.

Inicia la configuración del servicio de SSH, para conseguir una seguridad altamente efectiva.(19)

## 4.10 USAR UN PUERTO NO-ESTÁNDAR

Normalmente el SSH escucha las conexiones entrantes en el puerto 22. Un programa malicioso determina, si SSH se está ejecutando en su máquina, y más probable es que escanee el puerto 22.

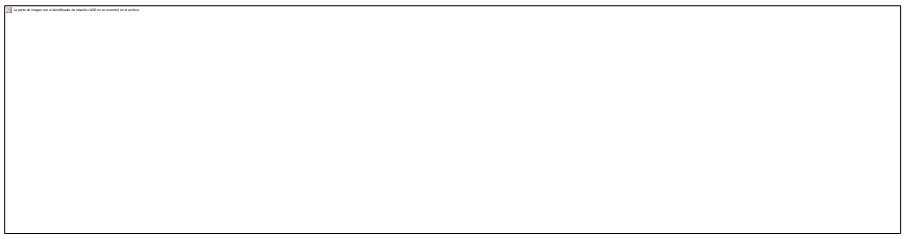
Lo seguro es ejecutar SSH en un puerto no-estándar, esto quiere decir que se puede cambiar el número de puerto, cualquier puerto se puede usar y funcionará, pero es preferible usar uno por encima del 1024, se puede escoger el 7634 como un puerto alternativo. Cualquier programa malicioso escaneará el puerto 22. Es mejor escoger cualquier puerto alto al azar que no sea usado por ningún servicio conocido.(20)

- La instrucción siguiente muestran cómo se puede configurar el puerto SSH para que no sea estándar, para hacer los cambios, añada la siguiente línea en el terminal del CentOS.

***/etc/ssh/sshd_config***

***# vissh /sshd_config***

- En la pantalla siguiente muestra cómo se cambia el número de puerto, en este caso se cambia el 22 por 7634.



Luego iniciar el servicio SSHD. Con el siguiente comando:

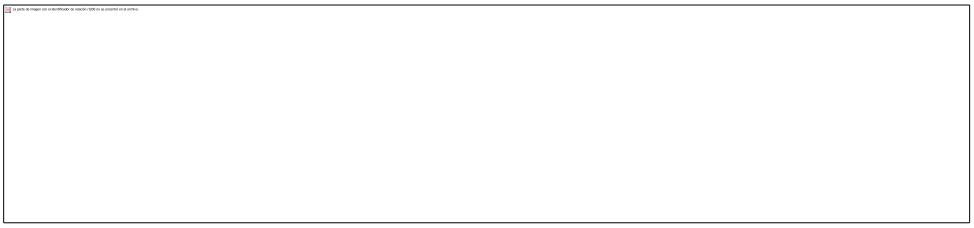
**#service sshd start**

## 4.11 UTILIZANDO EL SERVICIO DE FAIL2BAN

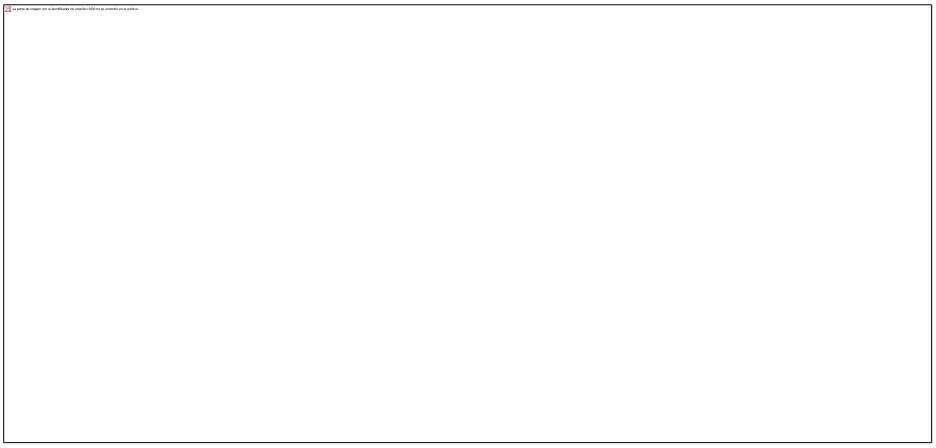
El Fail2Ban es un analizador que busca intentos fallidos de ingreso al servidor y bloquea las IP’s de donde provienen estos intentos. Se distribuye bajo la licencia Linux, funciona en todos los sistemas que tengan interfaz con un sistema de control de paquetes o un firewall local.

Fail2Ban tiene una gran configuración pudiendo, además, crear reglas para programas propios o de terceros.

Para su funcionamiento se inicia la instalación del comando ***python*** que nos ayuda para la configuración delanalizadorFail2Ban, la siguiente ventana muestra como instalar mencionado comando.(21)
Digitando en el terminal de CentOS la línea:
***# yum install python***



- Las pantallas siguientes nos indica como levanta los servicios del comando python.



## 4.12 INSTALANDO EL FAIL2BAN

Se inicia instalando el servicio Fail2ban digitando la siguiente línea en el terminal de CentOS.

***# yum –y install fail2ban***

*Una vez instalado se debe levantar el servicio digitando el terminal el siguiente código.*

***# service fail2ban start*** *.-Inicia el servicio*

***# chkconfig fail2ban on.****- Para que se ejecute al arranar el equipo*

La pantalla siguiente muestra cómo se inicia los servicios de **fail2ban**

Se ha instalado **Fail2Ban** en /usr/share/fail2ban, los scripts se encuentran en /usr/bin.

Ahora se configura **Fail2Ban** para que analice los intentos de ingreso fallidos, y sean enviados por notificaciones vía e-mail.

- Para ello editamos con el comando **vi** el archivo **jail.conf** que se encuentra en **/etc/fail2ban**.
- El siguiente script indican el estado actual del archivo que se debe modificar y guardar.

  **[ssh-iptables]**
  **enabled = false**
  **filter = sshd**
  **action = iptables[name=SSH, port=ssh, protocol=tcp]**
  **sendmail-whois[name=SSH, dest=you@hotmail.com,**
  **sender=fail2ban@mail.com]**
  **logpath = /var/log/sshd.log**
  **maxretry = 5**

- El siguiente script indica cómo queda el archivo ya modificado, listo para ser utilizado.

**[ssh-iptables]**
**enabled = true**
#la línea anterior se activa como verdadero para su reconocimiento del archivo
**filter = sshd**
**action = iptables[name=SSH, port=22, protocol=tcp]**
**sendmail-whois[name=SSH,** dest=jorvichr@yahoo.es,
#la línea anterior es donde se debe ingresar el correo del administrador del servidor en este caso es jorvichr@yahoo.es
**sender=fail2ban@mail.com]**
**logpath = /var/log/ secure**
# la línea anterior indica que log controlar es el log secure o seguridad
**maxretry = 3**
# la línea anterior indica los intentos que puede hacer el intruso para ingresar al servidor en este caso son 3 intentos
**bantime = 36000**
#la línea anterior muestra el tiempo en segundos que la ip se queda bloqueada.

- La siguiente pantalla muestra cómo debe quedar el archivo **jail.conf,** ya editado.

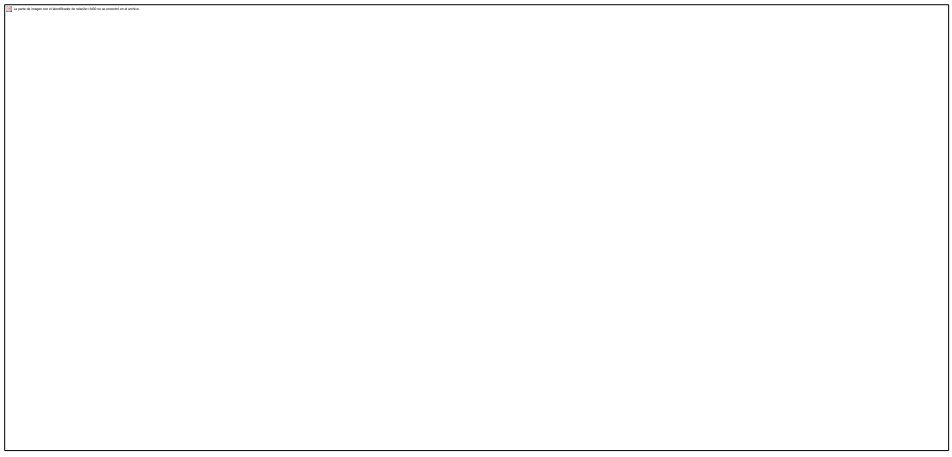
- Ahora ya se puede iniciar el servicio digitando:

  **# service fail2ban start**.

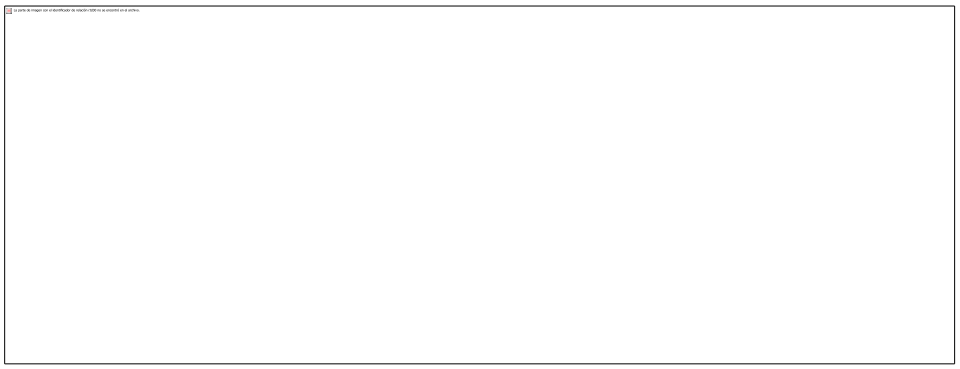
- Para que inicie el servicio automáticamente cada vez que se inicia el equipo, se usa el comando:

  **# chkconfig fail2ban on**

- La pantalla siguiente muestra los mensajes que envía el servidor al correo indicado. **Protocolos iniciados.**



- En la siguiente pantalla muestra los protocolos que se han pausado al finalizar el servidor.



# CAPÍTULO V
# CONCLUSIONES Y RECOMENDACIONES

## 5.1 CONCLUSIONES

El presente proyecto ha terminado con las siguientes conclusiones, en base a la investigación y la experiencia adquirida personalmente.

- La implementación de un servidor de seguridad con el sistema operativo CentOS, permite analizar el procedimiento para configurar adecuadamente el software y brindar todos los niveles de seguridad, para garantizar más protección y confianza de su información.

- La configuración del sistema operativo CentOS ha permitido implementar un servidor de seguridad a nivel de permisos de usuarios, permisos de archivos, configuración de corta fuegos, para evitar acceso desde redes externas, vaneo de ips y control de puertos.

- El respectivo análisis e implementación del servidor, permite tener el control de la infraestructura que debe tener un servidor de seguridad, esto es memoria, procesamiento, almacenamiento, componentes de red, entre otros, los cuales en conjunto brindan las garantías suficientes para poder optimizar la seguridad y dar protección a los archivos y todo tipo de información.

- La implementación de un servidor de seguridad permite crear ambientes de trabajo con distintos sistemas operativos como Linux, Microsoft Windows, Mac, entre otros y aplicaciones dentro de un mismo servidor y garantizar que la información se encuentra segura.

## 5.2 RECOMENDACIONES

Las recomendaciones vertidas a continuación representan las sugerencias a raíz de inconvenientes posibles en la implementación de servidores de seguridad y maneras positivas de poder expandir este crecimiento tecnológico en muchos factores de una empresa o institución.

- Es recomendable analizar y establecer un consenso entre los sistemas operativos adecuados para la implementación del servidor de seguridad, realizar pruebas y simulaciones de esta nueva plataforma para minimizar posibles inconvenientes que se presentan en el funcionamiento, teniendo fiabilidad y garantía de protección de la información de cualquier institución o empresa donde se implemente.

- Se sugiere realizar actualización del software periódicamente, a fin de continuar con la eficiente seguridad en la configuración de usuarios, archivos, corta fuego, vaneo de ips y control de puertos, para mantener la confidencialidad de la información.

- Analizar los requerimientos de seguridad que demande la institución, a fin de implementar el servidor de seguridad adecuado, debe ser parametrizable a necesidades futuras para que el sistema operativo no llegue a su límite de utilidad.

- Implementar un servidor de seguridad que permita garantizar el intercambio de información entre usuarios de distintas plataformas de trabajo en la institución o empresa, ayudando así a optimizar la reutilización de recursos informáticos, pero garantizando los niveles de seguridad a nivel de usuarios y servicios.

# REFERENCIAS BIBLIOGRÁFICAS


| | |
|---|---|
| **(1)** | **ORACLE.** Java. *Java.* [En línea] 5 de Mayo de 2010. [Citado el: 10 de Abril del 2013.] http://www.java.com/es/download/faq/firewall.xml. |
| **(2)** | **ALVARES, Gonzalo.** Seguridad en Linux. *Seguridad en Linux.* [Online] 1999. [Cited: Octubre 3, 2012.] http://www.centos/Seguridad en Linux - Introducción.mht. |
| **(3)** | **MICRO, Trend.** Seguridad, privacidad y fiabilidad. *El blog de trend micro.* [En línea] 25 de Marzo de 2013. [Citado el: 10 de Abril de 2013.] http://blog.trendmicro.es/seguridad_en_servidor/ |
| **(4)** | **WIKIPEDIA.***La enciclopedia Libre.* [Online] Abril 22, 2013. [Cited: Abril 24, 2013.] http://es.wikipedia.org/wiki/Contrase%C3%B1a |
| **(5)** | **WIKIMEDIA.** Wikipedia la enciclopedia libre. *Wikipedia la enciclopedia libre.* [En línea] 9 de Marzo de 2013. [Citado el: 10 de Abril de 2013.] http://es.wikipedia.org/wiki/PuTTY |
| **(6)** | **CENTOS.** Avanet. [Online] Febrero 19, 2013. [Cited: Abril 17, 2013.] http://avanet.org/netfilteriptables-firewall-en-centos.aspx |

| | |
|---|---|
| **(7)** | **MARAÑON, Gonzalo Alvarez.** Seguridad de red. [En línea] 9 de Mayo de 1999. [Citado el: 10 de Abril de 2013.] http://www.iec.csic.es/criptonomicon/linux/introsegred.html |
| **(8)** | **WINDOWS, Aplicacion de la tienda.** Como establecer las funcionalidades de red. [En línea] 4 de Enero de 2013. [Citado el: 10 de Abril de 2013.] http://msdn.microsoft.com/eses/library/windows/apps/hh770532.aspx. |
| **(9)** | **MESA, Silvia.** Seguridad en redes. [Online] Abril 22, 2010. [Cited: Abril 17, 2013.] http://redesysegu.blogspot.com/2010/04/vulnerabilidades-y-amenazas.html. |
| **(10)** | **WIKIPEDIA.** La enciclopedia libre. [Online] Marzo 12, 2013. [Cited: Abril 17, 2013.] http://es.wikipedia.org/wiki/Secure_Shell |
| **(11)** | **LA ENCICLOPEDIA LIBRE**. [Online] Marzo 24, 2013. [Cited: Abril 24, 2013.] http://es.wikipedia.org/wiki/Sistema_operativo. |
| **(12)** | **USUARIOCENTOS.** Buenas Tareas. [Online] Noviembre 10, 2011. [Cited: Abril 24, 2013.] http://www.buenastareas.com/ensayos/Sistema-Operativo-Centos/3118225.html. |

| | |
|---|---|
| **(13)** | **HALL, Prentice.***Linux Maxima Seguridad.* s.l. : Edicion Especial uno, 2002. |
| **(14)** | **MARTINEZ, Rafael.** El rincon de Linux. [Online] Abril 10, 2012. [Cited: Abril 24, 2013.] http://www.linux-es.org/sobre_linux. |
| **(15)** | **NACX.** Adslayuda.com. [Online] Febrero 10, 2013. [Cited: Abril 29, 2013.] http://www.adslayuda.com/Linux-usuarios.html |
| **(16)** | **LINUX, Introduccion a.** WIKILIBROS. *WIKILIBROS.* [Online] Julio 3, 2009. [Cited: Mayo 20, 2013.] http://es.wikibooks.org/wiki/Introducci%C3%B3n_a_Linux/Archivos_y_permisos. |
| **(17)** | **BASICO, Centos.** Techotopia. *Techotopia.* [Online] Marzo 16, 2012. [Cited: Mayo 20, 2013.] http://www.techotopia.com/index.php/Basic_CentOS_6_Firewall_Configuration. |
| **(18)** | **LINUX, Seguridad en servidores.** Elastix. *Elastix.* [Online] Agosto 1, 2010. [Cited: Mayo 20, 2013.] http://indetics.com/docs/SeguridadenServidores0-8-7.pdf |

| | |
|---|---|
| **(19)** | **CENTOS, Seguridad en servidores.** Elastix. *Elastix.* [Online] Agosto 1, 2010. [Cited: Mayo 20, 2013.] http://indetics.com/docs/SeguridadenServidores0-8-7.pdf |
| **(20)** | **MARTIN, Rodrigo A.** Seguridad en Servidores Centos. *Buenas Practicas.* [Online] 03 28, 2009. [Cited: 10 8, 2012.] http://creativecommons.org/licenses/by/3.0/ |
| **(21)** | **LOPEZ, J.** Instalaciòn de programas Linux. [Online] 02 11, 2005. [Cited: 09 20, 2012.] http://es.onsoftware.com/p/instalar_programas_linux_codigo_fuente. |
| **(22)** | |

# ANEXOS

## GLOSARIO DE TÉRMINOS

**Servidor.-** Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

**Autenticidad.-** Es obrar conforme al propio ser, al propio usuario.

**Confidencialidad.-** Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado.

**Sistema operativo.-** Es un software que actúa de interfaz entre los dispositivos de hardware y los programas usados por el usuario.

**Firewall.-** Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado.

**Proxy.-** Su función es interceptar las conexiones de red que un cliente hace a un servidor de destino.

**Protocolo SSH.- (Intérprete de orden segura)** Es un **protocolo** que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor

**Root.-** Es el nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos de usuario.

**Iptables.-** Es un filtro disponible en el núcleo Linux que permite interceptar y manipular paquetes de red.

**Comando Python.-** Es un programa escrito en **PYTHON** se utiliza el **comando** input() para habilitar el teclado y que el usuario ingrese su información.

**Linux.-** Es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre similar a Unix.

**Ofimáticos.-** Es el conjunto de técnicas, aplicaciones y herramientas informáticas que se utilizan en funciones de oficina para optimizar, automatizar y otras.

**Putty.-** Es un programa que permite conectar con máquinas remotas y ejecutar programas a distancia.

**Teletipo.- E**s un dispositivo telegráfico de transmisión de datos.

**Red.-** Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos**.**

**Hardware.-** Corresponde a todas las partes físicas y tangibles de una computadora.

**Software.-** Es el equipamiento lógico o soporte lógico de una computadora digital.

**Hackers.-** Es una persona que pertenece a una de estas comunidades o subculturas distintas pero no completamente independientes.

**CentOS.-** Es un clon a nivel binario de la distribución Linux.

**Kernel.-** Es un software que constituye la parte más importante del sistema operativo.

**Wireshark.-** Es un analizador de protocolos, utilizado para realizar análisis y solucionar problemas en redes.

**FTP.-** Protocolo de Transferencia de Archivos

**FileZilla.-** Es un cliente FTP multiplataforma de código abierto y software libre.

# UNIVERSIDAD DE LAS FUERZAS ARMADAS-ESPE

# DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

## CERTIFICACIÓN

**Se certifica que el presente trabajo fue desarrollado por los señores: Jorge Vinicio Chalacán Reyes y Ruperto Iván Revelo Yépez, bajo nuestra supervisión.**

Ing. Raúl Cajas.

DIRECTOR DEL PROYECTO

Ing. Nancy Jacho.

CODIRECTOR DEL PROYECTO

Ing. Lucas Garcés G.

DIRECTOR DE CARRERA

Dr. Rodrigo Vaca

SECRETARIO ACADÉMICO