ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría En Seguridad Informática Aplicada

"ASEGURAMIENTO Y OPTIMIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL DESPLIEGUE DEL SISTEMA OPERATIVO W7 / W8 / W10 EN ESTACIONES DE TRABAJO DE UNA ORGANIZACIÓN, UTILIZANDO HERRAMIENTAS DE SOFTWARE LIBRE CLONEZILLA (IMAGEN DE DISCO DURO) Y DRBL (DISKLESS REMOTE BOOT IN LINUX) PARA CLONACIÓN EN RED POR MULTICAST."

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

HUGO IVÁN CHANG MIRANDA

GUAYAQUIL-ECUADOR

AÑO: 2016

AGRADECIMIENTO

En primer lugar a Dios por darme la bendición de haber llegado hasta esta etapa, a mi madre por los consejos y ejemplos dados a lo largo de mi vida, a mi padre por desafiarme siempre hacer más de lo que se puede, a mis hermanos por su incondicional apoyo, a mis colegas por el compañerismo, a todos mis amigos por su amistad y en especial a K. Nólivos, a mi hija Emily por su amor y a Johanna por su amor, apoyo y paciencia.

DEDICATORIA

El presente trabajo se lo dedico a mi familia, colegas y compañeros que puedan hacer un buen uso en el diario de sus actividades de TI / Soporte algunas veces engorrosas y repetitivas, este trabajo tiene como objetivo minimizar ese esfuerzo.

TRIBUNAL DE SUSTENTACIÓN

ING. LENIN FREIRE COBO

DIRECTOR MSIA

MGS. ROKY BARBOSA

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

MGS. OMAR MALDONADO

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El objetivo de este trabajo es proveer una solución o procedimiento al departamento o personal de TI en el despliegue de nuevos o actuales equipos en la organización utilizando un conjunto de mejores prácticas , conceptos de optimización del rendimiento de sistemas operativos, de seguridad de la información hardening y de herramientas de software libre para minimizar esfuerzo, recursos y tiempo, factores que normalmente son elevados en la tarea de despliegue de equipos o incidentes de seguridad con equipos comprometidos, a un mínimo costo en comparación con el de herramientas propietarias que automatizan estos mismos procesos pero a un alto costo a veces restrictivo para el presupuesto de la organización.

Una vez que se dominen los conceptos propuestos y las herramientas indicadas cada cual puede personalizar su procedimiento y ajustarlo a su realidad y su necesidad, automatizando y mejorando el tiempo de implementación, talvez el recurso más preciado en la organización.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

BIOS	Basic Imput Output System
CDROM	Compact Disk Read Only Memory
CIB	Centro Informacion Bibliotecario
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRBL	Diskless Remote Boot in Linux
DVDROM	Digital Versatile Disc Read Only Memory
ESPOL	Escuela Superio Politecnica del Litoral
GB	GigaByte
IP	Internet Protocol
ISO	es un archivo informático que almacena una copia o imagen exacta de un sistema de archivos de un disco óptico.
LAN	Local Area Network

LIVECD	es un sistema operativo almacenado en un un CD o DVD , que puede ejecutarse directamente en una computadora.
MAC	Media Access Control
MB	Mega Byte
NAS	Network Attached Storage
NCHC	National Center for High-Performance Computing
NIC	Network interface controller
PC	Personal Computer
PXE	Preboot Execution Environment
SDA	Serial Disk A, nomenclatura que usa Linux para identificar los discos
SE	Server Edition, para el caso de Clonezilla
SO	Sistema Operativo
SSH	Secure SHell
TI	Tecnologías de la Informacion
USB	Universal Serial Bus
WSUS	Windows Server Update Services
XFCE	XForms Common Enviroment

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Una de las tareas más engorrosas para el departamento de TI dentro de una organización es la renovación o actualización del sistema operativo o sus equipos de cómputo generalmente PCs, pues dependiendo del número de equipos la tarea previa es la planificación de como y cuando se puede ir realizando gradualmente esta tarea en la organización sin afectar el normal desarrollo de las actividades de los usuarios. Además se debe considerar la seguridad informática pues este tema ya no es un lujo sino una necesidad obligatoria que todo departamento de TI debe considerar e implementar en el despliegue tanto de software como de hardware evitando caer en el alto impacto de tiempo y costos para minimizar esta tarea con aplicaciones de pago.

Sin embargo combinando conceptos de seguridad, rendimiento, buenas prácticas y herramientas open source podremos diseñar soluciones a nuestra realidad, para ello revisaremos varios conceptos útiles de mejora en rendimiento, seguridad y reducción en el tiempo de despliegue de nuevos equipos o sistemas operativos en la organización con el uso de DRBL [1].

CAPÍTULO 1

GENERALIDADES

1.1. DESCRIPCIÓN DEL PROBLEMA.

El dolor de cabeza de todo departamento de TI o soporte de una organización es cuando por motivos como el plan de renovación de equipos o de migración del sistema operativo debe empezar a preparar los equipos uno por uno asegurando que estos estén óptimos para el uso del usuario final, preparando cada pc de acuerdo al perfil o área a la cual va a servir. Esto conlleva severas horas de planificación previa, configuraciones, almacenamiento, personal y muchas horas hombre para asegurar que cada equipo cumple las configuraciones adecuadas que aseguren el buen uso del equipo en la organización y que no sea blanco de ataques informáticos externos e internos. En un escenario real la preparación de un computador desde que se lo saca de su caja,

se le instala el sistema operativo, aplicaciones, perfiles, protecciones hasta que se lo entrega para su uso a un usuario final puede ser de 8 horas por equipo, si se necesita actualizar ya sea el sistema operativo o el equipo en una organización de 50 PC , se necesitarían 400 horas que equivale a 50 días, y si se desea reducir la fecha de entrega se necesitara un gran número de personal para realizar una tarea tan trivial y repetitiva. Así mismo el problema que se da cuando un equipo falla por problemas de hardware como disco duro o tarjeta madre el tiempo en proveerle un equipo al usuario podría representar un gran malestar para este y una pérdida considerable para la organización dado a la naturaleza de estas situaciones y de las comunes soluciones que existen para resolverlas. Todo se resumiría en reinstalar el sistema operativo en un pc nuevo, instalar sus drivers, aplicaciones, perfiles, parches, personalización, etc.

1.2. SOLUCIÓN PROPUESTA.

La solución que se plantea en esta propuesta es la de combinar conceptos y técnicas para minimizar el esfuerzo ,tiempo y recursos necesario para realizar esta tarea y al mismo tiempo considerar normas de seguridad informática .La estrategia parte de usar conceptos de clonación de disco actualmente muy optimizados para entornos

virtuales y físicos por la flexibilidad y gran ahorro de tiempo que representa sin incurrir en la compra de herramientas de pago pues a mejor rendimiento y opciones mayor es su coste e infraestructura necesaria para utilizarlas, por lo cual el desafío es usar realizar esta tarea con herramientas de software libre que trabajando en conjunto y sintonía nos darán la ventaja de realizar esta tarea con la misma calidad y rendimiento , el éxito radica en la planificación y secuencia en la que hagamos y usemos dichas técnicas y herramientas.

La idea básica es la de preparar un computador cuya instalación y configuración será la plantilla para la imagen de disco duro que se creara con la herramienta de clonación y posteriormente se desplegara por medio de la red local de la organización gracias a un entorno de arranque sin disco de una distribución de Linux , donde cada PC objetivo podrá arrancar un sistema operativo Linux ligero y se le adjunta la tarea de escribir la imagen de disco duro base sobre su disco duro local utilizando clonación en red usando multicast [11], esto último nos permitirá clonar hasta 100 computadores al mismo tiempo, tarea que demorara mucho menos que clonar los computadores uno por uno.

.

CAPÍTULO 2.

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1. PREPARACIÓN DEL EQUIPO BASE

Se debe es escoger y preparar el computador objetivo que servirá como base para los demás computadores, cabe señalar que previo a iniciar esto del departamento de TI tiene que tener identificados los modelos de computadores a desplegar pues el objetivo es preparar un computador base por modelo si es el caso para crear el archivo de imagen de disco duro del computador base y desplegarlo a los computadores respectivos de igual modelo o características, en caso de haber varios modelos de computadores se prepararan varios computadores base y se crearan varios archivos de imagen de

disco.(Esto se deberá hacer hasta que no se domine “recreación de imagen de disco sobre hardware diferente”).

Asumiendo el caso ideal de que la organización por ejemplo tiene en varios de sus departamentos el mismo modelo de computador y así mismo sean unos 100 de estos, deberá escoger uno de estos como base para prepararlo según la configuración de la organización, departamento, cargo, tipo de usuario. Lo más recomendable es preparar un computador lo más general posible con la mayoría de aplicaciones y configuraciones comunes a todos los departamentos, perfiles o tipos de usuarios y en la fase final de personalización de cada computador habilitar lo que corresponda, así se evita el tener que realizar varias imágenes de disco duro y se optimiza el almacenamiento del equipo destinado a albergar las imágenes de disco duro para tareas posteriores. Bien sea un computador de caja u operativo lo primero es cuestionarse si la información actual del disco que se necesite respaldar o copiar se lo haya realizado, puede que de fábrica el disco duro venga con una partición conocida de restauración a fabrica si lo amerita lo deberá respaldar caso contrario puede empezar formateando el disco duro pues generalmente las aplicaciones de fábrica para la organización son consideradas de relleno, son de prueba y consumen

recursos innecesarios por lo que para nuestro caso lo mejor es partir de cero.

2.2. PARTICIONAMIENTO DEL DISCO DURO

Una de las mejores prácticas que debemos tomar en cuenta por lo menos aún para los discos duros convencionales (platos y cabezas) es la del concepto de Particionamiento del disco duro [2] [3] , esto en palabras más simples es la de segmentar un disco duro físico en 2 o 3 discos lógicos “volúmenes”, es decir varios discos lógicos dentro de un físico, con el único propósito de mejorar el rendimiento y velocidad de acceso en las operaciones de lectura/escritura, para nuestro caso el disco lo particionaremos en 2 volúmenes, uno para la unidad de sistema C y el otro para los datos de usuario E, que no serán parte del sistema operativo y servirá también para el almacenamiento de la imagen de sistema del computador una vez se termine la tarea de personalización para cada usuario. Esto garantiza que la unidad C no se fragmentara muy rápido por causa de mezclar datos del sistema operativo/aplicaciones con los del usuario (archivos de trabajo y multimedia), ya que el volumen C ahora, será exclusivamente para el sistema operativo y el volumen E para archivos de usuario e imagen de sistema, a la vez con esto ,en caso de tener que restaurar el computador

por algún incidente o problema se evita perder tiempo en respaldar los archivos del usuario primero, como ahora el volumen E será para tal efecto solo hay que asegurarse más adelante que en la cuenta o perfil del usuario cambiar que la ruta por defecto de la carpeta mis documentos y sus subcarpetas apunten a la unidad E.(Se escoge la letra E porque generalmente el sistema operativo asigna D para la unidad óptica).

2.3 HARDNENING E INSTALACIÓN DE APLICACIONES AL SISTEMA OPERATIVO.

Para la instalación del sistema operativo sea cual fuere nuestra elección entre los productos Microsoft Windows 7/8/10 hay que tener en cuenta la versión que se vaya a preparar es decir entre las de 32 y 64 bits, la consideración que más nos debe interesar es la de los drivers de hardware para la versión de 64 bits si existen o no. Además se asume que como organización se posee un sistema de licenciamiento por volumen, es decir una misma licencia de sistema operativo para todos los computadores, esta licencia se activa al momento de conectarse a internet o en su defecto se activa por medio de su red local a un servidor KMS de licencias o en el peor de los casos se cuenta con una respectiva licencia por cada computador , esta se tendrá que ingresar en la

personalización de cada computador para que se active y pueda descargar las actualizaciones de seguridad.

Luego de instalar el sistema operativo se deben instalar los parches de seguridad respectivos, programas y sistemas propios de la organización, utilitarios, programas de ofimática, navegadores, antivirus, drivers de impresoras, programas de soporte remoto, programas de almacenamiento en la nube y todo lo que el departamento de TI o soporte considere primordial y necesario para las tareas de soporte posterior. Como consejo se puede crear una carpeta de ubicación y nombre solo conocido por el personal de TI donde se pueden dejar programas o utilitarios de soporte más habitual para la organización, esta es una muy buena práctica cuando se pierde conectividad de red local o internet y se necesitan estos utilitarios de manera local.

Luego de instalar, configurar y probar el correcto funcionamiento de cada una las aplicaciones y demás programas, se recomienda aplicar un tema muy útil y poderoso de seguridad informática denominado

“hardening” aplicado para nuestro caso a sistemas operativos Windows 7/8 [4],[5] y el paquete de ofimática Microsoft office 2013 [6].

Otro consejo que puede llegar a minimizar la tarea de las actualizaciones de Windows y office es poder ser capaces si la situación del ancho de banda apremia o no se desea esperar las casi 2 horas que tomaría descargar e instalar un aproximado de 2000MB de actualizaciones urgentes e importantes es el de previamente tener descargado las actualizaciones esto se puede hacer con un programa que descarga las actualizaciones para hacer una instalación offline crea un instalador automatizando la tarea de que actualización necesita el sistema operativo, el programa se llama WSUS Offline Update [7].

2.4 CREAR IMAGEN DEL DISCO DURO/PARTICIÓN

Una vez que se tenga el computador listo y operativo con todas las aplicaciones instaladas, configuradas y probadas a satisfacción podemos pasar al siguiente paso que es la creación de imagen de disco duro. Primero debemos recordar que deseamos crear o extraer una imagen del estado actual del disco o partición del computador finalmente terminado ,asegurado y operativo, esta imagen deseamos sea lo más neutra y general posible, por lo tanto previo a la creación de la imagen será muy recomendable que por ejemplo el nombre del pc no

esté definido explícitamente sino puede quedar como especie de plantilla Ej:WrksXXLocXX, así como la IP dejar que sea por DHCP hasta el final en la personalización fijar los respectivos y definitivos nombre e IP que corresponda con cada equipo.

Una ver cubierto este tema empezaremos a usar una de las herramientas de software libre más poderosa con la que hayamos podido imaginar contar para poder resolver varios temas con una sola herramienta me refiero a DRLB [1], esta solución se basa en un Livecd basado en una distribución de Linux debian con entorno grafico XFCE [8] que nos facilitara en un solo cdrom varias herramientas poderosas entre ellas las que nos interesa para esta parte del procedimiento es:

Clonezilla [9], este programa viene en 2 versiones, live para la creación de imagen / clonación discos duros o particiones de manera local similar a herramientas de pago costosas como Norton Ghost o Acronis y la versión *SE (server edition)* que brinda la infraestructura a nivel de software para poder desplegar masivamente el archivo de imagen a más de un computador a la vez por medio de la red LAN.

El Procedimiento genérico de “cómo usar de DRBL” [9] para tener una idea más clara del potencial de esta herramienta combinada con los

temas anteriormente mencionados dos da un mecanismo para lidiar con el problema planteado a un menor costo económico y esfuerzo horas/hombre.

Debemos descargar el archivo ISO con la versión de hardware que usemos en la organización, también se puede convertir esta ISO para hacer un flash drive booteable, sea como fuere el primer paso es descargar y quemar el cdrom o crear el flash drive, botear el pc usado como base y arrancar el entorno DRBL una vez cargado veremos el escritorio de un Linux debían XFCE con los accesos directos a los programas que nos facilitaran la vida, para nuestro caso Clonezilla live.

Figura 2.1 Pantalla de opciones de inicio de Livecd DRBL

Una vez que carga el Livecd esta será la primera pantalla que veremos, escogeremos la primera opción DRBL Live, luego aparecerá otra pantalla que nos pedirá que elijamos el idioma del teclado, escogeremos el que nos corresponda, luego nos pedirá escoger el mapa del teclado, escogeremos" no tocar mapa del teclado", luego una pantalla para la distribución del teclado, escogeremos la que diga por defecto, por ultimo una pantalla sobre qué modo grafico queremos, pulsamos 0 por defecto. Luego de eso cargara el entorno grafico del Livecd.

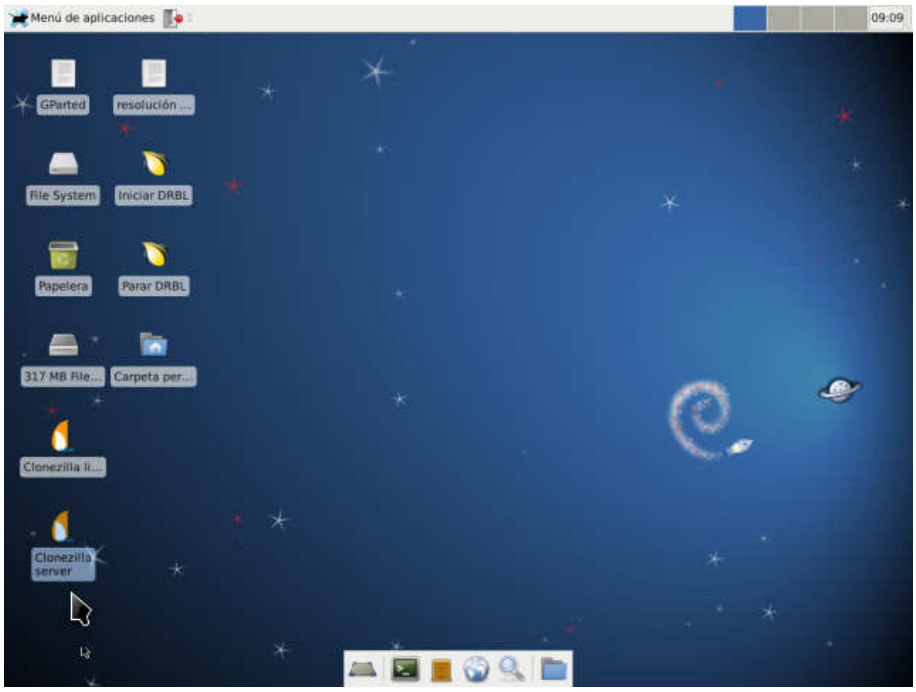

Figura 2.2 Escritorio de Livecd DRBL Linux debian XFCE

Iniciamos Clonezilla Live.

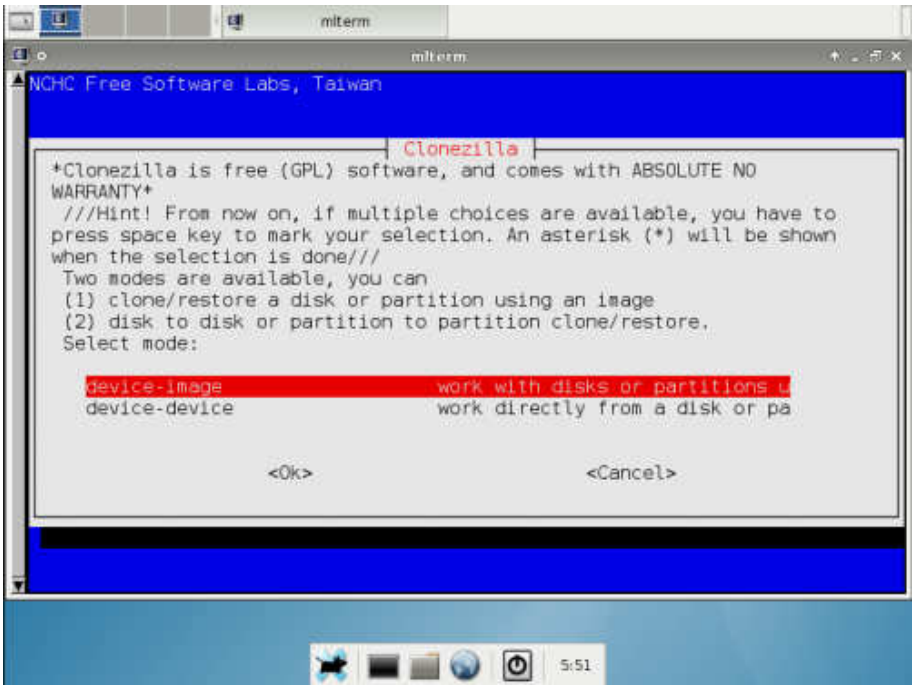

Figura 2 3 Pantalla inicial de Clonezilla Live

Aquí tenemos dos opciones. Device-Image y Device-Device la primera es la que vamos a escoger pues es la que significa que deseamos hacer el archivo de imagen del disco duro o dicho de otras palabras hacer que el dispositivo disco se vuelva una imagen o archivo. La opción device-device es la que usaríamos para clonar o hacer copia de disco a disco Continuemos.

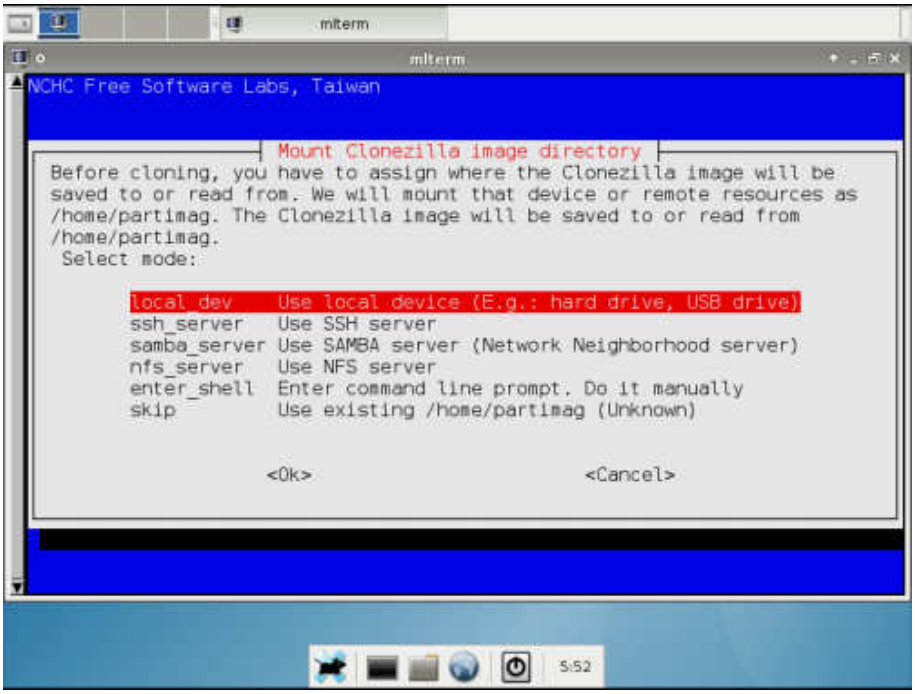

Figura 2.4 Ubicación de almacenamiento de Clonezilla

Aquí es donde guardaremos el archivo de imagen de disco duro. La primera opción “Local_dev” nos facilita el guardar la imagen en otra partición, disco o unidad USB del mismo equipo local. La segunda en equipo remoto que tenga espacio y un servicio SSH activo.

La tercera en un equipo que tenga habilitado un servicio samba. Luego te da la opción de hacerlo uno mismo manualmente. Si se tiene otra partición con espacio o un disco duro externo USB conectado al pc escogeremos la primera opción, si tenemos ya una

infraestructura de servidor de archivos con servicio el SSH o samba para almacenar las imágenes escogeremos la que corresponda. Para nuestro ejemplo escogeremos la primera opción. La siguiente pantalla pedirá escoger en que disco o unidad se desea guardar la imagen. Luego

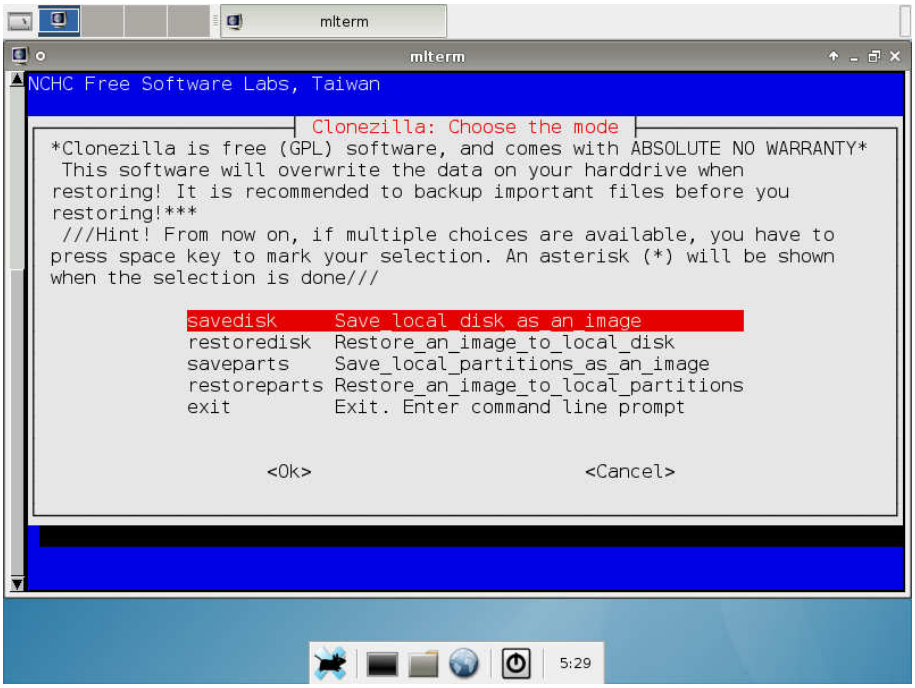

Figura 2.5 Menú modo de operación de Clonezilla

Esta pantalla nos pide escoger que debe hacer Clonezilla las opciones son:

savedisk -> Crear imagen del disco duro completo

restoredisk -> Restaurar disco duro a partir de una imagen

saveparts -> Crear imagen de una o varias particiones

restoreparts -> Restaurar particiones a partir de una imagen

exit -> salir

En nuestro caso, seleccionaremos “savedisk”

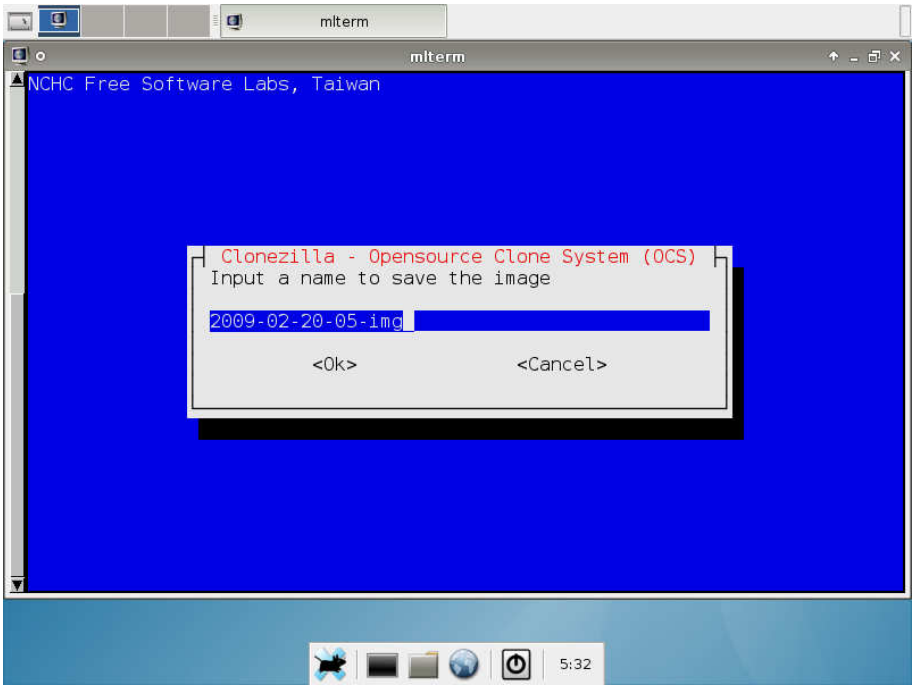

Figura 2.6 Pantalla nombre de archivo de imagen Clonezilla

Clonezilla pone la fecha y hora como nombre de archivo por defecto eso está bien pero le podemos poner un nombre más representativo como el modelo del pc, área, departamento, sucursal, etc.

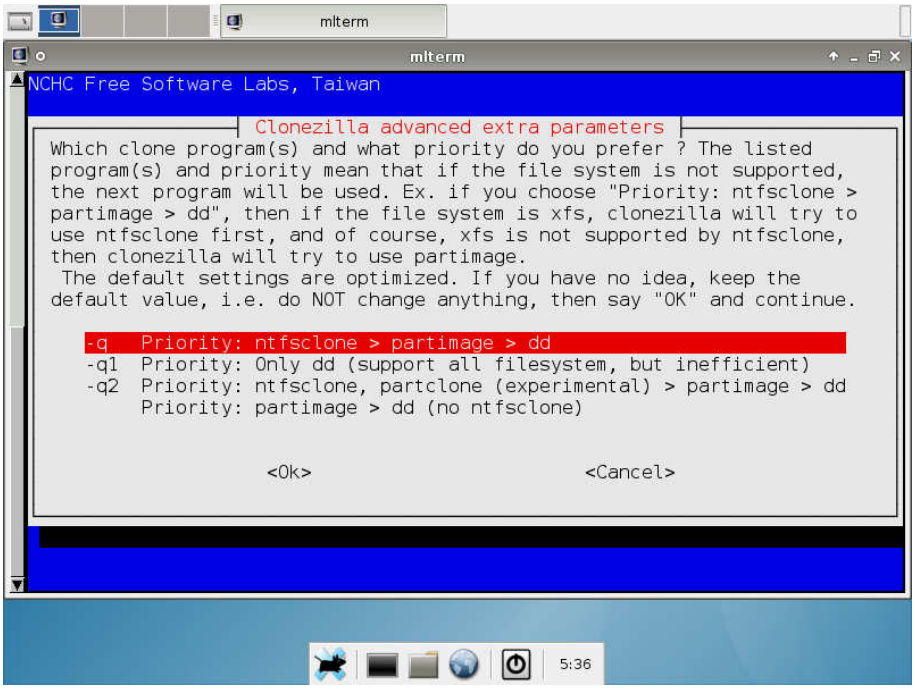

Figura 2.7 Pantalla de parámetros de Clonezilla

Aquí se nos pregunta cómo queremos crear el archivo de imagen:

-q -> Forma estándar, recomiendo usar esta ya que la imagen también se comprime

-q1 -> Réplica exacta usando dd. Esta opción es útil para cuando tenemos particiones cifradas.

Escogemos la primera, luego saldrán dos pantallas más pues Clonezilla ofrecerá opciones avanzadas sobre la creación del archivo de imagen referente al nivel de compresión del archivo, también sobre si deseamos el archivo de imagen de pedazos o un solo archivo esto en caso de

quererlo por decir en varios cdroms, o dvdroms recomiendo siempre solo aceptar la primera opción por defecto que es compresión normal y 1 solo archivo hasta llegar a la pantalla final.

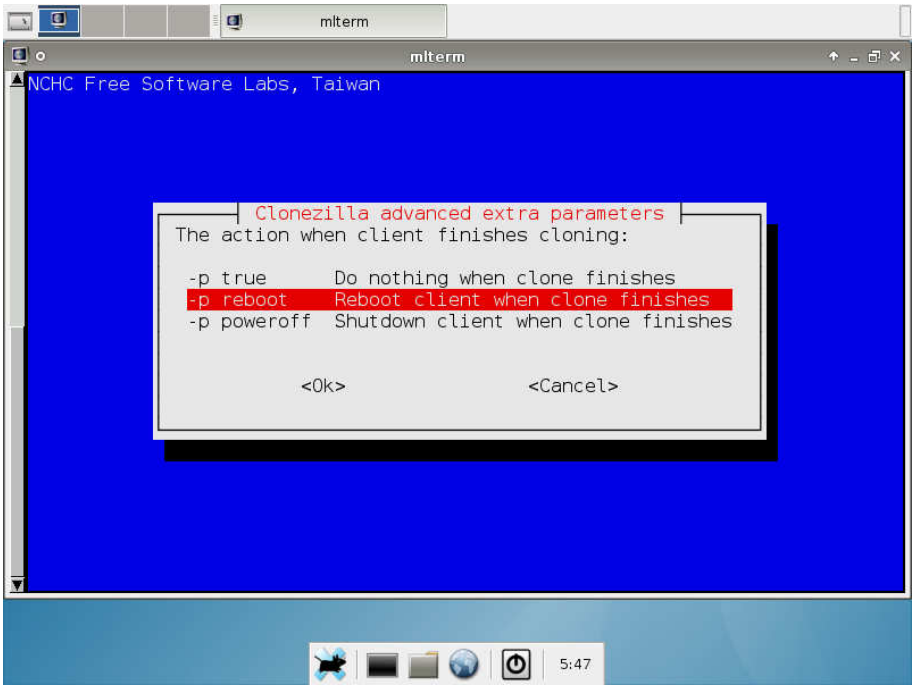

Figura 2.8 Pantalla final creación de imagen Clonezilla

En esta pantalla podemos elegir que hará Clonezilla al termino de creación del archivo de imagen la primera opción es no hacer nada lo que implica quedara esperando por nuestra acción, la segunda opción indica que reinicie el pc y la tercera que apague el equipo al término. Ya depende de que se quiera hacer lo más usual es no hacer nada, pues luego usaremos la misma máquina para usarla como servidor de

imágenes para las computadoras objetivos por medio de una vez más DRBL + Clonezilla SE.

Aquí ya debemos tener una carpeta con el nombre que le hallamos dado al archivo de imagen en la ruta que hayamos indicado, este será el archivo que usaremos en el siguiente paso.

2.5 DESPLIGUE DE LA IMAGEN DISCO EN RED LAN USANDO MULTICAST

DRBL provee un entorno de arranque remoto sin disco duro en Linux en una red de computadores por medio de PXE [10] para que los pc clientes de una red puedan cargar un sistema operativo en este caso Linux debían por medio de la tarjeta de red sin que intervenga el disco duro local de cada computador y por medio de este Linux armar el entorno de red necesario para armar una red privada con su respectivo DHCP server que le asignara una IP a cada pc cliente y poder asignarle la tarea de recibir la imagen de disco duro previamente creada por Clonezilla lite y enviada por medio de Clonezilla SE con la tarea de sobrescribir el disco duro o partición local con el contenido de la imagen enviada, todo esto por medio de la red LAN local la mejora en rendimiento de que la imagen de disco duro enviada se hará por medio de MULTICAST [11] lo que permitirá poder clonar hasta 100

computadores logrando un gran ahorro de tiempo para el departamento de soporte / TI y de trabajo repetitivo.

Para iniciar la tarea de despliegue del archivo de imagen creado en el paso anterior debemos tener primeramente las siguientes consideraciones. Un pc que hará de servidor de imagen, generalmente seria el mismo que usamos como base, pero si esta tarea la hacemos en otro momento diferente al de creación de imagen el pc que se use como servidor de imagen puede ser cualquiera lo único que se necesitara ser el disco Livecd o el flash drive de DRBL y el archivo de imagen del disco a clonar ya sea disponible en un disco duro externo, en el disco del pc que se use como servidor o en un servidor de archivos remoto que se conozca la IP, ruta, usuario y contraseña de acceso. Para nuestro ejemplo usaremos el mismo computador en que se creó la imagen, y el archivo de imagen que está en una partición del disco de esta computadora. Para iniciar esta tarea iniciaremos como en el paso para crear la imagen, es decir cargaremos en el computador el disco Livecd DRBL hasta cargar la interfaz gráfica y estemos en el escritorio, ahora ejecutaremos Clonezilla Server.

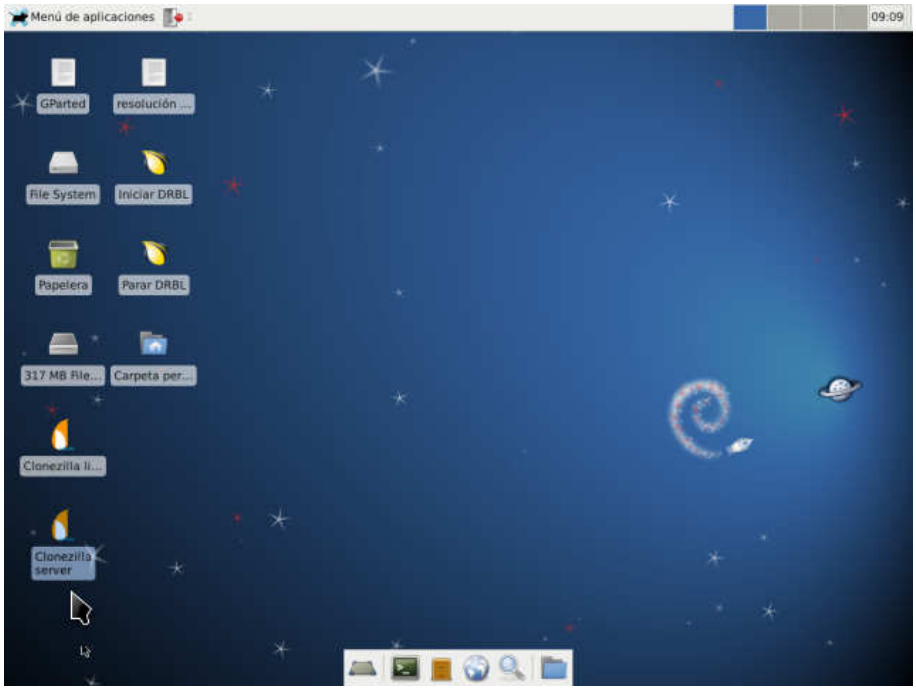

Figura 2.9 Ejecutando Clonezilla Server

Sólo tenemos una NIC o tarjeta de red: eth0. DRBL asume que debemos tener 2 NICs: Una que conectará el servidor de clonación a una red y otra que conectará el servidor de clonación a la subred de los computadores a clonar. Como sólo tenemos una, DRBL creará una tarjeta virtual para tener dos.

Primero nos preguntara de qué modo se configurara la tarjeta de red.

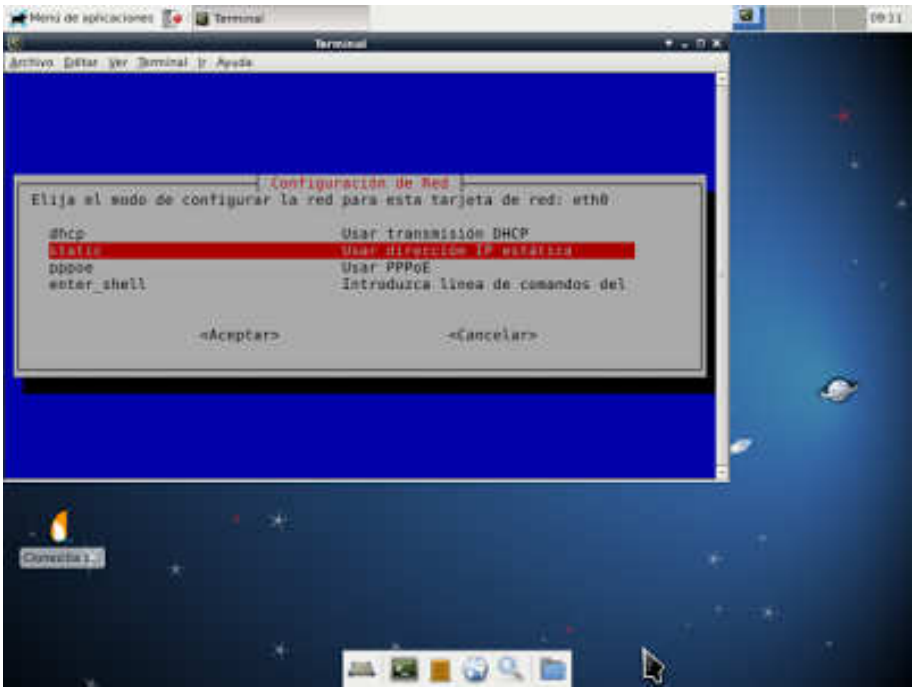

Figura 2.10 Clonezilla Server configuración de tarjeta de red

Escogeremos static e introduciremos la IP que queramos asignar, generalmente será una IP de tipo privada si es que se hace la tarea de manera aislada fuera de nuestra red convencional.

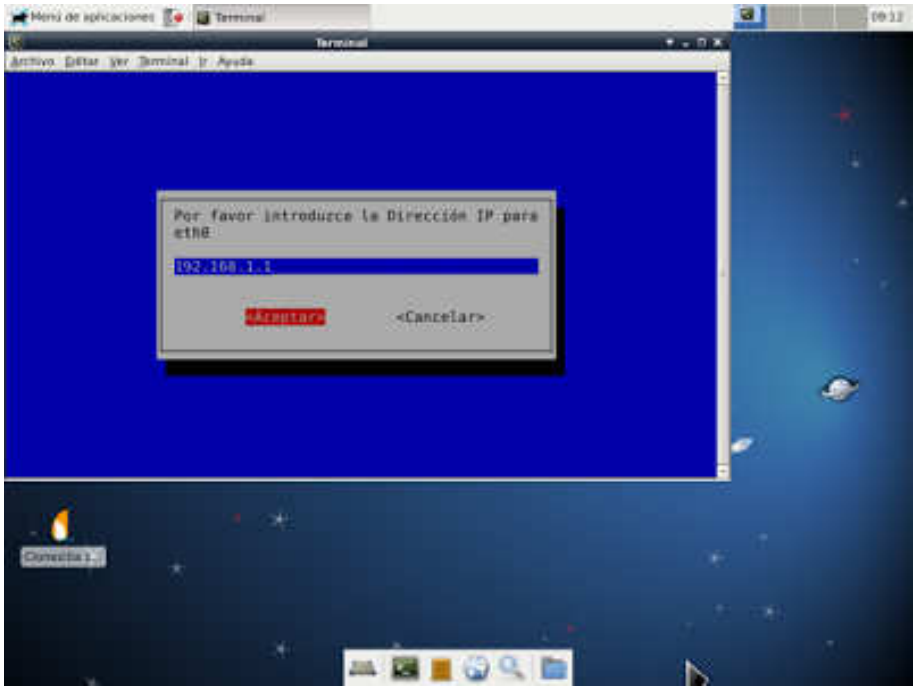

Figura 2.11 Clonezilla Server seteando IP a tarjeta de red

Aparecerán otras 3 pantallas, una pidiendo mascara de subred pondremos 255.255.255.0, la segunda la puerta de enlace aceptaremos la que nos pone por defecto y la tercera el DNS aceptamos también la dirección por defecto.

Luego aparecerá esta ventana de letras amarillas.

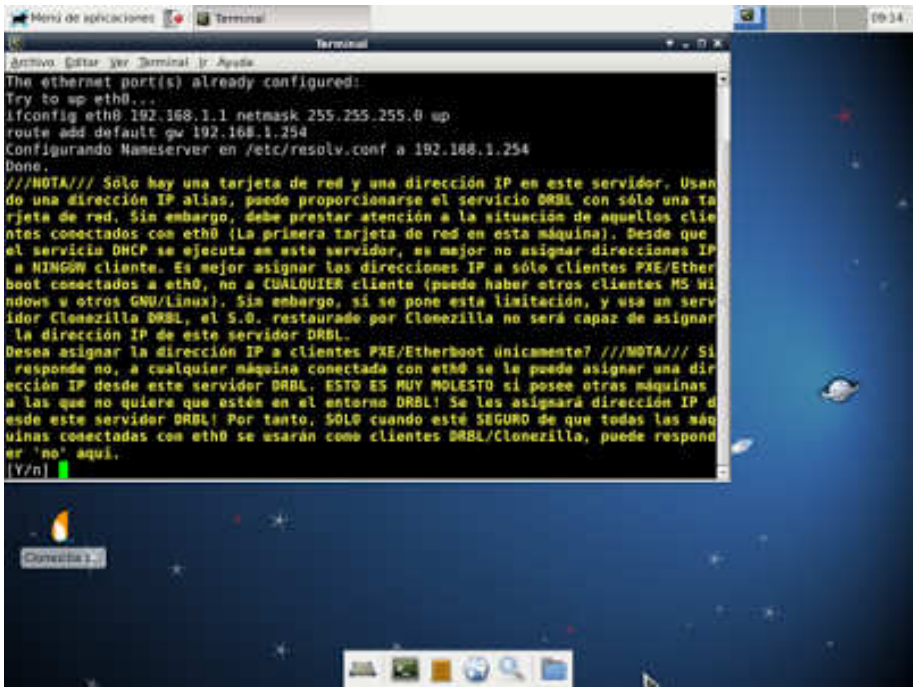

Figura 2.12 Clonezilla Server NIC setup

Pulsamos enter pues la opción por defecto es “yes”. Luego nos pedirá que indiquemos donde está el archivo de imagen, como esta en una partición del disco duro local del pc o en un disco duro externo USB conectado al computador ponemos local_dev.

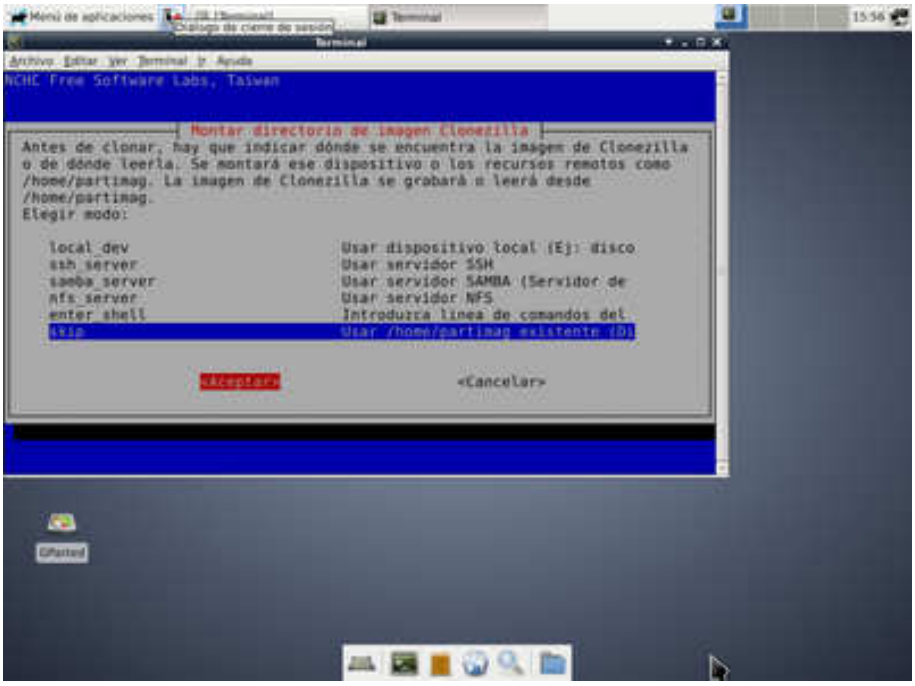

Figura 2.13 Clonezilla Server ubicación de archivo de imagen de disco duro

Luego aparecerá una ventana indicándonos que se ejecutara el script drblpush el cual se encarga de la configuración del servidor de clonación.

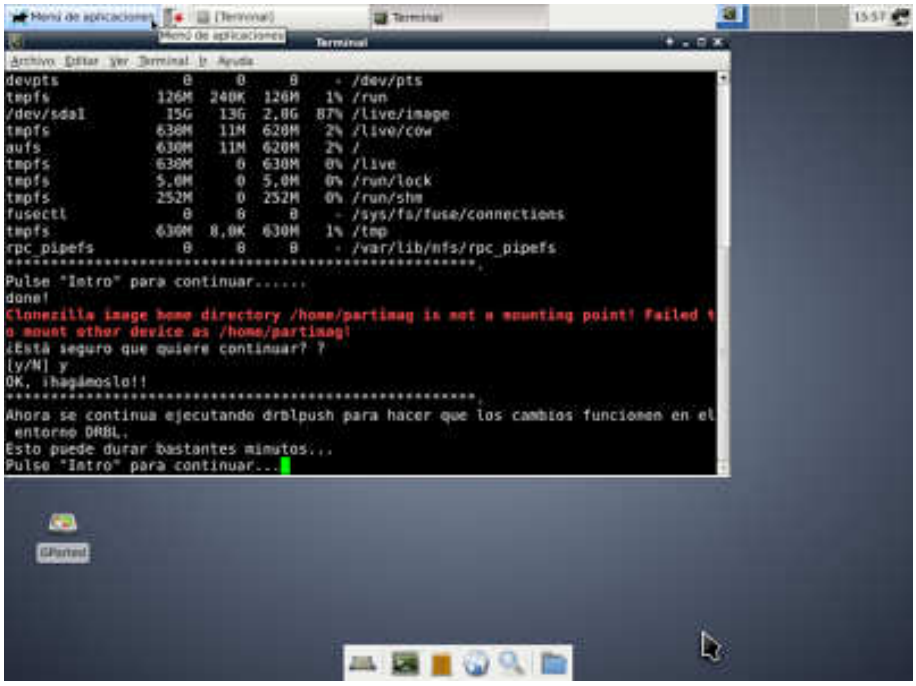

Figura 2.14 Clonezilla Server Script configuración de servidor DRBL

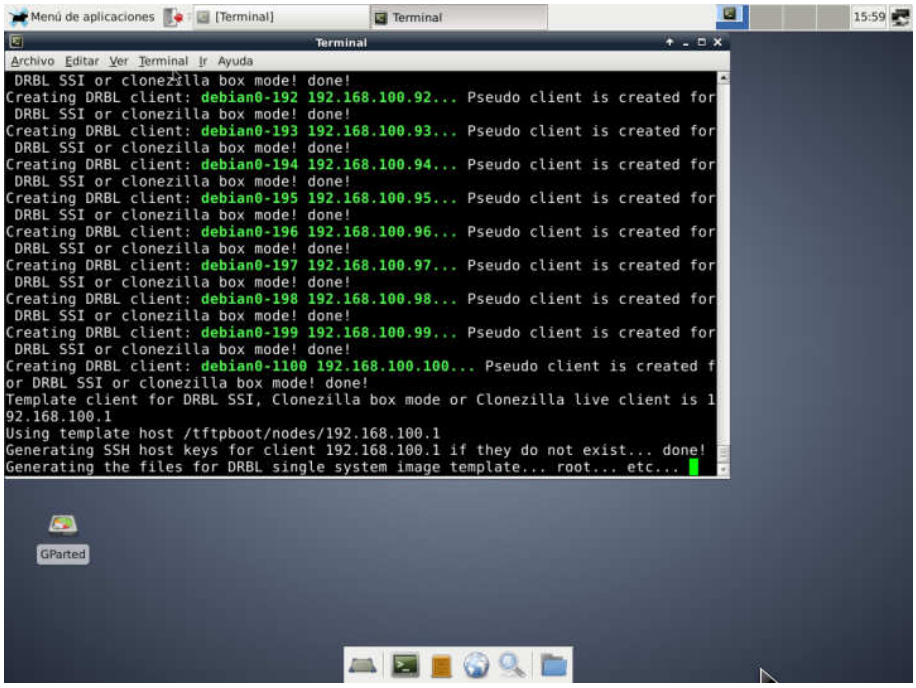

Figura 2.15 Clonezilla Server Proceso Configuración del servidor DRBL

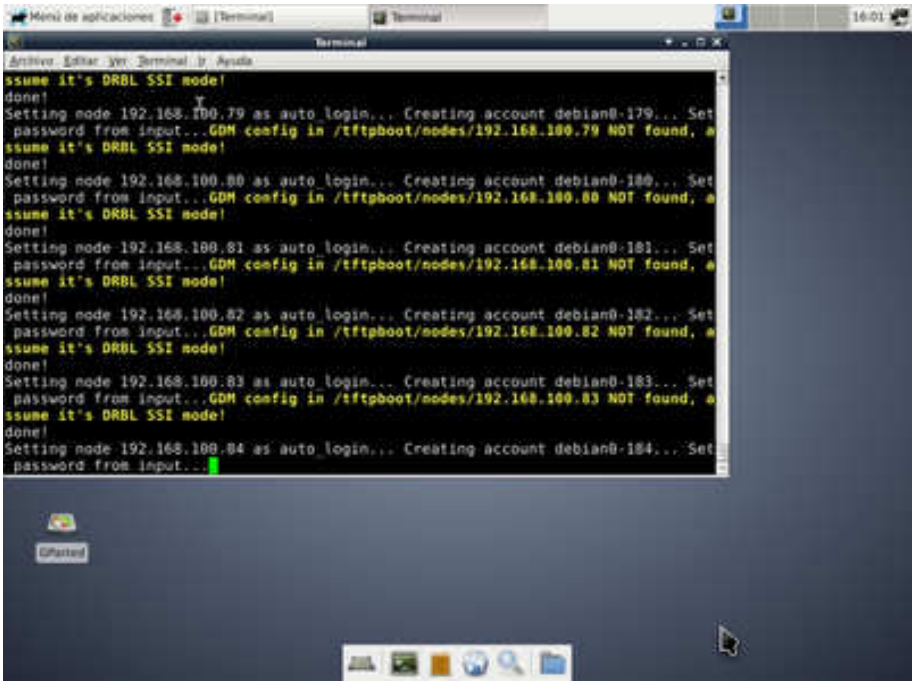

Figura 2.16 Clonezilla Server Proceso Configuración del servidor DRBL continuación

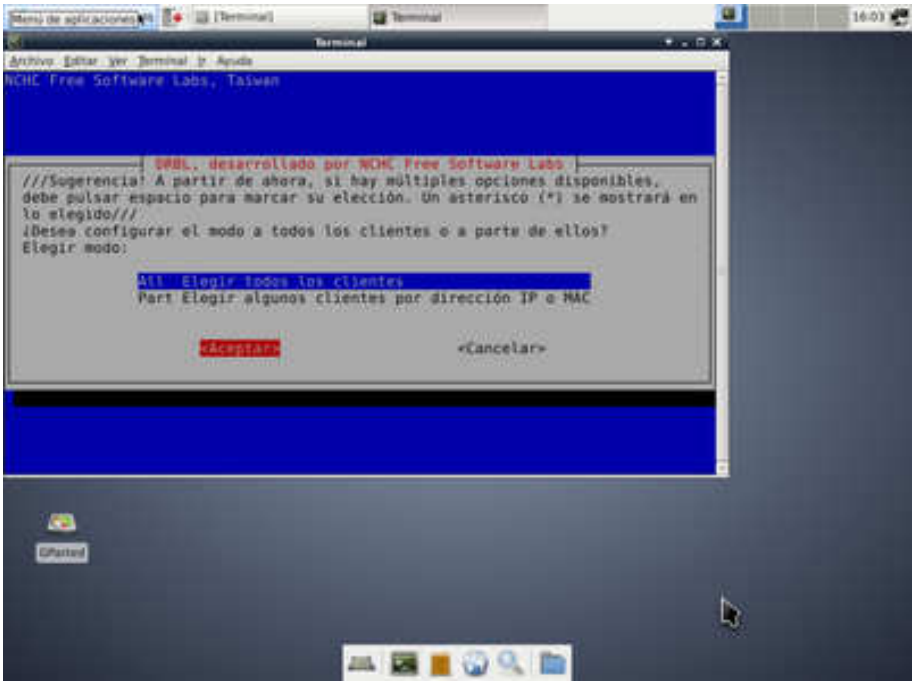

Figura 2.17 Clonezilla Server Selección de computadores a clonar

Una vez configurado el servidor e iniciados los servicios, nos pregunta si queremos elegir todos los clientes o tan sólo algunos por IP o MAC. Seleccionamos "All Elegir todos los clientes" y pulsamos "Aceptar.

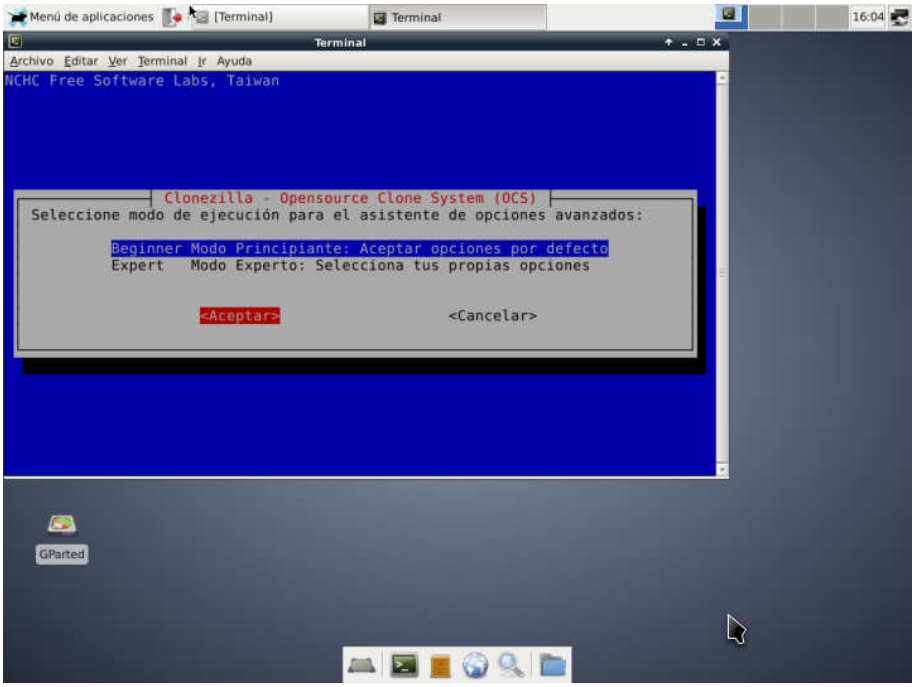

Figura 2.18 Clonezilla Server Selección de operación

En la pantalla de modo de operación de Clonezilla Server Elegimos el modo principiante aceptando las opciones por defecto. Si tuviéramos algún problema, podemos volver a iniciar el proceso de nuevo cambiando al modo experto.

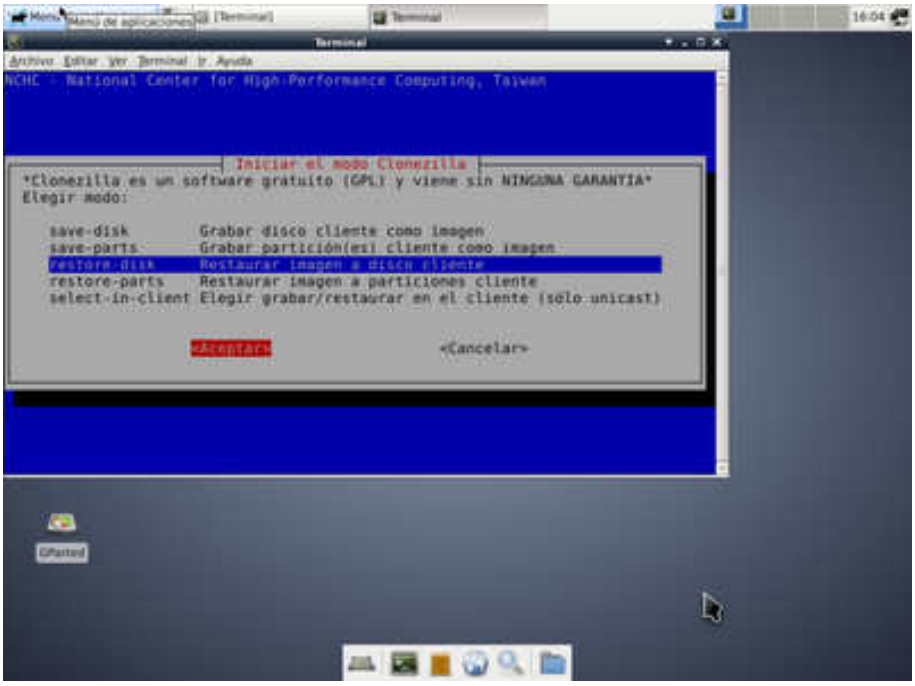

Figura 2.19 Clonezilla Server Restaurar Imagen de Disco opción

En esta pantalla elegimos lo que deseamos hacer que es restaurar una imagen de disco duro en todos los clientes elegimos “restore_disk”.

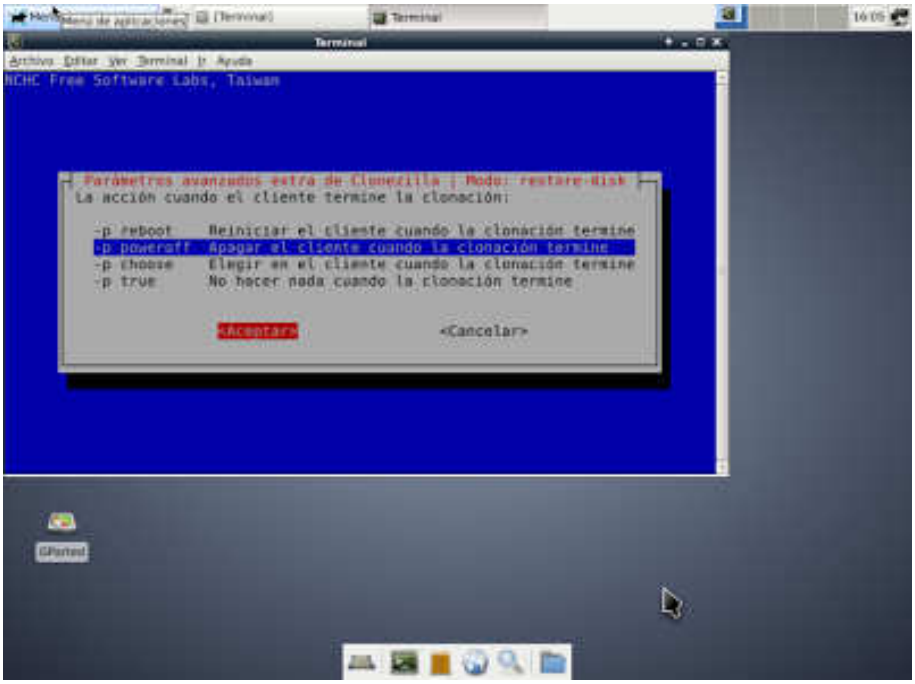

Figura 2.20 Clonezilla Server opción al finalizar la tarea de clonado

Que hacer la terminar la tarea de clonación en las maquinas destino.

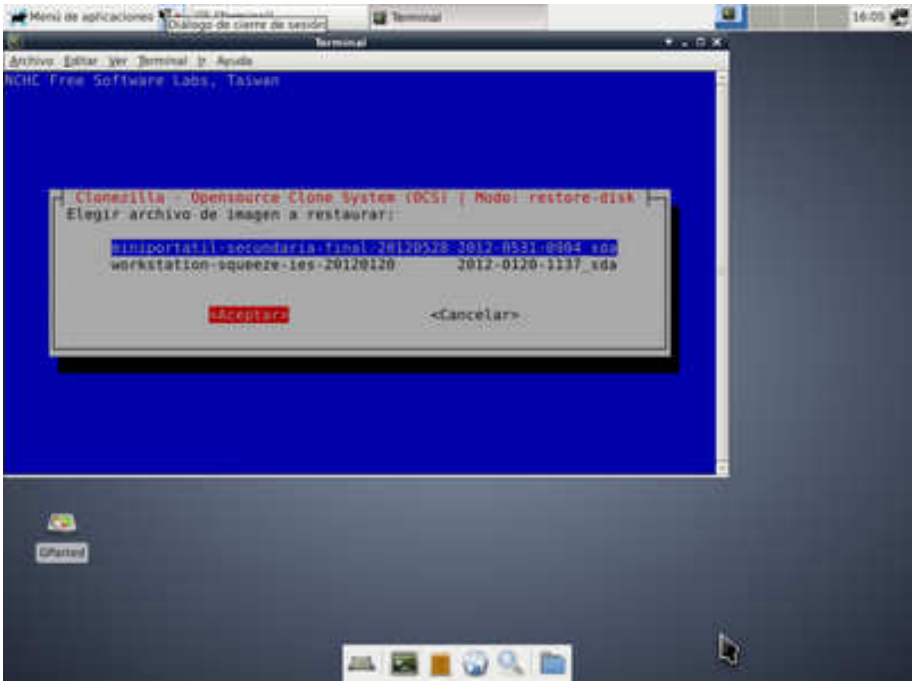

Figura 2.21 Clonezilla Server Selección de Imagen de disco a usar

Se nos mostrara todos los archivos de imagen que tengamos almacenados y debemos escoger cual usaremos.

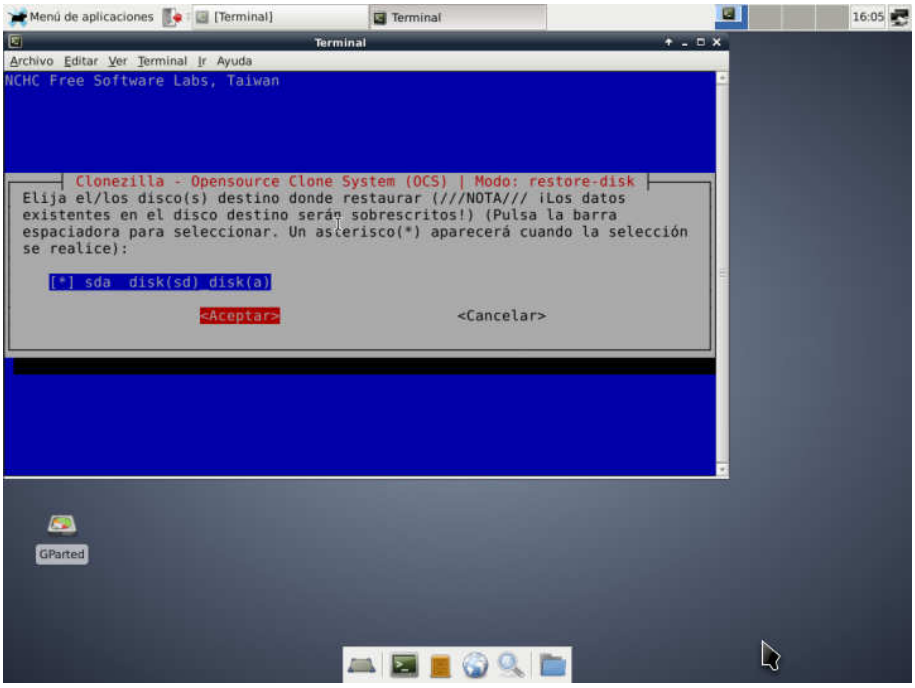

Figura 2.22 Clonezilla Server Disco destino a restaurar

Nos pregunta que disco debe ser escrito en el destino si hubiera más de 1 deberíamos escoger el que posee el sistema operativo en Linux es sda.

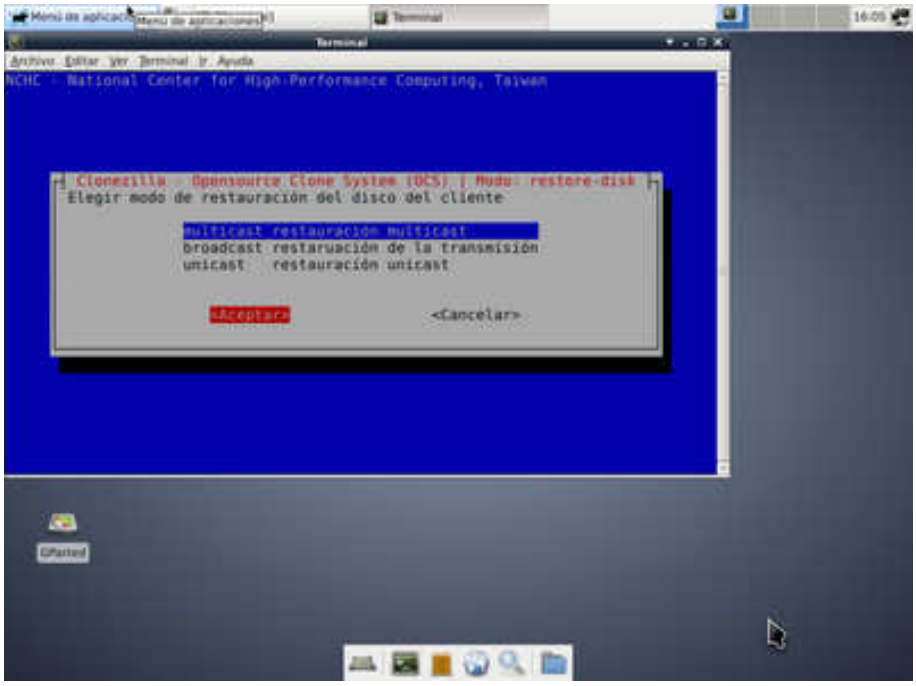

Figura 2.23 Clonezilla Server activación de MULTICAST

IMPORTANTE: Puesto que queremos restaurar todos los equipos a la vez, seleccionamos el modo de restauración "multicast" y pulsamos "Aceptar": Con esto todos los computadores conectados a este servidor se clonaran al mismo tiempo a la máxima tasa de transferencia que ofrezca la red local.

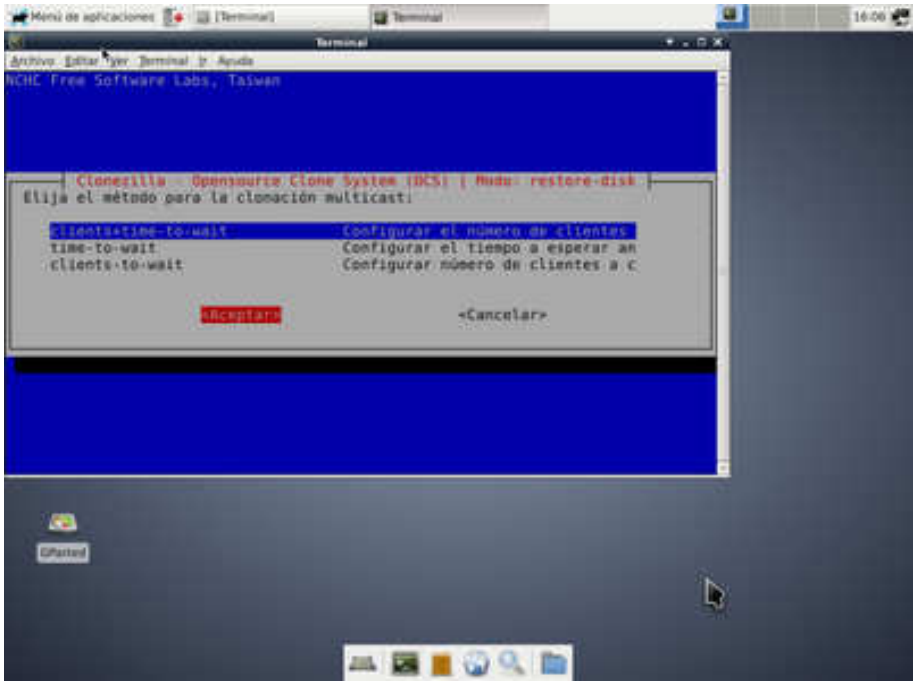

Figura 2.24 Clonezilla Server Modo de espera del servidor

Clonezilla preguntara sobre como esperara a los computadores se conecten a él para empezar la tarea de clonado, hay 3 opciones la primera “clients+time to wait” significa que esperara por dos criterios por el número de pc que se conecten a él o por el tiempo que digamos debe esperar para iniciar la tarea , en este caso lo que ocurra primero hará que se empiece con la tarea, es la que se recomienda usar , para el caso de querer clonar 40 pc, y estimando que en prender cada pc y hacerla botear por medio de su tarjeta de red tome 1 minuto pondríamos en clients 40 y time 2400s (el valor de tiempo se ingresa en segundos)

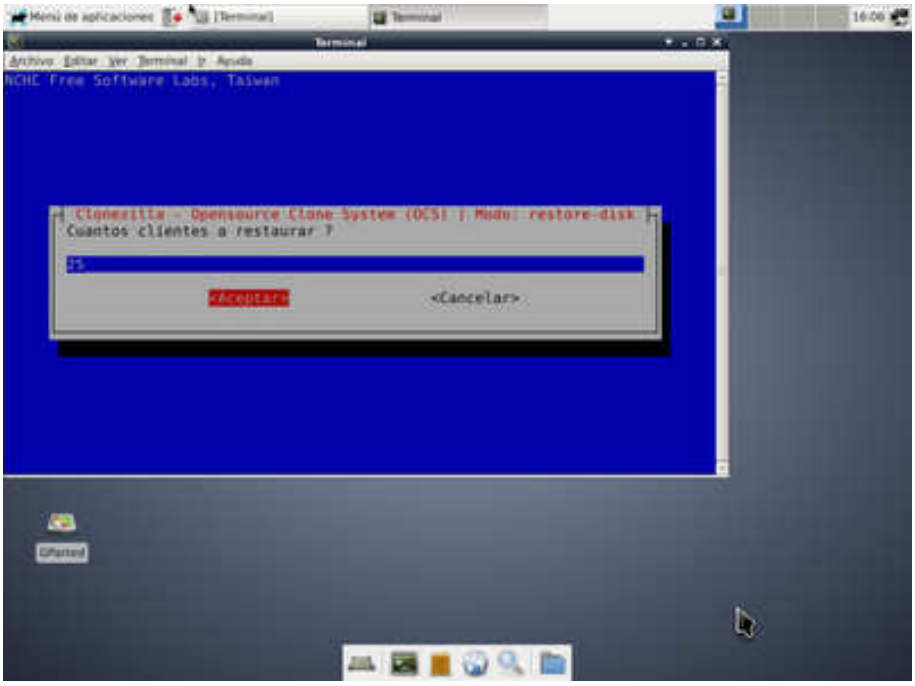

Figura 2.25 Clonezilla Server número de PCs a clonar

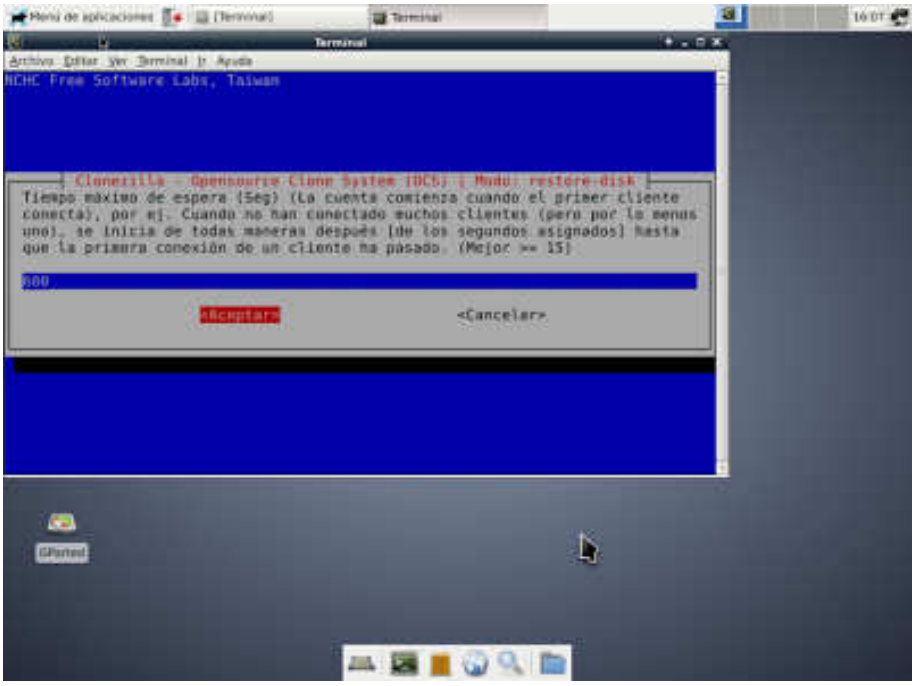

Figura 2.26 Clonezilla Server Tiempo a esperar para iniciar la clonación

De aquí aparecen 2 pantallas más pulsaremos enter y finalmente.

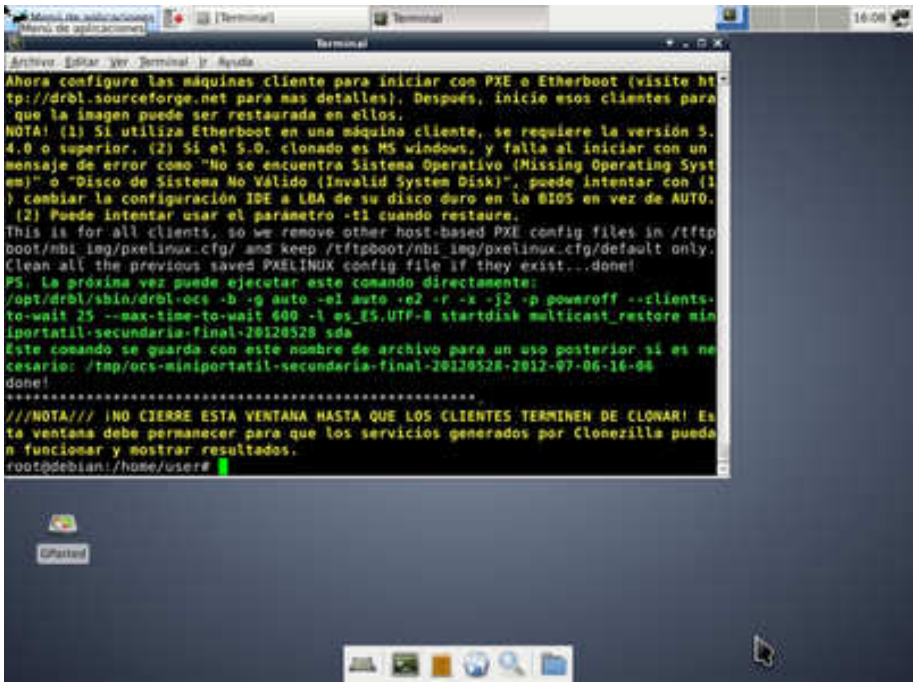

Figura 2.27 Clonezilla Server Listo en espera

Se nos avisa de que no debemos cerrar esta ventana hasta que los computadores que se conecten terminen la tarea de clonar sus respectivos discos duros con el archivo de imagen de disco duro enviado.

A continuación empezamos a encender los equipos y hacerlo arrancar vía PXE, bien configurándolo en la BIOS de cada uno de los

computadores o pulsando la tecla asignada para arrancar vía PXE (por red) para el caso de PCs Intel es F12.

Poco a poco irán arrancando y quedando a la espera de que se inicie el proceso de clonación, bien porque se hayan conectado el número de equipos o porque haya transcurrido el tiempo indicados.

Figura 2.28 Clonezilla Server Inicio de proceso de clonación en red por multicast y pxe

Por ultimo inicia el proceso de clonación simultáneamente en todos los pc dependiendo del tamaño del archivo de imagen a restaurar y de la velocidad de la red para un caso de una imagen de disco de 30/200GB toma aproximadamente 30 minutos clonar 40 Pc.

2.6 PERSONALIZACIÓN DE LOS COMPUTADORES CLONADOS

La personalización de los computadores clonados no es más que la tarea de configurar los valores que identifican como único a cada equipo en la organización esto es su nombre de pc, IP, mascara de red, Gateway, DNS, dominio, configurarlo para el tipo de usuario final, por departamento, activar el sistema operativo, el office, iniciar los servicios de almacenamiento en nube. Esta tarea es trivial pues ya lo más pesado se superó en el paso anterior. En esta fase de personalización de los equipos para el usuario final cada equipo quedara configurado según el usuario o por tipo de área o departamento que use este computador. La ultima tarea de esta fase deberá ser la creación de imagen de sistema que se ofrece desde Windows 7, esto consiste en crear una imagen de la partición del sistema o mejor dicho el volumen C y lo guardaremos en nuestra partición E. Con esto nos aseguramos de tener una imagen o respaldo local del estado 0 de este equipo, en caso de que se corrompa el sistema operativo nuestra primera opción será recrear el volumen C a partir de su propia imagen de sistema guardada en E. En el peor escenario de que por ejemplo se dañara el disco duro físico y perdiéramos la imagen de sistema siempre contaremos con la imagen de disco creada por Clonezilla y la recrearemos en un nuevo disco usando DRBL+Clonezilla Live. Así mismo como se ha venido

recomendado la data del usuario debió haber estado sincronizado con algún servicio de almacenamiento en la nube así cuando se ponga el disco nuevo y se lo vuelva a personalizar para el usuario en cuestión todos sus archivos personales deberán sincronizarse con su disco en la nube.

Otra alternativa que el departamento de soporte /TI debería proveer para garantizar la integridad y disponibilidad de la información de sus usuarios en la organización es además del mecanismo de almacenamiento en la nube podrían implementar un sistema de almacenamiento local como un NAS server (Network Attached Storage) para aplicar el concepto de redundancia.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 ANÁLISIS DE TIEMPO INVERTIDO DE MÉTODO NORMAL VS EL PROPUESTO

Basado en experiencias personales y de estudios sobre el costo total de propiedad de empresas como Dell [11] en el costo para una organización en la tarea de despliegue de equipos y desde que el concepto de clonación fue conocido y aplicado en los tiempos que fui estudiante universitario y labore en los laboratorios de biblioteca de CIB-ESPOL que manejaba 4 laboratorios cada uno de entre 40 y 80 PCs, la tarea de preparar un computador en el mejor de los casos para un usuario capacitado desde cero hasta quedar finalmente operativa y lista oscila entre 6 y 8 horas de trabajo continuo, este número de horas debía multiplicarse por el número de computadores que se preparaban desde

que se los sacaba de la caja por cada laboratorio ,si fueran 200 Pc serian 1600 horas de trabajo , si se trabajan 8 horas diarias serian 200 días , esto sería una sola persona como se requiere que máximo en un mes laboral se tenga listo los laboratorios serena 200/20 días da 10 personas o ayudantes para poder tener listo 200 pc en 20 días. Con la clonación de los años 2000 la tarea tomaba el tiempo necesario en preparar la Pc origen 8 horas y clonar cada pc que tomaba 1 hora, es decir serian 8 horas 1 pc más 199 horas las 199 pc dan un total de horas de 207 horas si se trabajan 8 horas se requieren 26 días una sola persona, si se desea terminar en 2 semanas se requieren 3 personas trabajando 8 horas para terminar 200 pc en 2 semanas(10 días).El problema de la clonación de esos días era que se tenía que destapar las pc sacar el disco origen e ir instalándolo en la pc objetivo, si se quería avanzar como se quiere 3 personas había que tener 3 discos duros idénticos, quemar 3 cdroms e ir avanzando, esto con el riesgo de dañar el disco fuente ya sea por mala manipulación o estática. Usando el método de clonación en red con DRBL que usa Clonezilla, PXE, y multicast esas 200 máquinas serian 8 horas para preparar 1 pc + 30 minutos en clonar 100 Pc + 30 minutos en clonar 99Pcs total 9 horas es decir máximo 1 día de 8 horas laborables más 1 hora extra una sola persona. Hay que indicar que no se ha tomado en cuenta el tiempo de personalización de cada computador lo que dispararía aún más el

tiempo en el método normal, la clonación básica pero aun así la clonación en red por multicast usando DRBL es para considerar los ahorros en tiempo, esfuerzo y uso de personal.

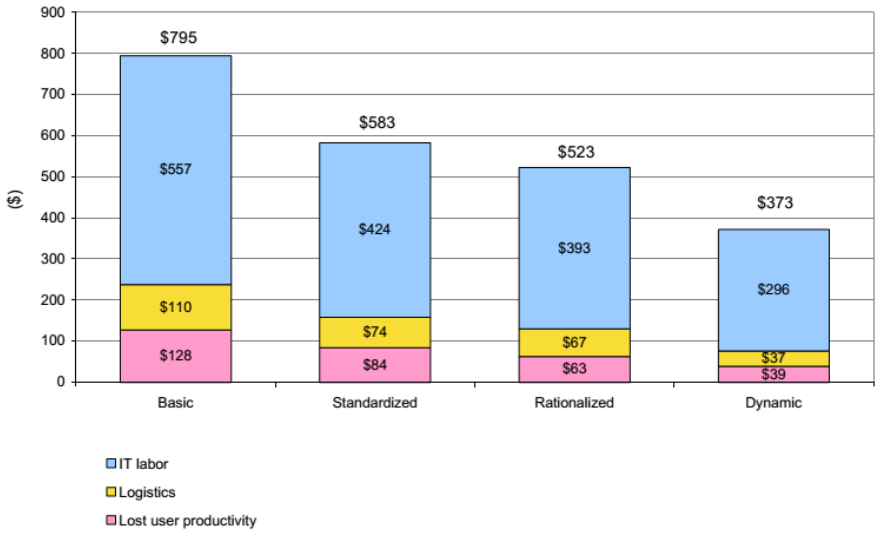

Figura 3. 1 Costo de despliegue de computadores según modelo de optimización [14]

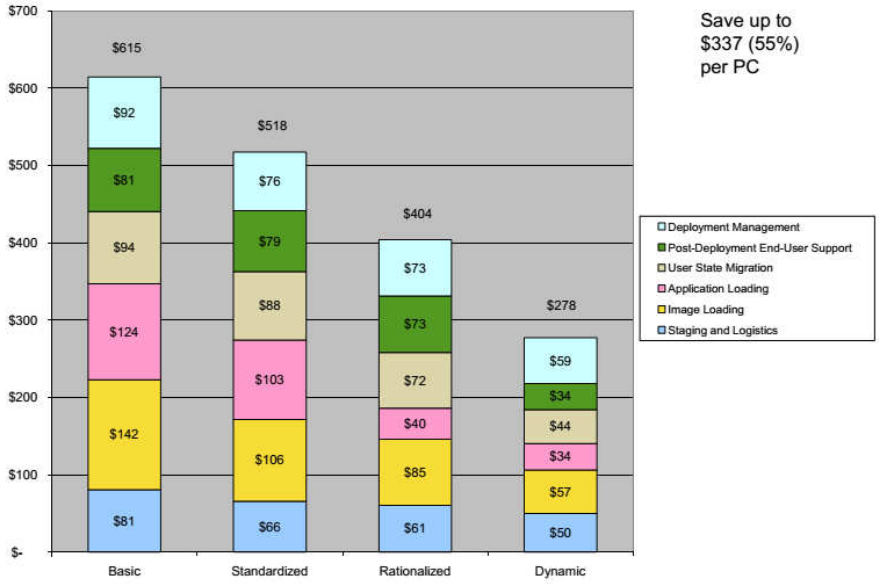

Figura 3. 2 Costo de despliegue de un computador por actividad [14]

3.2 TIEMPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD O DAÑO A LOS EQUIPOS

Los tiempos de respuesta ante incidentes de seguridad como secuestro de pc, corrupción del SO por algún malware o problemas de hardware como disco duro o tarjeta madre de un computador en la organización también se ven favorecidos, partiendo del supuesto que la organización posee la infraestructura para desplegar una imagen de disco o inclusive si no la tuviera y solo tuviera las imágenes de disco duro previamente hechas y almacenadas de sus modelos de computadores que usen sus colaboradores, la tarea sería tan trivial como sacar un computador nuevo de bodega, clonarlo con la imagen de disco respectiva y

personalizarlo según el usuario o departamento al cual pertenece este computador, esta tarea demoraría el tiempo que tome sacar el computador de la caja y armarlo unos 30 minutos + los 30 minutos en clonarlo + 60 minutos(como máximo) en personalizarlo y 30 minutos más entre dejárselo instalado en su puesto de trabajo al usuario final, daría en el mejor de los casos de 2 a 3 horas volver a restablecer el servicio de un computador dañado de un usuario vs 10 horas con el método convencional de instalar todo desde cero.

Tabla 3.1 Tiempo requerido para desplegar un computador [14]

PC Deployment Maturity Level	Hours	% Reduction Compared with Basic
Average	1.66	43%
Basic	2.90	NA
Standardized	1.73	40%
Rationalized	1.29	56%
Dynamic	0.70	76%

Source: IDC, 2010

Tabla 3.2 Diferencias Regionales en costos de despliegue de computadores [14]

	Worldwide	US	EMEA	AP
IT labor	$436	$394	$523	$575**
Logistics	$91	$97	$70	$90
Lost user productivity	$51	$54	$66	$26
Total	$578	$546	$659	$690

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

1. Utilizando conceptos de clonación, multicast, PXE y distribución de imagen de disco duro por medio de red local utilizando DRBL los tiempos de despliegue de un laboratorio de 60 Pc pasan de varias horas a un par de horas.

2. Previo a la creación de imagen y clonación de una pc, el hardening que se aplica al sistema operativo y todas la previsiones de seguridad del caso como parches y actualizaciones, así como

configuraciones mínimas redujeron los tiempos de preparación que se necesita hacerlo maquina por maquina así como el esfuerzo y el riesgo de olvidar hacer los mismo en muchas maquinas.

3. Aplicando el concepto de Particionamiento de disco duro en sistema y usuario se logra un mejor rendimiento del sistema operativo así como al momento de restaurar la Pc con su imagen de disco se garantiza que la data del usuario se mantenga intacta y se evita el tiempo perdido de respaldar primeramente esta información para poder restablecer el sistema operativo así mismo restablecer el pc a un estado anterior saludable es más rápido y mejor que averiguar que corrompió el sistema operativo.

RECOMENDACIONES:

1. Tener un servidor de imágenes de disco duro, para hacer las tareas de despliegue y restauración.

2. Tener una imagen de disco base por modelo de Pc que se tenga en la organización o por perfil si el almacenamiento lo permite como respaldo.

3. Actualizar cuando amerite las imágenes de disco, restaurándolas en un equipo de prueba correspondiente al hardware de la imagen y partir de

ahí con las actualizaciones como por ejemplo nuevos parches, actualizaciones, nuevas versiones de aplicaciones para así volver a desplegar dicha imagen en los planes de mantenimiento correspondientes.

4. Buscar la mejora continua en la tarea del creación de imágenes, clonación, el mercado siempre está ofreciendo nuevas alternativas de cómo hacer mejor lo que ya se hace con mejores aplicaciones open source, como por ejemplo poder tener una sola imagen de disco base y poder restaurarla en cualquier otro equipo aun con hardware diferente, esto se llama “Image disk Restoring over dissimilar hardware”

BIBLIOGRAFÍA

[1] Free Software Labs NCHC.org.tw, DRBL, http://drbl.org/about/ ,fecha de consulta diciembre de 2015.

[2] Max Lyadvinsky, Particionamiento de disco duro aumenta el rendimiento,www.acronis.com/es-mx/resource/tech-talk/2004/partitioning-1-introduction.html, fecha de consulta diciembre de 2015.

[3] André Sanchez, Como mejorar el rendimiento del disco duro, www.taringa.net/post/hazlo-tu-mismo/16295691/Formatear-y-Particionar-Disco-Duro-para-mejorar-Rendimiento.html, fecha de consulta diciembre de 2015.

[4] Australian Cyber Security Centre, Hardening para Sistemas Operativos Windows 7 SP1, www.asd.gov.au/publications/protect/Hardening_Win7_SP1.pdf, fecha de consulta diciembre de 2015.

[5] Australian Cyber Security Centre, Hardening para Sistemas Operativos Windows 8.1, www.asd.gov.au/publications/protect/Hardening_Win8.pdf, fecha de consulta diciembre de 2015.

[6] Australian Cyber Security Centre, Hardening Microsoft Office 2013, www.asd.gov.au/publications/protect/Hardening_MS_Office_2013.pdf, fecha de consulta diciembre de 2015.

[7] Torsten Wittrock, WSUS Offline Updater, www.wsusoffline.net/, fecha de consulta diciembre de 2015.

[8] xfce.org, Entorno de escritorio Linux XFCE, www.xfce.org/, fecha de consulta diciembre de 2015.

[9] Free Software Labs NCHC.org.tw, Clonezilla, http://clonezilla.org/, fecha de consulta diciembre de 2015.

[10] Wikipedia, PXE (Preboot eXecution Enviroment), https://es.wikipedia.org/wiki/Preboot_Execution_Environment, fecha de consulta diciembre de 2015.

[11] Ivan Estevez, Que es Multicast, www.somosbinarios.es/que-es-multicast/, fecha de consulta diciembre de 2015.

[12] Manuel Domínguez, Clonación multicasting con DRBL, https://madoti.wordpress.com/2013/03/30/clonacion-multicasting-con-drbl, fecha de consulta diciembre de 2015.

[13] techsoupforlibraries.org, Desplegando computadoras nuevas que preguntarse y porque?, www.techsoupforlibraries.org/cookbook-3/buying-and-deploying-technology/tools/deploying-new-computers-what-to-ask-and-why, fecha de consulta diciembre de 2015.

[14] Matt Healey (Dell), Modelo optimizado de despliegue de Computadores Dell, http://marketing.dell.com/Global/FileLib/hp_microsite/idc-client-deploy.pdf, fecha de consulta diciembre de 2015.

[15] techsoupforlibraries.org , Estandarizando la infraestructura TI, www.techsoupforlibraries.org/cookbook-3/buying-and-deploying-technology/standardizing-your-it-infrastructure, fecha de consulta diciembre de 2015.

[16] techsoupforlibraries.org, 8 consejos inteligentes para estandarizar su equipo de cómputo, www.techsoupforlibraries.org/Cookbooks/ PlanningforSuccess/BuyingandDeployingTechnology/Tools/eight-smart-tips-for-standardiz, fecha de consulta diciembre de 2015.

[17] techsoupforlibraries.org, Que buscar en un de software de Clonación, www.techsoupforlibraries.org/Cookbooks/PlanningforSuccess/BuyingandDeployingTechnology/Tools/guidelines-for-diskcloning, fecha de consulta diciembre de 2015.

[18] drive-image.com, Clonación de disco y despliegue masivo, www.drive-image.com/Disk_Cloning_and_Mass_System_Deployment.shtml, fecha de consulta diciembre de 2015.