UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Reingeniería del sitio y el servidor web del Laboratorio de Redes y Seguridad FI

TESIS

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A N

Hernández Mendoza Gerardo Daniel
Luna Flores Lorena

DIRECTORA DE TESIS

M.C. María Jaquelina López Barrientos

Ciudad Universitaria, Cd. Mx., 2019

Agradecimientos

Agradezco a Dios por brindarme todas las oportunidades para poder llegar a este punto de la vida donde no solo estamos logrando concluir la meta de un ciclo académico, también finalizamos una etapa de conocimientos y aprendizaje continuo, y en esta meta no solo somos nosotros quién la alcanzamos también es nuestra familia quien forma parte de este logro, padres, hermanos y familiares son un gran regalo que Dios nos da para poder apoyarnos cuando nuestra alma se siente cansada, gracias familia por todo.

Cuando hablo de mi familia me gustaría regalarle unas palabras a mis padres que me han dado todo y más para llegar a lo que hoy en día soy, con ayuda y sacrificios que ellos hicieron, su apoyo que me brindaron en situaciones complicadas me hacen darme cuenta que una vida académica no solo te pertenece a ti que asistes a clases y cursos también es de los que te brindaron la oportunidad. Gracias María Eugenia Flores Olmos y Vicente Luna Sandoval por permitirme demostrarles que los retos se pueden cumplir con mucho esfuerzo, dedicación y disciplina, los amo con todo mi corazón y siempre serán las mejores personas que yo jamás habré conocido en la vida.

A mis hermanos les debo de agradecer por todo el conocimiento que me brindaron, agradezco ser la menor porque Areli Luna Flores y Omar Luna Flores son unos excelentes ejemplos para mí, siempre pensaré que debo de hacer más para poder ser merecedora de pertenecer a una familia de unos grandes como ellos lo son, su esfuerzo diario es una gran inspiración y la actitud que me han enseñado a mantenerme fuerte para poder superar cada reto que se me presente. Gracias hermanos por todo lo que me han ayudado, los amo y no imagino a unos mejores hermanos que pude tener.

Many people think that it is difficult to find someone who can complete you in almost all aspects, it can even take many years to find a perfect person for you and, in fact it is, because each person is different and has their qualities and defects, but God is so wise that he sent me someone who filled me in all aspects, thanks to José Alfredo Morquecho for making me so happy and for giving me many moments that I will never forget. I want you to continue on my path forever and I hope so, but meanwhile I want to tell you that I love you very much and I want to thankfully because since you entered my life I feel more alive and nobody has made me feel in that way before.

Hay alguien a quien no podía dejar de agradecer por todo lo que hemos logrado juntos y es Gerardo Hernández Mendoza, amigo, eres una persona talentosísima, gracias por ser mi hermano en nuestra carrera, siempre lo hemos dicho y pensado que somos un gran equipo y de verdad no quisiera realizar un trabajo para concluir una etapa muy importante en mi vida sin ti, gracias por ayudarme siempre a ser mejor, por ayudarme a siempre mantenerme en la carrera y gracias por ser mi apoyo en los momentos más difíciles.

También deseo agradecerle a mi Universidad que me ha dado tanto en tan poco tiempo, gracias a todos los profesores por enseñarnos el camino que nosotros hemos decidido seguir, gracias a nuestra asesora M.C. Ma. Jaquelina López Barrientos por darnos una oportunidad de crecimiento y apoyarnos cuando necesitábamos.

Lorena Luna Flores

Agradecimientos

A Dios y a Santiago Apóstol por haberme brindado grandes bendiciones y la oportunidad de seguir siendo mejor cada día.

A mi abuelita Rebeca, porque sé que siempre está a mi lado cuidándome. Te dedico este trabajo con todo mi amor y agradecimiento.

A mis padres, que son los que me impulsan día con día a seguir adelante, por guiarme desde pequeño y por todo su apoyo. Este logro se los debo a ustedes.

A ti mamá, por ser una gran amiga y una gran mujer. Gracias por tu paciencia, tu tolerancia y por siempre confiar en mí. Todo tu esfuerzo se ve reflejado en este trabajo y esta etapa que termina, espero que te llene de orgullo y satisfacción tanto como a mí.

A mi manita Jessy, que se convirtió en mi confidente, en mi cómplice y con la que me divierto como enano porque todo lo que hacemos termina en risas. Llegar hasta este punto no hubiera sido lo mismo sin ti.

A mi familia, un ejemplo de unión, alegría y fortaleza. Me siento orgulloso de decir que soy Mendoza.

A mi abuelito y a mis tías, porque en gran medida se debe a ustedes la persona que soy ahora. Muchas gracias por estar siempre al pendiente de mí y porque están ahí en el momento justo.

A mi querida Universidad, a mi Facultad y a todos los profesores que compartieron conmigo sus conocimientos y experiencias, las cuales sin duda han sido valiosas en mi formación académica.

A nuestra asesora, la M.C. Ma. Jaquelina López Barrientos, por su paciencia, dedicación, apoyo y por confiar en nosotros para llevar a cabo este proyecto. Gracias por hacerme parte del Laboratorio de Redes y Seguridad.

A la M.C. Cintia Quezada Reyes, por sus valiosos consejos, su apoyo y el tiempo que invirtió para escucharnos y asesorarnos.

A mi gran amiga Lorena, por todos los momentos que hemos compartido, clases, proyectos, desveladas, salidas y una que otra escapada. Este trabajo representa todo el esfuerzo que realizamos como equipo. No pude haber tenido mejor compañía.

A mis comadres, porque, aunque a veces es complicado vernos, la amistad continúa.

A los amigos que conocí a lo largo de la carrera, en mi paso por UNICA, con los que tuve el privilegio de cantar siendo parte de Ars Iovialis, con los que me tocó trabajar en la DICT y a los que la vida me puso en el camino. No los nombro por el temor a dejar fuera a alguno, a cada uno de ustedes le tengo un gran aprecio y cariño.

Gerardo Daniel Hernández Mendoza

Índice

Índice de Figuras

Índice de Tablas

Introducción

Con el auge de las redes informáticas y la llegada de Internet, el estilo de vida de las personas ha cambiado y en el día a día cada vez es más común utilizar un navegador para buscar información, hacer transacciones, comprar por Internet o simplemente hacer uso de redes sociales. Indudablemente el acceso a Internet se ha convertido en algo indispensable en la vida cotidiana de la sociedad en la actualidad.

El avance tecnológico ha dado la oportunidad de acceder a Internet prácticamente desde cualquier lugar y desde distintos dispositivos como computadoras de escritorio, computadoras portátiles, teléfonos inteligentes y tabletas electrónicas, entre otros; cambiando completamente el estilo de vida, en especial los hábitos de los consumidores a la hora de buscar un producto o servicio.

En la actualidad se ha vuelto necesario para cualquier organización, desde la más grande a la más pequeña, disponer de una página web, con el fin de darse a conocer a través de Internet, divulgando su negocio, su identidad y su imagen.

Con base en lo antes expuesto, desde semestres atrás el Laboratorio de Redes y Seguridad de la Facultad de Ingeniería cuenta con una página web propia, la cual no solo da a conocer los cursos y las diferentes actividades que en él se llevan a cabo, también en dicha página los alumnos inscritos pueden descargar las prácticas que cada semana se realizan, entre otras cosas.

La página web del laboratorio recientemente ha presentado algunos problemas, tanto en su ejecución como en la administración de la misma. Debido a la premura con la que en su momento se realizó, la creación de la página web no cuenta con una documentación detallada, lo que ahora representa un problema, puesto que para administrar la página se ha invertido tiempo en tratar de entender la forma en que esta trabaja.

Otro problema, es la obsolescencia de las aplicaciones con las que opera la página web, la cual constantemente se está renovando en cuanto a contenido se refiere, pero no se ha llevado a cabo una actualización de las aplicaciones que se requieren para que funcione adecuadamente, ahora las versiones con las que se cuenta son obsoletas.

Entre más antigua es una versión de software, más vulnerable es. Por lo general, conforme se van descubriendo las vulnerabilidades, se van parchando por el fabricante, estos parches son liberados con las actualizaciones, pero ya no están disponibles cuando se cuenta con una versión que ha dejado de existir.

Por lo expuesto, es importante realizar una nueva investigación que permita identificar claramente las necesidades actuales del laboratorio, desarrollar e implementar la solución adecuada y tomar las precauciones necesarias a fin de que esto no se vuelva a presentar.

De esta forma, el capítulo 1 inicia con una descripción de los temas necesarios para el desarrollo de este trabajo. Los temas que se abordan son servidores, sistema operativo Linux, páginas web y seguridad informática. Todos ellos en un lenguaje claro y entendible incluso para usuarios ajenos al área computacional.

Posteriormente, en el capítulo 2 se da una descripción detallada de la solución propuesta para la configuración del servidor y el diseño del sitio del Laboratorio de Redes y Seguridad. La primera parte del capítulo corresponde a la configuración del servidor, es decir, la elección del sistema operativo y la instalación de las aplicaciones necesarias para convertirse en un servidor web. La segunda parte corresponde al diseño de la página web, incluyendo la elección de las herramientas de apoyo para la creación de la misma, así como el diseño basado en las necesidades actuales y futuras del Área de Redes y Seguridad y su laboratorio.

Enseguida, el capítulo 3 describe las configuraciones que se le deben hacer a un servidor después de instalar el Sistema Operativo y antes de ser conectado a Internet, con el objetivo de fortalecer su seguridad. De igual manera, se propone una serie de modificaciones a nivel de BIOS y en los servicios instalados en el sistema.

Finalmente, en el capítulo 4 se muestra la metodología con la que se lleva a cabo la implementación de la solución propuesta en el capítulo 2, así como las pruebas para garantizar el correcto funcionamiento del servidor y el sitio web.

Por último, se presentan las conclusiones a las que se llegaron en el presente trabajo, basadas completamente en los resultados obtenidos.

Objetivos

La presente tesis tiene un objetivo general y cuatro objetivos específicos. El objetivo general es tener un servidor y un sitio web funcionales para el Laboratorio de Redes y Seguridad. Todo lo anterior con la debida documentación de los pasos realizados, que serán de utilidad para quien administre el servidor y el sitio web.

Para alcanzar el objetivo general, se persiguen cuatro objetivos específicos. El primer objetivo específico busca describir los conceptos básicos, tipos de servidores, las características principales de un sistema operativo Linux, características de una página web y conceptos básicos de seguridad informática con el fin de hacer un análisis y con base en ello tomar decisiones a lo largo del proyecto.

El segundo objetivo específico consiste en plantear una solución, definiendo las configuraciones necesarias para el servidor web, tales como el sistema operativo a instalar, el esquema de particionado y las aplicaciones necesarias para la operación del mismo. Además, de diseñar el sitio web del Laboratorio de Redes y Seguridad.

El tercer objetivo específico fortalece la seguridad del servidor, definiendo las configuraciones necesarias posteriores a la instalación del sistema operativo,

El cuarto objetivo específico constituye la implementación de la solución propuesta, aplicando las configuraciones planteadas en ella al servidor y al sitio web del laboratorio, además de hacer las pruebas necesarias para garantizar su correcto funcionamiento.

Capítulo 1

Antecedentes

En el primer capítulo se definen los conceptos básicos de temas complementarios para el desarrollo de este trabajo de tesis, los cuales sirven como referente para hacer un análisis y tomar decisiones en los capítulos posteriores.

1.1. Sistema operativo

Un sistema operativo es un programa que actúa como intermediario entre el usuario de una computadora y el hardware de ésta, su objetivo es utilizar el hardware de la computadora de una manera cómoda, segura y eficiente.

Un sistema de cómputo tiene recursos que son utilizados para resolver un problema: espacio de memoria, espacio de almacenamiento de archivos, dispositivos de entrada y salida, entre otros. El sistema operativo actúa como gestor de dichos recursos y los asigna a programas y usuarios específicos según los necesiten para sus tareas. Además, controla la ejecución de los programas de los usuarios a fin de evitar errores [1].

Un sistema operativo está formado por tres capas principales, como se muestra en la Figura 1.1. La capa más cercana al hardware se denomina núcleo (*kernel*) y es la que gestiona los recursos hardware del sistema y la que suministra la funcionalidad básica del sistema operativo.

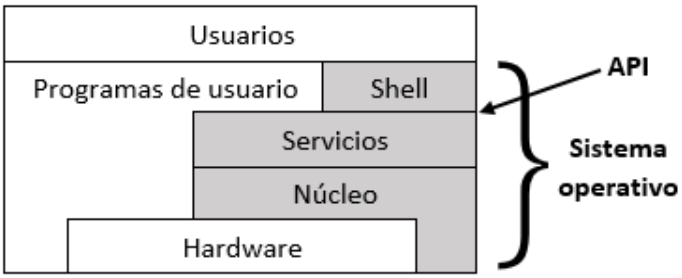


Figura 1.1 Niveles del sistema operativo
Nota. Imagen recuperada de "Sistemas operativos: Una visión aplicada", de Carretero, J. (2001).

La capa de servicios ofrece a los programas unos una interfaz gráfica o *API*, de esta forma se facilita la elaboración de los servicios, puesto que se apoyan en las funciones que se suministra el sistema operativo.

La capa de intérprete de comandos o *shell* suministra una interfaz a través de la cual el usuario interactúa con la computadora. El shell recibe los comandos u órdenes del usuario, los interpreta y, si puede, los ejecuta [2].

1.1.1. Sistemas operativos más comunes

Los sistemas operativos más comunes que se ofrecen en el mercado cuando son: Microsoft Windows, Mac OS X y Linux.

Microsoft Windows

Fue desarrollado en la década de los ochenta. Sus versiones más recientes son Windows 10; Windows 8, creado en el año 2012 y Windows 7, en el 2009.

[1] Silberschatz, Abraham. (2004). "Sistemas operativos". México, D.F.: Limusa.
[2] Carretero, J. (2001). "Sistemas operativos: Una visión aplicada". Madrid: McGraw-Hill.

Windows viene preinstalado en la mayoría de las computadoras nuevas, haciéndolo el sistema operativo más utilizado en equipos personales.

Mac OS X

Es el sistema operativo creado por Apple Inc. el cual viene instalado en todas sus computadoras. Todas las versiones recientes son conocidas como MacOS X y los nombres específicos de cada una de estas son: Mavericks, lanzada en 2013; Mountain Lion, en el 2012; Lion, en el 2011 y Snow Leopard que fue creada en el 2009.

Apple también ofrece una versión llamada MacOS X Server que está diseñado para ejecutarse en servidores.

Linux

Es un sistema operativo de código abierto, esto significa que puede ser modificado y distribuido por cualquier persona alrededor del mundo. Esta es una de sus ventajas, ya que no se tiene que pagar por él y se puede elegir entre las diferentes versiones que existen.

En las computadoras personales, Linux, a pesar de ser gratuito, es muy poco usado, pero la mayoría de servidores lo utilizan, ya que es fácil de personalizar.

En la Tabla 1 se muestran algunas características de cada sistema operativo y la comparación entre los sistemas más populares.

Tabla 1.1 Comparativa de sistemas operativos

	Windows	**Linux**	**MacOS X**
Costo	✓	✗	✓
Buena gestión de recursos	✗	✓	✓
Interfaz gráfica	✓	✓	✓
Necesidad de conocimientos para operarlo	✗	✓	✗
Estabilidad	✗	✓	✓
Facilidad de uso	✓	✓	✓
Soporta diferentes sistemas de archivos	✗	✓	✗

Variedad en programas	✓	✓	✕
Rápida solución de errores	✕	✓	✕
Facilidad de instalación	✓	✓	✕
Interoperabilidad	✕	✓	✕
Código abierto	✕	✓	✕
Estabilidad	✕	✓	✕
Actualizaciones automatizadas	✕	✓	✕

1.2. Linux

Linux es un sistema operativo diseñado y desarrollado por cientos de programadores informáticos, con él se pretendía realizar una réplica del sistema operativo privativo *MINIX*, sin programas registrados de por medio, para que todos los usuarios que así lo desearan pudieran utilizarlo [3].

Linux es el resultado del trabajo de miles de desarrolladores en todo el mundo bajo las ideas del Software Libre. El movimiento de Software Libre fue iniciado por Richard Stallman en 1984 con el proyecto *GNU*. Sus postulados, o en este caso libertades, sobre los que se basa son los siguientes:

- La libertad de usar el programa, con cualquier propósito
- La libertad de estudiar cómo funciona el programa y modificarlo, adaptándolo a las necesidades del proyecto.
- La libertad de distribuir copias del programa, con lo cual se puede ayudar al prójimo.
- La libertad de mejorar el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie.

Las características más relevantes del sistema operativo Linux son:

- Multitarea: Se pueden realizar varias actividades a la vez (navegar por Internet, editar un documento, compilar un programa, entre otras).
- Multiusuario: Varios usuarios pueden trabajar concurrentemente en una única computadora con varios terminales (teclado y monitor) de forma que tengan la sensación de que es el único que está trabajando en el sistema. Cada usuario almacena sus datos en una cuenta privada.

[3] Tackett, J. (2000). "Edición especial Linux". México: Prentice Hall.

- Conectividad: Permite las comunicaciones en red y el acceso a recursos remotamente. Por ejemplo, se puede acceder a datos situados en una máquina a través de otro equipo, conectados ambos a Internet.
- Multiplataforma: Se puede instalar en multitud de dispositivos, desde todo tipo de computadoras, portátiles y servidores hasta videoconsolas.
- Libre: Su código fuente está disponible. Cualquiera puede usarlo, modificarlo y distribuir. Una consecuencia de esto es que es gratis.

1.2.1. Sistema de archivos de Linux

Se puede definir de forma genérica al archivo como un conjunto de datos con un nombre asociado. Los archivos suelen residir en dispositivos de almacenamiento secundario, tales como cintas o discos rígidos.

Un sistema de archivos es aquella parte del sistema responsable de la administración de los datos en dispositivos de almacenamiento secundario. El sistema de archivos debe proporcionar los medios necesarios para un almacenamiento seguro y privado de la información y, a la vez, la posibilidad de compartir esa información en caso de que el usuario lo desee.

En Linux los archivos están organizados en lo que se conoce como directorios, que a su vez pueden contener nuevos directorios, los cuales se denominan subdirectorios. El sistema de archivos de Linux tiene una estructura de árbol invertido. En él, todos los archivos y directorios dependen de un único directorio denominado directorio raíz o root, el cual se representa por el símbolo "/", como se muestra en la Figura 1.2.

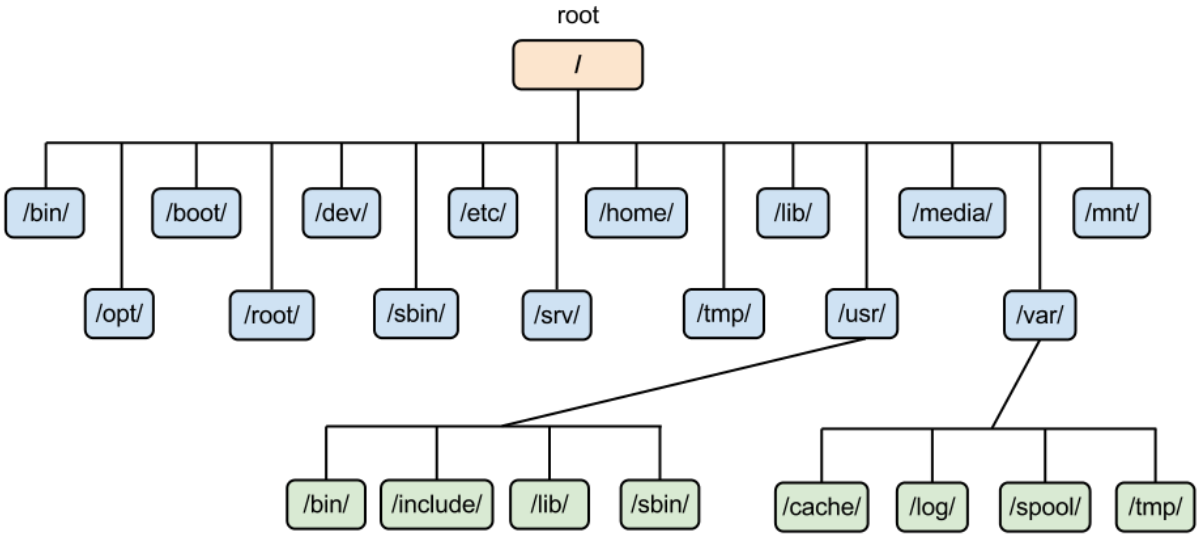


Figura 1.2 Árbol de directorios de Linux

Nota. Imagen recuperada de "Jerarquía estándar sistema de ficheros UNIX", de Alonso, J. (3 enero 2018). Recuperado de: https://javiermartinalonso.github.io/linux/2018/01/03/linux-jerarquia-sistema-ficheros.html

El estándar de jerarquía del sistema de archivos (FHS, del inglés Filesystem Hierarchy Standard) es una norma que define los directorios principales y sus contenidos en el sistema operativo GNU/Linux y otros sistemas de la familia Unix. Se diseñó originalmente en 1994 para estandarizar el sistema de archivos de las distribuciones de Linux, basándose en la tradicional organización de directorios de los sistemas Unix.

Los directorios definidos por FHS, se definen en la Tabla 1.2.

Tabla 1.2 Estándar de jerarquía del sistema de archivos.

Directorio	Contenido
bin	Binarios esenciales del sistema
boot	Ficheros estáticos utilizados por el cargador de arranque
dev	Ficheros de dispositivo
etc	Ficheros de configuración específicos del equipo
home	Directorios de los usuarios
lib	Bibliotecas compartidas esenciales y módulos del núcleo
media	Puntos de montaje para medios extraíbles
mnt	Punto de montaje temporal para un sistema de ficheros
proc	Directorio virtual que contiene la información del sistema
root	Directorio del usuario administrador del equipo
run	Run-time variable data
sbin	Binarios esenciales del sistema
sys	Directorio virtual que contiene la información del sistema
tmp	Ficheros temporales
usr	Jerarquía secundaria
var	Datos variables
srv	Datos de los servicios ofrecidos por el sistema
opt	Paquetes de programas y aplicaciones opcionales instalados manualmente

1.2.2. Particiones

Las particiones en el disco son parte estándar de los entornos de un ordenador y lo han sido durante bastante tiempo. Sin embargo, con tantos sistemas operativos pre-instalados, pocas veces se entiende el funcionamiento de las particiones. Los discos duros cumplen una función sencilla, pueden contener datos y recuperarlos de manera segura.

Para crear particiones en el disco duro, es importante saber lo que sucede cuando se particiona un disco duro, la siguiente figura muestra un disco nuevo sin utilizar (Figura 1.3).

Figura 1.3 Disco duro sin usar

Si se quiere guardar datos en un disco que no se ha usado antes, no funcionará, puesto que es necesario *formatear* el disco, con el fin de crear el *sistema de archivos* (véase Figura 1.4).

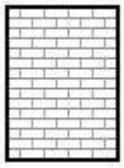


Figura 1.4 Disco formateado

Comparando la Figura 1.3 y 1.4, se aprecia que una vez formateado el disco duro, este queda segmentado en bloques de tamaño consistente, es en esos bloques donde se almacenará la información.

Es importante recalcar que no hay un único sistema de archivos (véase Figura 1.5), a lo largo del tiempo se han desarrollado diferentes sistemas para la administración de la unidad de almacenamiento y la asignación de espacio a los archivos, depende del sistema operativo y del tipo de información que se van a almacenar, es el sistema de archivos con el que se decida trabajar.

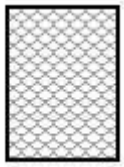


Figura 1.5 Disco duro con sistema de archivos diferente

Escribir un sistema de archivos es sólo el principio, ya que el objetivo de este proceso es realmente el de almacenar y recuperar datos, la Figura 1.6 muestra una unidad tras la escritura de algunos archivos.

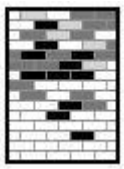


Figura 1.6 Disco duro con datos escritos

Con el avance de la tecnología, también las unidades de disco han cambiado, en concreto, los discos son más grandes, sin referirnos al tamaño, sino a su capacidad de almacenamiento, misma que ha llevado a un cambio en la manera en que se utilizan los discos.

El particionamiento de un disco duro permite dividirlo en secciones aisladas, donde cada sección se comporta como un disco duro independiente. El particionamiento es especialmente útil si se ejecuta más de un sistema operativo, cada una de las particiones creadas tiene sus propios atributos físicos y lógicos de los cuales los más relevantes son tamaño, tipo de partición, formato y punto de montaje.

Para acceder a cada una de las particiones se hace por medio de una *tabla de particiones*.

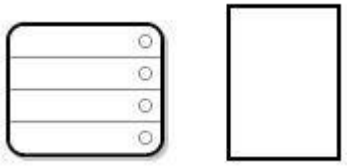


Figura 1.7 Disco duro con tabla de particiones

Como se muestra en la Figura 1.7, la tabla de particiones está dividida en cuatro secciones o cuatro particiones primarias. Una partición primaria es aquella que puede contener solamente una unidad lógica o sección. Cada sección puede contener la información necesaria para definir una sola partición, esto quiere decir que la tabla de las particiones puede definir no más de cuatro particiones.

Cada elemento de la tabla de las particiones contiene importantes características relativas a la partición:

- Los puntos en el disco donde la partición empieza y termina
- Si la partición está "activa"
- El tipo de partición

Los puntos de comienzo y de fin realmente definen el tamaño de las particiones y su posición en el disco. La bandera "activa" es utilizada por algunos gestores de arranque de sistemas operativos. En otras palabras, el sistema operativo que se encuentra con la partición definida como "activa" es donde arrancará el ordenador.

Algunos sistemas operativos utilizan un tipo de partición para detectar un tipo específico de sistema de ficheros, para asociar la partición a un sistema operativo, para indicar que la partición contiene un sistema operativo que puede ser arrancado o para una combinación de los tres.

Existen tres tipos de particiones, las cuales a continuación se definen dando a conocer sus limitaciones y el correcto uso de ellas.

1. Primaria

Este tipo de partición es definida directamente sobre el disco duro y está escrita en la tabla de particiones. En esta partición es donde se instalan los sistemas operativos. Solo existe una limitación sobre esta partición y es que en un mismo disco duro solo puede haber 4 particiones primarias.

2. Extendida

Fue creada para poder tener más de 4 particiones en un disco y en teoría se pueden tener tantas como se requieran. El principal inconveniente es que no se puede instalar un sistema operativo sobre esta partición y simplemente se puede usar para almacenar datos.

3. Lógica

Son las particiones que se crean como parte de una partición extendida, y se les asigna un tamaño, un sistema de ficheros y son usadas por el sistema operativo.

1.2.3. Logical Volume Management

LVM es una implementación que consiste en un administrador de volúmenes lógicos para el núcleo de Linux y está disponible en la mayoría de los sistemas Linux para utilizarlo al momento de la instalación.

Los conceptos elementales de LVM son:

- Volumen físico (PV): Un PV es un disco rígido, una partición o un RAID.
- Volumen lógico (LV): Un LV es el equivalente a una partición tradicional.
- Grupo de volúmenes (VG): un grupo de volúmenes reúne uno o más PVs.

Las funcionalidades que ofrece son:

- Redimensión de grupos de volúmenes y volúmenes lógicos.
- Crear instantáneas (snapshot) de lectura/escritura del sistema de archivos.
- Constituir los volúmenes lógicos separados en los diferentes volúmenes físicos.
- Mover los volúmenes lógicos entre los diferentes volúmenes físicos.

La principal ventaja de LVM es que quita el inconveniente de dimensionar exactamente las particiones tal cuál se necesitan, encontrando después que el esquema de particionado escogido no es el más adecuado. Con LVM se puede aumentar o disminuir el espacio de una partición, aunque el servidor esté en producción.

1.2.4. Distribuciones para servidores

Las distribuciones de Linux, son una colección de software basada en el núcleo de Linux que incluye determinados paquetes de software para satisfacer las necesidades de un grupo específico de usuarios. Por lo general, están compuestas total o mayoritariamente de software libre, aunque a menudo incorporan aplicaciones o controladores propietarios.

Existen distintas distribuciones diseñadas para servidores, en la Tabla 1.3, se listan y se comparan las más populares de ellas.

Tabla 1.3. Distribuciones Linux para servidores

Red Hat Enterprise Linux	Ubuntu Server	Debian
		
Entorno de virtualización.	Soporte para diferentes configuraciones de red.	Admite una gran cantidad de arquitecturas de computadora.
Su modelo de negocio se basa en la suscripción por servicios de mantenimiento y asistencia técnica.	Eficiente para crear centros de datos empresariales de alto rendimiento escalables, flexibles y seguros.	En los repositorios hay más de 51,000 programas estables y libres, que utilizan un eficiente sistema de empaquetado.
Optimizado para procesadores multinúcleo.	Actualmente existen proyectos de Ubuntu para Internet of Things.	Tiene un sistema de seguimiento de errores y se puede obtener soporte consultando su documentación y recursos web gratuitos.
Admite las arquitecturas x86, x86-64, Itanium, PowerPC e IMB System Z.	Sistema operativo basado en Debian.	Sus características más relevantes son: estabilidad, soporte y compatibilidad.
Estable y seguro para centros de datos con almacenamiento orientado a software.	Admite las arquitecturas x86, ARM y Power.	Debian es estable, sencillo de administrar, y con soporte por parte de una gran comunidad.

La aplicación Network Manager proporciona configuración automática de redes cableadas e inalámbricas.	Cuenta con Ubuntu Advantage, con la cual se obtiene soporte comercial y servicios como la administración de sistemas de auditoría de seguridad.	Cuenta con múltiples entornos de escritorios como Aweome, Black Box, Fluxbox, KDE, Openbox y muchos más.
Gráficos mejorados mediante el uso de diversas herramientas.	Cuenta con varios entornos de escritorio como Gnome, Unity, KDE, entre otros.	Distribución de Linux más popular por su estabilidad, rapidez y por ser ligera.
Admite sistemas operativos invitados virtualizados.	Linux Mint, Kubuntu, Lubuntu, entre otros, están basados en esta distribución.	Un amplio abanico de organizaciones e individuos hacen uso Debian.

1.3. Arquitectura cliente/servidor

Cliente/servidor es una arquitectura de red en la que cada ordenador o proceso en la red es cliente o servidor.

El término *servidor* se aplica a cualquier programa que ofrece un servicio que se puede obtener en una red, mientras que el *cliente* es un programa que manda una petición a un servidor y espera una respuesta. Normalmente, los servidores son computadoras potentes dedicadas a gestionar recursos y los clientes son máquinas menos potentes y usan los recursos que ofrecen los servidores, como se muestra en la Figura 1.8. [4]

Figura 1.8 Arquitectura cliente/servidor
Nota. Imagen recuperada de "Estructura de un sistema operativo".
Recuperado de: http://wiki.inf.utfsm.cl/images/6/68/Cliente-servidor.png

El funcionamiento básico de la arquitectura cliente/servidor es el siguiente:

1. Se inicia el servidor. Esto ocurre durante el arranque del sistema operativo o con la intervención posterior del administrador del sistema, cuando termine de iniciarse, esperará de forma pasiva las solicitudes de los clientes.

[4] Comer, D. "Redes globales de información con Internet y TCP/IP". México: Prentice-Hall

2. En algún momento, uno de los clientes conectados a la red realizará una solicitud al servidor.
3. El servidor recibe la solicitud del cliente, realiza cualquier verificación necesaria y, si todo es correcto, la procesa.
4. Cuando el servidor disponga del resultado solicitado, lo envía al cliente.
5. Finalmente, el cliente recibe el resultado que solicitó. A continuación, realiza las comprobaciones oportunas (si son necesarias) y, si era ese el objetivo final, lo muestra al usuario.

1.4. Página web

1.4.1. Internet

Internet se puede definir como una "red de redes", es decir, una red que no sólo conecta computadoras, sino que interconecta redes de computadoras entre sí. Esta red conecta a millones de usuarios a nivel mundial y funciona, al igual que la línea telefónica, mediante cables convencionales, digitales, fibra óptica, vía telefonía celular, vía satélite u otro medio[5].

A través de Internet se puede intercambiar archivos, encontrar información, realizar compras electrónicas mediante tarjeta de crédito, contactar personas por medio de texto, sonido o imagen, por mencionar algunas.

El origen de Internet se debe gracias a un proyecto militar del Ministerio de Defensa de los Estados Unidos, el cual buscaba crear una red de computadoras que uniera los centros de investigación de defensa en caso de ataques para así mantener contacto remotamente y no se viera interrumpido su funcionamiento.

1.4.2. World Wide Web

La tecnología de Internet facilita la conectividad global, y World Wide Web es un medio funcional para que la gente de todo el mundo localice información y comparta el conocimiento.

Por definición, World Wide Web o WWW, es un sistema de navegación para Internet con un formato dinámico para la comunicación masiva. Además de que suministra un sistema de administración y distribución de información.

El sistema Web comenzó en el Laboratorio Europeo de Partículas Físicas, conocido como el *CERN*. Fue en 1989 cuando el físico Tim Berners-Lee propuso el concepto de Web como un sistema para transferir ideas e investigación entre la comunidad de científicos relacionados con la física y la energía de alto nivel.

[5] Kent, P. (1995). "World Wide Web: fácil". México: Prentice Hall.

La propuesta definía un sistema simple que usa *hipertexto*, una forma de organizar la información, de manera que algunas partes del texto, denominadas enlaces, se muestran resaltadas, permitiendo acceder al pulsar ellas a diferentes partes del mismo documento o a otros documentos diferentes.

Con la idea de la creación del hipertexto surgió la idea de la *hipermedia*, en la cual, mediante los enlaces no sólo es posible acceder a otros documentos, sino también a imágenes, animaciones, video y audio [6].

1.4.3. Definición página web

Una página web por definición es un documento electrónico que puede ser escrito en el lenguaje HTML. Se integra por texto, imágenes, videos, animaciones y sonido que son visualizados por un usuario desde un dispositivo a través de un navegador web.

Las palabras sitio web y página web, están estrechamente relacionadas entre sí, motivo por el cual en la mayoría de las ocasiones son usadas como si fueran sinónimos, cuando en realidad se hace referencia a dos cosas diferentes.

Cuando se utiliza la expresión sitio web, se está hablando de un conjunto de páginas que tocan un tema en común contenido en la Web. Por lo que cuando se habla de páginas web, en realidad se refiere a una pequeña parte de un sitio web [7].

Los sitios web se pueden dividir en dos tipos:

- Sitio web estático:

Son sitios enfocados principalmente a mostrar una información permanente, donde el usuario se limita a obtener la información sin poder interactuar con el sitio visitado, se crean mediante código HTML.

- Sitio web dinámico:

Son aquellos en los que la información presentada se genera a partir de una petición del usuario al sitio. La creación de un sitio web dinámico es más compleja, ya que se requiere de conocimientos específicos de lenguajes de programación y gestión de bases de datos.

[6] López, A. & Novo, A. (2000). "Protocolos de Internet: Diseño e implementación en sistemas UNIX". México: Alfaomega.

[7] McFedries, P. (1996). "¡Creando una página web con HTML fácil!". México: Prentice Hall

1.5. Aplicaciones web

Una aplicación web es un programa cliente/servidor, donde tanto el cliente como el servidor se comunican mediante el protocolo HTTP.

El cliente web es un programa con el que interacciona el usuario para solicitar a un servidor web el envío de los recursos que desea obtener mediante HTTP. La misión del cliente es interpretar las páginas web que están formadas por código HTML y recursos hipermedia para mostrarlas al usuario.

Por otro lado, el servidor web es un programa que está esperando permanentemente las solicitudes de conexión por parte de los clientes web [8].

1.5.1. Protocolo HTTP

Para poder navegar por la WWW, se crea el protocolo HTTP (HyperText Transfer Protocol), el cual es un protocolo utilizado para el intercambio de información hipermedia dentro de la WWW.

Es un protocolo que se basa en la filosofía cliente/servidor y su funcionamiento es el siguiente:

- El cliente se conecta al servidor web
- El cliente envía una petición
- El servidor responde a dicha petición

HTTP funciona generalmente sobre TCP/IP y las conexiones se realizan al puerto TCP 80. Sin embargo, muchos servidores colocan el servicio en un puerto diferente, ya sea por motivos de seguridad o para tener varios servidores, cada uno con su propio puerto, ofreciendo un mismo servicio [9].

1.5.2. Servidor web

Apache HTTP y Nginx son los dos servidores web de código abierto con mayor popularidad, cubriendo una gran parte de los sitios web a nivel mundial.

Apache ha sido el más popular en internet desde 1996, cuenta con una gran documentación y soporte proveniente de diferentes proyectos. Debido a su popularidad y al ser de código abierto, cuenta con una gran comunidad de usuarios que son capaces de crear parches y correcciones de errores técnicos muy rápidamente. Además, la documentación se extiende a lo largo de múltiples sitios, foros y blogs.

[8] Luján, S. "Programación de aplicaciones web". España
[9] Comer, D. "Redes globales de información con Internet y TCP/IP". México: Prentice Hall

Por su parte, Nginx fue escrito para atender las limitaciones que tenía Apache. Ha tenido una gran aceptación entre los sitios web de todo el mundo. Es usado por grandes compañías por su estabilidad y bajo consumo de recursos, tales como Dropbox, Netflix, Airbnb, por mencionar algunas. Nginx está experimentando un rápido incremento en su comunidad; mientras que el interés va creciendo, la documentación ha ido en aumento en el sitio de Nginx y a través de terceros.

En la Existen distintas distribuciones diseñadas para servidores, en la Tabla 1.3, se listan y se comparan las más populares de ellas.

En la Tabla 1.4 se presentan algunas de las características de Apache y Nginx.

Tabla 1.4 Características servidores web

Apache	Nginx
	
Es potente y flexible, por lo que funciona en una gran variedad de plataformas y entornos.	Es multiplataforma, esto quiere decir que se puede utilizar en la mayoría de los sistemas operativos.
Cuenta con un diseño modular, el cual, permite a los administradores de sitios web elegir las características que serán incluidas en el servidor, seleccionando los módulos a cargar, ya sea al compilar o al ejecutar el servidor.	Es usado como proxy inverso para IMAP y POP3.
Cuenta con una variedad de módulos de multi-procesos que determinan cómo se manejan las peticiones de los clientes, esto permite a los administradores intercambiar la conexión con un manejo fácil de la arquitectura. Los módulos pueden ser mpm_prefork, mpm_worker y mpm_event.	Tiene un diseño base que utiliza un algoritmo de manejo de conexiones que fuese asíncrono, sin bloqueo y gestionado por eventos.

Genera procesos para manejar nuevas solicitudes entrantes.	No interpreta archivos .htaccess ni provee mecanismo alguno para evaluar la configuración por directorio fuera del archivo de la configuración principal.
Existe una biblioteca extensa de documentación disponible para el servidor y para los escenarios basados en tareas que involucran implementación.	En uso de memoria se mantiene estático independientemente del volumen de tráfico.
Por su gran popularidad, cuenta con amplia documentación sobre su uso y se actualiza frecuentemente.	La documentación fue creada en Rusia con documentación y soporte rusos, lo que incrementa el tiempo y dificultad de documentación.
Crea hilos y sub-hilos para manejar conexiones adicionales, los cuales, el administrador configura en el servidor para controlar el crecimiento de estos, dependiendo del hardware de memoria.	Debido a su multifuncionalidad puede ser utilizado para equilibrar la carga entre los servidores back-end o caché en servidores lentos.

1.6. Seguridad Informática

1.6.1. Amenazas y vulnerabilidades

Es importante hacer notar la diferencia entre amenaza y vulnerabilidad, ya que a menudo se piensa que tienen el mismo significado.

Una amenaza es todo aquello que intenta o pretende destruir o dañar un recurso. Se puede presentar a través de una persona, una circunstancia o evento.

En tanto que una vulnerabilidad es un punto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Puede ser aprovechada por una o varias amenazas para dañar total o parcialmente un bien [10].

[10] López, M. J. & Quezada, C. "Fundamentos de seguridad informática". México, D.F.: UNAM

1.6.1.1. Clasificación general de las amenazas

Las amenazas se clasifican de acuerdo a la fuente de la cual provienen:

- De humanos

La amenaza surge por ignorancia en el manejo de la información, por descuido, por negligencia o por inconformidad. Algunos ejemplos son la ingeniería social, el robo, el fraude, el terrorismo, por mencionar algunos.

- Errores de hardware

Esta amenaza se presenta por fallas físicas en cualquier elemento de los dispositivos de la computadora. Se puede ocasionar pérdida de información, mal funcionamiento del equipo o incluso la pérdida total o parcial del equipo.

- Errores de la red

La amenaza se presenta cuando hay alguna falla en la red, ya sea que se sature el canal de comunicación o por alguna razón se desconecte, provocando pérdida de información o que alguien esté fisgoneando en la red.

- Problemas de tipo lógico

Se presenta cuando un mecanismo de seguridad no cumple con las especificaciones del diseño y se implementa mal en el sistema. Un ejemplo común se presenta cuando el usuario desconoce el software que tiene instalado y un mal manejo permite la entrada de virus o código malicioso al sistema.

- Naturales

Surgen por acciones provocadas por la naturaleza y donde los humanos no tienen participación directa. Este tipo de amenazas repercute en el funcionamiento físico de las computadoras o las líneas de comunicación.

1.6.1.2. Clasificación general de las vulnerabilidades

Las vulnerabilidades se clasifican de acuerdo a las debilidades que están presentes en los sistemas o entornos de información:

- Física

Se refiere al control de acceso físico al sistema. Se relaciona con la posibilidad de entrar o acceder físicamente al lugar donde se encuentra el sistema para dañar, modificar o robar información.

- Natural

Se presenta cuando hay un descuido o falta de precauciones ante un desastre natural. Por ejemplo, la falta de extintores en caso de incendio o el no estar informado de las condiciones climatológicas donde se construye el centro de cómputo.

- De hardware

La principal causa de esta vulnerabilidad son los posibles defectos en la fabricación o configuración en los dispositivos.

- De software

Esta vulnerabilidad se presenta cuando en el sistema existen programas mal diseñados y programados, carentes de seguridad o con errores de configuración. También puede presentarse cuando los programas instalados o el sistema operativo no están debidamente actualizados.

- De red

Una vulnerabilidad de este tipo se presenta cuando existe un mal diseño o planeación de la red, o incluso una mala configuración de la misma.

- Humana

El factor humano es la mayor de las vulnerabilidades además de ser el que causa la mayoría de ellas. Estas pueden ser desde el descuido, la falta de capacitación, la desactualización, la negligencia o la malicia.

Capítulo 2

Diseño de la solución

En el segundo capítulo se describe de manera detallada la solución propuesta para la configuración del servidor web y el diseño del sitio del Laboratorio de Redes y Seguridad.

La primera parte corresponde a la configuración del servidor, es decir, la elección del sistema operativo y la instalación de las aplicaciones necesarias para convertirse en un servidor web.

La segunda parte corresponde al diseño de la página web, incluyendo la elección de las herramientas de apoyo para la creación de la misma, así como el diseño basado en las necesidades actuales y futuras del Área de Redes y Seguridad y su laboratorio.

2.1. Diseño del servidor web

2.1.1. Recursos del servidor

Para este proyecto, el Laboratorio de Redes y Seguridad provee un servidor con las especificaciones que se muestran en la Tabla 2.1.

Tabla 2.1 Especificaciones del servidor

Tipo de servidor	Servidor en rack
Procesador	Intel® Xeon® CPU E3-1230 @ 3.50 GHz
Memoria RAM	40 GB
Almacenamiento	2 discos duros SATA 2.5” 1 TB 7200 RPM
Controlador RAID	PERC H330
Controladora de red	2 de 1 Gigabit Ethernet
Puerto USB	2 frontales, 2 traseros y 1 interno
Administración remota	iDRAC 8 con controladora del ciclo de vida

Se trata de un servidor nuevo, por lo que se planea hacer una instalación desde cero del sistema operativo y las aplicaciones, las cuales se plantean más adelante.

2.1.2. Esquema de particionado

Para el servidor se propone el siguiente esquema de particionado, el cual contará con 3 particiones primarias que se muestran que se muestran en la Tabla 2.2.

Tabla 2.2 Particiones primarias

Punto de montaje	Tamaño
/	50 GB
/boot	2 GB
swap	16 GB

- La partición / es la cima de la estructura del directorio
- La partición swap sirve para soportar la memoria virtual, es decir, los datos se escriben en una partición swap cuando no hay suficiente memoria RAM para almacenar la información que el sistema está procesando.
- La partición montada en /boot contienen el kernel del sistema operativo junto con archivos utilizados durante el proceso de arranque. Para algunos sistemas operativos, una partición de 250 MB es suficiente.

Se separan los directorios /tmp, /usr, /var, /home y /var/www en particiones separadas, ya que son los directorios en los que se espera un mayor crecimiento a futuro. Además, se busca implementar volúmenes lógicos, con los que se puede incrementar el tamaño de las particiones si así se requiere.

Tabla 2.3 Volúmenes Lógicos

Punto de montaje	Tamaño
/tmp	2 GB
/usr	50 GB
/var	200 GB
/home	200 GB
/var/www	800 GB

El servidor cuenta con 2 TB de espacio en disco duro y las particiones de la Tabla 2.2 y 2.3 suman 1320 GB. Por lo que el servidor cuenta con **680 GB libres** que pueden ser utilizados por alguno de los volúmenes lógicos para aumentar su espacio en un futuro.

El esquema de particionado elegido se implementa durante la instalación del sistema operativo, explicado a detalle en el *Anexo A*.

2.1.3. Sistema operativo

- Sistema Operativo

Se decide utilizar un sistema operativo de la familia Linux debido a que es software libre, con lo que no se genera un costo extra, además de que se puede adaptar a las necesidades del laboratorio.

La distribución elegida es en la versión 9.0 “Stretch”. Sus ventajas se describen en la Tabla 2.4.

Tabla 2.4 Ventajas del sistema operativo Debian

Ventajas de usar Debian	Descripción
Es mantenida por sus usuarios	Si algo requiere ser arreglado o mejorado, simplemente se hace.
Soporte técnico incomparable	Cuando se envía una pregunta a las listas de correo, se obtienen respuesta en menos de 15 minutos, gratuitamente, y por las personas que lo desarrollaron.

Instalación sencilla	Se ha mejorado la simplicidad y facilidad de instalación de Debian (ambiente gráfico).
Más de 51,000 elementos de software	Cada paquete es 100% libre, es decir, se puede modificar, redistribuir y no se infringe ninguna ley.
Buena integridad de los paquetes	Todos los paquetes se encuentran en un mismo sitio. Además, es la única distribución que se rige por normas y estándares de calidad.
Fácil actualización	Tan solo con ejecutar `apt-get update; apt-get dist-upgrade`, se puede actualizar el sistema de forma completa.
Sistema de seguimiento de errores	Es un sistema público. Debian responde a los problemas de forma clara, honesta y abierta.
Estabilidad	Existen muchos casos de máquinas que trabajan durante más de un año seguido sin reiniciarse.
Rápido y ligero en memoria	Al estar basado en GNU/Linux, Debian es ligero en casi todos los aspectos a diferencia de otros sistemas (Windows).
Buena seguridad del sistema	La disponibilidad del código fuente permite que la seguridad en Debian se evalúe de forma abierta, lo que evita que se implementen modelos de seguridad pobres.
Software de seguridad	Alta disponibilidad de herramientas de seguridad.

Las desventajas del sistema operativo Debian se describen en la Tabla 2.5.

Tabla 2.5 Desventajas del sistema operativo Debian

Desventajas de usar Debian	**Descripción**
Falta de software popular	Debian no dispone de algunos paquetes de software populares, debido a que no son gratis, e incluirlos significaría un costo para el usuario final.
Debian es difícil de configurar	Si bien la instalación puede ser más fácil que la de otros sistemas, configurar dispositivos como impresoras no es una tarea sencilla en Debian y en los sistemas Linux en general.
No todo el hardware está soportado	El hardware viejo, raro o muy reciente no está soportado, o bien, aquel hardware complejo que el fabricante genera solo para sistemas Windows.

La instalación del sistema operativo se describe paso a paso en el *Anexo A*.

2.1.4. Aplicaciones elegidas

En este apartado se mencionan los principales servicios con los que debe contar un servidor web y las aplicaciones elegidas para tal fin.

- Servidor web

Para elegir un servidor web a instalar se toman en cuenta Apache y Nginx, siendo estos dos los de mayor popularidad.

Apache ha sido el más popular en Internet desde 1996, por ello cuenta con una documentación que se extiende a lo largo de múltiples sitios, foros y blogs, así como soporte de diferentes proyectos y de una extensa comunidad de usuarios que hacen uso del servicio. Por su parte, el interés en Nginx va creciendo al igual que su documentación en su sitio oficial y a través de terceros.

En cuanto a la velocidad, los dos servidores son rápidos, sobre todo en webs y plataformas con pocos usuarios simultáneos. Sin embargo, Nginx se comporta más rápido en comparación con Apache a la hora de que aumenta el tráfico y el número de usuarios.

Hablando de configuraciones, en comparación con Nginx, Apache puede ser configurado fácilmente. Además, Nginx tiene menos componentes para agregar más características, mientras que Apache soporta más de 60 módulos, haciéndolo altamente extensible.

Otro aspecto fundamental de un servidor web es la seguridad. Ambos servidores cuentan con medidas de seguridad para mitigar ataques DDoS, malware y phishing, y publican periódicamente informes de seguridad y actualizaciones de mantenimiento.

Para este servidor se ha elegido instalar Apache como servidor web, por su flexibilidad, facilidad en la instalación y la cantidad de documentación disponible. Además, el sitio del Laboratorio de Redes y Seguridad no es un sitio con un tráfico grande y Apache tiene la capacidad de soportarlo. La versión estable actual de Apache es la 2.4.

- Base de datos

El gestor de base de datos elegido para esta propuesta fue MariaDB, el cual es software libre y está basado enteramente en MySQL, por lo que hay una completa compatibilidad entre ambos.

Actualmente MySQL es patrocinado por la empresa Oracle Corporation que posee el copyright de la mayor parte del código. Cuenta con una versión comercial y una versión gratuita, la diferencia entre ellas radica en el tipo de soporte y certificaciones.

MariaDB es un sistema de gestión de bases de datos derivado de MySQL, desarrollado por Michael Widenius (fundador de MySQL) y la comunidad de desarrolladores de software libre. Su popularidad ha ido en incremento y ha recibido el respaldo de la Wikipedia Foundation y varias distribuciones de Linux.

Ventajas de MariaDB sobre MySQL:

- Agrega nuevos y más eficientes motores de almacenamiento.
- Mejoras de velocidad, sobretodo en consultas completas.
- Se añaden nuevas tablas de sistema para almacenar estadísticas, con lo que se optimizan las bases de datos.
- Se mejora el sistema para manejar las conexiones, con el cual se pueden llegar a tener hasta 200,000 conexiones a MariaDB.

- Procesador de PHP

PHP es un lenguaje de código abierto popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML. PHP está enfocado a la programación de scripts del lado del servidor, por lo que se usa principalmente para recopilar datos de formularios, generar páginas con contenidos dinámicos o enviar y recibir *cookies*.

Una de las características más potentes y destacables de PHP es su soporte para bases de datos. Escribir una página web con acceso a una base de datos es simple utilizando una de las extensiones de bases de datos.

Actualmente existen una gran cantidad de módulos o extensiones que aumentan el potencial de PHP. Además de poseer una amplia documentación y una gran comunidad de desarrolladores y usuarios.

La versión estable actual del procesador de PHP es la 7.3

2.2. Diseño del sitio web

2.2.1. Requerimientos

Revisando los servicios que brinda el Laboratorio de Redes y Seguridad se llegó a la conclusión que también es necesario que el Área de Redes y Seguridad cuente con un sitio web propio, ya que hay servicios que forman parte del área, pero no del laboratorio.

Por lo anterior, el primer requerimiento es que se construyan dos sitios web, uno correspondiente al Área de Redes y Seguridad y otro al Laboratorio de Redes y Seguridad.

El sitio web del Área de Redes y Seguridad se conforma de las siguientes secciones:

1. Nosotros
    a. Misión, visión y objetivos
    b. Profesores
    c. Asignaturas
2. Laboratorio de Redes y Seguridad
3. Cisco Networking Academy
4. Diplomado de Ciberseguridad

Quedando como se muestra en la Figura 2.1.

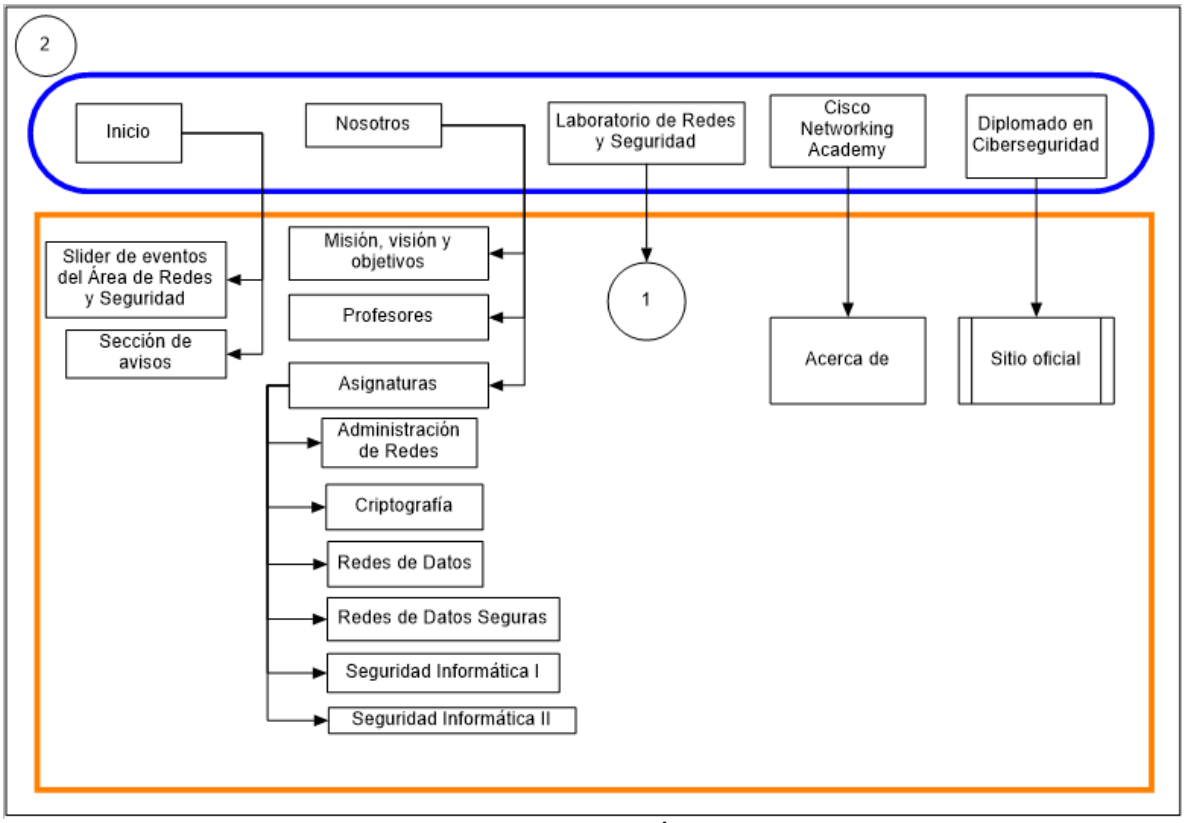


Figura 2.1 Diagrama del sitio web del Área de Redes y Seguridad

El sitio web del Laboratorio de Redes y Seguridad cuenta con las siguientes secciones:

1. Redes y Seguridad
2. Nuestro Laboratorio
    a. Misión, visión y objetivos
    b. Reservación
    c. Contacto
3. Sistema de Gestión de Calidad
    a. Política de la Calidad
    b. Plan de la Calidad
    c. Reglamento
    d. Calendario de prácticas
    e. Control de entrega de prácticas
4. Asignaturas
    a. Redes de Datos
    b. Administración de Redes

Quedando como se muestra en la Figura 2.2.

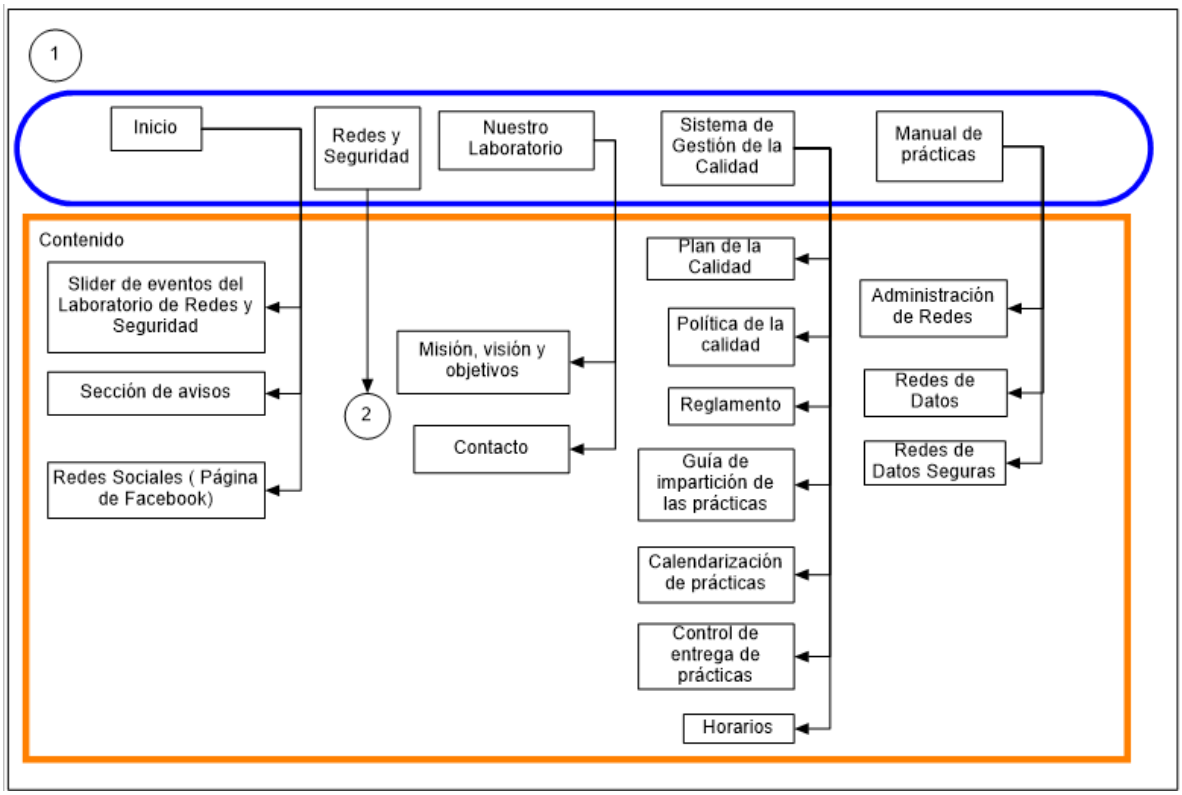


Figura 2.2 Diagrama del sitio web del Laboratorio de Redes y Seguridad

El Laboratorio de Redes y Seguridad cuenta con 6 grupos para la asignatura Administración de Redes, 4 grupos para Redes de Datos y 5 grupos para Redes de Datos Seguras, todos ellos con un cupo de 20 alumnos; se toma en cuenta también el Diplomado en Ciberseguridad con 24 alumnos por generación. Por lo tanto, alrededor de 400 alumnos toman clase en el Laboratorio, los cuales acceden al sitio web para descargar material didáctico, por lo que el servidor debe soportar esa cantidad de conexiones.

2.2.2. Lineamientos para sitios web de la UNAM

La UNAM, por medio del Consejo Asesor de Tecnologías de Información y Comunicación da a conocer, en octubre de 2009, los Lineamientos para sitios web institucionales de la UNAM, teniendo una actualización en octubre de 2016. Estos lineamientos establecen las pautas para la creación, actualización y mantenimiento de sitios web institucionales con el fin de cuidar la imagen institucional y lograr una mayor difusión del conocimiento generado en la Universidad.

A continuación, se muestran brevemente los lineamientos:

- Facilidad de uso: La facilidad de uso impacta la arquitectura del sitio, el diseño de la interfaz de usuario y el desarrollo de contenido.
- Navegación: Todas las páginas deben de estar enlazadas a la de inicio y las secciones más importantes del sitio deben ser accesibles directamente desde la página principal.
- Funcionalidad: El sitio debe ser de fácil acceso y disponible en todo momento, evitando el uso de *frames* o extensiones del navegador.
- Lenguaje y contenido: El lenguaje debe ser simple, claro y directo. El responsable del sitio debe actualizar de manera permanente la información.
- Claridad arquitectónica y visual: El diseño del sitio debe ser sencillo y utilizar de forma moderada elementos decorativos.
- Versiones en otros idiomas: Los servicios que puedan tener público extranjero deben contar, por lo menos, con una versión en idioma inglés.
- Ayuda en línea y guías de usuario: El sitio debe de diseñarse de manera que la ayuda e instrucciones requeridas sean mínimas, puesto que su uso y navegación es sencillo.
- Retroalimentación del sitio web: Permitir a los usuarios proporcionar información de sugerencias mediante correo electrónico o un formulario de comentarios.
- Coherencia: El título de la página estará acorde con su contenido y reflejar a lo que se hace referencia.
- Visibilidad: Se deben incluir las palabras clave más importantes que den una referencia al contenido del sitio web, con el objetivo de que los buscadores lo encuentren.
- Pie de página: El pie de página contendrá la leyenda y deberá estar presente para los sitios web estáticos.

- Imagen institucional: Los sitios deben incorporar el encabezado institucional, el cual está integrado por dos elementos.
    - Imagen de la UNAM y el nombre completo de la universidad a la izquierda del encabezado.
    - Imagen a la derecha del encabezado que puede ser un collage con fotos relativas al servicio.

2.2.3. Sitios web de la Facultad de Ingeniería

En el Plan de Desarrollo 2015-2019 de la Facultad de Ingeniería elaborado por el Dr. Carlos Agustín Escalante Sandoval se presenta el proyecto "Difusión y Proyección Institucional", en donde uno de los puntos es la reingeniería del sitio de la Facultad de Ingeniería, en donde se reconfigure la estructura y el diseño gráfico del sitio web.

Una vez puesto en marcha el nuevo sitio web de la Facultad de Ingeniería (véase Figura 2.1), la Secretaría General de la Facultad de Ingeniería a través de la Coordinación de Vinculación Productiva y Social proporciona a las diferentes áreas de la Facultad una plantilla con el formato institucional para la homogenización del diseño de los sitios web.

Figura 2.3 Sitio web de la Facultad de Ingeniería

Para el diseño del sitio web del Área de Redes y Seguridad y del Laboratorio de Redes y Seguridad, se toma como base la plantilla proporcionada por Secretaria General, la cual utiliza código HTML y PHP. Lo que se busca es respetar el diseño de la plantilla y acoplarla a las necesidades del área y el laboratorio.

Capítulo 3

Hardening del servidor web

En este capítulo se describen las configuraciones que se le deben hacer a un servidor después de instalar el Sistema Operativo y antes de ser conectado a Internet, con el objetivo de fortalecer su seguridad.

Se propone una serie de configuraciones que incluyen modificaciones a nivel de BIOS y en los servicios instalados en el sistema.

3.1. Definición de hardening

Hardening es una palabra en inglés que significa endurecimiento, en seguridad informática se trata de un conjunto de actividades realizadas por el administrador del sistema, con la intención de fortalecer la seguridad del mismo mediante la eliminación de software, servicios y usuarios innecesarios en el sistema, así como la aplicación de herramientas y técnicas que contribuyan a reducir las vulnerabilidades en los sistemas.

El propósito del hardening es hacerle la vida difícil a un intruso o a un atacante, ganando tiempo para minimizar las consecuencias de un inminente incidente de seguridad y de ser posible impedir que se concrete.

Se sabe que ningún sistema operativo por naturaleza es seguro y el hardening debería ser la primera estrategia de seguridad implementada por el administrador antes de conectar el servidor a la red, y más aún si se planea ubicarlo en la *DMZ* (Zona Desmilitarizada).

3.2. Hardening propuesto

Para el servidor del Laboratorio de Redes y Seguridad se propone una serie de configuraciones para fortalecer la seguridad del sistema operativo, tomando en cuenta que se trata de un Servidor Web y puede ser administrado de manera remota.

3.2.1. Acceso al BIOS

En los sistemas operativos Linux el flujo de control durante el arranque inicia en el BIOS (Basic Input/Output System), después pasa el control al *gestor de arranque* (LILO o GRUB) y posteriormente al núcleo (*kernel*) como se observa en la Figura 3.1.

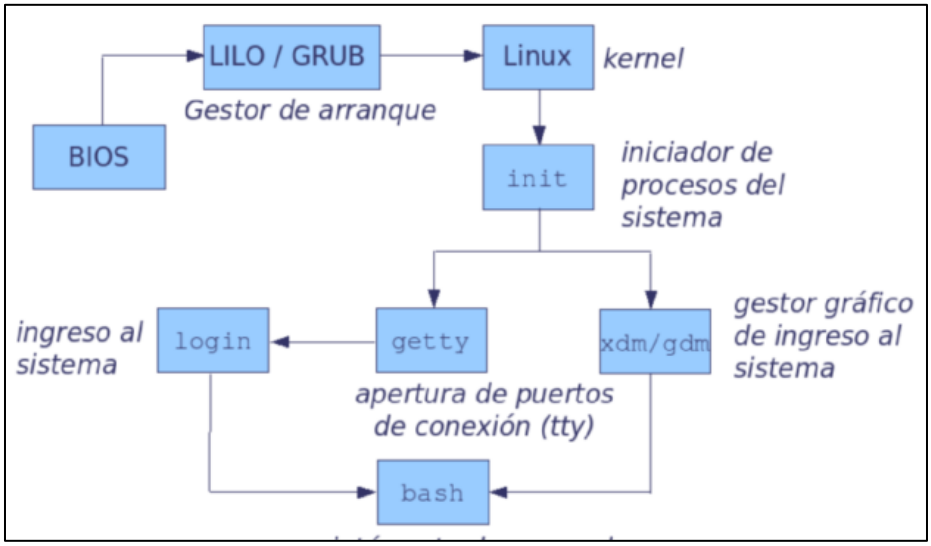


Figura 3.1 Flujo del proceso de arranque del sistema operativo
Nota. Imagen recuperada de "Inicio/arranque del sistema", de Ovejero, M. (30 noviembre 2011). Recuperado de: http://servuntu.blogspot.com/2011/11/inicioarranque-del-sistema.html

Para proteger el servidor contra modificaciones se recomienda:

- Establecer una contraseña.
- Quitar arranque por CD.
- Quitar arranque por USB.

Estas medidas aseguran que en casos de que alguien tuviera acceso físico al servidor no podrá hacer cambios en él, ya que para ello tendría que conocer la contraseña o tener habilitados los medios para hacer uso del mismo.

En el *Anexo B* en el apartado 2.1 se muestra el proceso realizado en el servidor.

3.2.2. Colocar contraseña a GRUB

Después de que se carga el BIOS, entra en acción el gestor de arranque, su función es la de cargar el kernel de un sistema operativo y pasarle el control de ejecución para que continúe con el resto del proceso de arranque del sistema.

En Debian, el gestor de arranque por default es *GRUB*, desarrollado por el proyecto *GNU* y que se usa comúnmente para iniciar uno de dos o más sistemas operativos instalados en un mismo equipo.

Una vez cargado el menú, como el que se muestra en la Figura 3.2, con las teclas de arriba y abajo del teclado se puede seleccionar un sistema operativo u otras opciones; con la tecla "e" se pueden modificar las opciones de arranque; y con la tecla "c" se puede acceder a una pequeña consola, con una serie de comandos limitados.

Figura 3.2 Menú de GRUB en Debian 9

Las funcionalidades anteriormente descritas de GRUB pueden ser una vulnerabilidad del sistema, ya que si una persona externa tiene acceso físico al servidor podría modificar los parámetros de arranque y acceder a una consola con permisos de root. La solución a este problema es definir una contraseña, que será requerida cada vez que se quieran editar los parámetros de arranque.

En el *Anexo B* en el apartado 2.2 se muestra el proceso realizado en el servidor.

3.2.3. Configuración de Secure Shell

Secure Shell o *SSH*, es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación como FTP o *Telnet*, SSH encripta todo lo que envía y recibe, incrementando la seguridad de las conexiones del equipo.

Al ser uno de los protocolos más usados, es propenso a ataques cibernéticos si no se tiene una buena configuración. De manera inicial, se debe cambiar la configuración que se tiene por defecto al instalar SSH.

Entre las configuraciones que se deben hacer son:

- Cambiar el puerto. Por defecto SSH funciona en el puerto 22, y es por ello que muchos de los ataques están dirigidos a este puerto.
- Denegar el acceso del usuario root por vía remota. Todos los sistemas Linux crean al usuario root por defecto, por lo que la mayoría de los ataques de fuerza bruta se concentran en este usuario, esperando que tenga una contraseña débil.
- Indicar la cantidad de veces que se puede ingresar erróneamente el usuario y/o la contraseña. Después de los intentos indicados se cerrará la conexión, de esta manera evitamos un ataque de fuerza bruta automatizado.
- Indicar la cantidad de conexiones simultáneas que permitirá SSH por IP que intente conectarse. Algunos ataques con mayor complejidad dividen el ataque en una gran cantidad de conexiones, aumentando las posibilidades de entrar al sistema.
- Restringir el acceso al sistema vía remota solo a los usuarios indicados.

Otra buena configuración a tomarse en cuenta es el mensaje de bienvenida que se muestra al acceder a Secure Shell, el cual es eficiente para disuadir a un posible intruso de seguir o no conectado a un sistema. De lo que se trata es poner sobre advertencia a la persona que ha ingresado a un sistema sobre las repercusiones que podrían existir en caso de un acceso no autorizado o de que se realicen acciones no permitidas con el sistema. Tomando en cuenta los siguientes aspectos:

- Debe advertirse sobre el uso autorizado del equipo y su información.
- Advertir que la actividad que se lleve a cabo en el equipo está siendo registrada.

- Dejar claro que el usuario está ingresando a un equipo restringido y en caso de haber iniciado sesión remota por error, debe desconectarse de forma inmediata y contactar al administrador.
- No usar palabras como “bienvenido”.
- Escribir el mensaje en el idioma local.
- El mensaje debe ser lo más corto y concreto posible.

En el *Anexo B* en el apartado 2.3 se muestra el proceso realizado en el servidor.

3.2.4. SUDO

Es un programa diseñado para facilitar a los administradores del sistema permitir a algunos usuarios ejecutar comandos como root (u otro usuario), registrando quién ejecutó el comando y cuándo. La filosofía básica es dar los menos privilegios posibles, pero permitiendo a las personas que su trabajo pueda ser realizado.

El uso de sudo es más seguro que abrir una sesión de root por las siguientes razones:

- Ningún usuario necesita conocer la contraseña de root, puesto que sudo solicita la contraseña del usuario actual. Privilegios extra pueden ser cedidos a usuarios individuales temporalmente, y sin necesidad de cambiar la contraseña actual.
- Es fácil ejecutar comandos que requieren privilegios especiales con sudo, trabajando el resto del tiempo como un usuario sin privilegios, reduciendo los daños que un error puede causar.
- Cuando sudo se ejecuta, el nombre original del usuario y el comando son registrados.

En Debian no viene instalado y configurado por defecto, pero está disponible en los repositorios. A partir de Debian 6 “Squeeze”, si se instala sudo, la configuración predeterminada da derechos de sudo a cualquier miembro que pertenezca al grupo sudo.

En el *Anexo B* en el apartado 2.4 se muestra el proceso para la instalación y correcta administración de sudo.

3.2.5. Iptables

Iptables es un sistema de firewall vinculado al kernel de Linux. La ventaja es que se encuentra integrado con el sistema operativo.

Al igual que otros tipos de firewalls, iptables funciona a través de reglas. De esta manera, es posible definir a que tipos de paquetes se les permite el paso, sobre qué puerto y protocolo.

Iptables posee tres grupos de reglas:

Reglas de filtrado: Esto se logra a partir de las reglas INPUT, OUTPUT y FORWARD. Permite determinar el tipo de paquetes que pueden ingresar a la red y redireccionarlos al destino de interés.

NAT: Son el grupo de reglas que permiten aplicarse a partir de la dirección IP de origen y destino, y así impactar en la forma en que el tráfico es ruteado.

Mangle: Este tipo de reglas se aplican sobre las banderas de los paquetes.

En el *Anexo B* en el apartado 2.5 se muestra el proceso realizado en el servidor.

3.2.6. Certificado SSL

SSL son las siglas de Secure Sockets Layer (capa de sockets seguros) y es la tecnología estándar para mantener segura una conexión a Internet, así como para proteger toda información confidencial que se envía entre dos sistemas, e impedir que los delincuentes lean y modifiquen datos que se transfieras, incluso datos que pudieran considerarse personales.

Esto se lleva a cabo haciendo que todos los datos que se transfieren entre usuarios y sitios web, o entre dos sistemas, sean imposibles de leer. Se utilizan algoritmos de cifrado para codificar los datos que se transmiten y así impedir que los delincuentes los lean al enviarlos a través de la conexión. Esta información puede ser cualquier dato confidencial o personal como números de tarjetas de crédito y otros datos bancarios, nombres y direcciones.

Para establecer una conexión segura, se instala en un servidor web un certificado SSL (también llamado "certificado digital") que cumple dos funciones:

- Autenticar la identidad del sitio web, garantizando a los visitantes que no están en un sitio falso.
- Cifrar la información transmitida.

Los certificados SSL son emitidos por Autoridades de Certificación (CA), que son organizaciones de confianza a cargo de verificar la identidad y legitimidad de la entidad que solicita un certificado. El rol de la CA es recibir solicitudes de certificados, autenticar las solicitudes, emitir certificados y mantener información sobre el estado de los certificados emitidos.

En un sitio web que está protegido por un certificado SSL, las siglas *https* (protocolo seguro de transferencia de hipertexto) aparecen en la dirección URL. Los detalles del certificado, por ejemplo, la entidad emisora y el nombre corporativo del propietario del sitio web, se pueden ver haciendo clic en el símbolo de candado en la barra del navegador.

Para el servidor web del Laboratorio de Redes y Seguridad, se propone utilizar un certificado SSL emitido por Let’s Encrypt, la cual es una autoridad de certificación (CA)

libre y gratuita impulsada por la Fundación Linux, que permite generar certificados SSL gratuitos y automáticos. Hoy en día Let's Encrypt cuenta con el apoyo de empresas como Mozilla, Google y Facebook, cuyo objetivo es promover que el tráfico de Internet sea seguro.

Las principales características de los certificados emitidos por Let's Encrypt son:

- Son totalmente gratuitos, aunque se pueden hacer donaciones al proyecto.
- La instalación en un servidor web es sencilla.
- Los principales navegadores reconocen los certificados.
- Los certificados tienen una duración por defecto de 3 meses, pero son renovables y se puede automatizar la renovación.
- Transparente: Todos los certificados emitidos o revocados son registrados públicamente y están disponibles para que cualquier persona pueda inspeccionarlos.
- Open Source: El protocolo de emisión y renovación automática se publica como un estándar abierto que otros pueden adoptar.

En el *Anexo B* en el apartado 2.5 se muestra el proceso para la instalación del certificado SSL en el servidor.

Capítulo 4

Implementación y pruebas

En este capítulo se muestra la metodología con la que se lleva a cabo la implementación de la solución propuesta en el capítulo 2, así como las pruebas para garantizar el correcto funcionamiento del servidor y el sitio web.

4.1. Implementación del servidor web

Para la implementación de la solución propuesta para la configuración del servidor web, se sigue el diagrama de flujo que se muestra en la Figura 4.1.

Figura 4.1 Diagrama de flujo de la implementación

Como se observa en el diagrama de flujo, lo primero a realizar en el servidor es instalar el sistema operativo. Una vez que se tenga el sistema operativo se instalan las aplicaciones necesarias para que se convierta en un servidor web:

- Apache
- MariaDB
- Procesador de PHP

El proceso de instalación del sistema operativo y las aplicaciones se detalla en el *Anexo A*.

Cuando las aplicaciones se hayan instalado y antes de conectar al servidor a Internet, se aplica el hardening propuesto en el capítulo 3, con el fin de quitar algunas de las configuraciones por defecto de las aplicaciones instaladas y así fortalecer la seguridad del servidor. Las configuraciones a realizar son:

- Colocar contraseña a BIOS
- Colocar contraseña a GRUB
- Configurar Secure Shell
- Configurar SUDO
- Configurar iptables

El proceso del hardening se detalla en el *Anexo B*, en el apartado 2.

Hasta este punto ya se puede cargar el sitio web en el servidor, para después poner el servidor en producción, es decir, conectarlo a Internet para que los usuarios puedan acceder al sitio web que alberga.

El certificado SSL se instala una vez que el servidor se encuentre en producción, ya que el instalador utilizado para tal fin verifica la autenticidad del dominio. En el *Anexo B* en el apartado 2.5 se muestra el proceso para la instalación del certificado SSL en el servidor.

4.2. Pruebas del servidor web

4.2.1. Instalación del sistema operativo y aplicaciones

Si durante el proceso de instalación del sistema operativo no se reporta ningún problema, aparece el mensaje que se muestra en la Figura 4.2, a continuación, el servidor se reinicia y con ello termina exitosamente la instalación del sistema operativo.

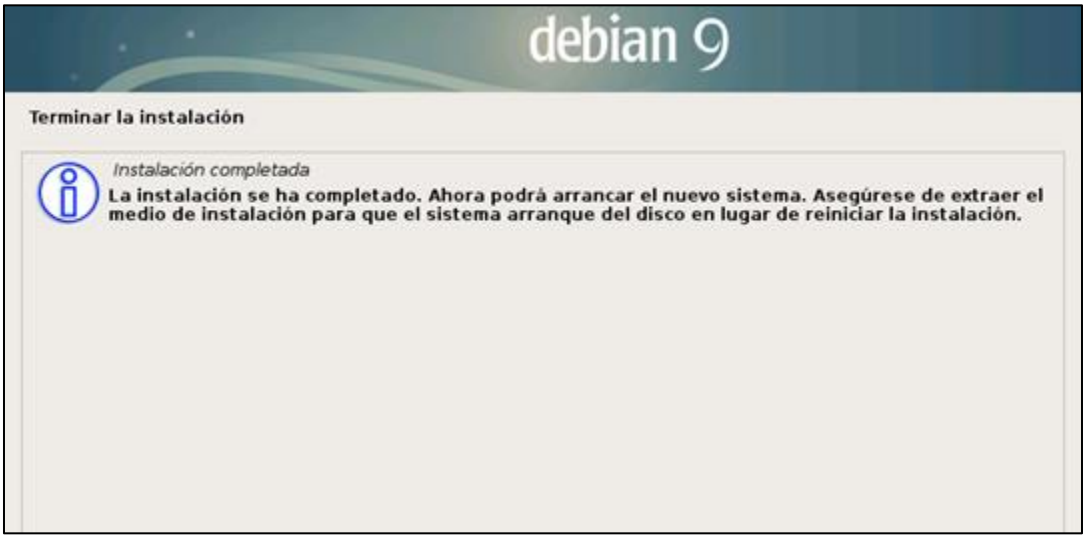


Figura 4.2 Instalación del sistema operativo completada.

Cuando se haya concluido la instalación de Apache, se verifica que funcione correctamente. En un navegador web se ingresa la dirección IP del servidor, debe de aparecer una página como la que se muestra en la Figura 4.3, lo que indica que Apache se ha instalado correctamente.

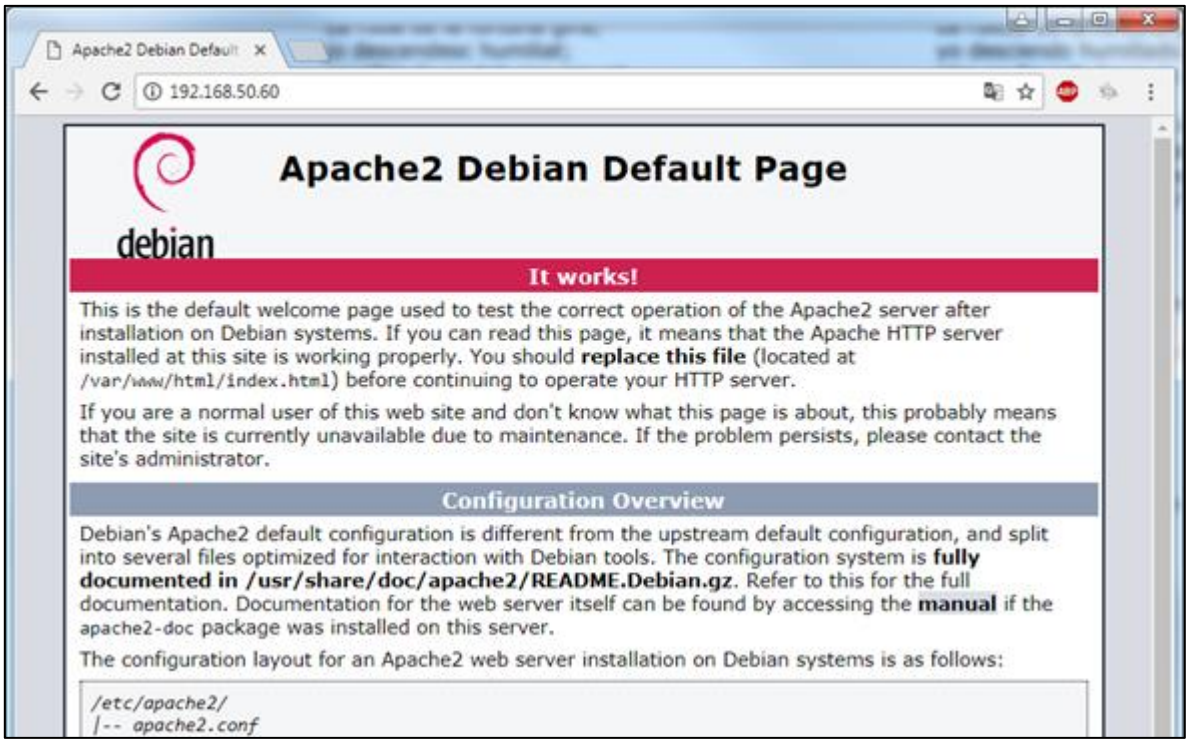


Figura 4.3 Instalación de Apache

Para verificar que la instalación de PHP se haya realizado correctamente, se crea un archivo en el directorio /var/www/html, el contenido del archivo queda como se muestra en la Figura 4.4.

```
<?php phpinfo(); ?>
~
~
```
Figura 4.4 Archivo info.php

En un navegador se introduce la dirección IP y el nombre del archivo *info.php*. Si se muestra una página similar a la que se muestra en la Figura 4.5, el servicio de PHP funciona de manera correcta.

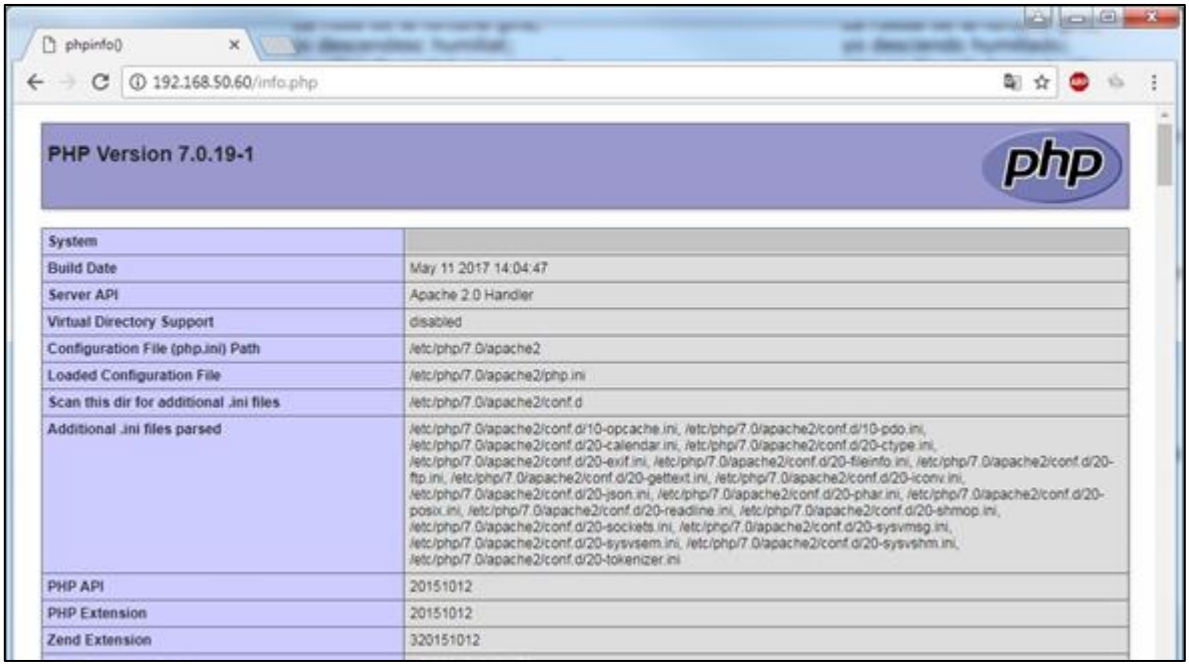


Figura 4.5 Instalación de PHP

4.2.2. Hardening

Para probar que la contraseña en el BIOS fue colocada, se reinicia el servidor, cuando aparezca la pantalla que se muestra en la Figura 4.6, se presiona F2 para entrar al sistema de configuración del BIOS.

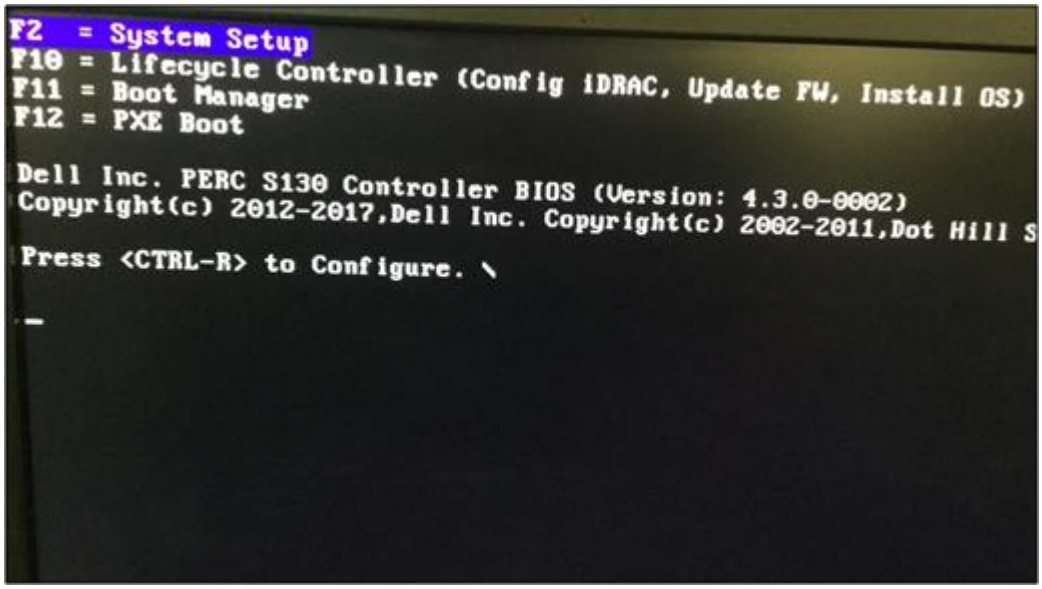


Figura 4.6 Pantalla inicial

Si la contraseña fue colocada correctamente, el sistema pide ingresar la contraseña como se muestra en la Figura 4.7.

Figura 4.7 Contraseña BIOS

Para probar que las configuraciones en el GRUB se hicieron correctamente, se reinicia el servidor y una vez cargado el gestor de arranque, se muestra el menú como en la Figura 4.8. Con las teclas de arriba y abajo se puede seleccionar un sistema operativo (si se tiene instalado más de uno), con la tecla 'e' se pueden modificar las opciones de arranque y con la letra 'c' se puede acceder a una pequeña consola, con una serie de comandos limitados.

Figura 4.8 Menú de GRUB

Si las configuraciones se hicieron correctamente, al presionar la tecla 'e' o 'c', el sistema pide el nombre de usuario y la contraseña que se establecieron, como se muestra en la Figura 4.9.

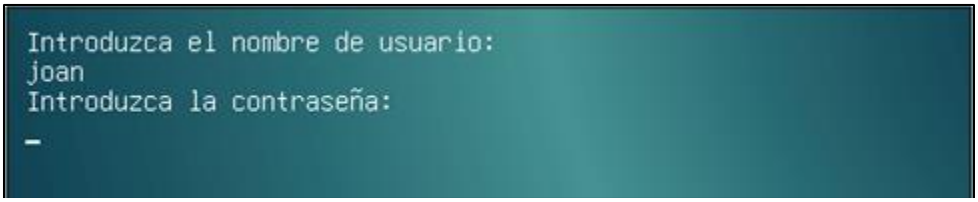


Figura 4.9 Acceso a GRUB

4.2.3. Certificado SSL

Para probar que la instalación del certificado SSL fue exitosa, se ingresa la dirección del sitio web del Laboratorio de Redes y Seguridad y se observa que a la dirección URL le anteceden las siglas https y la imagen de un candado de lado izquierdo, como se muestra en la Figura 4.10.

Figura 4.10 Dirección URL

Si se da click en la imagen del candado se puede obtener la información del certificado que se muestra en la Figura 4.11, donde se indica el dominio para el que fue emitido, la Autoridad Certificadora y la vigencia del certificado.

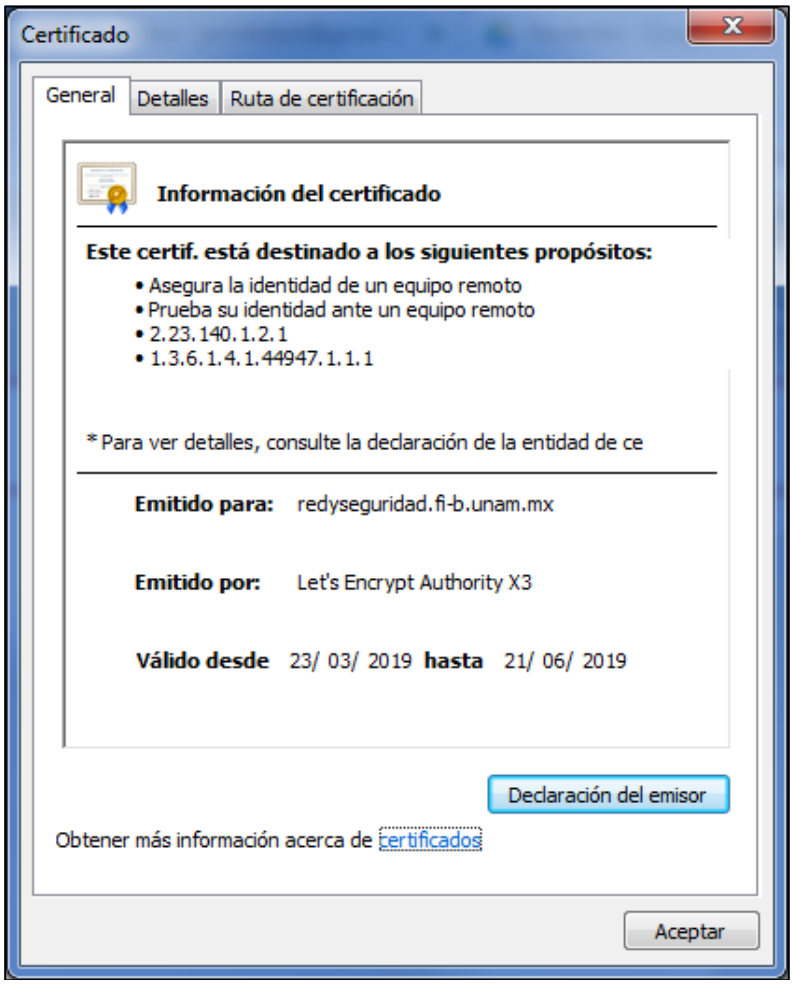


Figura 4.11 Información certificado SSL

Se hace la prueba utilizando Qualys SSL Labs, una herramienta online y gratuita para comprobar la seguridad de un sitio web. Las evaluaciones que realiza esta herramienta no son intrusivas y no consume recursos significativos, hace un escaneo enfocándose únicamente en la configuración SSL.

En la Figura 4.12 se muestra el resultado de la herramienta para el sitio web del Laboratorio de Redes y Seguridad, donde se le califica con la letra A y el color verde, lo que indica que el nivel de seguridad del certificado, y el protocolo de cifrado es alto.

Figura 4.12 Resultado Qualys SSL Labs

4.3. Implementación del sitio web

En el capítulo 2, en el apartado 2.2.1 se menciona la necesidad de tener dos sitios web, uno perteneciente al Área de Redes y Seguridad y otro al Laboratorio de Redes y Seguridad.

En cuanto al diseño, se toma como base la plantilla proporcionada por la Secretaría General, la cual utiliza código HTML y PHP. Se respeta el diseño de la plantilla y se adapta el contenido a la misma.

En el *Anexo C* se explica de manera detallada la forma en que están organizados ambos sitios web, así como las secciones principales que los componen y la manera de actualizarlos.

4.4. Pruebas del sitio web

Para ver el resultado final del sitio web del Área de Redes y Seguridad se ingresa en un navegador la dirección URL:

https://redyseguridad.fi-b.unam.mx/RyS/

En la Figura 4.13 se muestra como se ve el sitio web si se ingresa desde un navegador.

Figura 4.13 Sitio web del Área de Redes y Seguridad

Para ver el resultado final del sitio web del Laboratorio de Redes y Seguridad se ingresa en un navegador la dirección URL:

https://redyseguridad.fi-b.unam.mx/Lab/

En la Figura 4.14 se muestra como se ve el sitio web si se ingresa desde un navegador.

Figura 4.14 Sitio Web del Laboratorio de Redes y Seguridad

Una característica importante de los sitios web renovados es que se adapte a los diferentes tamaños de dispositivos desde los que se puede consultar un sitio web, incluso en los dispositivos móviles como tabletas electrónicas y teléfonos inteligentes.

En la Figura 4.15 se muestra la forma en que se ve el sitio web en un teléfono inteligente, se observa que las imágenes se adaptan al tamaño de la pantalla y el menú principal se despliega cuando se pulsa en el botón debajo de la leyenda Redes y Seguridad.

Figura 4.15 Sitio web visto desde un teléfono inteligente

En la Figura 4.16 se observa la forma en que se ve el sitio web desde una tableta electrónica, al igual que en un teléfono las imágenes se adaptan al tamaño de la pantalla y el menú se despliega cuando se pulsa el botón que se encuentra debajo del logo de la Universidad.

Figura 4.16 Sitio web visto desde una tableta electrónica

4.4.1. Cálculo de soporte de carga del sitio

El número de conexiones simultáneas que puede llegar a soportar un equipo depende de la memoria RAM con la que se cuente, para este caso se sabe que el servidor web cuenta con 40 GB o 40960 MB.

Lo primero que se debe saber es la memoria RAM que consume cada conexión a Apache, no todas las conexiones consumen lo mismo, pero se puede obtener un aproximado con el comando que se muestra en la Figura 4.17, con lo que se sabe que una conexión en promedio consume 21.46 MB de memoria RAM.

```
root@DebianLVM:~# ps -ylC apache2 --sort:rss | awk '{SUM += $8; I +=
 1} END {print SUM/I/1024}'
21.4609
```

Figura 4.17 Consumo de RAM por conexión de Apache

Es importante también saber la memoria RAM consumida por el resto de procesos activos en el sistema, ya que el servicio web no es el único que corre en el sistema operativo y es necesario dejar memoria RAM libre en el servidor para que ejecute el resto de tareas. Se puede obtener con el comando que se muestra en la Figura 4.18, obteniendo que se consume 891.863 MB.

```
root@DebianLVM:~# ps -N -ylC apache2 --sort:rss | awk '{SUM += $8}
END {print SUM/1024}'
891.863
```

Figura 4.18 Consumo de RAM procesos activos

Con la información obtenida se puede hacer un cálculo general de la cantidad de conexiones simultáneas que se pueden tener mediante la operación.

$$\frac{(\text{RAM\_TOTAL} - \text{RAM\_RESTOPROCESOS})}{\text{RAM\_POR\_CONEXION}}$$

El número máximo aproximado de conexiones simultáneas que el servidor soporta es de 1867 conexiones,

$$\frac{(40960 - 891.863)}{21.46} = 1867 \text{ conexiones simultáneas}$$

En el capítulo 2 se menciona que se espera un tráfico aproximado de 400 alumnos en el sitio web, por lo que con los cálculos anteriores se puede ver que se cumple satisfactoriamente.

Conclusiones

En este trabajo de tesis, el objetivo general fue tener un servidor y un sitio web funcionales para el Laboratorio de Redes y Seguridad, con la debida documentación de los pasos realizados, que serán de utilidad para los administradores del servidor y el sitio web. Para alcanzar el objetivo general, se plantearon cuatro objetivos específicos, cada uno de ellos correspondiente a cada uno de los capítulos que forman parte de este trabajo tesis.

Para cubrir el primer objetivo se hizo una investigación partiendo de lo general a lo particular, de temas como sistemas operativos, arquitectura cliente/servidor, páginas web y seguridad informática. Asimismo, en este capítulo se añadieron tablas comparativas de diferentes programas para hacer un análisis y avanzado el proyecto tomas las decisiones respecto a ellos.

En el capítulo 2 se buscó plantear una solución y así alcanzar el segundo objetivo. Contemplando las especificaciones del equipo provisto para este proyecto, se definió el esquema de particionado adecuado a los recursos que se tenían y contemplando el crecimiento a futuro del servidor. Con respecto al sistema operativo, se decidió instalar una distribución Linux por ser software libre, la distribución escogida fue Debian por su estabilidad, buena gestión de los recursos, extensa documentación y facilidad en la instalación. Las aplicaciones seleccionadas para su instalación fueron: como servidor web, Apache; como gestor de base de datos, MariaDB y el procesador de PHP, todas ellas en sus versiones estables actuales.

Por otro lado, para el sitio web se definieron los requerimientos con los cuales se llegó a la conclusión de que era necesaria la implementación de dos sitios web, uno perteneciente al Área de Redes y Seguridad y otro al Laboratorio de Redes y Seguridad. Para el diseño de los sitios web, se tomó como base la plantilla proporcionada por la Secretaría General, con el fin de mantener el diseño institucional de los sitios web de la Facultad de Ingeniería.

Para cumplir el tercer objetivo, se hizo una propuesta de las configuraciones necesarias posteriores a la instalación del sistema operativo y las aplicaciones, las cuales fueron: definición de contraseña para acceder a BIOS, definición de contraseña para acceder al GRUB, configuración de Secure Shell, implementación del comando SUDO, implementación de iptables e instalación del certificiado SSL; con el fin de robustecer la seguridad antes de poner en producción el servidor y cambiar las configuraciones por defecto.

Por último, para lograr el cuarto objetivo, a lo largo de la instalación y la configuración del servidor web se realizaron una serie de pruebas descritas en el capítulo 4, con las que se garantiza su correcto funcionamiento.

Una vez que se alcanzaron los cuatro objetivos específicos, se puede asegurar que mediante el desarrollo de este trabajo de tesis se cumplió con el objetivo fundamental, logrando así

tener un sitio y un servidor web funcionales que cumplen con las necesidades del Laboratorio de Redes y Seguridad.

Una parte importante de este trabajo fue la documentación de los pasos que se siguieron durante la instalación del servidor, los cuales se ven reflejados en los manuales anexos a este trabajo y que serán de utilidad para quien administre el sitio y el servidor web del Laboratorio.

Actualmente los sistemas informáticos y las aplicaciones se renuevan constantemente, teniendo la opción de ser mejorados día con día o de caer pronto en la obsolescencia. Hacemos la recomendación a los administradores mantenerse informados del lanzamiento de nuevas versiones de las aplicaciones instaladas y el sistema operativo, así como de parches de seguridad para que el servidor continúe funcionando en óptimas condiciones.

El desarrollo del presente trabajo contribuyó en primera instancia al crecimiento del Laboratorio de Redes y Seguridad en cuanto a infraestructura y presencia en línea, además de impactar en la formación de los futuros ingenieros en computación que hacen uso del Laboratorio.

Anexo A

Manual de instalación del sistema operativo del servidor web

Índice

1. Introducción

La importancia del servidor web para las actividades académicas del laboratorio, ha hecho necesario documentar todas las actividades relacionadas con el funcionamiento del servidor, razón por la cual se ha escrito este documento.

En este manual se explica paso a paso la instalación del sistema operativo, así como la instalación de los servicios necesarios para que el equipo se convierta en un servidor web.

El manual se encuentra dividido en secciones que detallan los puntos antes mencionados.

La primera sección, Introducción, es una breve explicación del contenido del "Manual de instalación del sistema operativo y los servicios del servidor web".

En la segunda sección, Configuración de RAID, se indica paso a paso la forma de hacer la configuración del arreglo de discos duros del servidor.

En la tercera sección, Instalación del sistema operativo, se indica paso a paso la forma de instalar el sistema operativo Debian 9.1, paquetes y herramientas requeridas, así como las configuraciones necesarias para el funcionamiento óptimo del servidor.

En la cuarta y última sección, Instalación de los servicios, se muestran todos los pasos para la instalación del servicio web, el manejador de base de datos, así como la configuración de los mismos.

2. Configuración de RAID

Lo primero que se debe hacer es ingresar al sistema de configuración del BIOS. Al encender el servidor, cuando aparezca la pantalla que se muestra en la Figura A.1 se presiona F2.

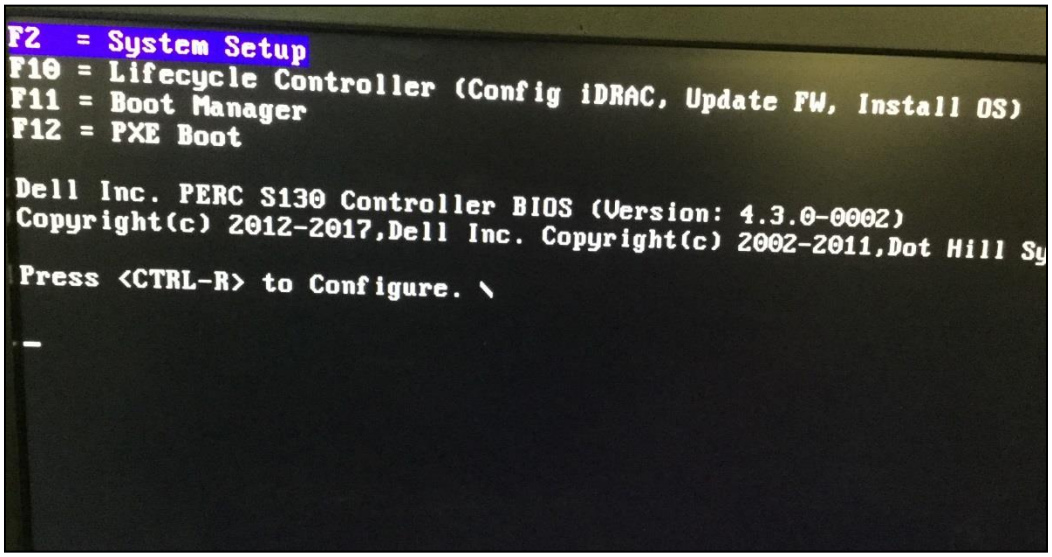


Figura A.1 Ingresar a BIOS

SATA Settings es el espacio de configuración de discos duros que muestra la opción "Embedded SATA" donde existen dos diferentes modos de configuración para el disco duro, los cuáles son AHCI Mode y RAID Mode. Se selecciona RAID Mode en la opción Embedded SATA y se dejan deshabilitadas las opciones de Security Freeze Lock y Write Cache como se muestra en la Figura A.2.

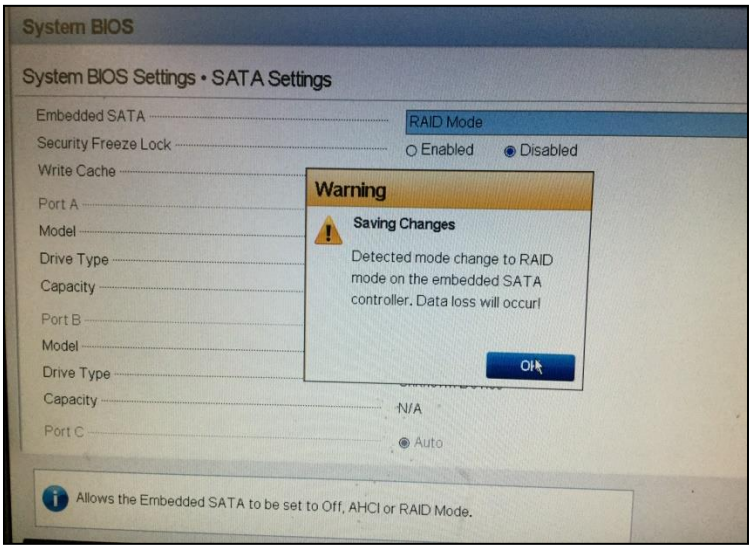


Figura A.2 SATA Settings

Al seleccionar el modo RAID se muestra una lista de los puertos habilitados de forma automática. (véase en la Figura A.3)

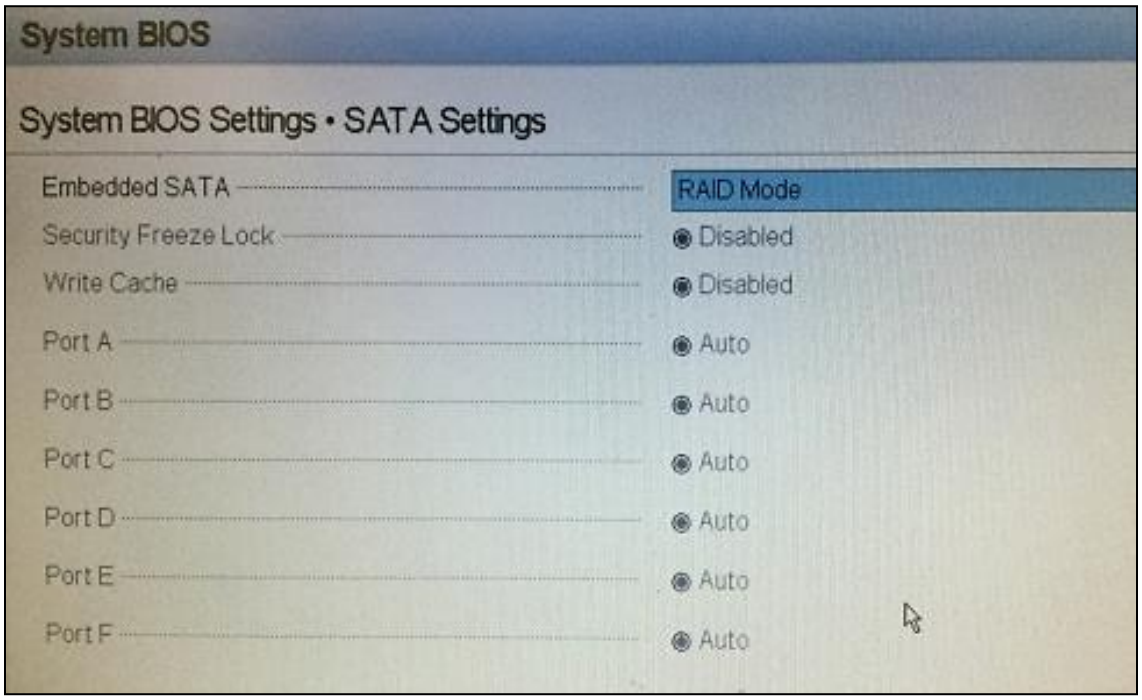


Figura A.3 Raid Mode

Seleccionar Siguiente en el botón de la parte inferior izquierda así el sistema reinicia y es necesario ingresar a Lifecycle Controller, para entrar al espacio de configuración se debe de acceder usando la tecla F10 cuando aparezca la pantalla que se muestra en la Figura A.4.

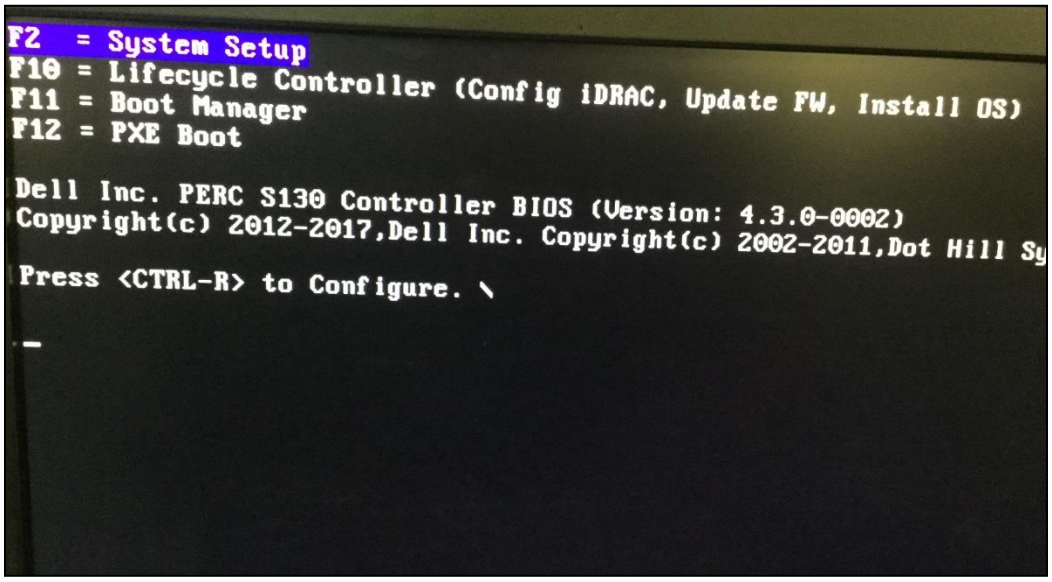


Figura A.4 Ingresar a Lifecycle Controller

Nota:

Dell creó Lifecycle Controller como una solución para la administración de sistemas. Se trata de una herramienta integrada e incorporada en una tarjeta de memoria flash integrada, por lo que no se ve afectada por el formateo o la reinstalación del sistema operativo.

La controladora Lifecycle Controller proporciona administración avanzada e integrada de sistemas para realizar las tareas de administración de sistemas, tales como implementar, configurar, actualizar, mantener y diagnosticar a través de una interfaz gráfica de usuario.

iDRAC es una controladora de acceso remoto integrada de Dell, junto con Lifecycle Controler se encuentra en todos los servidores Dell PowerEdge. Permite la administración remota de servidores sin la necesidad de un sistema operativo para trabajar.

Al entrar por primera vez a Lifecycle Controller iniciará “Initial Setup Wizard”, donde se deben seguir los 5 pasos que marca el proceso de Initial Setup Wizard en donde se elegirán las configuraciones iniciales, a continuación se describe cada paso y su forma de

Paso 1. Seleccionar lenguaje: Como primer paso se selecciona el lenguaje y el tipo de teclado como se muestra en la Figura A.5, al finalizar dar click en el botón Siguiente que se encuentra en la parte inferior derecha para pasar al paso dos.

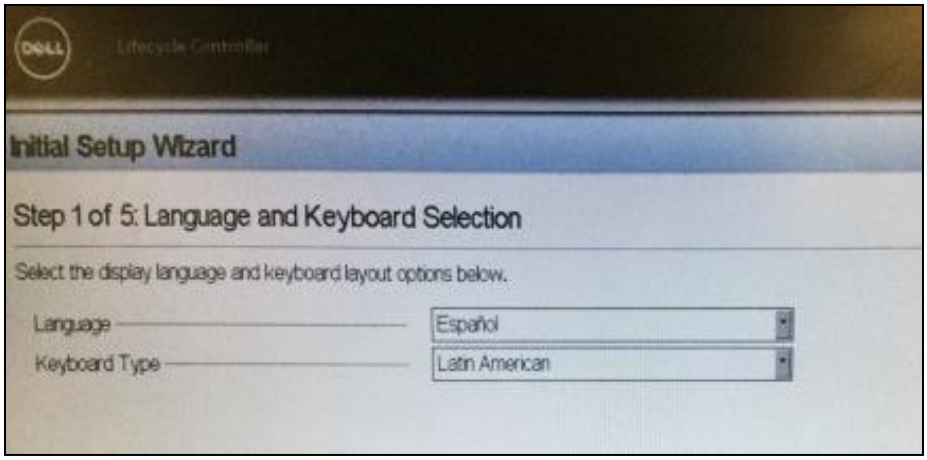


Figura A.5 Paso 1 - Selección de lenguaje

Paso 2. Información general del producto: Este paso es una síntesis sobre el software seleccionado Lifecycle Controller, iDRAC y recomendaciones Dell (véase Figura A.6), únicamente se selecciona Siguiente en el botón inferior derecho para continuar con el proceso de configuración RAID.

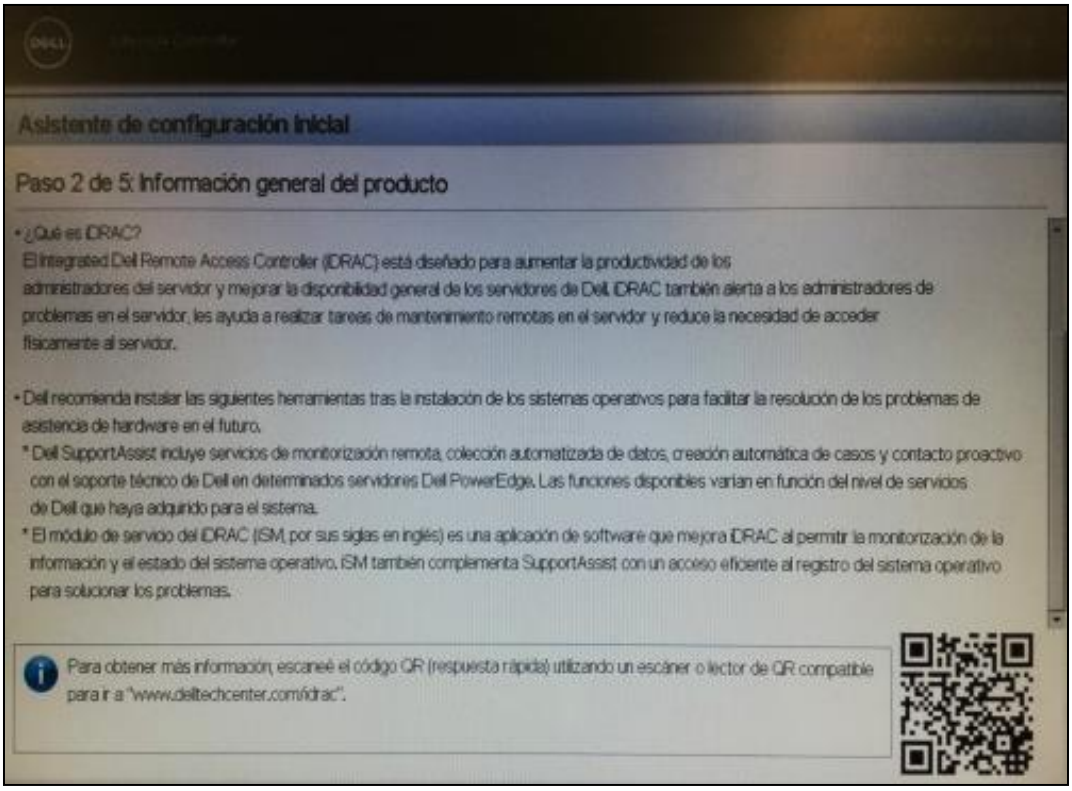


Figura A.6 Paso 2 - Información general

Paso 3. Configuración de la red: Este paso consiste en configurar la interfaz de red del Lifecycle Controller. Se selecciona la tarjeta NIC, en este caso se ha seleccionado la interfaz Embedded NIC 2, ya que físicamente es donde se ha conectado el cable de red. Posteriormente, se asigna una dirección IP utilizando la versión 4 del protocolo de internet (IPv4), además se asigna la dirección IP de manera estática esto para conocer en todo momento la dirección del servidor. Para ingresar más de una dirección de DNS es necesario colocar una coma entre cada una como se muestra en la Figura A.7. La configuración asignada se encuentra en la Tabla A.1.

Nota: La dirección IP elegida es la que el servidor utiliza para operar cuando se instala el sistema operativo. En este caso es una IP temporal, ya que posteriormente debe cambiarse a una dirección IP pública para que pueda ser accedida desde cualquier lugar

Tabla A.1 Configuración asignada al servidor

Configuración asignada
Dirección IP: 192.168.2.40
Puerta de enlace: 192.168.2.254
Máscara: 255.255.255.0
DNS 1: 132.248.204.1 DNS 2: 132.248.10.2

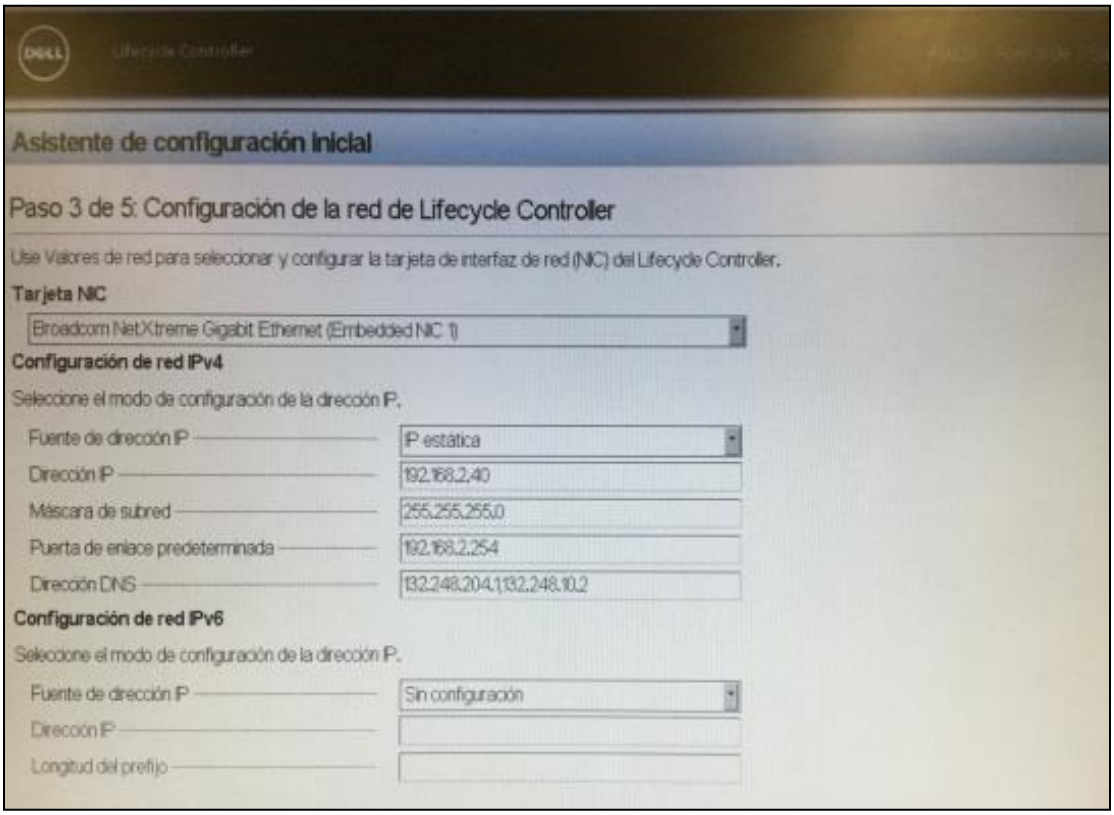


Figura A.7 Paso 3-Configuración de red

Paso 4. Red de iDRAC: En este paso se realiza la configuración de asignación de dirección IPv4 y credenciales para el acceso remoto de iDRAC, esta dirección IP puede ser asignada de manera estática o por DHCP, esta configuración se muestra en la Tabla A.2. De igual manera, se coloca un nombre de usuario y una contraseña para iDRAC en este caso se colocará el usuario root con la contraseña asignada en el sistema operativo, al finalizar con la configuración se selecciona el botón Siguiente ubicado en la parte inferior derecha como se muestra en la Figura A.8. Cuando se termina la configuración aparece una ventana emergente como la que se muestra en la Figura A.9 se da click en Aceptar para continuar con el proceso de la configuración de Initial Setup Wizard.

Nota: La dirección IP elegida no es la misma que la elegida en el paso anterior ya que la dirección IP anterior es la que tendrá la interfaz de red y la dirección IP de iDRAC es propia del controlador del servidor y ambas son independientes.

Tabla A.2 Configuración para iDRAC

Configuración asignada
Dirección IP: 192.168.2.41
Puerta de enlace: 192.168.2.254
Máscara: 255.255.255.0
DNS : 132.248.10.2

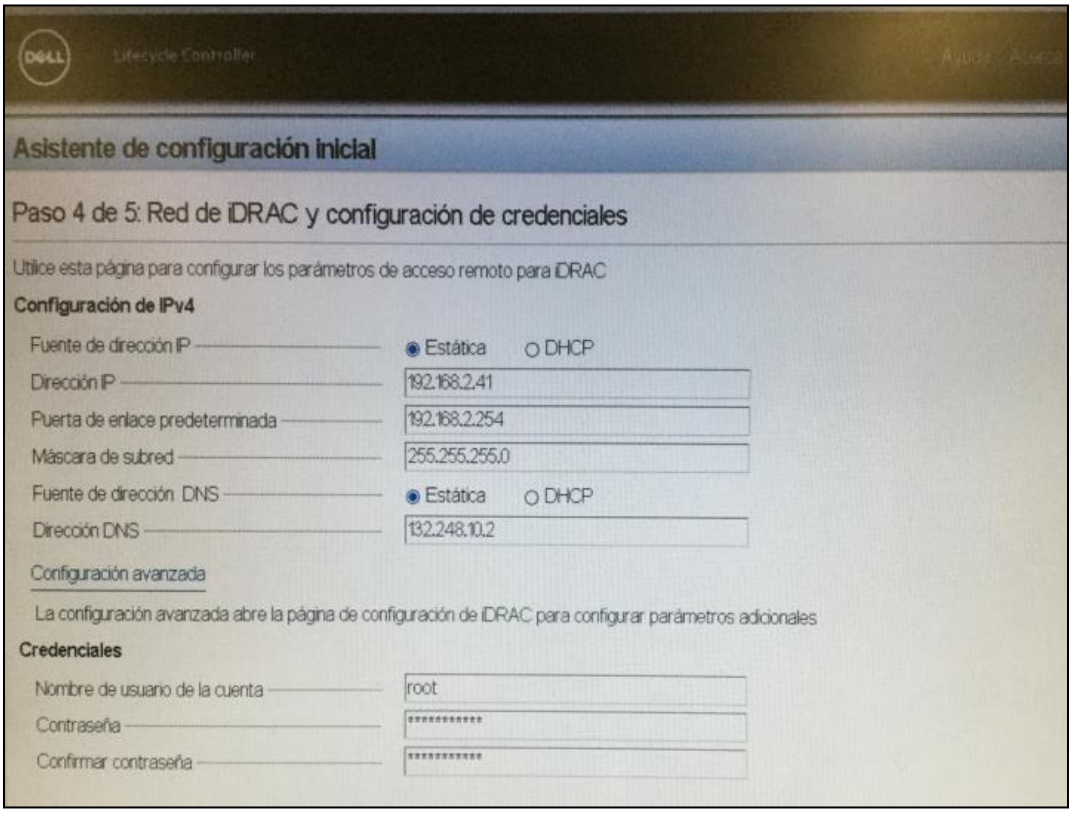


Figura A.8 Paso 4-Red iDRAC

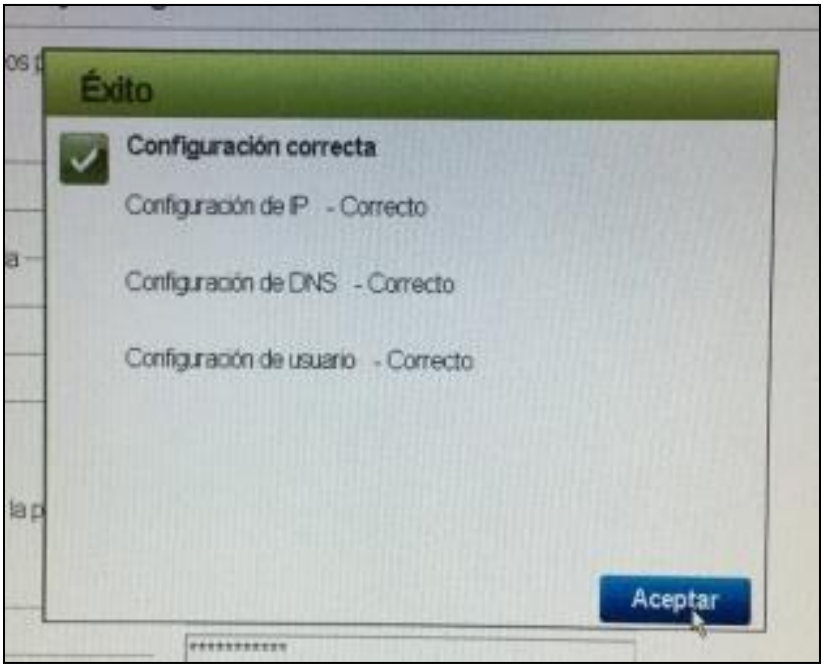


Figura A.9 Paso 4 - Configuración correcta

Paso 5. Resumen: En este paso se muestran las configuraciones que se realizaron en los pasos anteriores como se presenta en la Figura A.10. Se corrobora que sean las configuraciones adecuadas y se da click en Terminar.

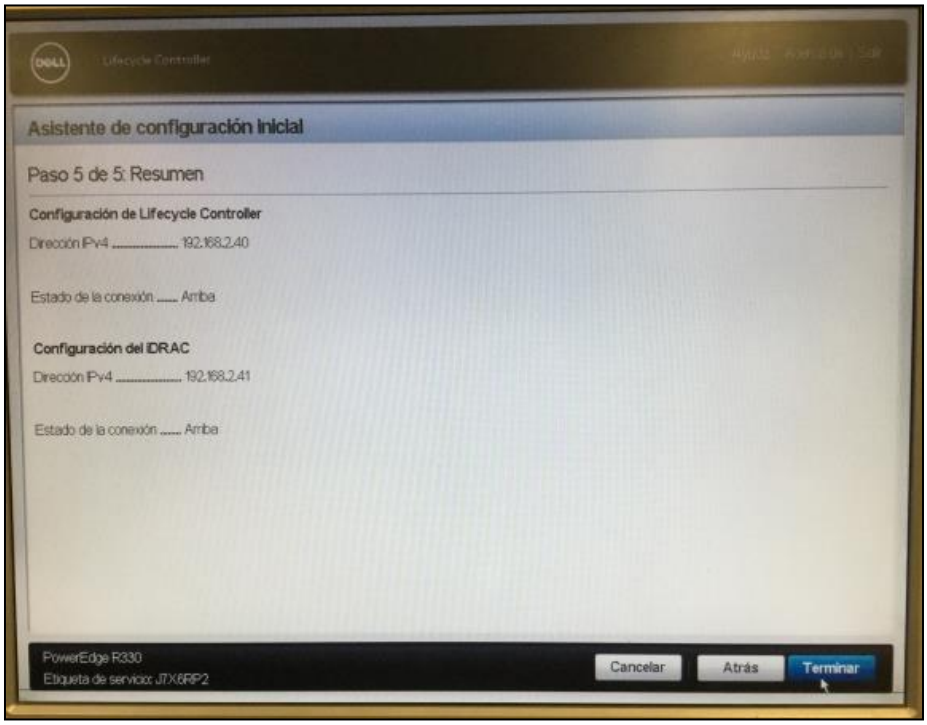


Figura A.10 Paso 5 - Resumen

Una vez terminado la configuración de Initial Setup Wizard, en la sección de Inicio de Lifecycle Controller se muestra una pantalla como se presenta en la Figura A.11, se selecciona la opción "Configurar RAID" para acceder a la configuración RAID.

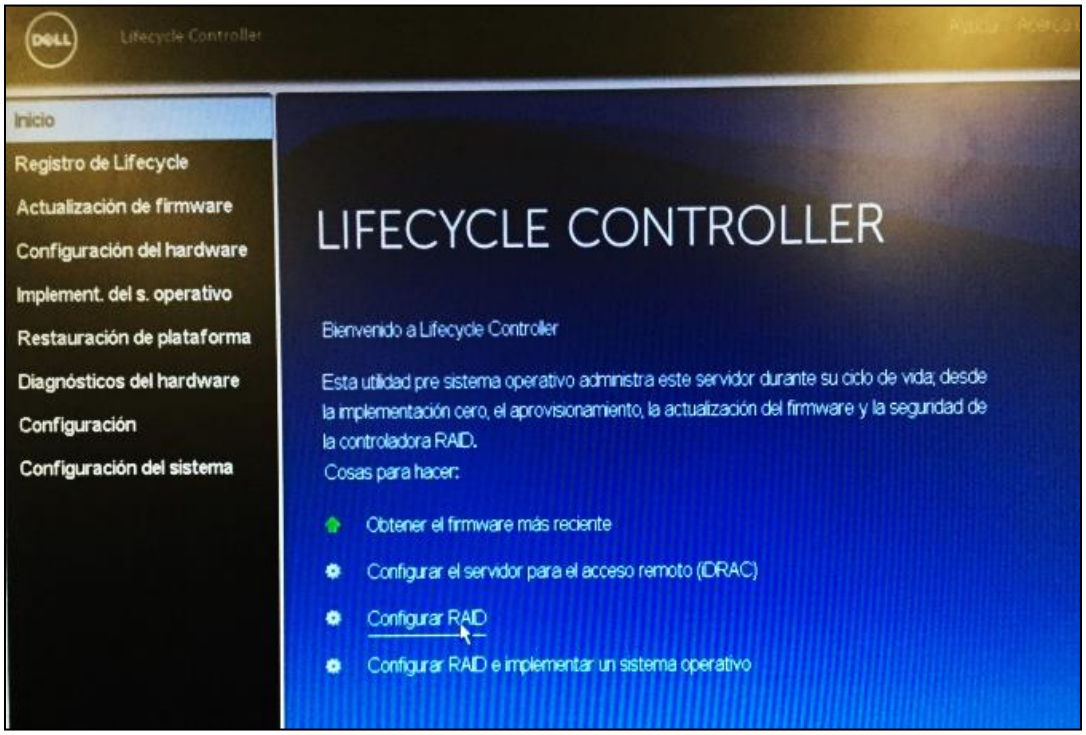


Figura A.11 Lifecycle Controller

Al entrar a Configurar RAID se activa un asistente de configuración, el cual consta de 5 pasos los cuales seguir como se describe a continuación.

Paso1. Configuración RAID actual: Se selecciona el controlador RAID, se elige PERC H330 y se selecciona el botón siguiente que se encuentra en la parte inferior derecha como se muestra en la Figura A.12.

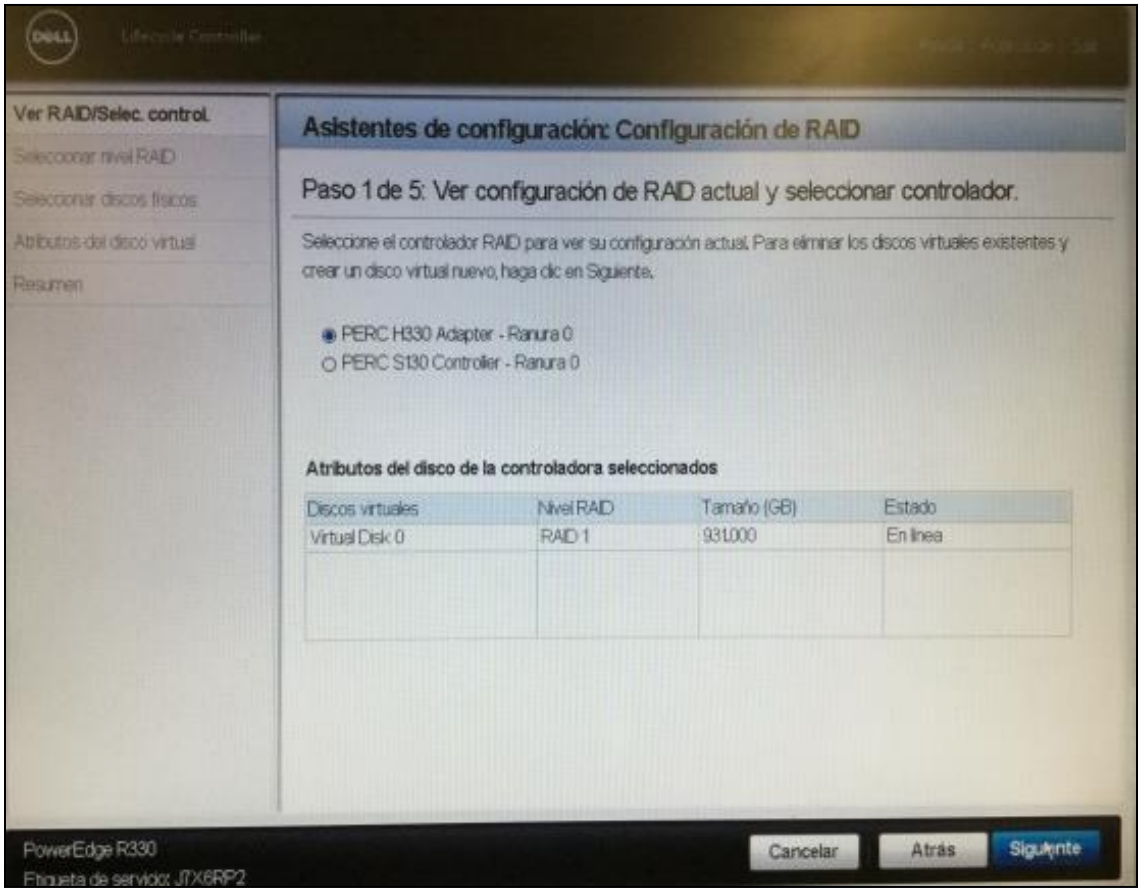


Figura A.12 Paso 1 - Controlador RAID

Paso 2. Nivel RAID: Se selecciona el nivel de RAID. Para este caso se selecciona RAID 0 como se describe en el capítulo X, como se muestra en la Figura A.13 al finalizar con la selección del nivel de RAID se selecciona el botón Siguiente para continuar con el paso 3 de la configuración.

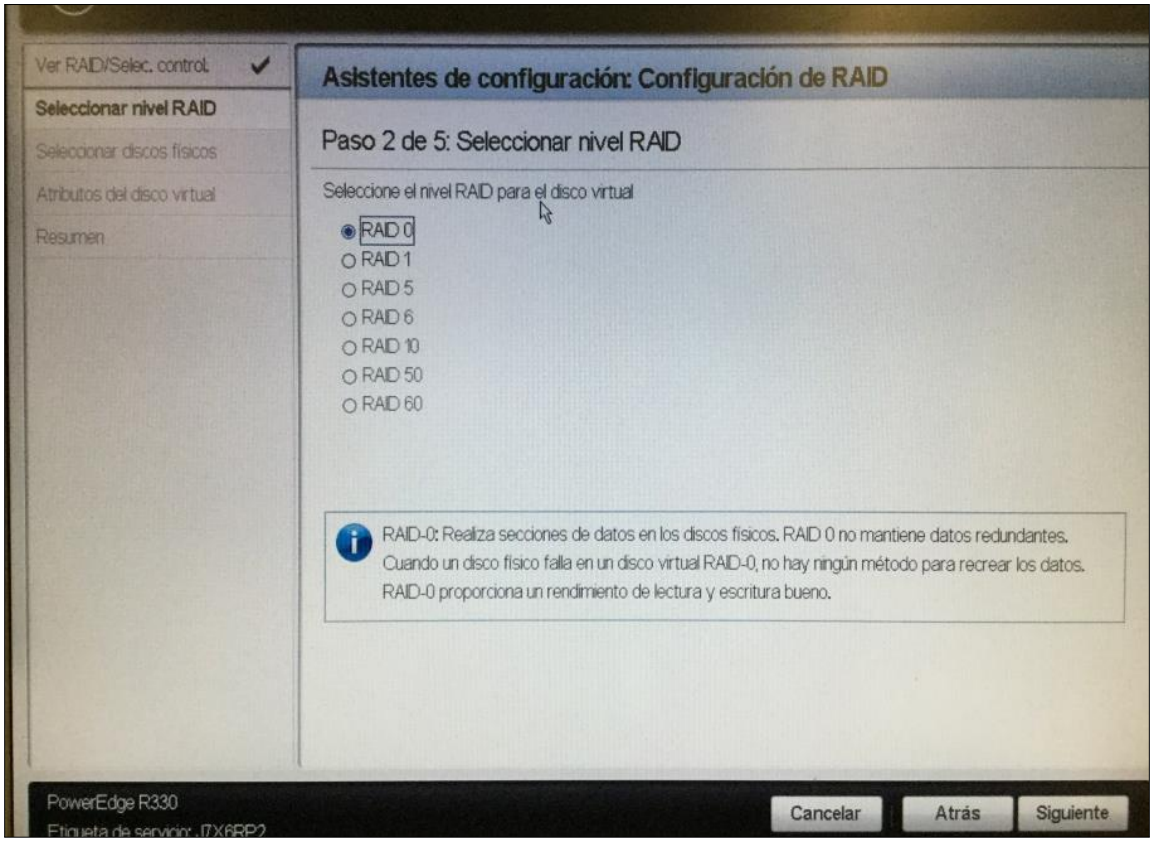


Figura A.13 Paso 2 - Nivel RAID

Paso 3. Selección de discos físicos: En esta sección se debe de utilizar el protocolo SATA, disco duro como tipo de medio y en Seleccionar grupo físico se seleccionan los dos discos de aproximadamente 1 TB cada uno, como se muestra en la Figura A.14.

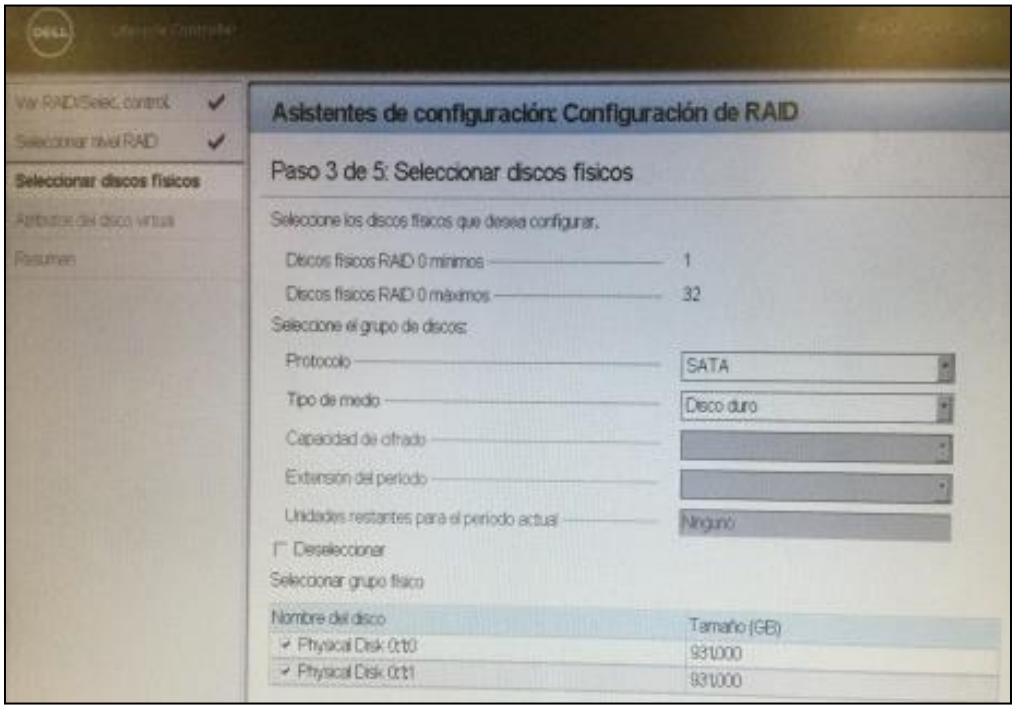


Figura A.14 Paso3 - Seleccionar discos físicos

Paso 4. Atributos del disco virtual: Constituye la selección de atributos del disco virtual, se elige un nombre para el disco virtual, en este caso se coloca el nombre de RAIDRyS, se indica que se utiliza todo el disco, entre otras configuraciones que se muestran en la Tabla A.3, quedando como se muestra en la Figura A.15, al finalizar se da click en el botón Siguiente para continuar con el paso 5.

Tabla A.3 Configuración de disco virtual

Nombre	RAIDRyS
Tamaño del disco	1862
Tamaño de elemento de sección	64 KB
Política de lectura	Sin lectura aceptada

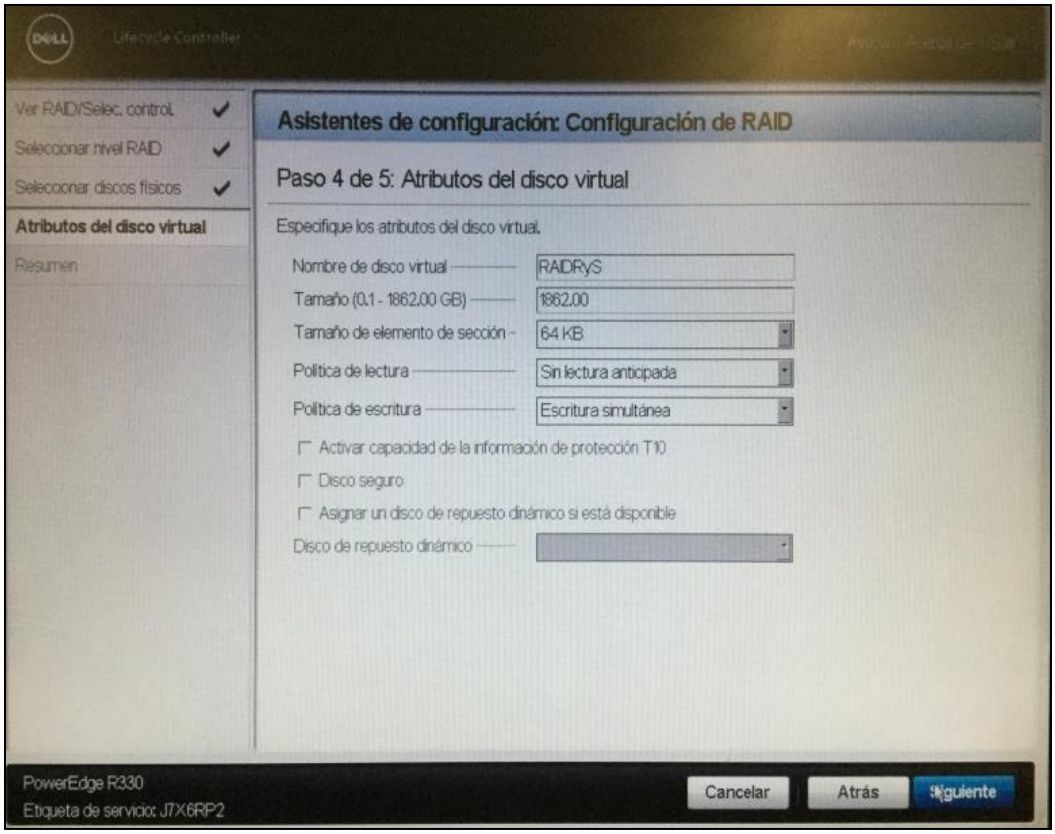


Figura A.15 Paso 4 - Atributos del disco virtual

Paso 5. Resumen: En este paso se muestran las configuraciones realizadas, en este espacio se puede identificar cualquier configuración no deseada y se puede volver a modificar cuantas veces sean necesarias antes de terminar dando clic en Atrás para poder modificar, cuando la configuración es la deseada se da click en Terminar (véase Figura A.16).

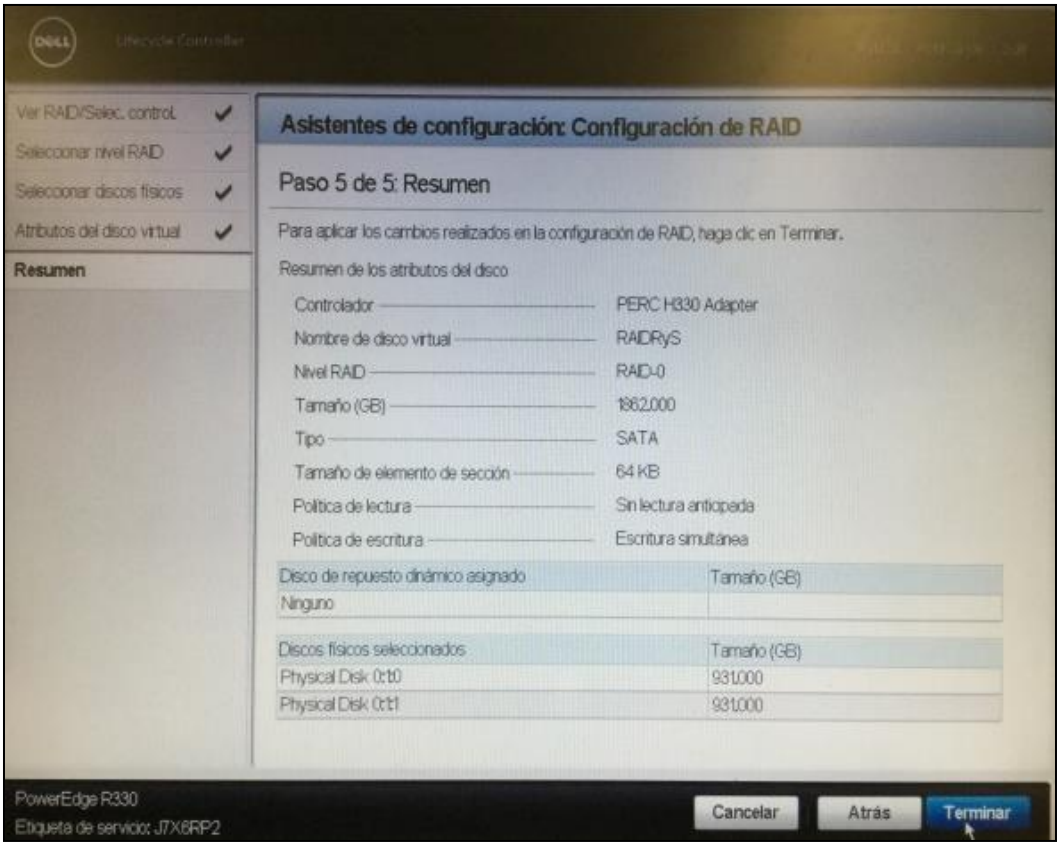


Figura A.16 Paso 5 - Resumen de configuración

Cuando se termina con la configuración de RAID se crea una ventana emergente con un mensaje de advertencia el cual notifica acerca de la aplicación de las nuevas configuraciones en los discos virtuales del sistema, se selecciona la opción "Sí" y aparece una nueva ventana emergente indicando que las configuraciones se aplicaron con éxito seleccionar "Aceptar" para finalizar el proceso. (Véase Figura A.17).

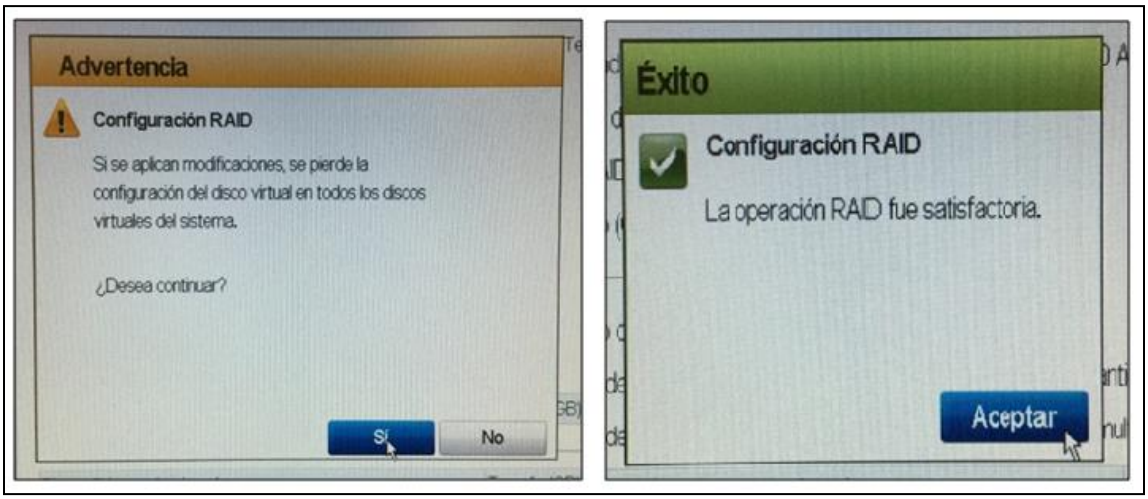


Figura A.17 Ventanas emergentes

Una vez finalizado, se debe implementar un sistema operativo, esto se realiza con la opción de "Implementación del sistema operativo" en el menú de Lifecycle Controller, como se muestra en la Figura A.18.

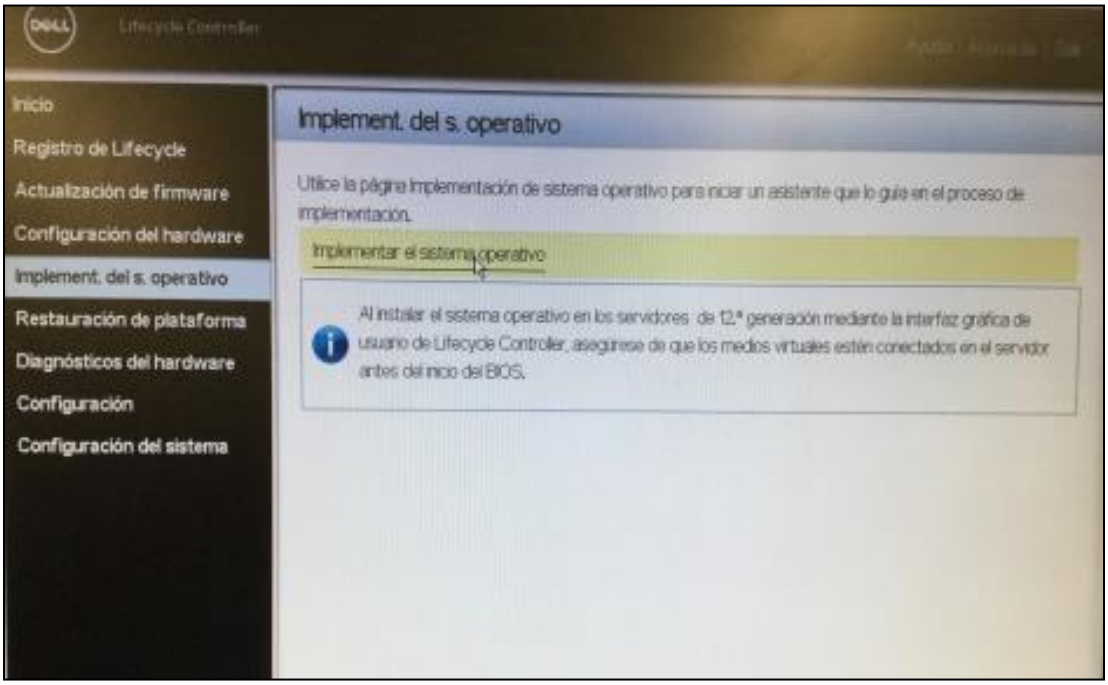


Figura A.18 Implementación del sistema operativo

Este proceso consta de 5 pasos los cuales se describen a continuación

Paso 1. Selección de ruta de implementación: Como ya se tiene configurado el RAID, se selecciona la opción de ir a la implementación del sistema operativo dando click en el botón Siguiente que se encuentra en la parte inferior derecha como se ve en la Figura A.19.

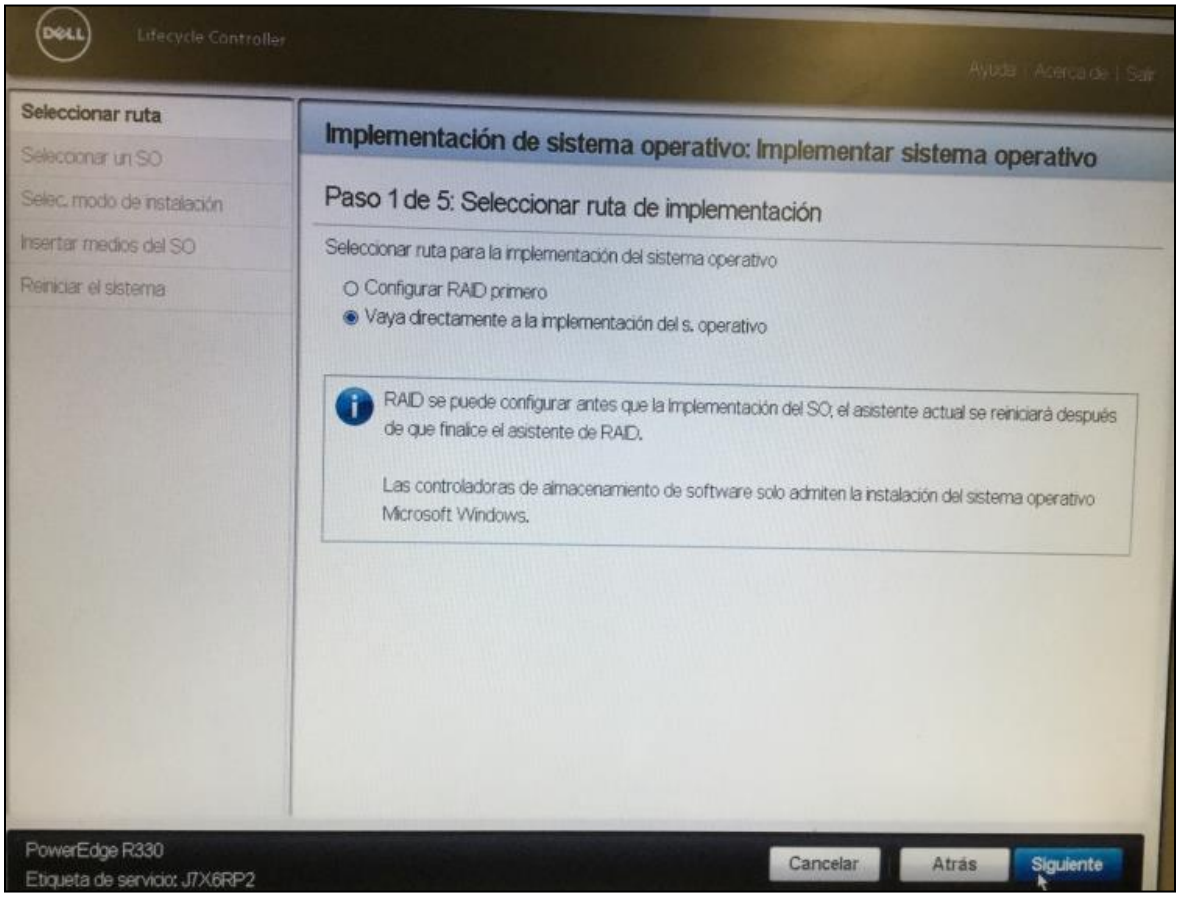


Figura A.19 Paso 1 - Seleccionar ruta de implementación

Paso 2. consiste en seleccionar el modo de inicio, puede ser BIOS y UEFI, para este servidor se selecciona la opción BIOS. El inicio seguro se deja desactivado, ya que solo funciona para el modo UEFI y se selecciona el Sistema Operativo, en las opciones no está como opción Debian, que es el sistema operativo a instalar descrita en el capítulo X por lo que se selecciona "Any Other Operating System", al terminar se selecciona Siguiente como se muestra en la Figura A.20.

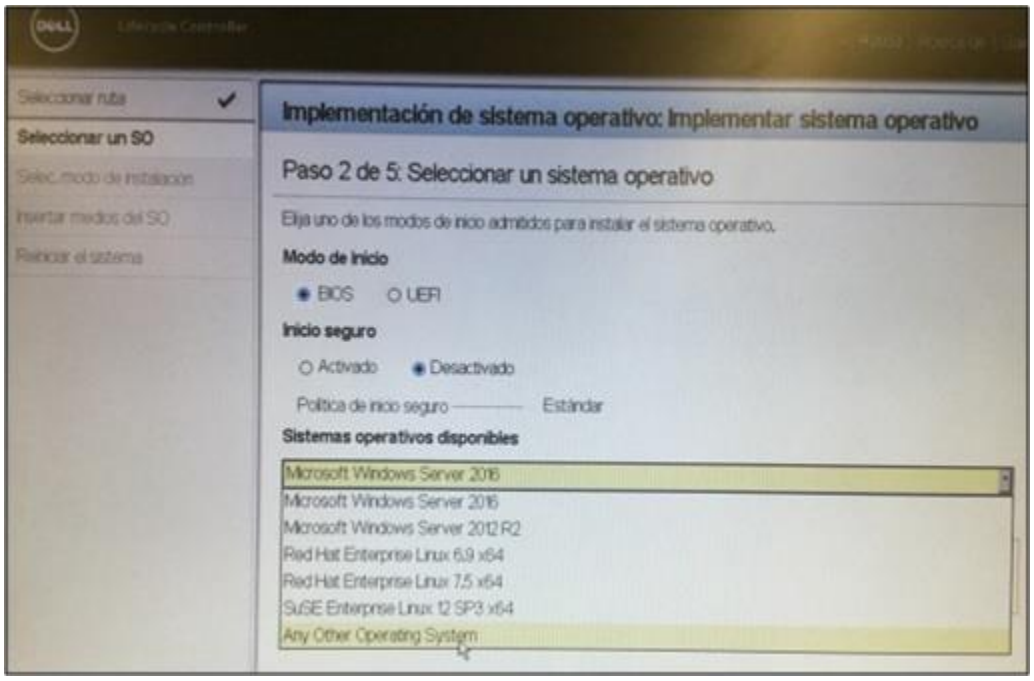


Figura A.20 Paso 2 - Seleccionar un sistema operativo

Paso 3. Selección modo de instalación: En este paso se selecciona “Instalación manual” como se muestra en la Figura A.21, al terminar se selecciona siguiente para seguir con el proceso.

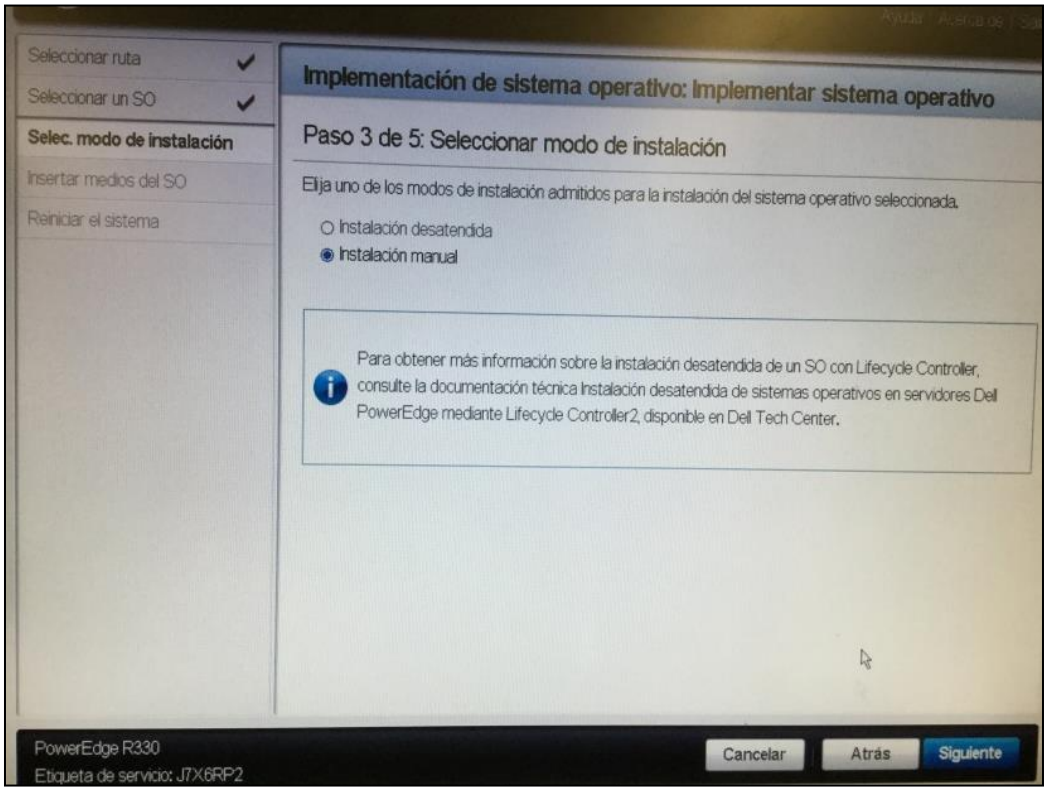


Figura A.21 Selección de modo de instalación

Paso 4. Insertar medios del SO: Consiste en insertar el medio para la instalación del sistema operativo, puede ser un CD o una unidad USB, cuando se inserta se debe seleccionar el botón Siguiente para poder seguir con el proceso, aparecerá una ventana emergente en la que se está procesando y validando la información del medio como se muestra en la Figura A.22.

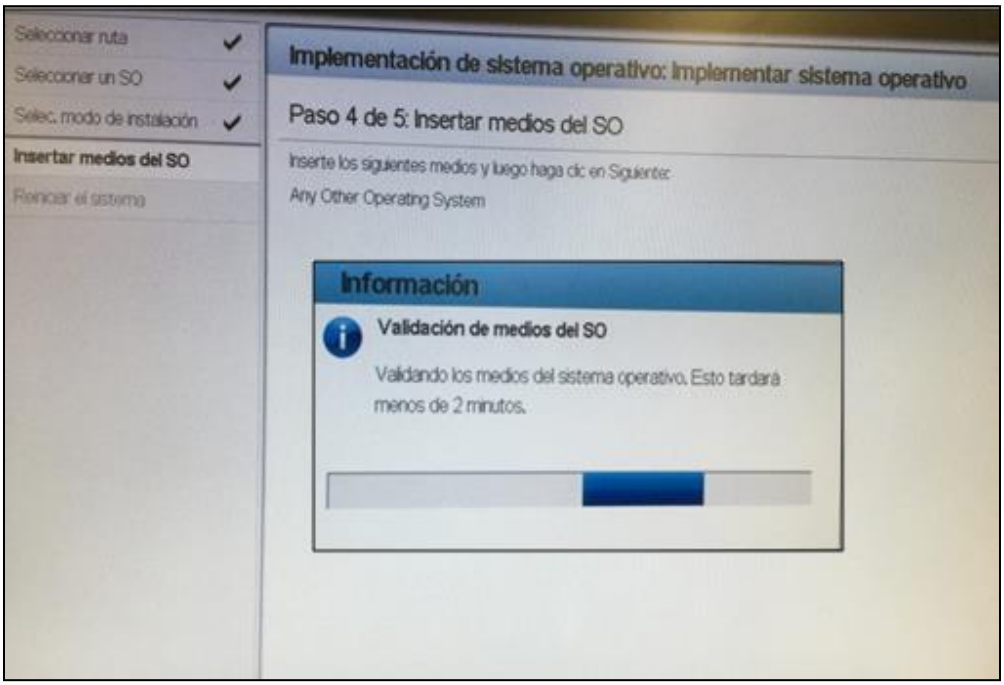


Figura A.22 Paso 4 - Insertar medio del sistema operativo

Paso 5. Reinicio de sistema: Se muestra un pequeño resumen de las configuraciones seleccionadas, se verifica toda la información con la que se comenzará el proceso de instalación del sistema operativo (véase Figura A.23). Se selecciona Terminar para que el sistema reinicie y comience la instalación.

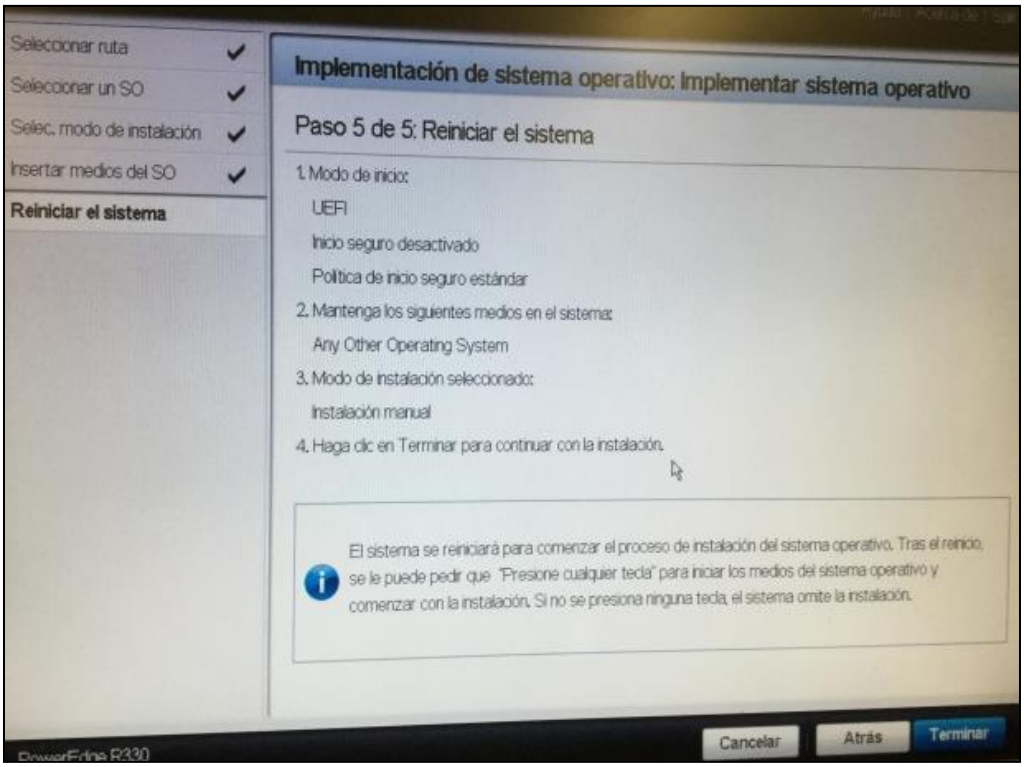


Figura A.23 Paso 5 - Reiniciar el sistema

3. Instalación del sistema operativo

El sistema operativo a instalar es Debian en la versión 9.6.0 “Stretch” para una arquitectura de 64 bits.

Para iniciar la instalación de Debian 9 basta con bajar un archivo ISO de instalación desde la página oficial de Debian: https://www.debian.org/. Véase Figura A.24. Una vez que se tenga descargado el ISO se puede usar para crear un LiveDVD o un LiveUSB como medio de instalación.

Figura A.24 Página oficial de Debian

Una vez creado el medio de instalación, se coloca en el servidor en este caso se utiliza un disco de instalación y se puede iniciar el equipo e iniciar la instalación. En la pantalla inicial se muestra en la Figura A.25, en esta se selecciona la opción instalación gráfica para instalar un sistema de escritorio utilizando las flechas del teclado y se da enter.

Figura A.25 Modo de instalación del Sistema Operativo

Se elige el idioma base para el sistema. (véase Figura A.26) dando click en Continuar.

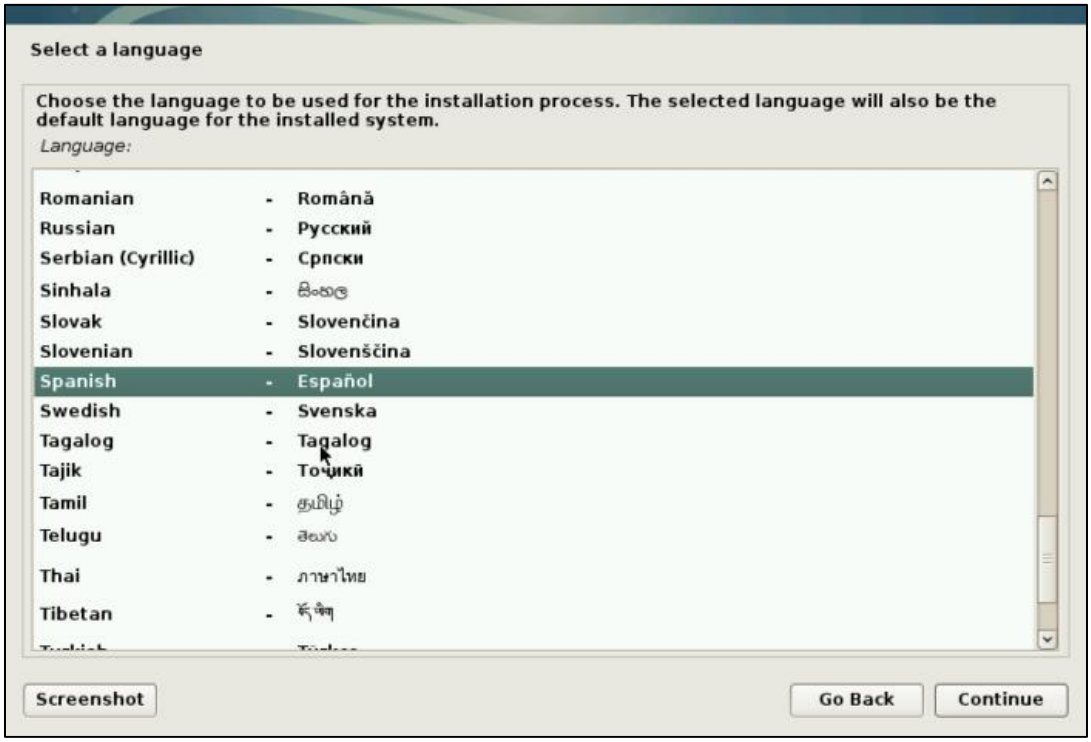


Figura A.26 Selección de idioma

Se selecciona la ubicación geográfica del servidor. (véase Figura A.27) dando click en Continuar.

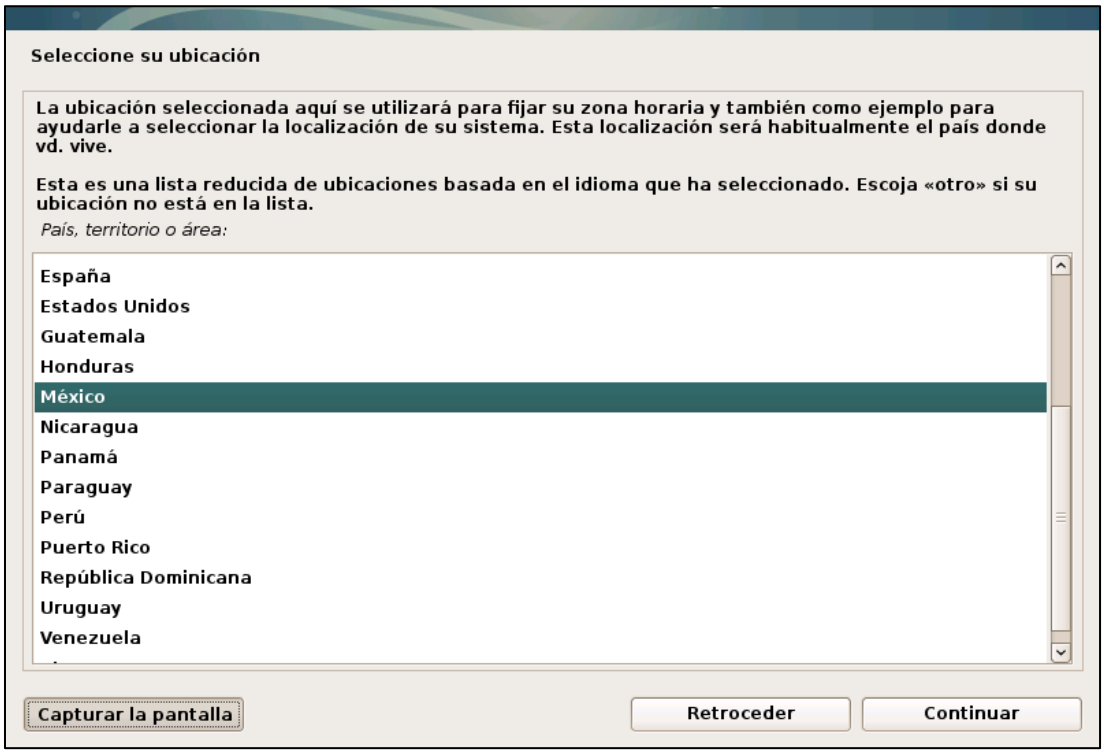


Figura A.27 Selección de ubicación geográfica

Se indica la configuración del teclado. (véase Figura A.28) dando click en Continuar.

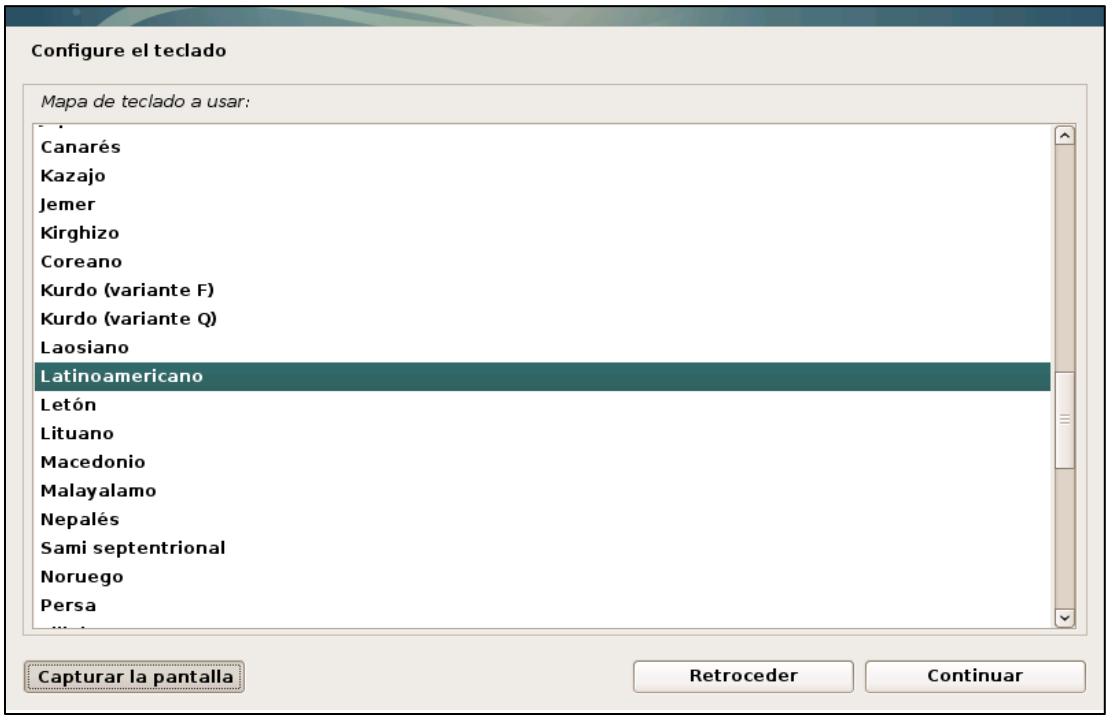


Figura A.28 Selección de configuración de teclado

Posteriormente, si no se tiene configurado previamente un servidor DHCP, al tratar de configurar la red se produce un fallo como se muestra en la Figura A.29.

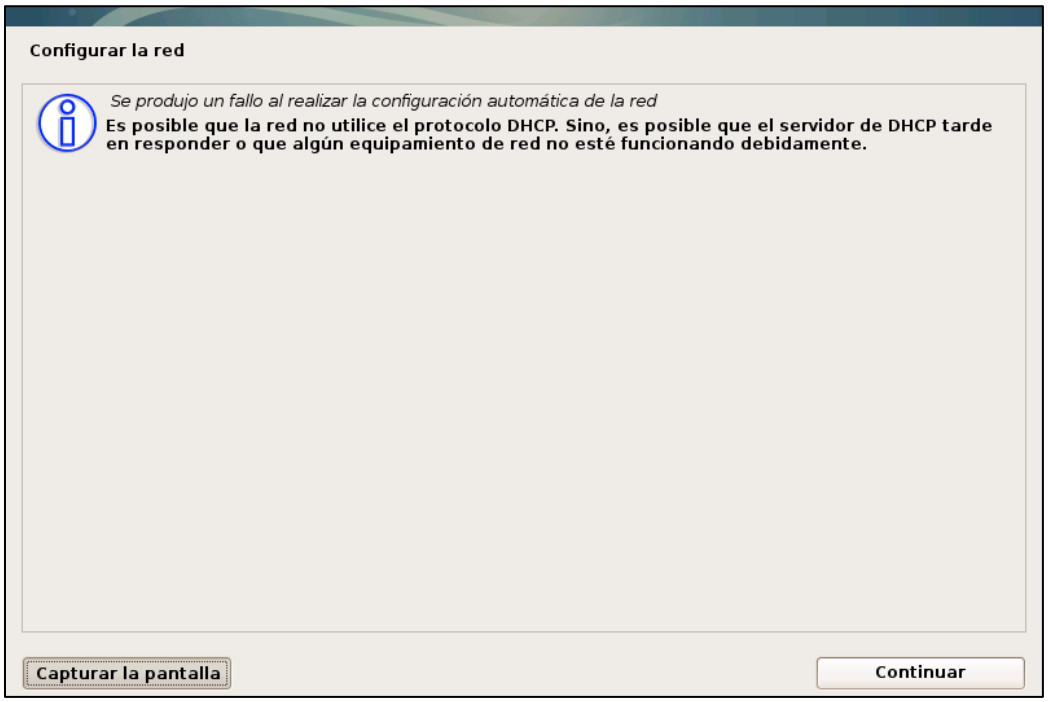


Figura A.29 Configuración de red

Si este es el caso, se debe configurar la red manualmente como se muestra en la Figura A.30.

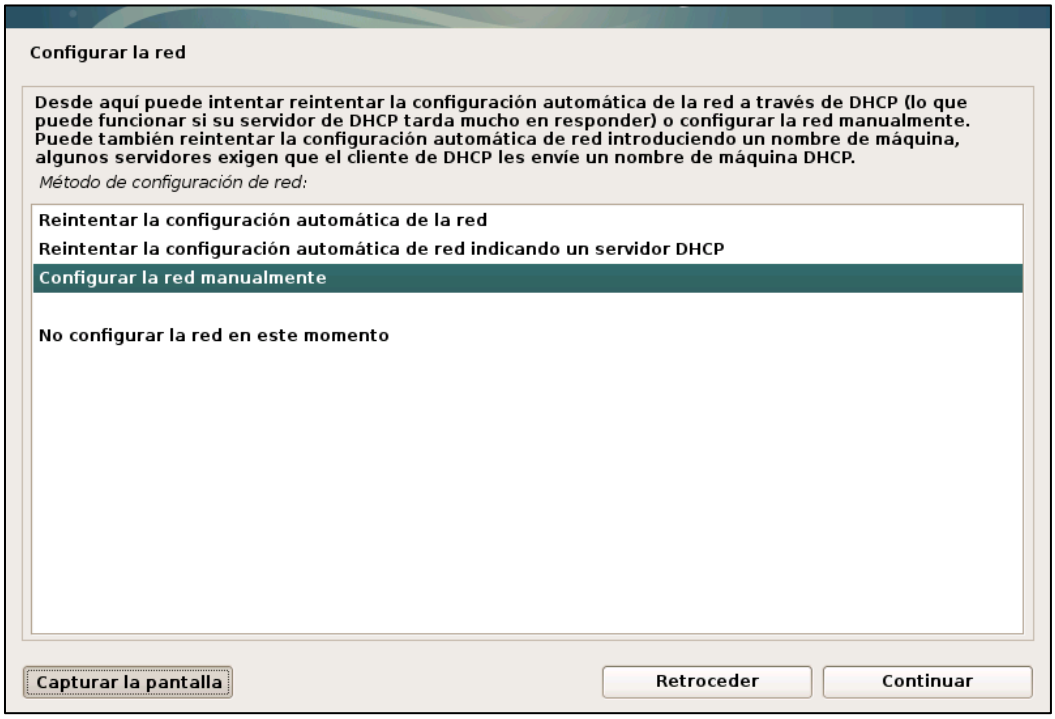


Figura A.30 Configuración de red manual

Primero se introduce la dirección IP. (véase Figura A.31). Por razones de seguridad esta configuración no se muestra en este manual de instalación.

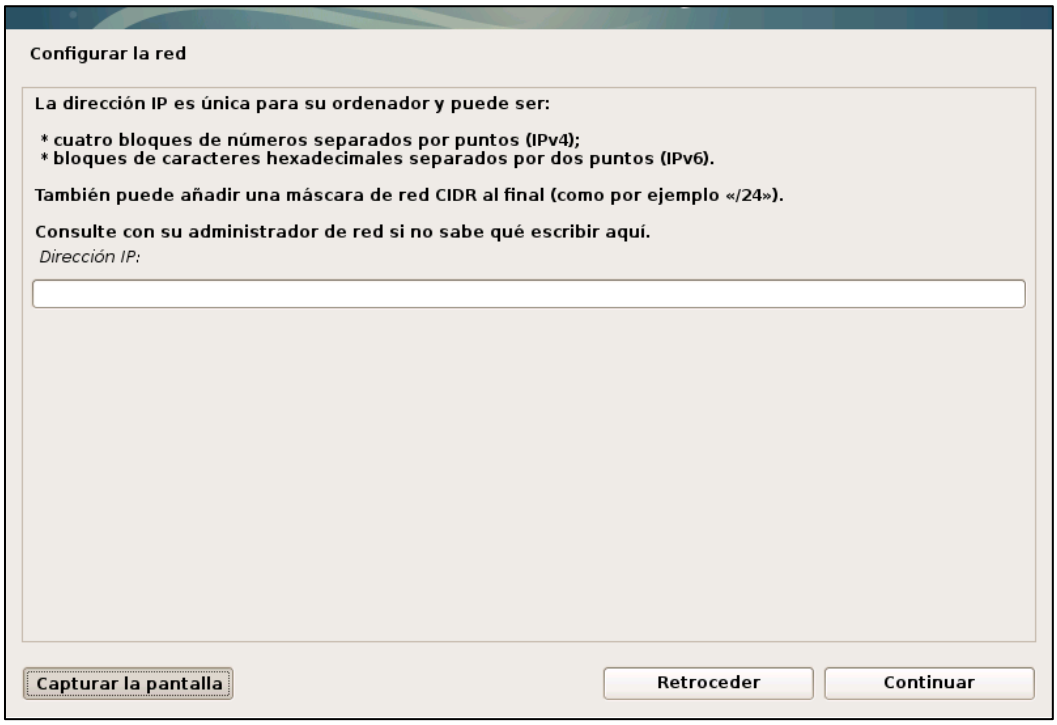


Figura A.31 Dirección de IP

En seguida se introduce la dirección del gateway de la red a la que se conecta. (véase Figura A.32).

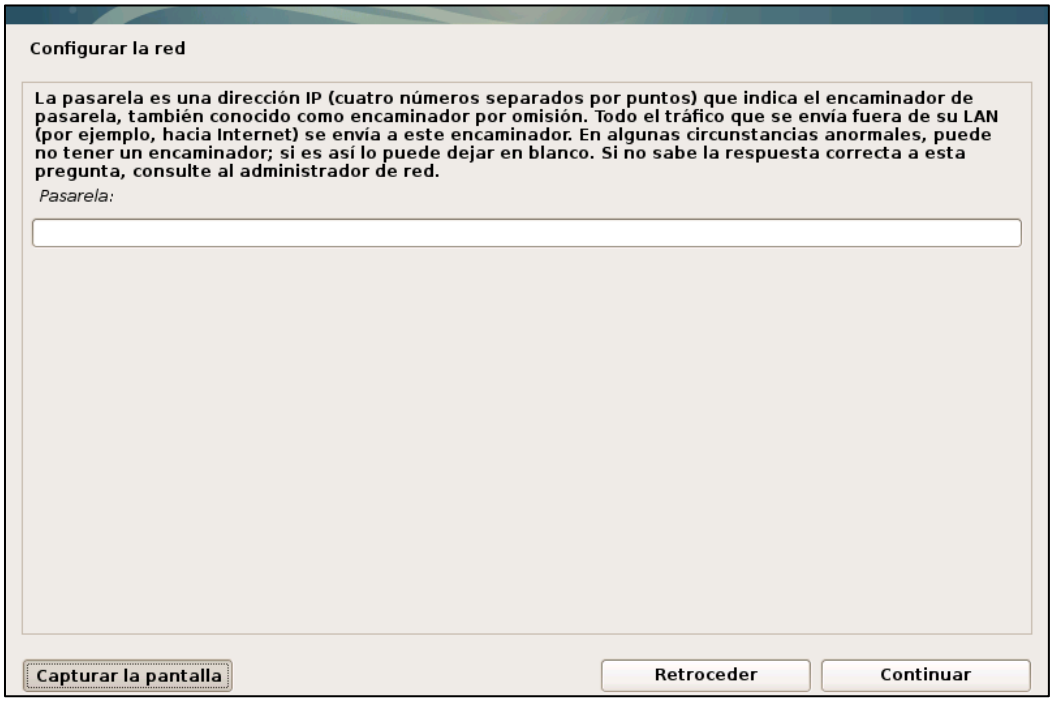


Figura A.32 Dirección de gateway

Se introduce la dirección del servidor de dominio, si es más de uno, se separa por espacios. (véase Figura A.33).

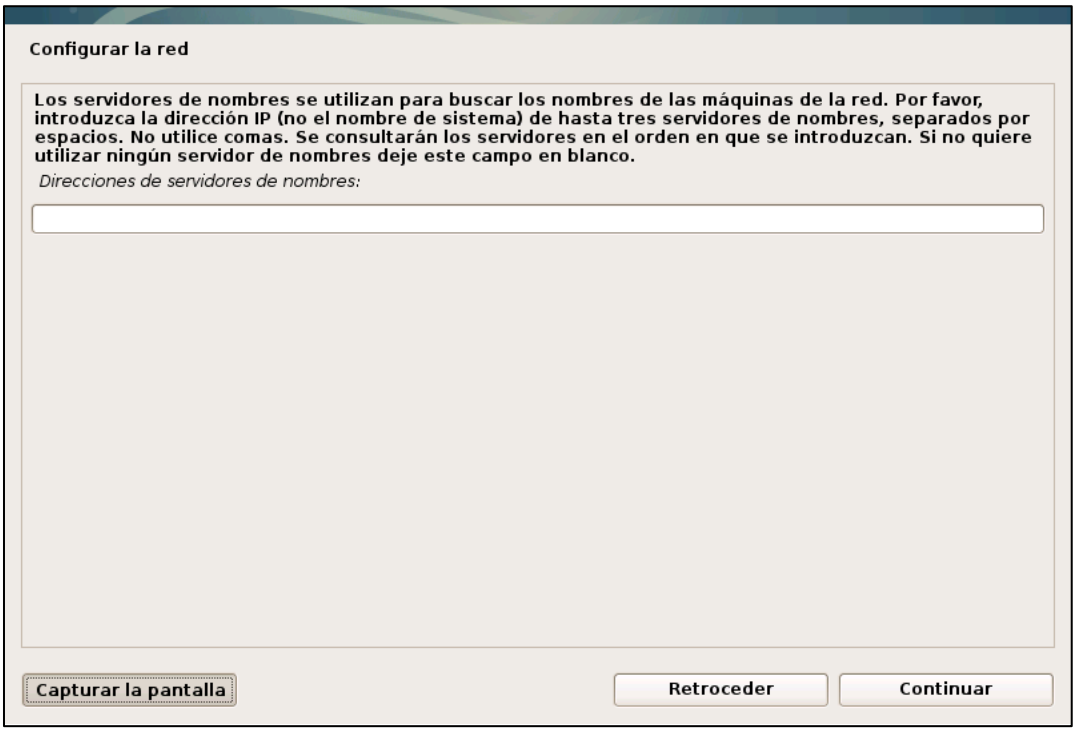


Figura A.33 Direcciones DNS

Introducir el nombre de la máquina (véase Figura A.34).

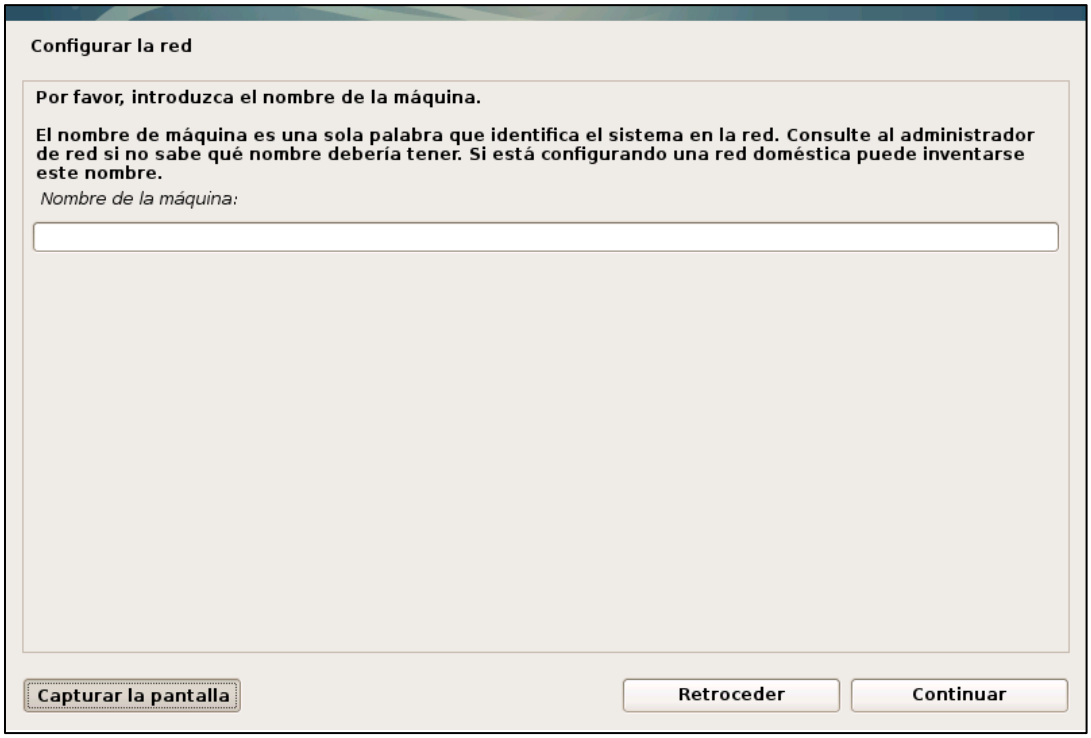


Figura A.34 Nombre de la máquina

Lo último para configurar la red es introducir el nombre de dominio, si no se pertenece a ninguno, se deja en blanco y se presiona continuar. (véase Figura A.35) en este caso se utilizó el que ya se tiene configurado en el Laboratorio.

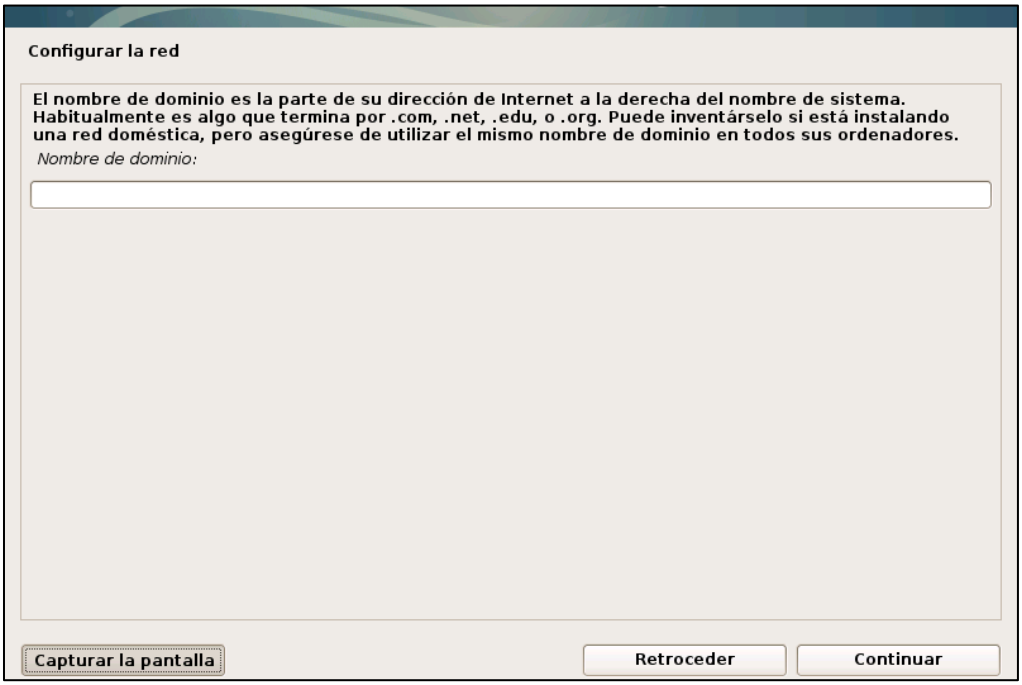


Figura A.35 Nombre de dominio

En el siguiente paso se debe indicar una contraseña para el superusuario. (véase Figura A.36)

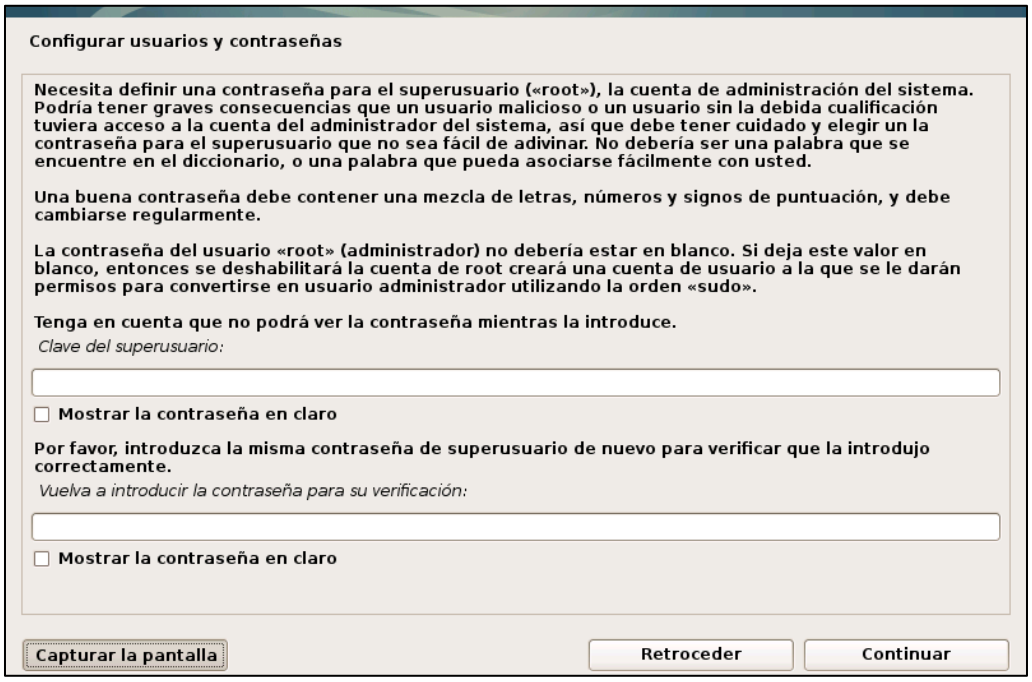


Figura A.36 Clave de superusuario

Asimismo, se debe crear un usuario que no tenga privilegios de superusuario, es decir, el usuario para el uso cotidiano del sistema. Primero se indica nombre completo del usuario. (véase Figura A.37)

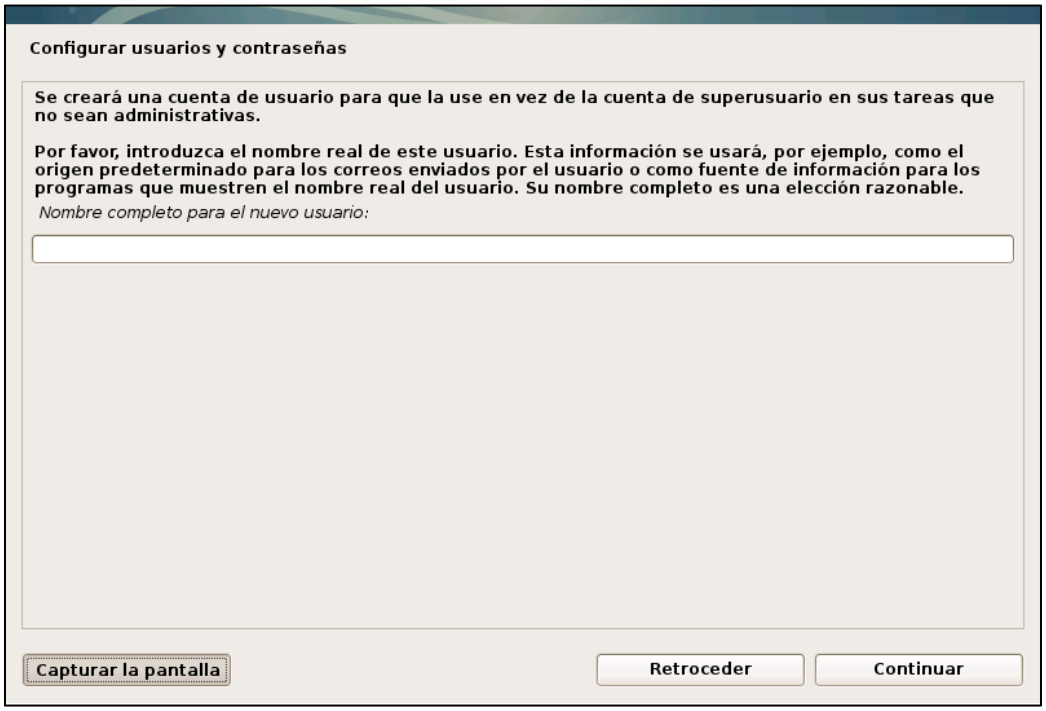


Figura A.37 Nombre completo del usuario

En seguida se indica el nombre de usuario. (véase Figura A.38)

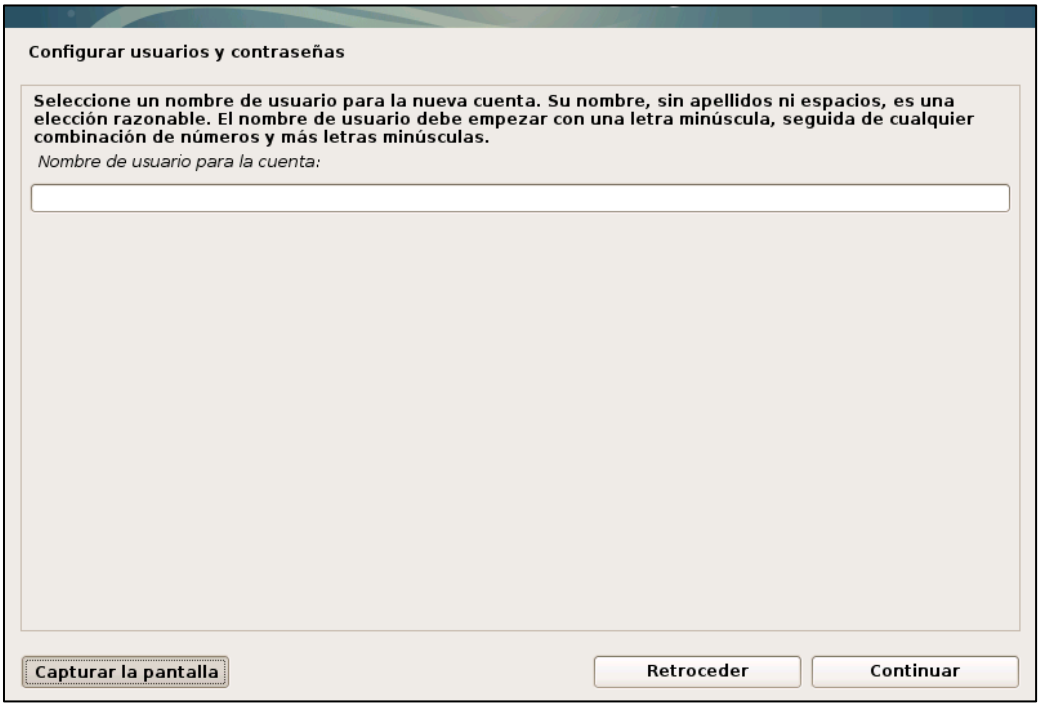


Figura A.38 Nombre de usuario

Se indica la contraseña para el usuario (véase Figura A.39)

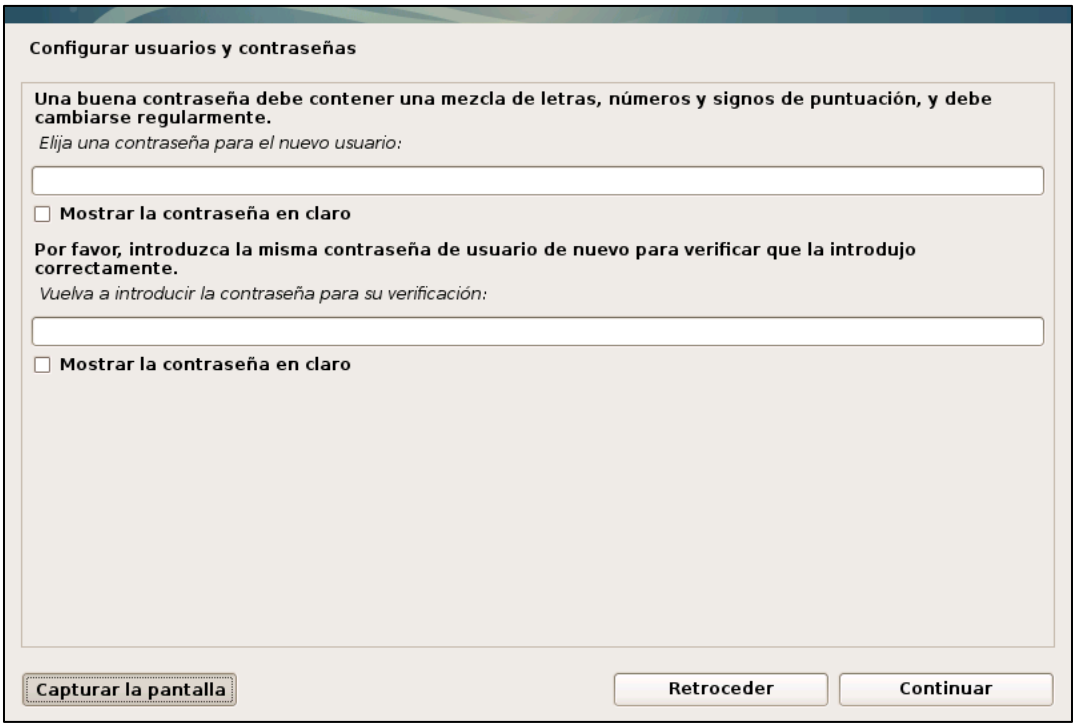


Figura A.39 Configuración de usuario (contraseña)

En la siguiente ventana se indica la zona horaria en donde se encuentra el servidor (véase Figura A.40)

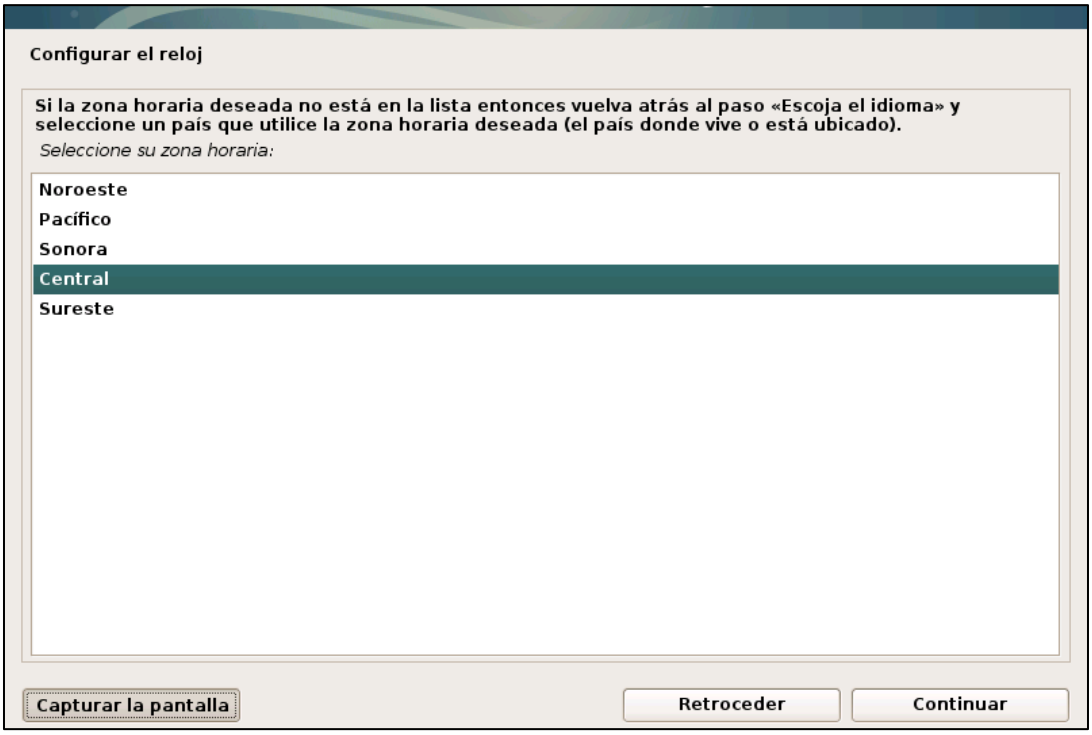


Figura A.40 Configuración de zona horaria

Para el particionado del disco se elige hacerlo de forma manual, ya que se va a definir un esquema de particionado específico. (véase Figura A.41)

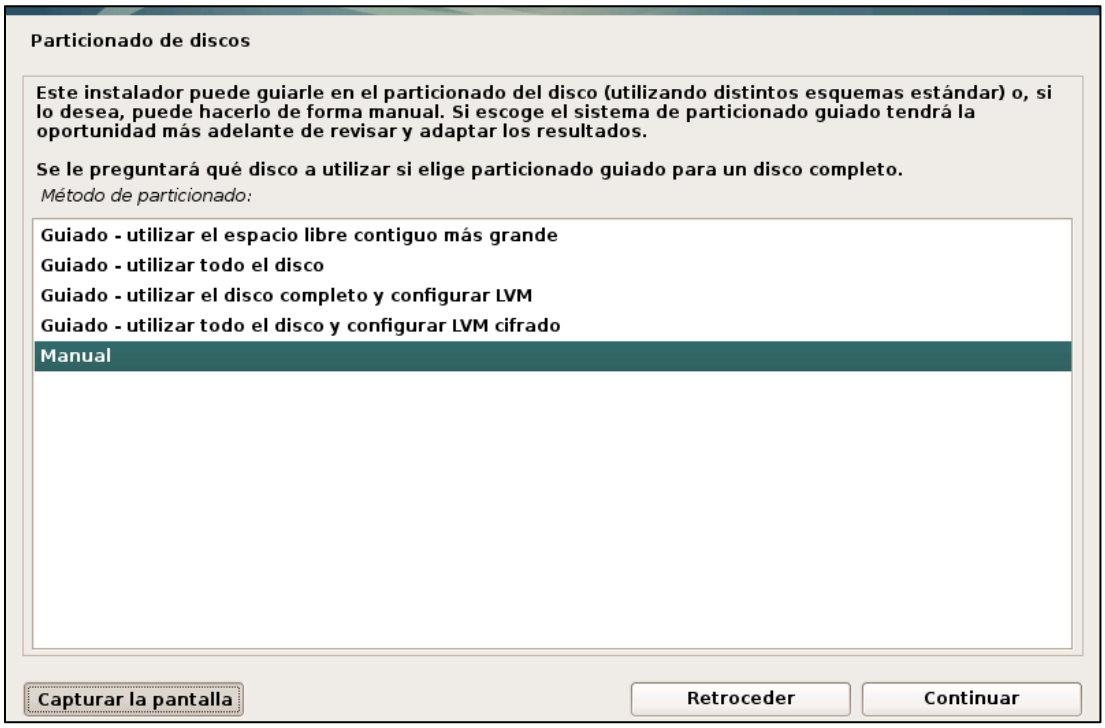


Figura A.41 Selección de particionado de disco duro

Lo primero que se debe hacer es elegir el disco duro a instalar, que va a ser el de mayor capacidad, como se muestra en la Figura A.42, ya que el otro corresponde a una USB.

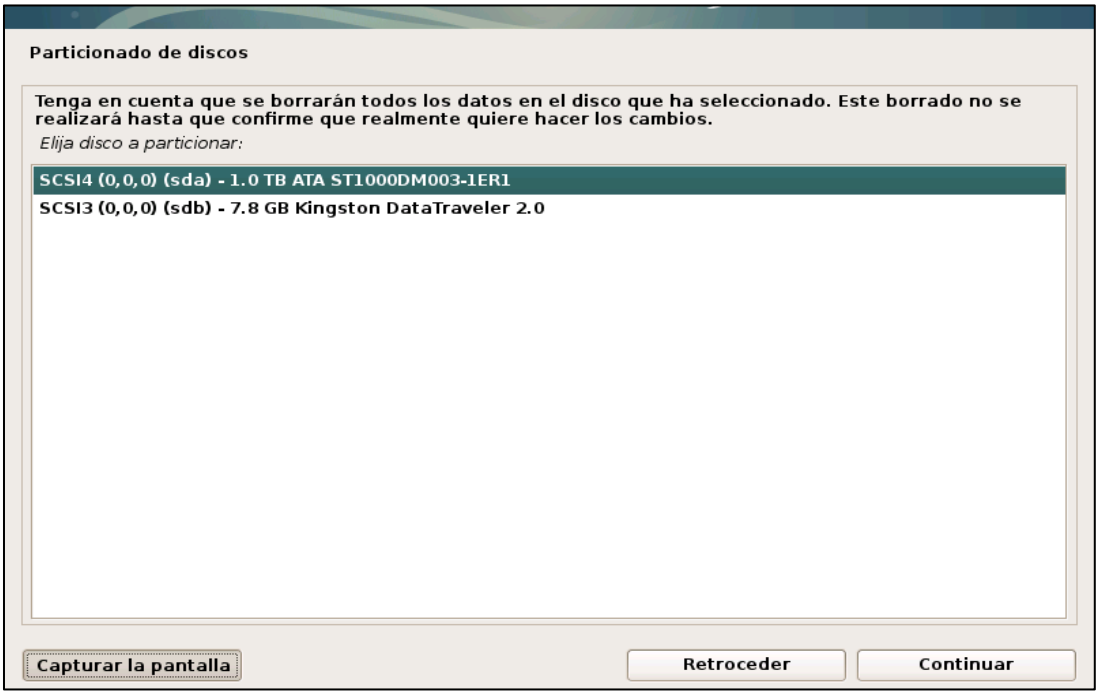


Figura A.42 Selección de disco

Si es un disco nuevo que no tiene particiones, el sistema pregunta si se desea crear una nueva tabla de particiones en el dispositivo, para lo cual se elige “Si”. (véase Figura A.43)

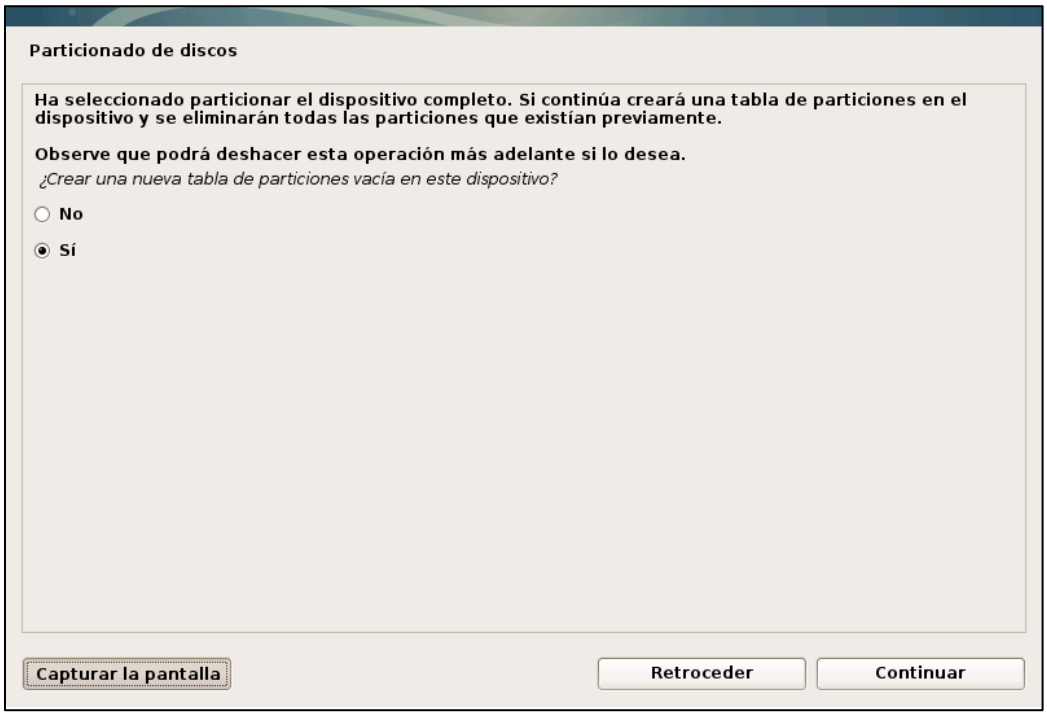


Figura A.43 Crear nueva tabla de particiones

Se crea una nueva tabla de particiones y debajo del disco seleccionado aparece la leyenda “ESPACIO LIBRE”. (véase Figura A.44)

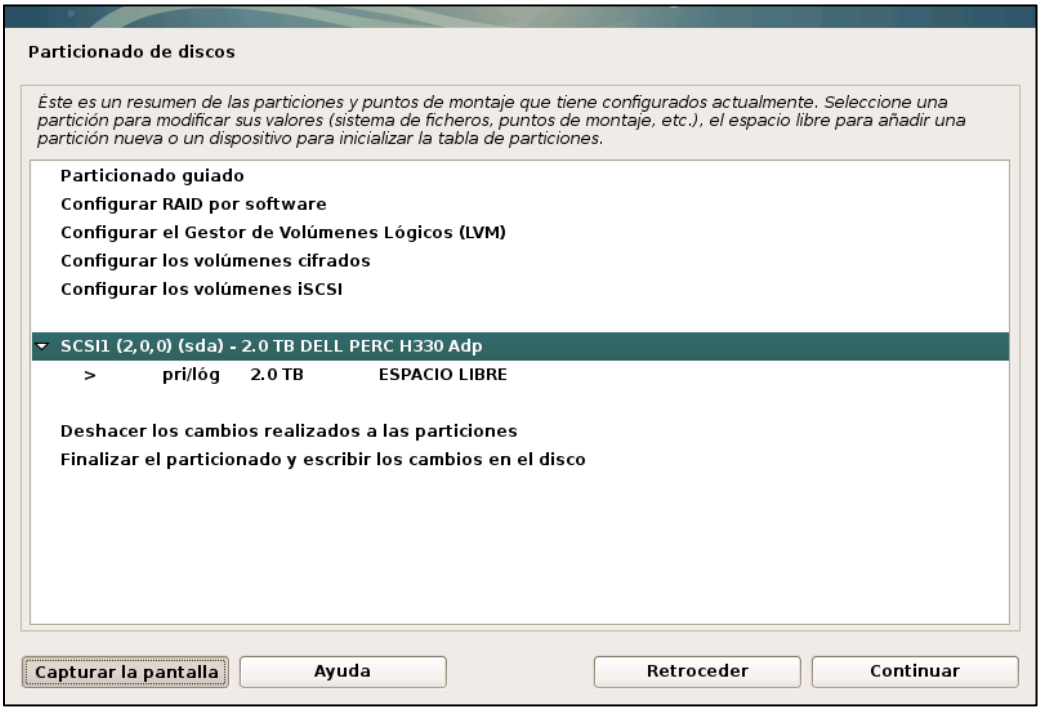


Figura A.44 Tabla de particiones

Lo primero a hacer es crear las 3 particiones primarias de acuerdo al esquema de particionado definido en el capítulo 2 en el apartado 2.1.2, quedando como se muestra en la Tabla A.4.

Tabla A.4 Particiones primarias

Punto de montaje	Tamaño
/	50 GB
/boot	2 GB
swap	16 GB

A continuación, se elige espacio libre y después se elige crear una partición nueva. (véase Figura A.45)

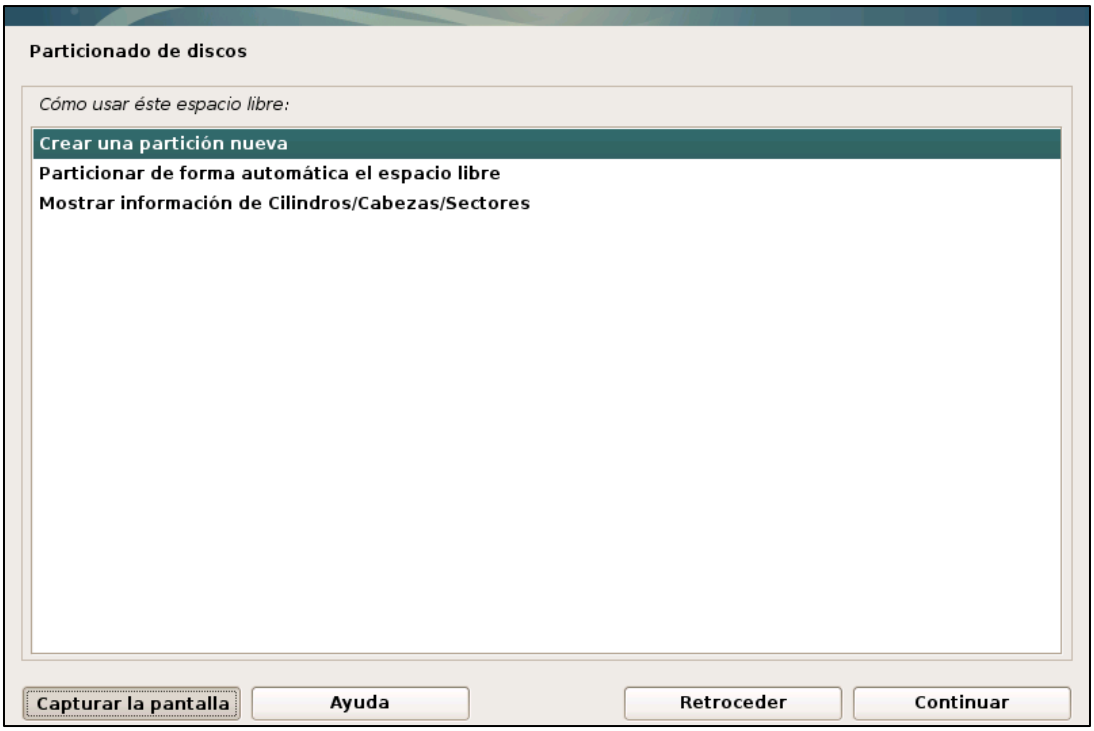


Figura A.45 Crear partición nueva

La primera partición que se crea es /boot, se indica el tamaño de la partición y se elige continuar. (véase Figura A.46)

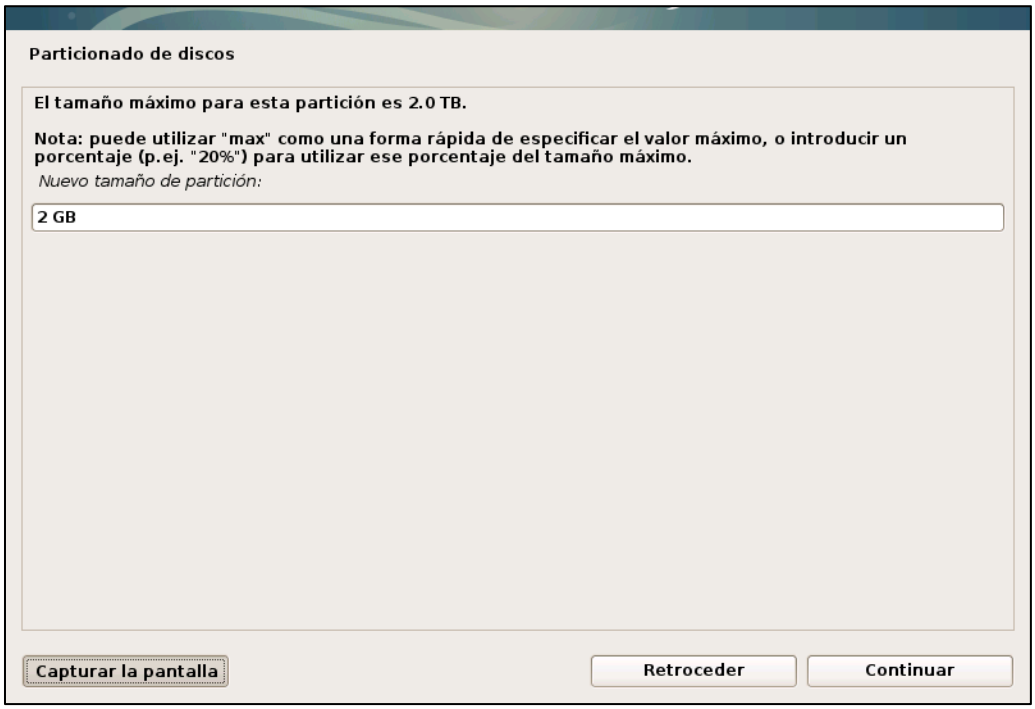


Figura A.46 Tamaño de partición

Posteriormente se elige el tipo de la partición, para /boot se elige una partición primaria. (véase Figura A.47)

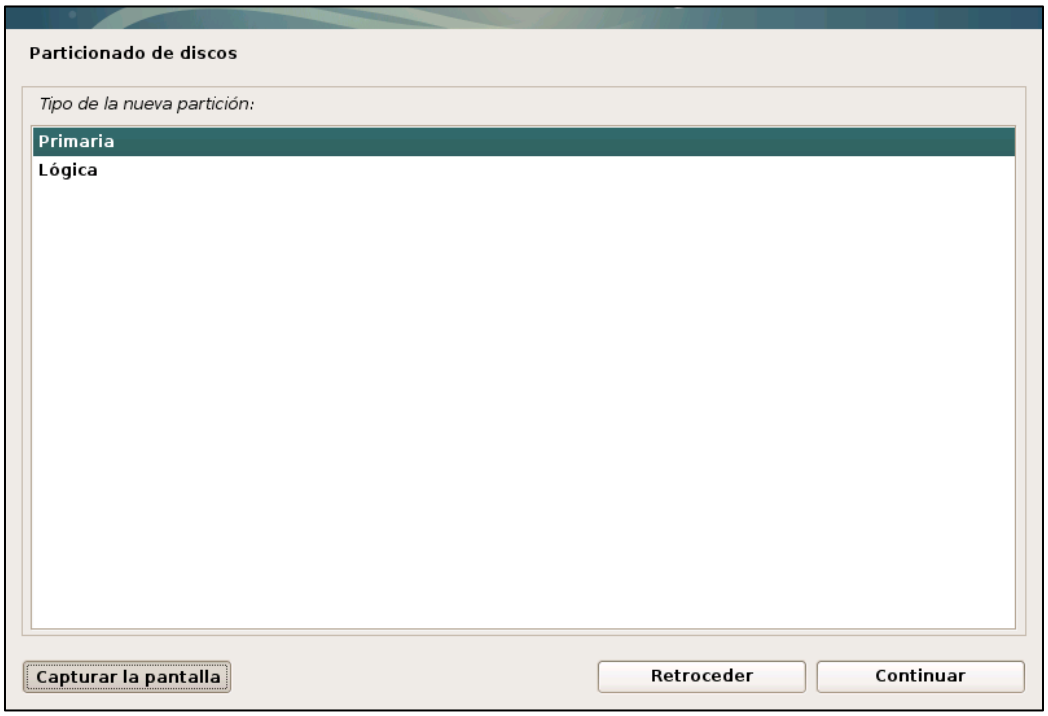


Figura A.47 Tipo de partición

Se elige que la nueva partición se cree al principio del espacio disponible, así la partición ocupará el espacio contiguo en disco duro y se elige continuar. (véase Figura A.48)

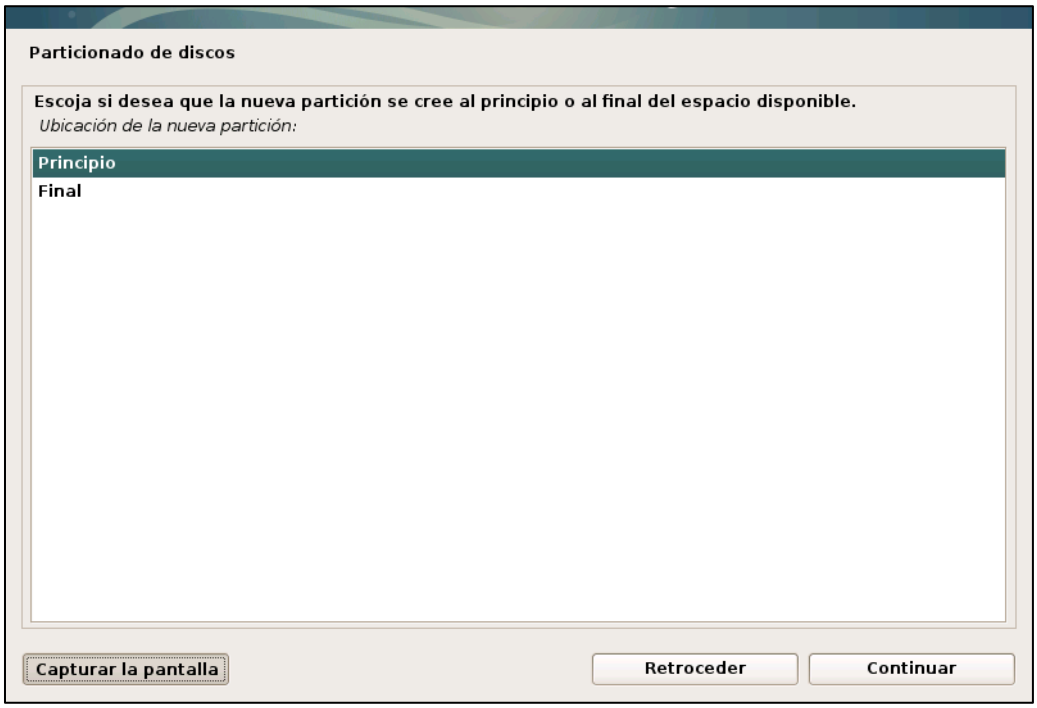


Figura A.48 Ubicación de la nueva partición

Se crea la partición y resta configurarla, se elige el punto de montaje y se presiona continuar. (véase Figura A.49)

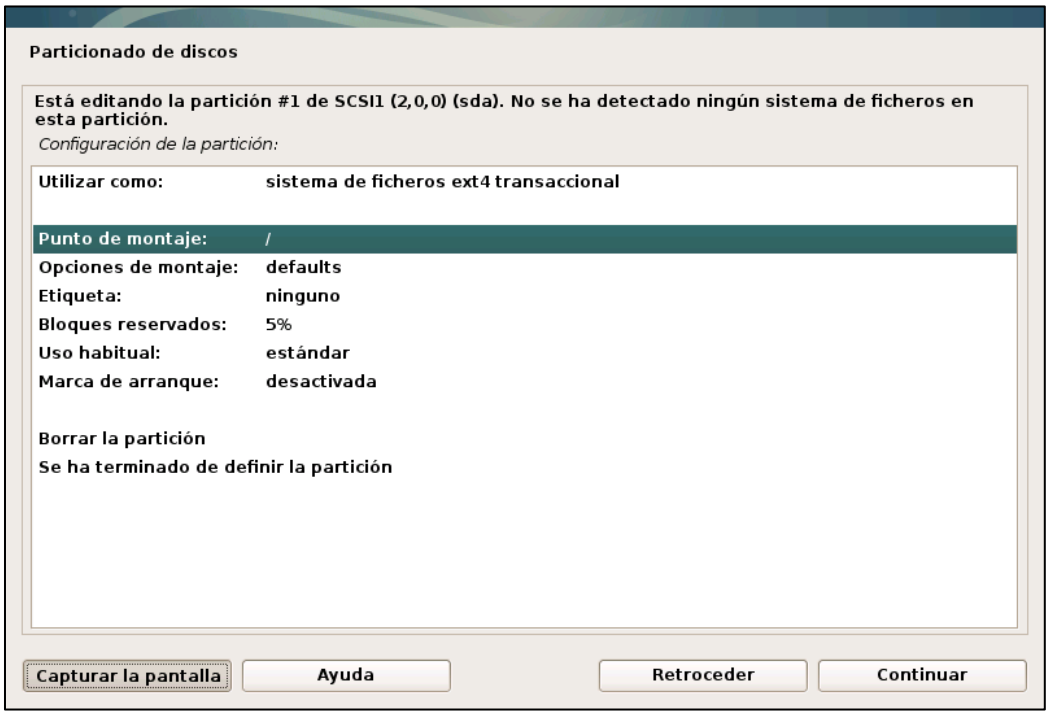


Figura A.49 Configuración de la partición

Como punto de montaje para la primera partición se elige boot y se presiona continuar. (véase Figura A.50)

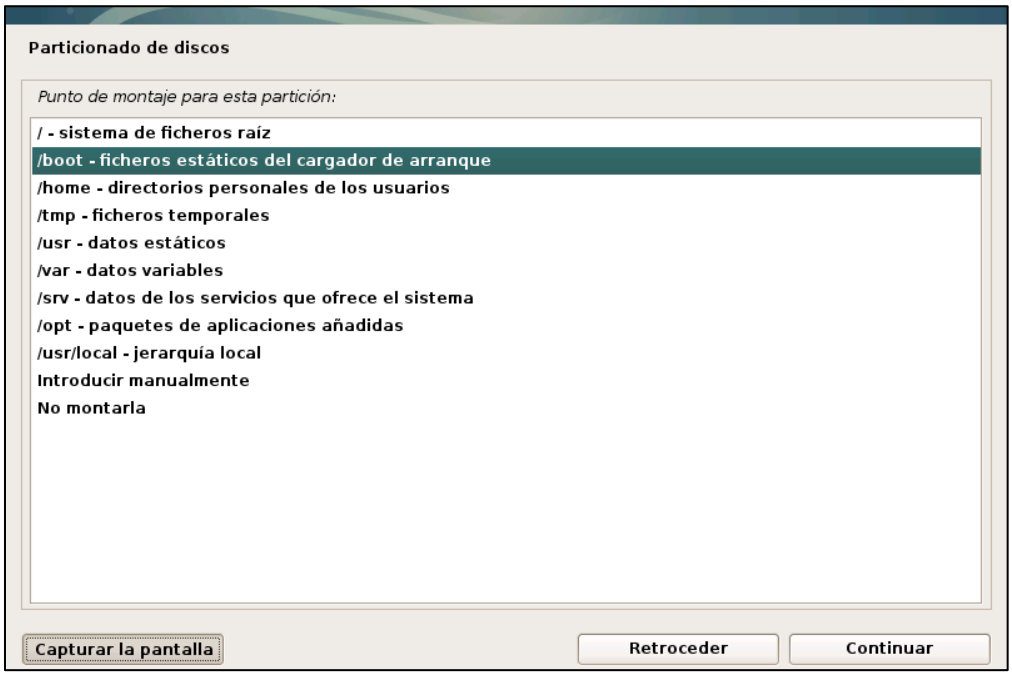


Figura A.50 Punto de montaje

Se elige marca de arranque y se selecciona continuar para que se active (véase Figura A.51)

Nota: /boot es la única partición primaria y que tiene activada la marca de arranque, ya que contiene los archivos utilizados durante el arranque del sistema.

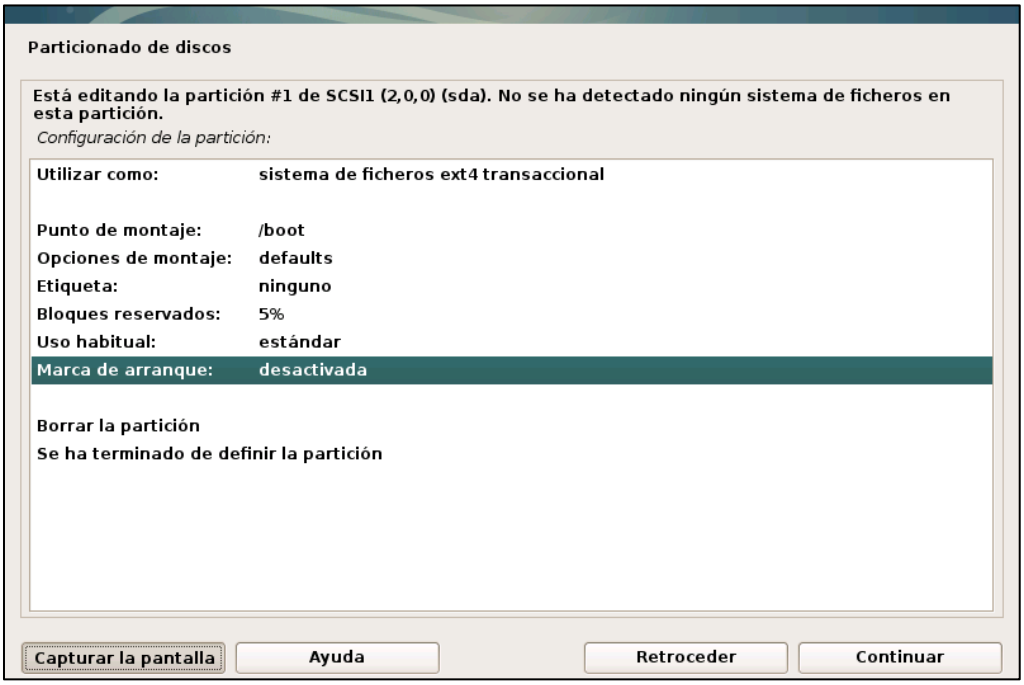


Figura A.51 Configuración de la partición

Una vez terminada la configuración de la partición se elige la opción de terminar de definir la partición y se presiona continuar. (véase Figura A.52)

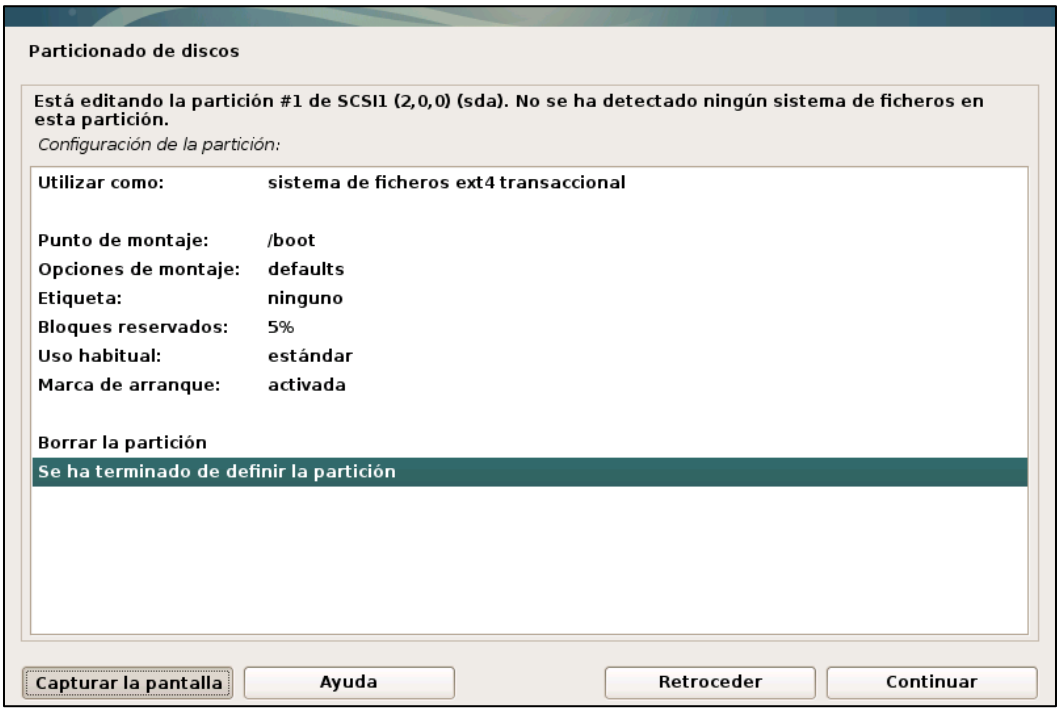


Figura A.52 Configuración de la partición

Ya se ha creado la partición /boot, se vuelve a elegir espacio libre para crear otra partición. (véase Figura A.53)

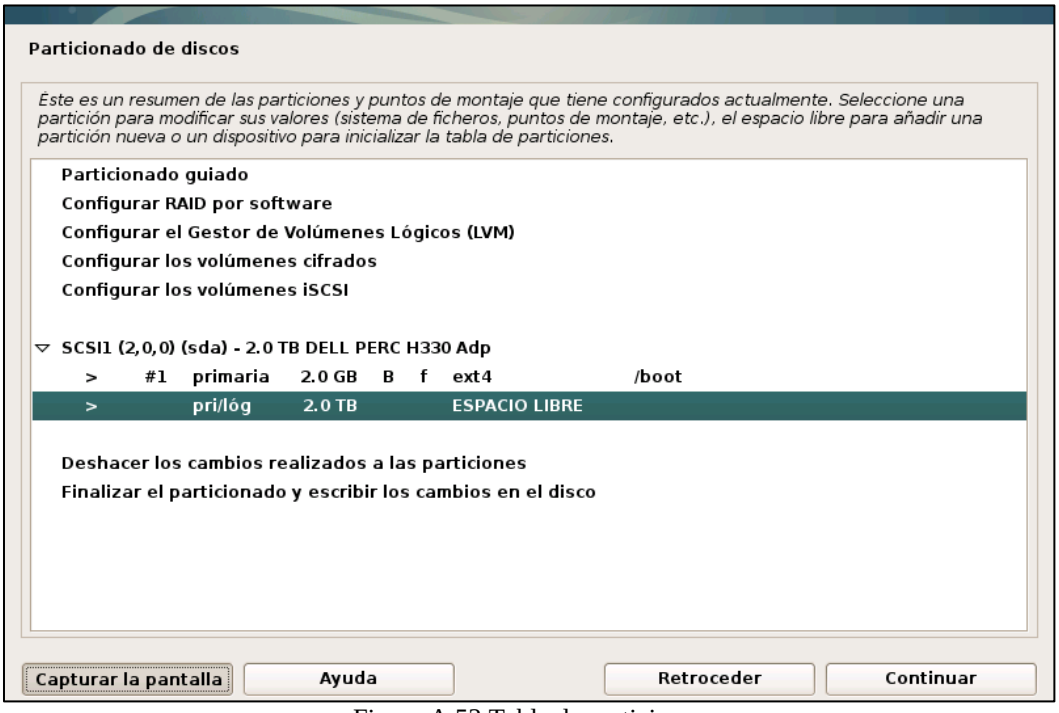


Figura A.53 Tabla de particiones

La siguiente partición a crear es swap, se repiten los pasos anteriormente realizados para crear la partición /boot. Se crea una partición de 16 GB, de tipo lógica, que se escriba al principio del espacio libre. Cuando se llegue a la configuración de la partición que se muestra en la Figura A.54 se elige la opción "Utilizar como" y se presiona continuar.

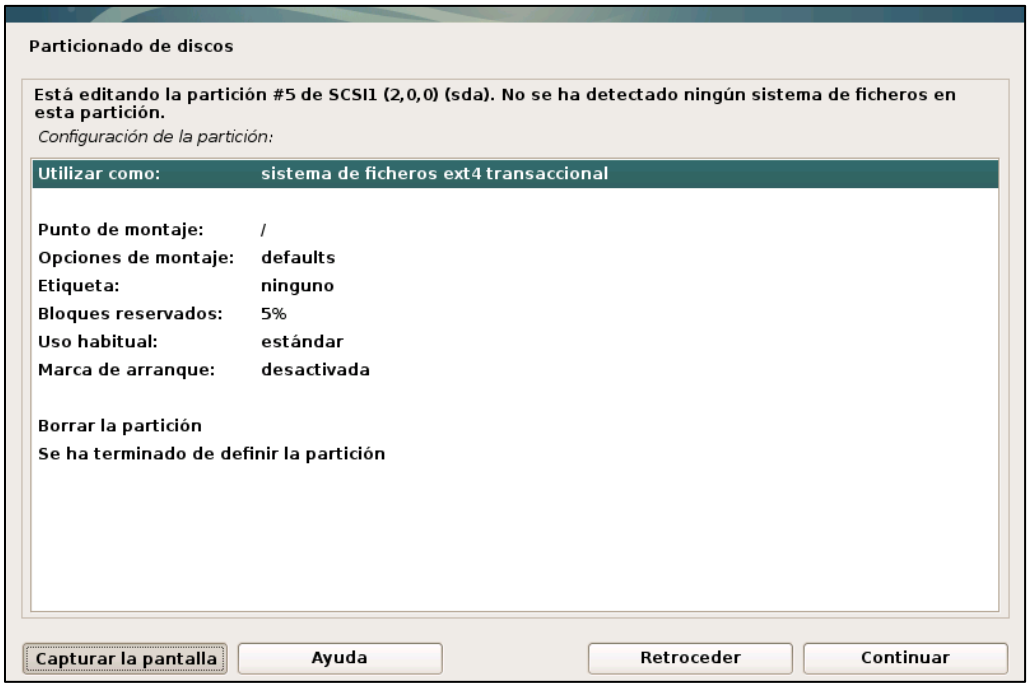


Figura A.54 Configuración de la partición

Para swap se elige el área de intercambio y se presiona continuar. (véase Figura A.55)

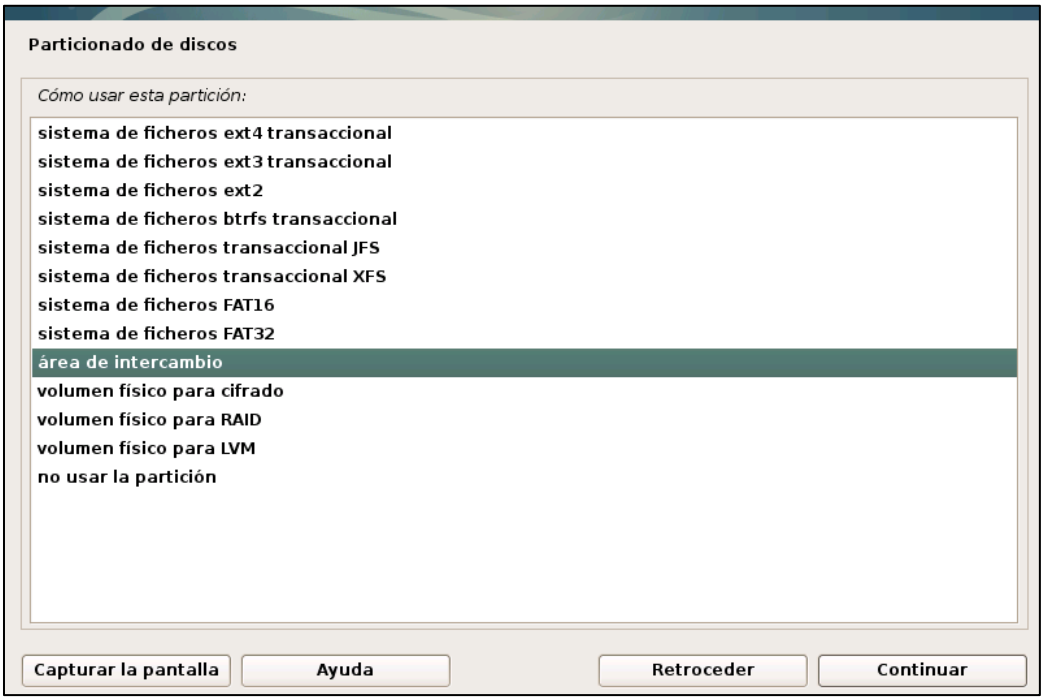


Figura A.55 Cómo usar la partición

Ahora se tienen dos particiones, se elige nuevamente espacio libre. (véase Figura A.56)

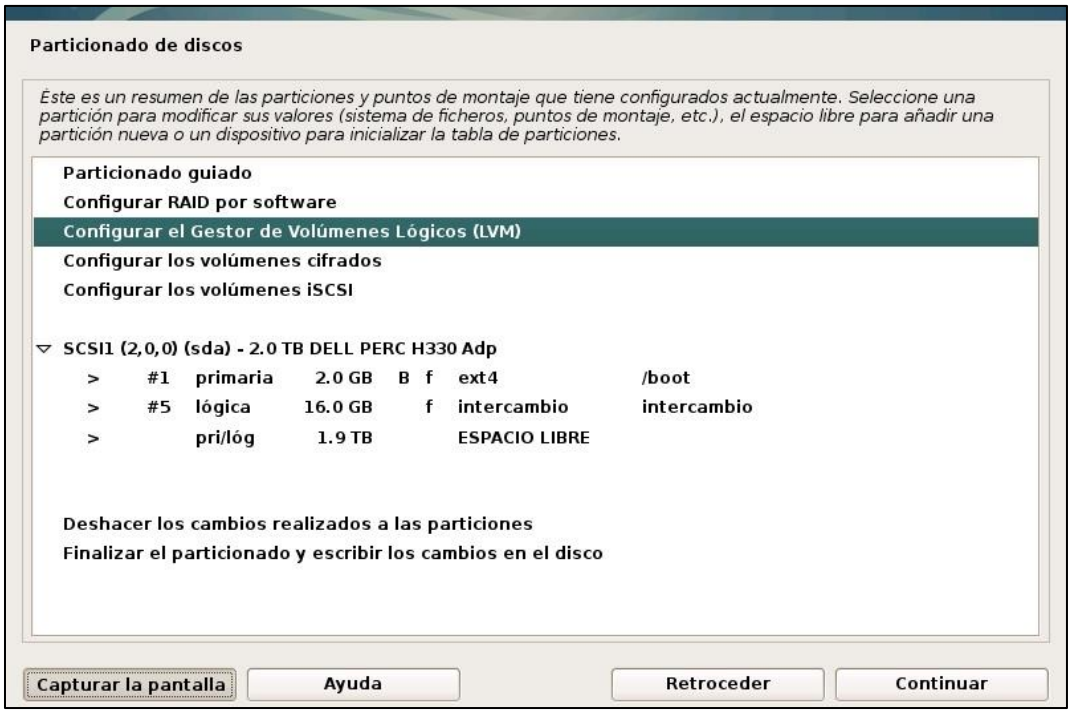


Figura A.56 Tabla de particiones

La siguiente partición a crear es la raíz (/). Se repiten los pasos, creando una partición de 50GB, de tipo lógica y que se escriba al principio del espacio libre, de forma que al finalizar se tengan tres particiones como se muestra en la Figura A.57.

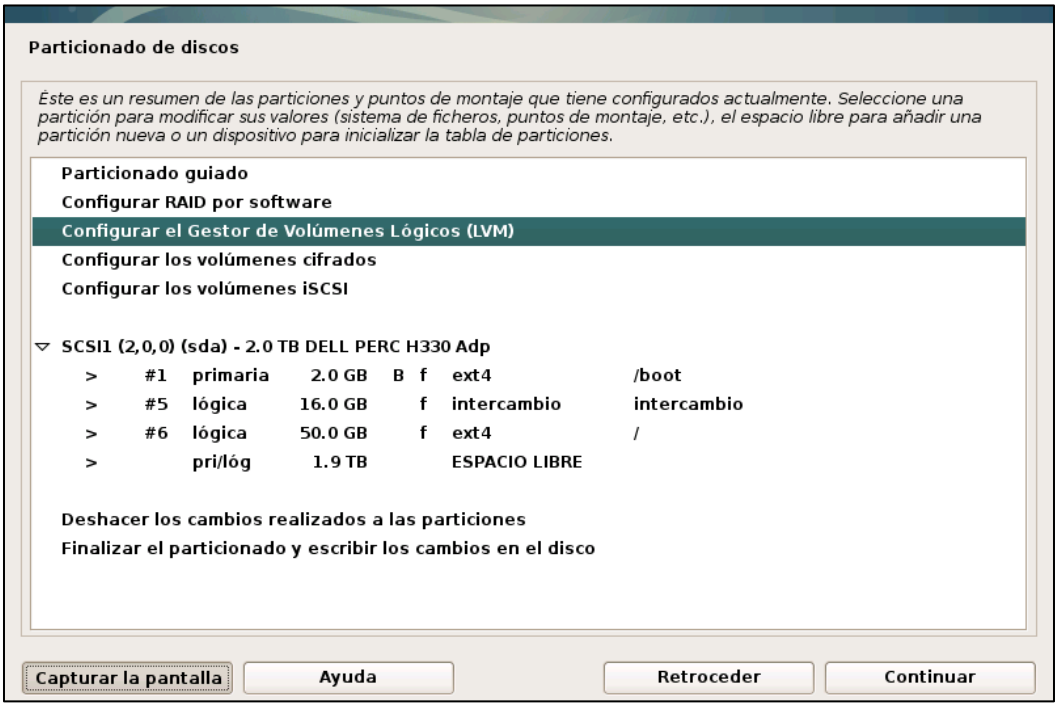


Figura A.57 Tabla de particiones

Nota: Una vez configuradas las particiones primarias, se configuran los volúmenes lógicos que se muestran en la Tabla 2.3, explicados en el capítulo 2 en el apartado 2.1.2.

Se elige la opción “Configurar el Gestor de Volúmenes Lógicos” mostrado en la Figura A.57, con ello se pregunta si se desean guardar los cambios al disco. Se elige la opción “Si”. (véase Figura A.58)

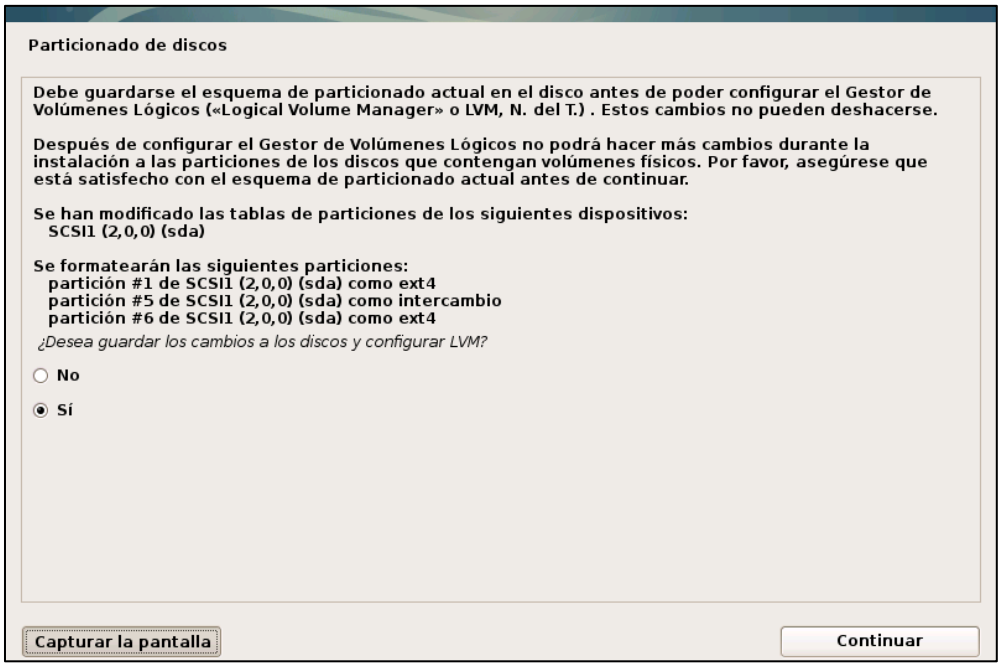


Figura A.58 Guardar los cambios al disco

Lo primero que se debe hacer es crear un grupo de volúmenes, el cual contendrá todos los volúmenes lógicos que se van a crear posteriormente. (véase Figura A.59)

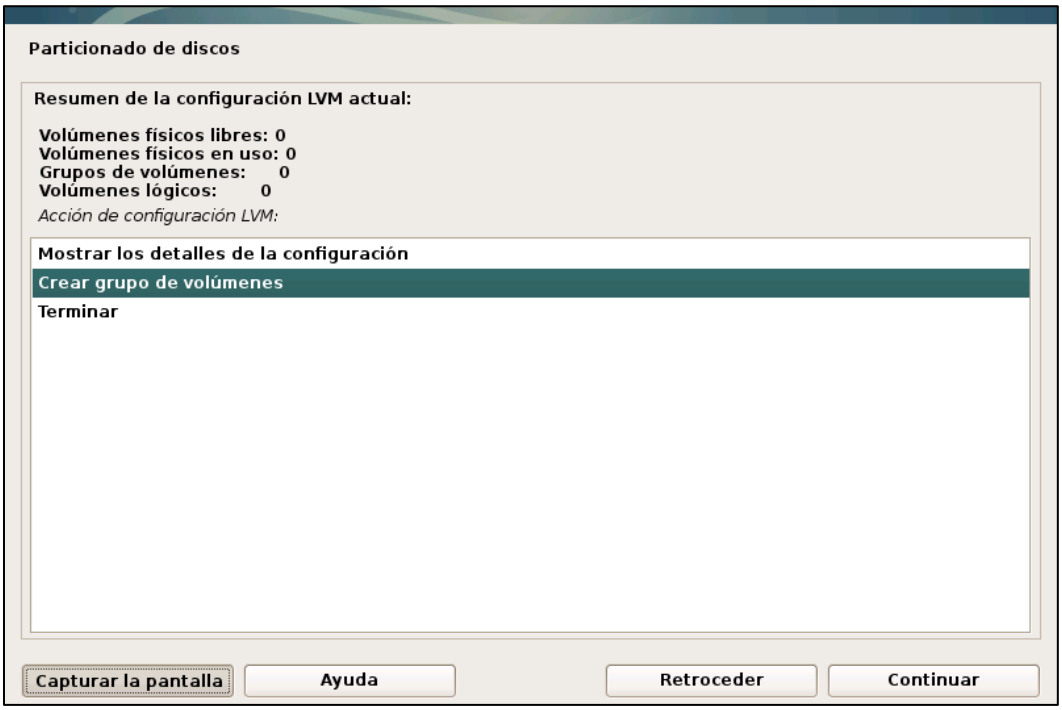


Figura A.59 Crear grupo de volúmenes

Se indica el nombre del grupo de volúmenes a consideración del administrador y se presiona continuar. (véase Figura A.60)

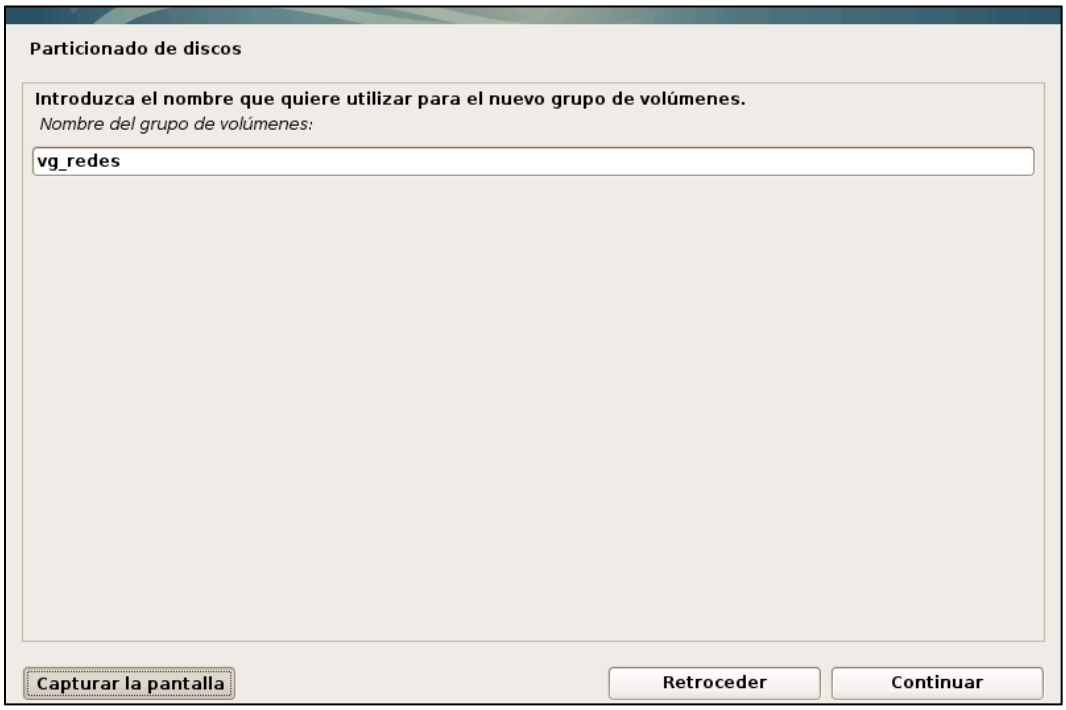


Figura A.60 Nombre del grupo de volúmenes

Se selecciona uno de las particiones para alojar al grupo de volúmenes, en este caso se elige el espacio libre como se muestra en la Figura A.61 y se presiona Continuar.

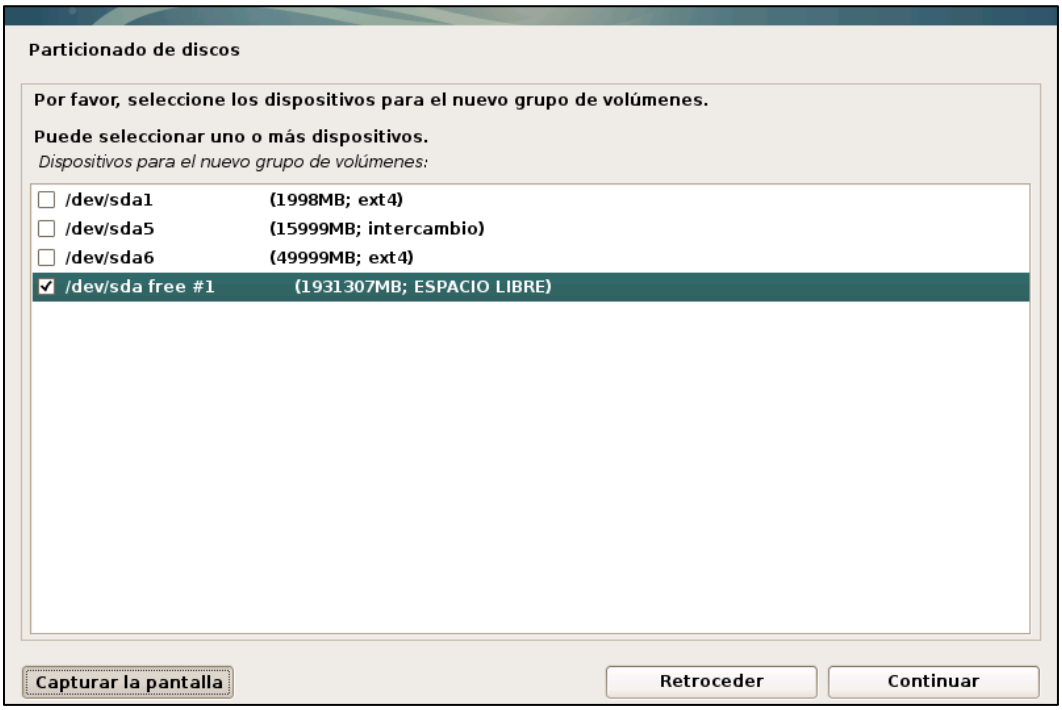


Figura A.61 Dispositivo para el grupo de volúmenes

Lo siguiente es confirmar que se desean guardar los cambios al disco para empezar a configurar los Volúmenes Lógicos. (véase Figura A.62)

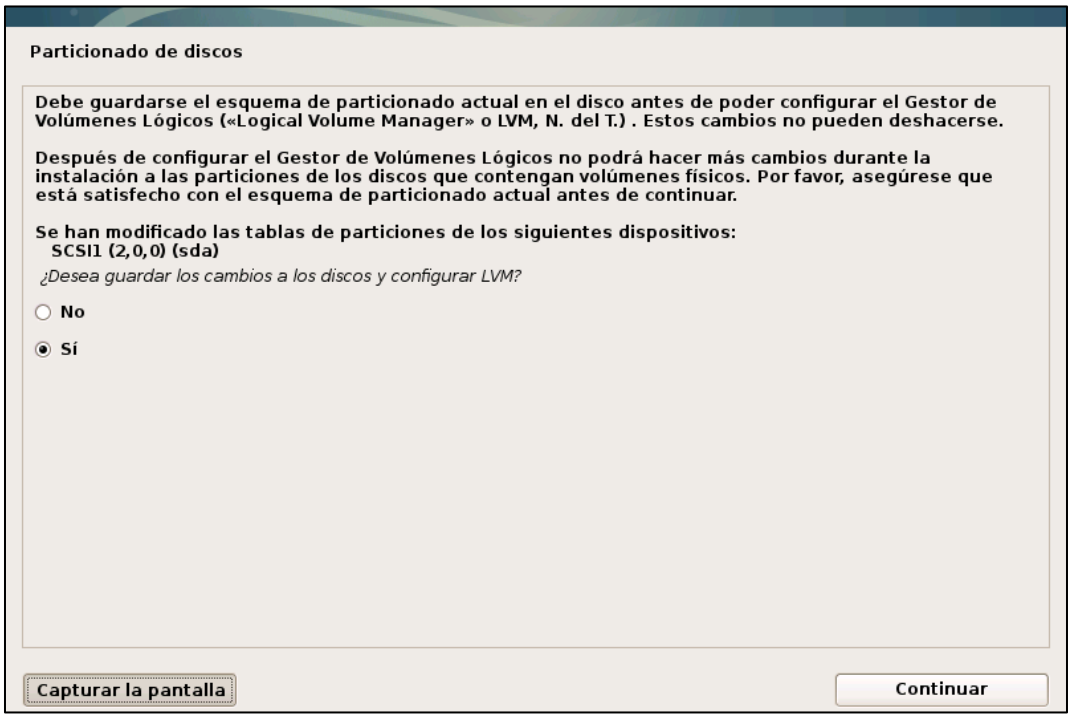


Figura A.62 Guardar cambios al disco

A continuación, se comienzan a crear Volúmenes Lógicos, se selecciona la opción "Crear un volumen lógico" y se presiona continuar. (véase Figura A.63)

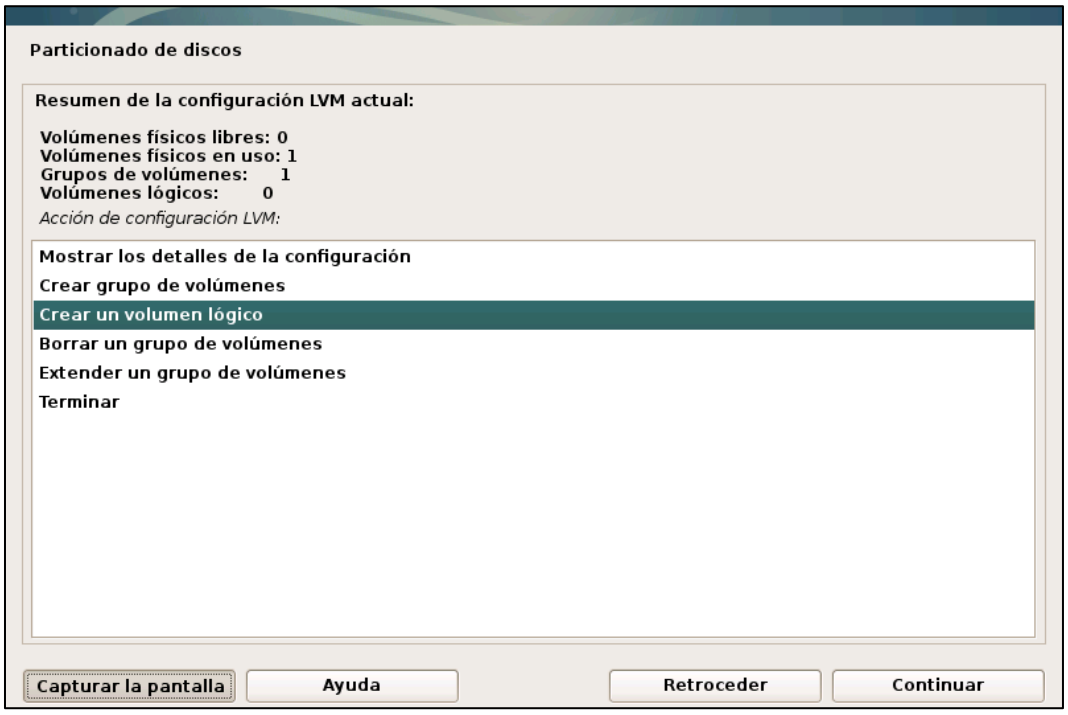


Figura A.63 Crear un volumen lógico

Se selecciona el grupo de volúmenes que se ha creado con anterioridad para que pertenezcan los volúmenes lógicos. (véase Figura A.64)

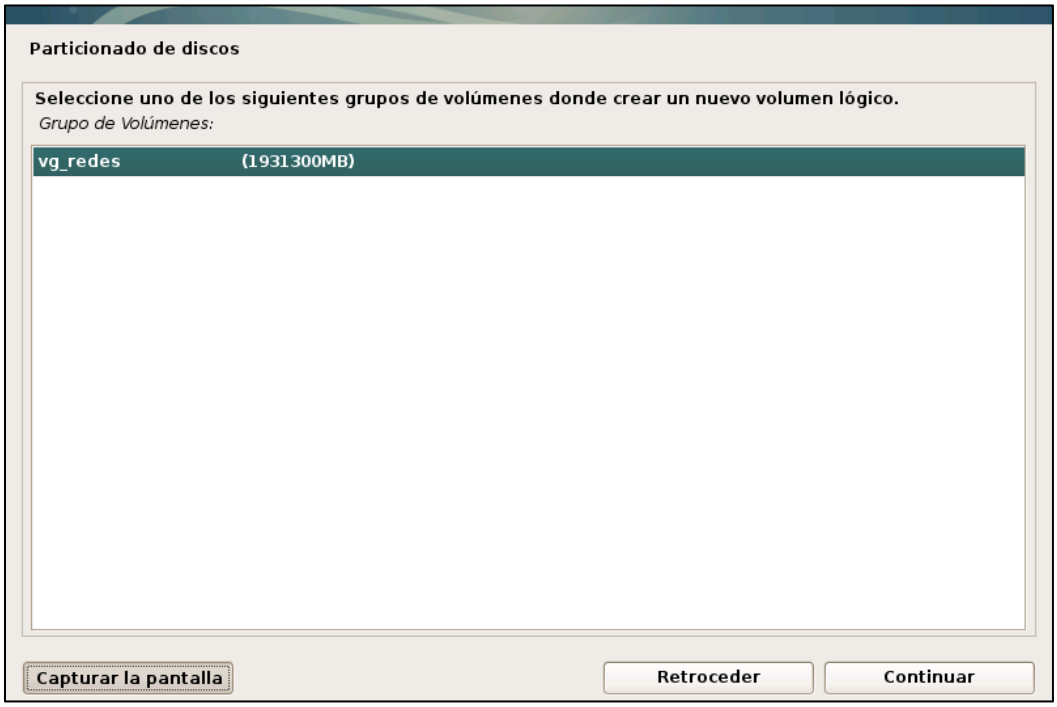


Figura A.64 Seleccionar grupo de volúmenes

Se introduce el nombre del volumen lógico, el primero que se va a crear es el correspondiente a /tmp. (véase Figura A.65) La nomenclatura es a consideración del administrador.

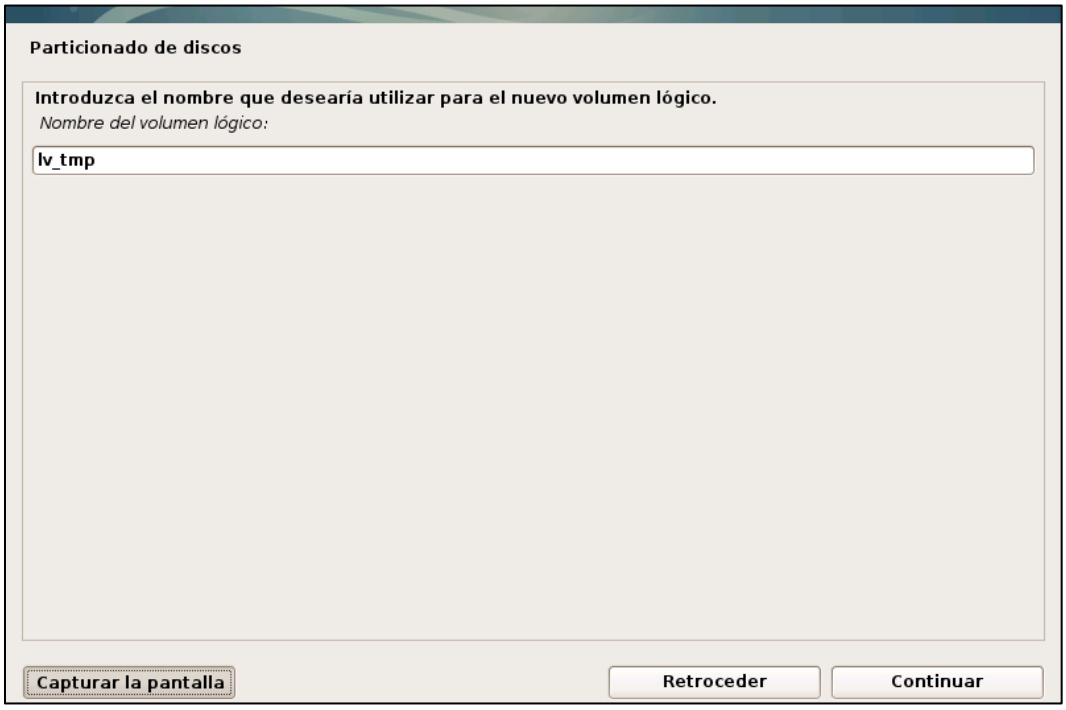


Figura A.65 Nombre del volumen lógico

Se indica el tamaño del volumen lógico. (véase Figura A.66)

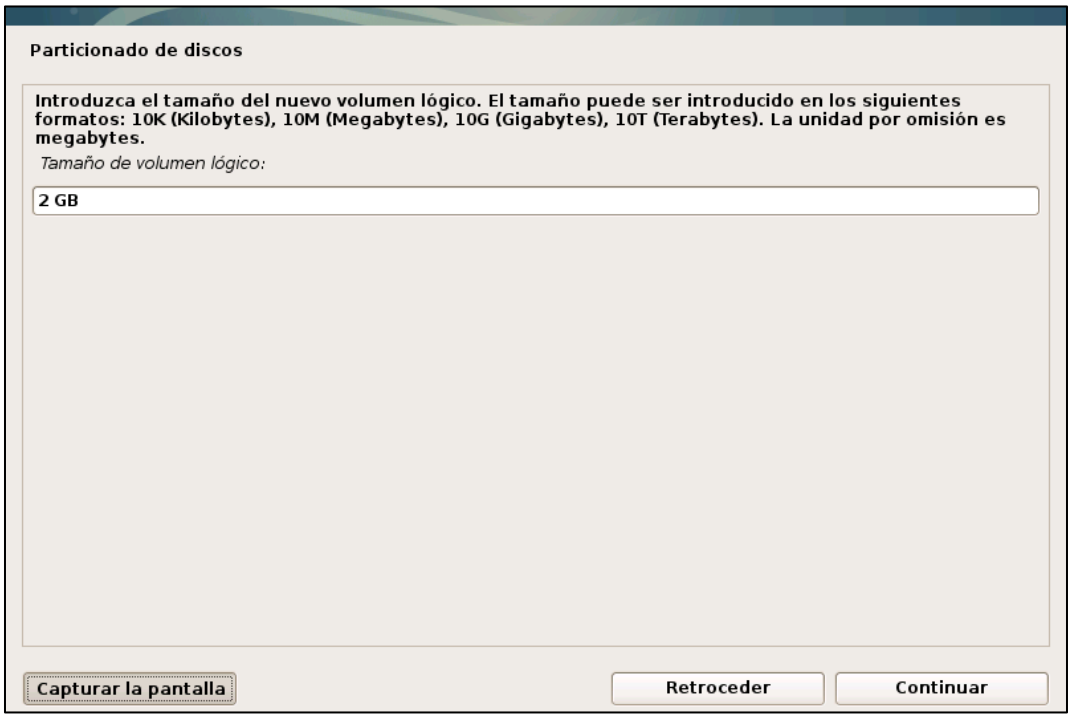


Figura A.66 Tamaño del volumen lógico

Se repiten los pasos con los que se creó el volumen lógico, para crear los volúmenes que se muestran en la Tabla A.5. Una vez que se han creado todos, se elige la opción "Terminar" y se presiona continuar como en la Figura A.67.

Tabla A.5 Nombre de los volúmenes lógicos

Nombre	Tamaño
lv_tmp	2 GB
lv_usr	50 GB
lv_var	100 GB
lv_home	100 GB
lv_varwww	500 GB

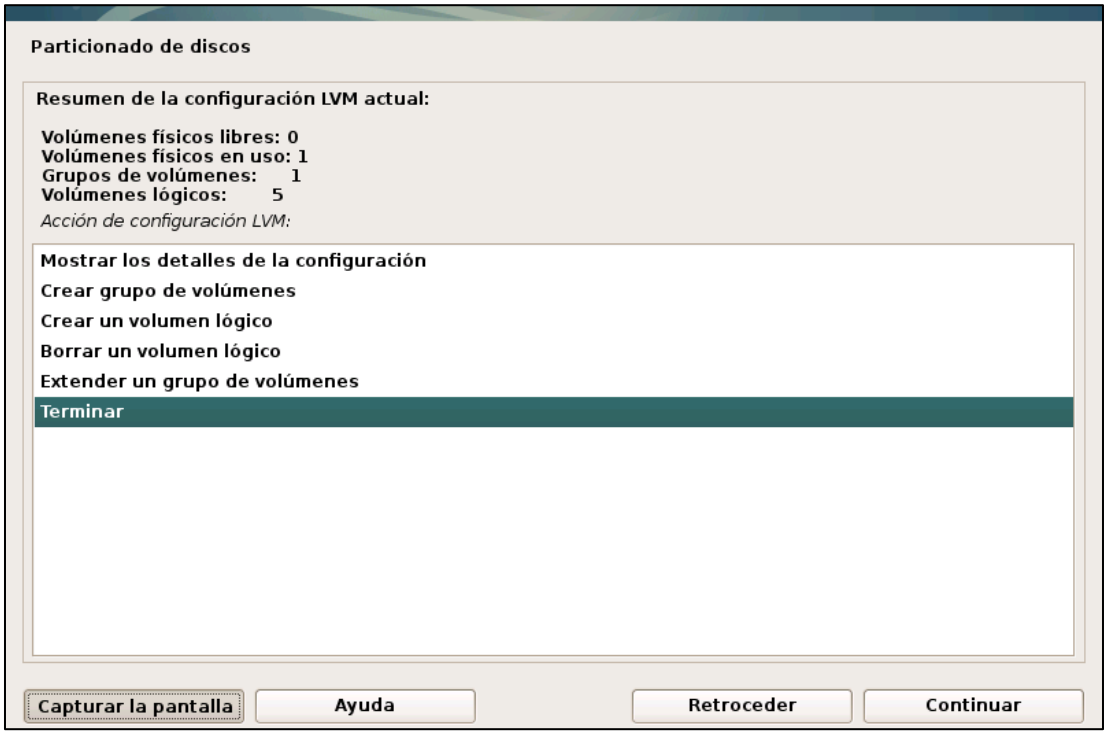


Figura A.67 Configuración LVM

Se han creado los volúmenes lógicos, pero aún no están asociados a un punto de montaje. Se selecciona el volumen con el nombre lv_tmp y se presiona continuar. (véase Figura A.68)

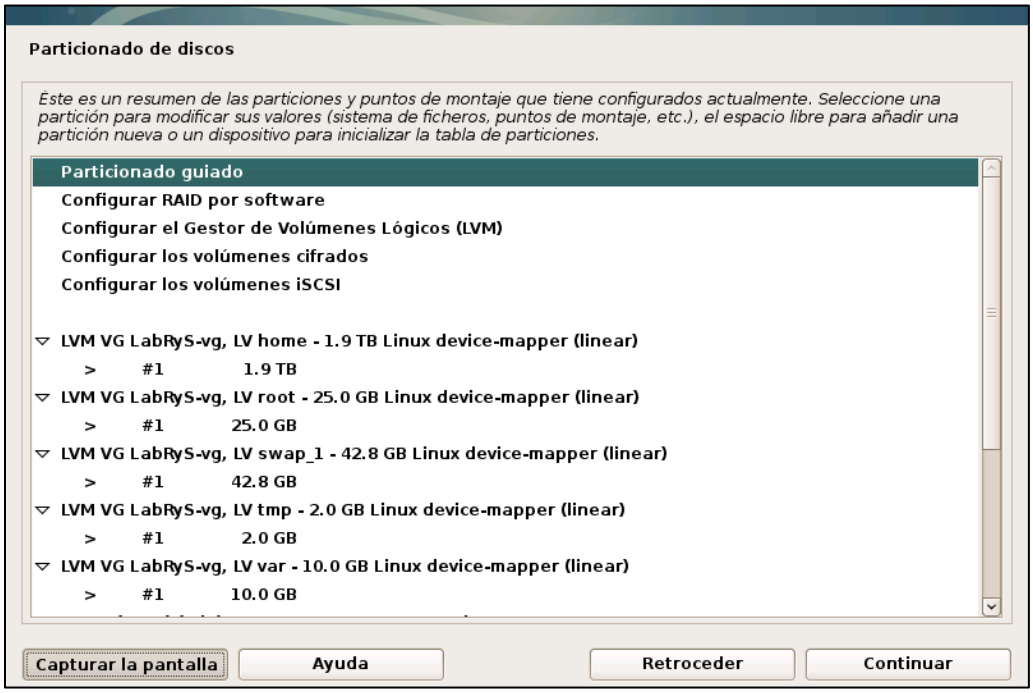


Figura A.68 Resumen de los volúmenes lógicos

Para poder utilizar el volumen lógico y guardar datos en él se elige la opción "Utilizar como" y se presiona continuar. (véase Figura A.69)

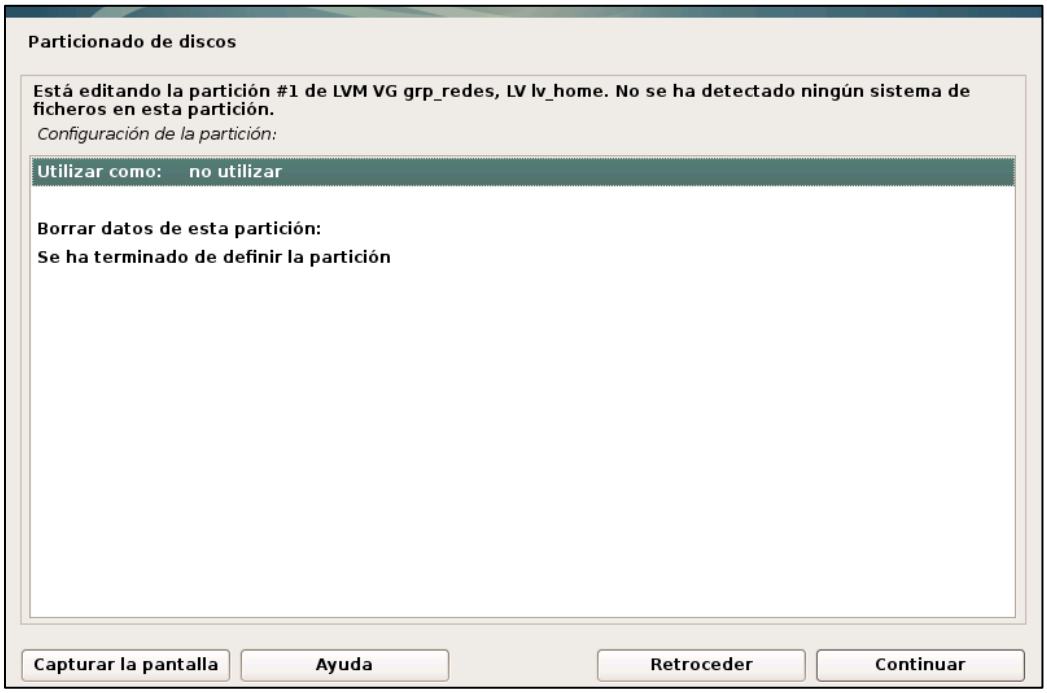


Figura A.69 Configuración de la partición

Se elige utilizar como un sistema de ficheros ext4, ya que es el sistema de archivos idóneo para un servidor. (véase Figura A.70)

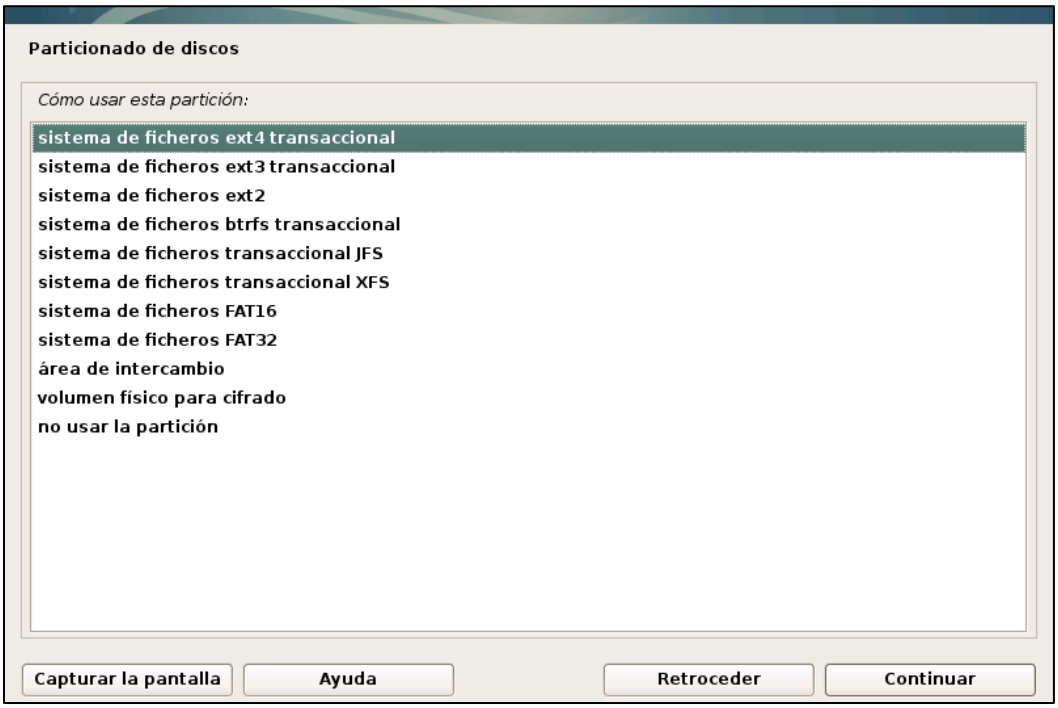


Figura A.70 Cómo usar la partición

Después de elegir cómo se utiliza la partición, se selecciona el punto de montaje y se presiona continuar. (véase Figura A.71)

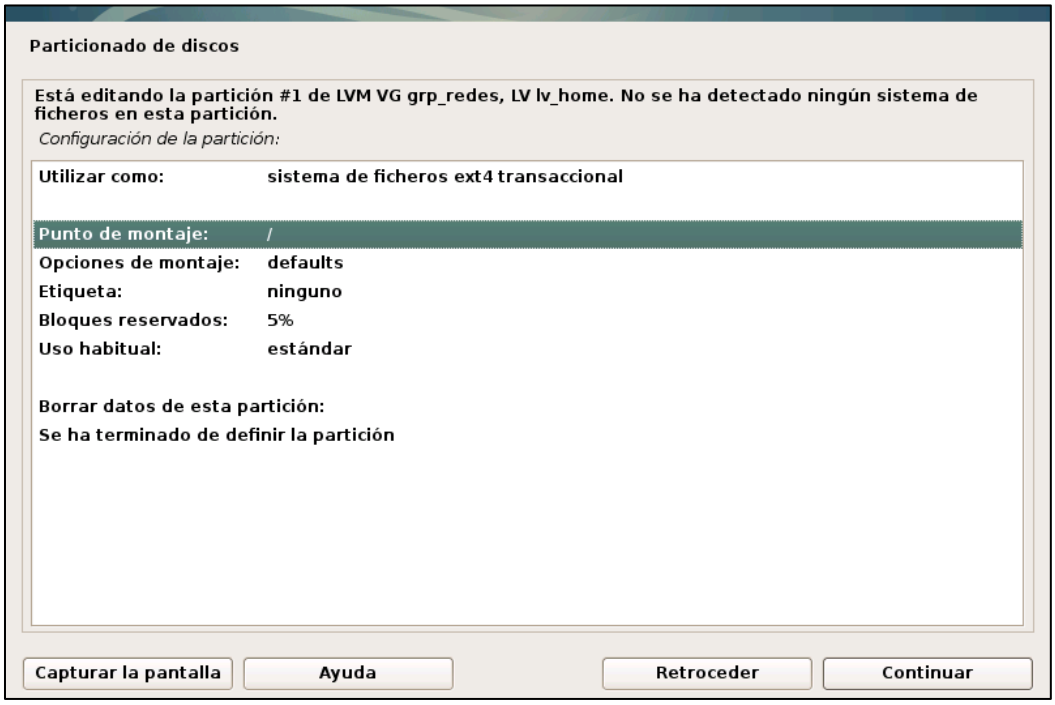


Figura A.71 Configuración de la partición

Se elige de la lista el punto de montaje, para este caso es /tmp. (véase Figura A.72)

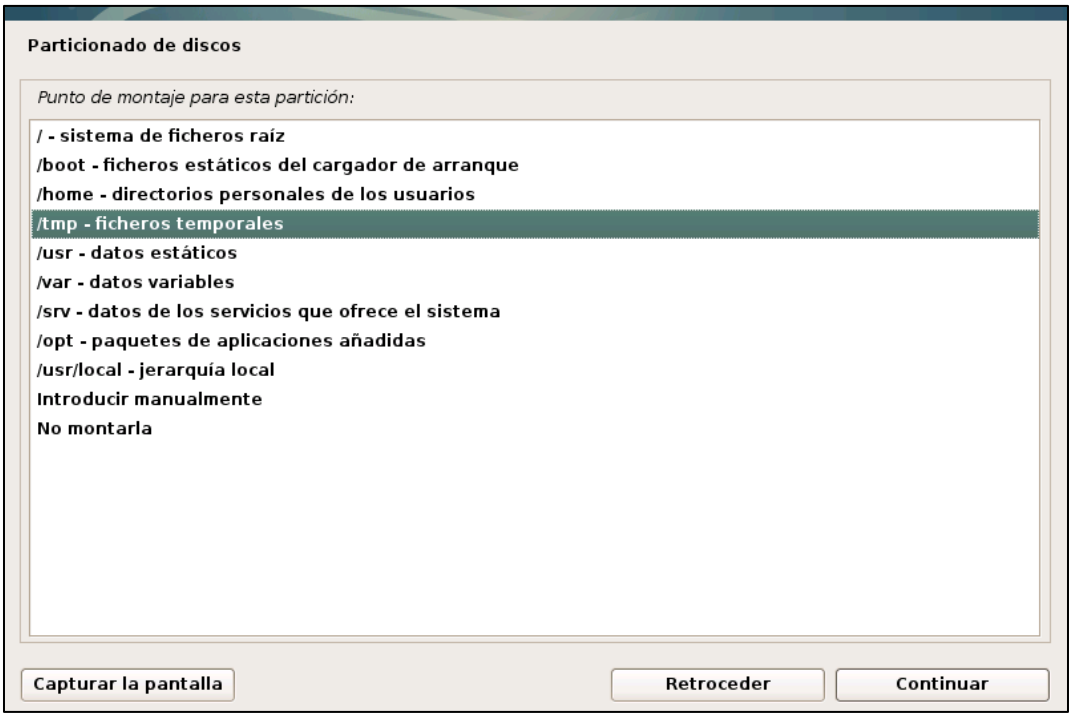


Figura A.72 Punto de montaje para la partición

Al finalizar la configuración, elegir terminar de definir la partición y presionar continuar. (véase Figura A.73)

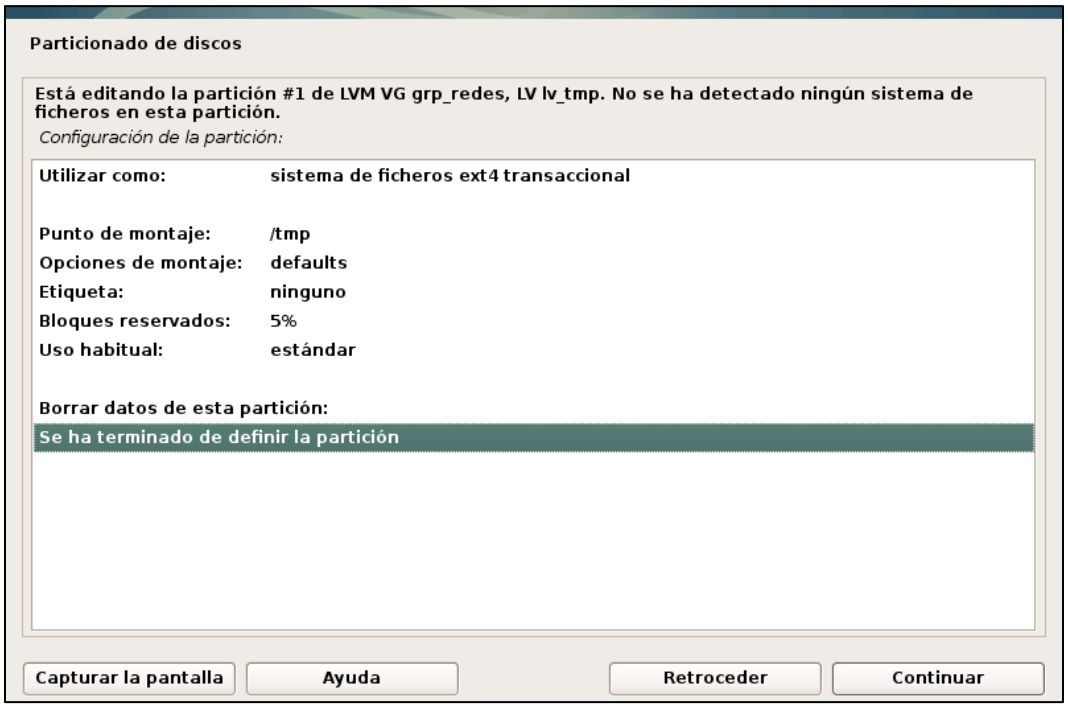


Figura A.73 Configuración de la partición

Se elige el punto de montaje de cada uno de los volúmenes lógicos, según la Tabla A.6. Una vez realizado, elegir la opción Finalizar el particionado como se muestra en la Figura A.74.

Tabla A.6 Punto de montaje de los volúmenes lógicos

Nombre	Tamaño	Punto de montaje
lv_tmp	2 GB	/tmp
lv_usr	50 GB	/usr
lv_var	100 GB	/var
lv_home	100 GB	/home
lv_varwww	500 GB	/var/www

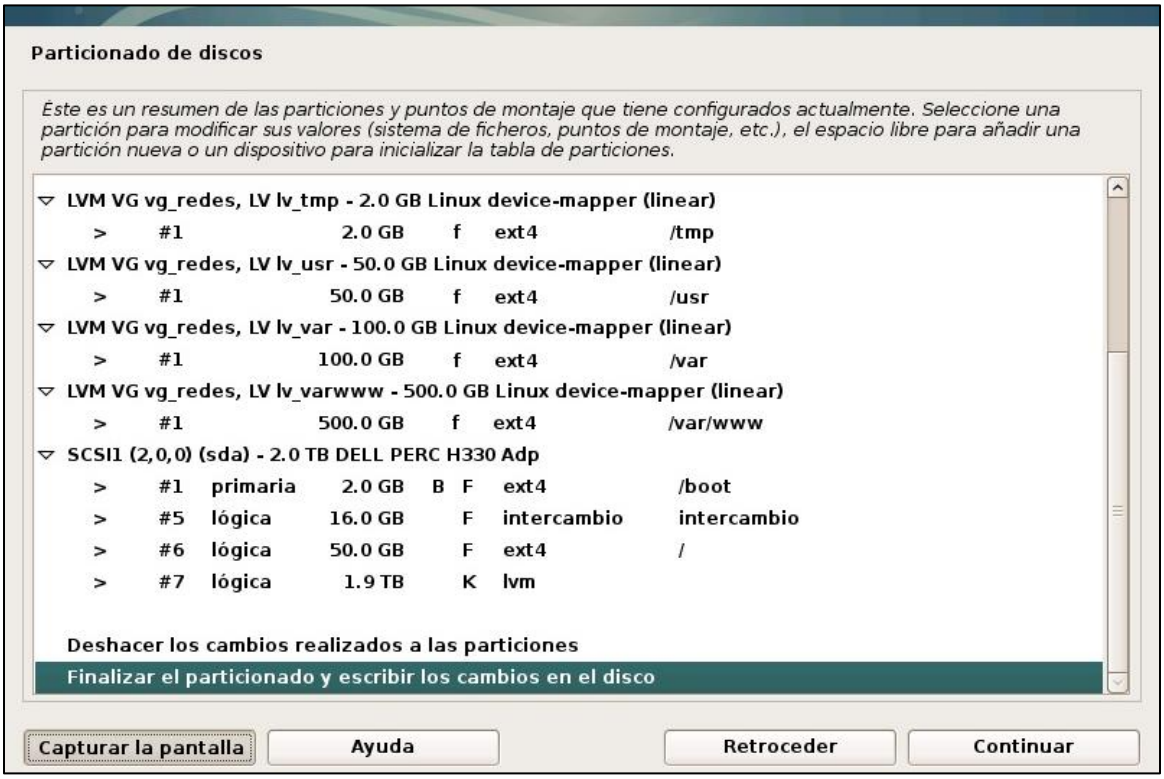


Figura A.74 Finalizar el particionado

Se muestra un resumen de los volúmenes físicos creados, se presiona continuar y se comienzan a hacer los cambios en el disco. (véase Figura A.75)

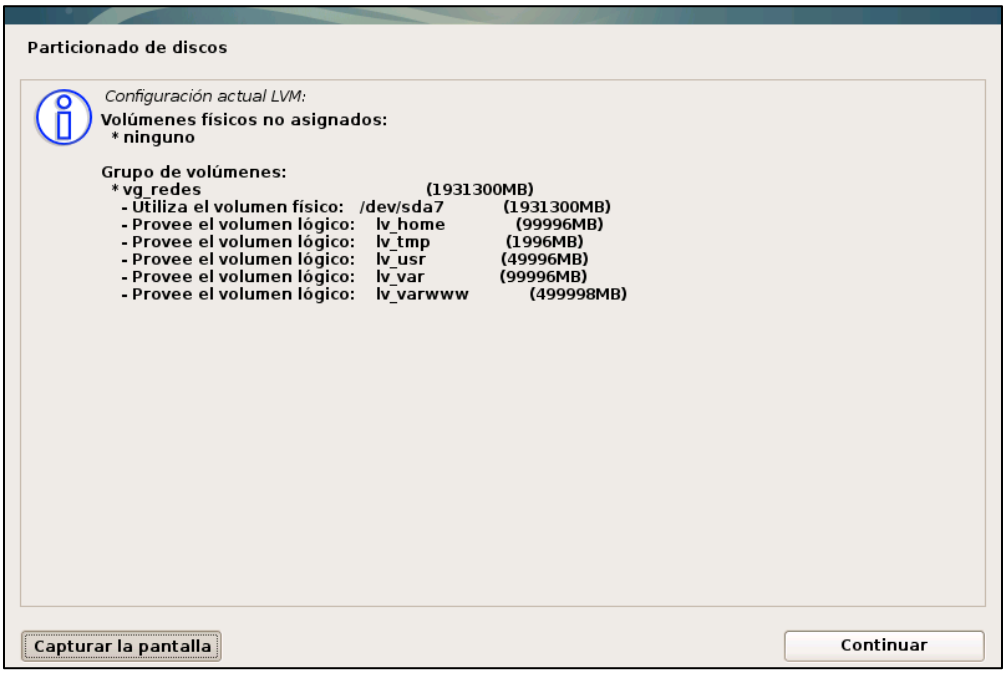


Figura A.75 Configuración actual LVM

Para configurar el Gestor de Paquetes, se debe indicar la opción Si y se presiona Continuar. (véase Figura A.76)

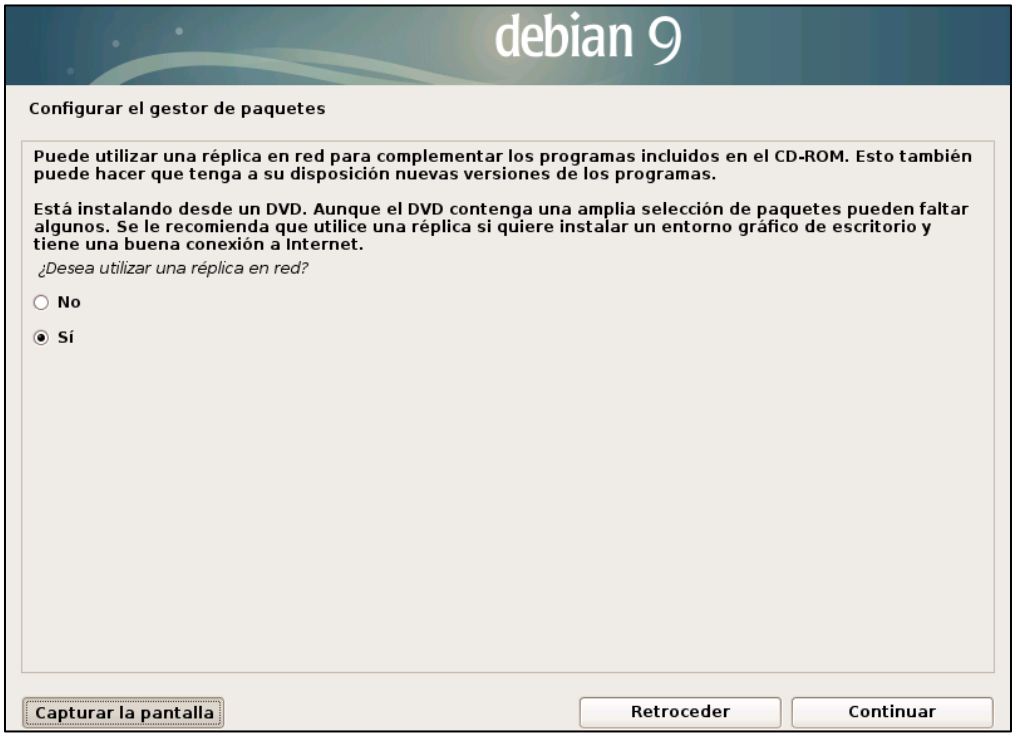


Figura A.76 Configuración de gestor de paquetes

Lo siguiente es seleccionar la ubicación geográfica para descargar los paquetes de software. (véase Figura A.77)

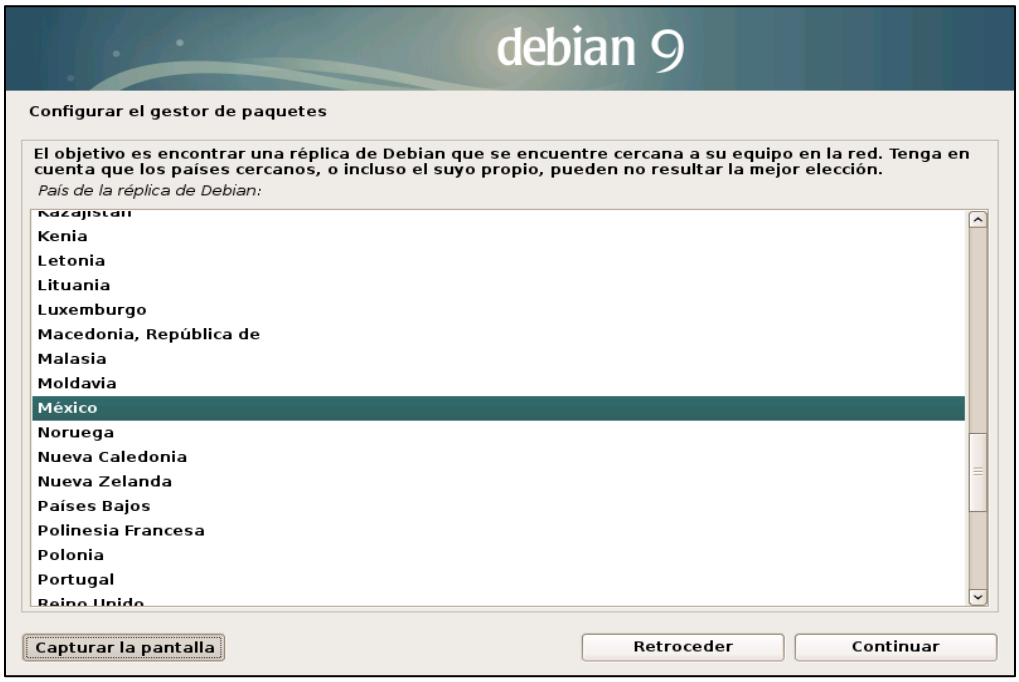


Figura A.77 Seleccionar ubicación geográfica

Una vez seleccionado el país, se escoge el servidor del cual se obtienen los paquetes, se elige el servidor oficial de Debian, como se muestra en la Figura A.78.

Figura A.78 Selección de servidor

Se debe indicar el proxy para acceder a la red. El Laboratorio no hace uso de proxy, por lo que se deja en blanco y **se** continúa con el proceso de instalación. (véase Figura A.79)

Figura A.79 Selección de proxy

En la siguiente pantalla se elige que no se desea participar en el envío de estadísticas de uso de paquetes. (véase Figura A.80)

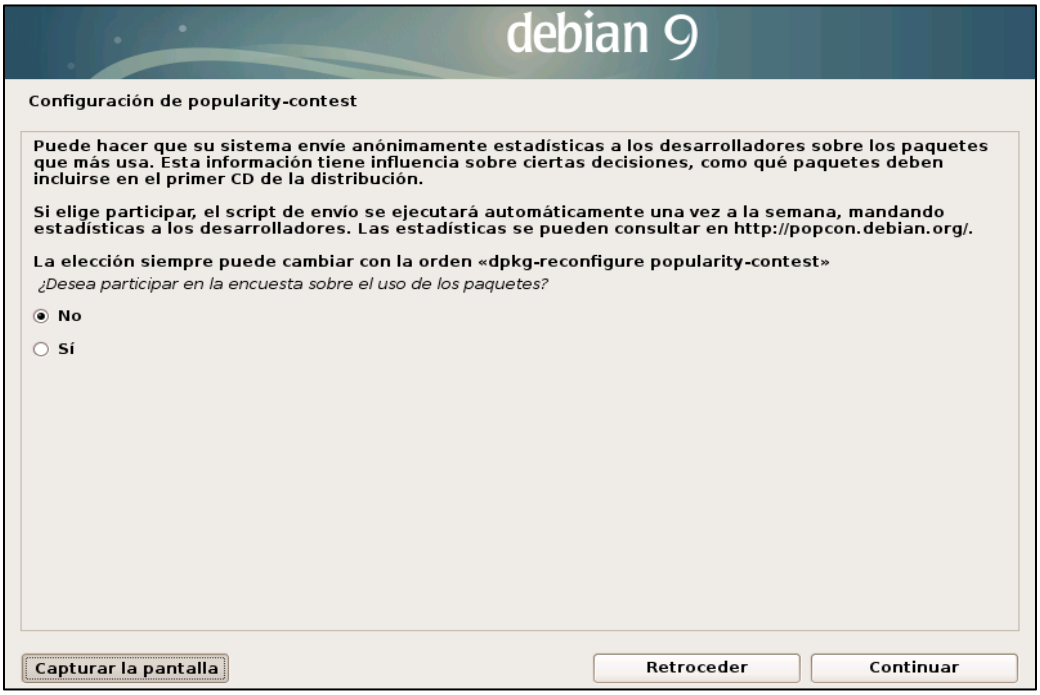


Figura A.80 Selección de participación de paquetes

Se seleccionan los paquetes a instalar, entre las opciones están distintos entornos: de escritorio, paquetería y herramientas para ser un servidor web. Para este caso se seleccionan los que se muestran en la Figura A.81. Una vez seleccionados se presiona Continuar.

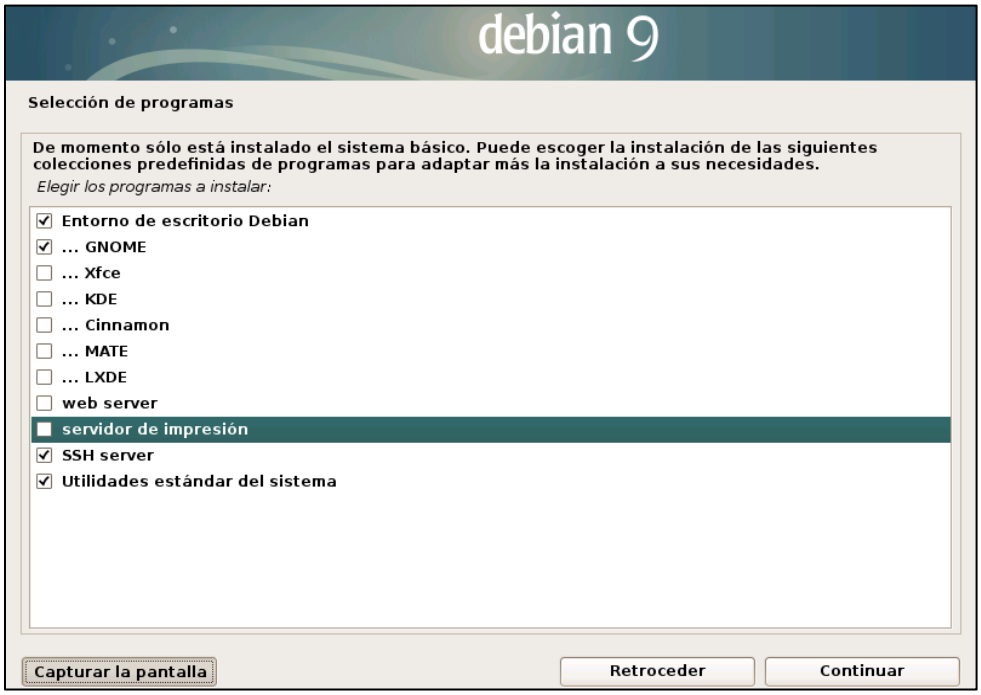


Figura A.81 Selección de paquetes

Se indica que el cargador de arranque (GRUB) se instala en el registro principal, eligiendo la opción Si y presionando Continuar (véase Figura A.82)

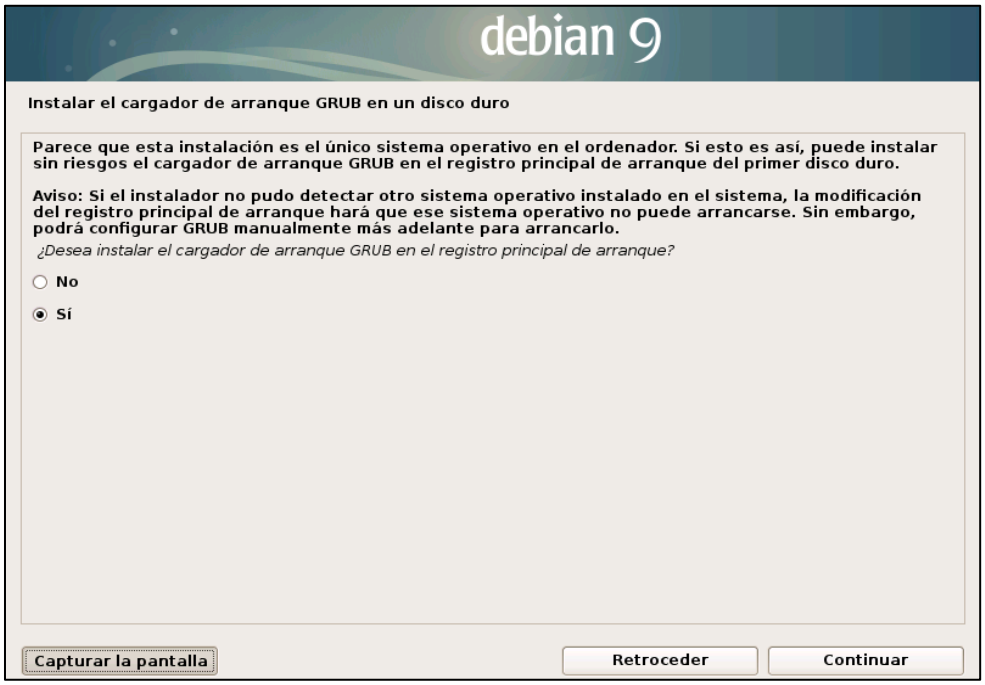


Figura A.82 Selección de cargador de arranque (GRUB)

Para terminar la instalación, si es que hay más de un disco, se debe indicar en cual se instala el cargador de arranque. (véase Figura A.83).

Figura A.83 Selección de cargador de arranque (GRUB)

La instalación ha concluido, solamente se presiona continuar y se reinicia el equipo con Debian 9 ya instalado. (véase Figura A.84) No olvidar retirar el medio de instalación.

Figura A.84 Instalación terminada

4. Instalación de los servicios

Ya que se tiene instalado y configurado el sistema operativo, se procederán a instalar las aplicaciones necesarias para tener un servidor web por medio de la consola de comandos. Para ello se accede a una terminal como usuario root para poder ejecutar los comandos mostrados.

4.1. Actualización del sistema

Antes de actualizar, se hace una lista de las aplicaciones que requieran una actualización y sus versiones, con el comando

```
apt-get update
```

como se muestra en la Figura A.85, cabe destacar que el comando no instala o actualiza.

```
root@DebianLVM:~# apt-get update
Ign:1 http://ftp.mx.debian.org/debian stretch InRelease
Obj:2 http://ftp.mx.debian.org/debian stretch-updates InRelease
Obj:3 http://ftp.mx.debian.org/debian stretch Release
Des:4 http://security.debian.org/debian-security stretch/updates InRe
lease [94.3 kB]
Descargados 94.3 kB en 0s (207 kB/s)
Leyendo lista de paquetes... Hecho
root@DebianLVM:~#
```

Figura A.85 Actualización de repositorios

Una vez que el comando anterior ha descargado la lista de software disponible y la versión en que se encuentra, se actualizan dichas aplicaciones usando el comando

```
apt-get upgrade
```

como se muestra en la Figura A.86, con esto se instalan las nuevas versiones respetando la configuración del software.

```
root@DebianLVM:~# apt-get upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
```

Figura A.86 Actualización de aplicaciones

En el caso del sistema operativo, Debian en su página oficial *https://www.debian.org/* publica cuando ha liberado una nueva actualización o una nueva versión estable de su sistema. Se utiliza el comando

```
apt-get dist-upgrade
```

como se muestra en la Figura A.87

```
root@DebianLVM:~# apt-get dist-upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
```

Figura A.87 Actualización de versión

4.2. Instalación del Servidor web

Se instalará Apache como aplicación de servidor web, para lo cual es necesario instalarlo con el comando apt-get.

```
apt-get install -y apache2 libapache2-mod-php7.0
```

Se inicia el servicio web y se habilita para que esté disponible cada vez que se inicia el sistema.

```
systemctl start apache2
systemctl enable apache2
```

Una vez instalado se puede acceder al servidor por medio de un navegador y debe mostrar una página como en la Figura A.88. Si se muestra, el servicio web ya está funcionando correctamente.

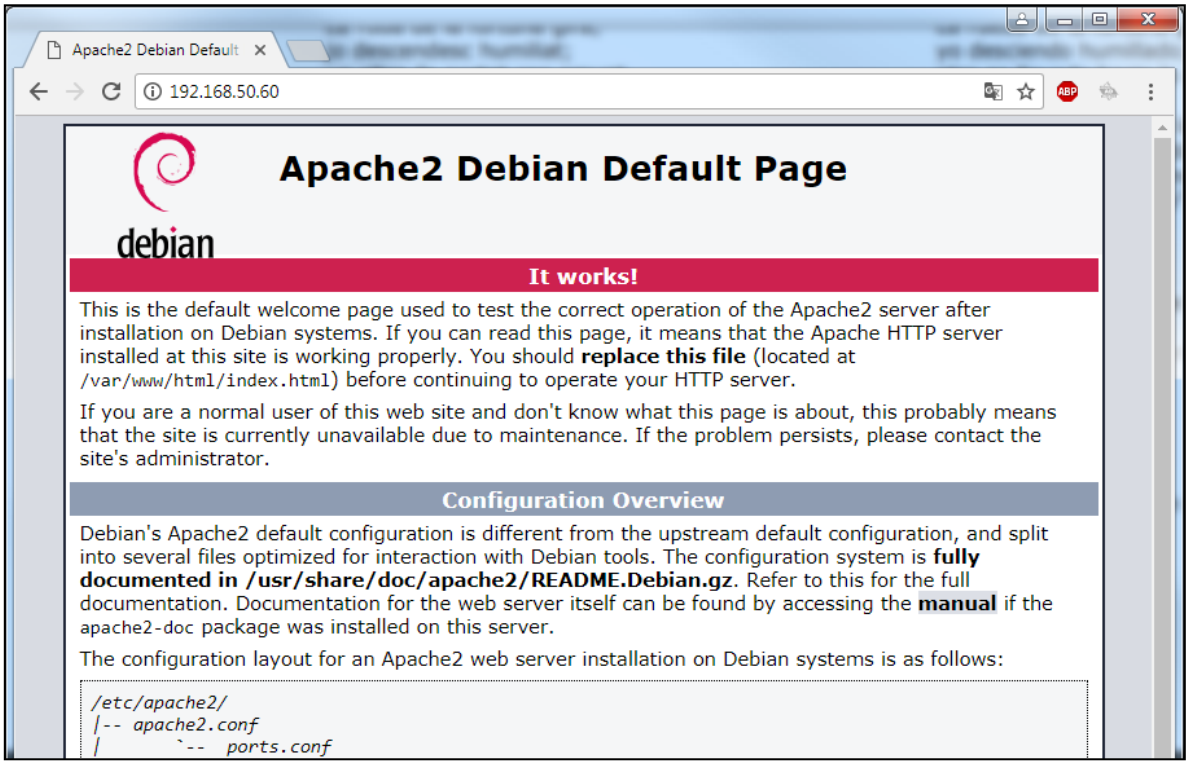


Figura A.88 Página inicial Apache

Los archivos que se muestran vía web serán los que se encuentren en el directorio */var/www/html/*

4.3. Instalación de MariaDB

Se instalará el gestor de base de datos MariaDB con el comando *apt-get*.

```
apt-get install -y mariadb-server
```

Se inicia el servicio de base de datos y se habilita para que se inicie automáticamente.

```
systemctl start mariadb
systemctl enable mariadb
```

4.4. Instalación de PHP

Se instala PHP en la versión 7.3 que es la más reciente, con el comando *apt-get*. Y se instalan en un solo paso las librerías requeridas, como se muestra en la Figura A.89

```
root@DebianLVM:~# apt-get install php7.3 libapache2-mod-php7.3 php7.3-cl
i php7.3-mysql php7.3-gd php7.3-imagick php7.3-recode php7.3-tidy php7.3
-xmlrpc
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Nota, seleccionando «php-imagick» en lugar de «php7.3-imagick»
Se instalarán los siguientes paquetes adicionales:
  libargon2-1 libpcre2-8-0 librecode0 libsodium23 libtidy5deb1
  libxmlrpc-epi0 php-common php7.3-common php7.3-json php7.3-opcache
  php7.3-readline ttf-dejavu-core
Paquetes sugeridos:
  php-pear
Se instalarán los siguientes paquetes NUEVOS:
  libapache2-mod-php7.3 libargon2-1 librecode0 libsodium23
  libtidy5deb1 libxmlrpc-epi0 php-common php-imagick php7.3 php7.3-cli
  php7.3-common php7.3-gd php7.3-json php7.3-mysql php7.3-opcache
  php7.3-readline php7.3-recode php7.3-tidy php7.3-xmlrpc
  ttf-dejavu-core
```

Figura A.89 Instalación de PHP

Una vez instalado PHP, se edita el archivo de configuración */etc/php/7.0/apache2/php.ini* y los siguientes valores, quedando.

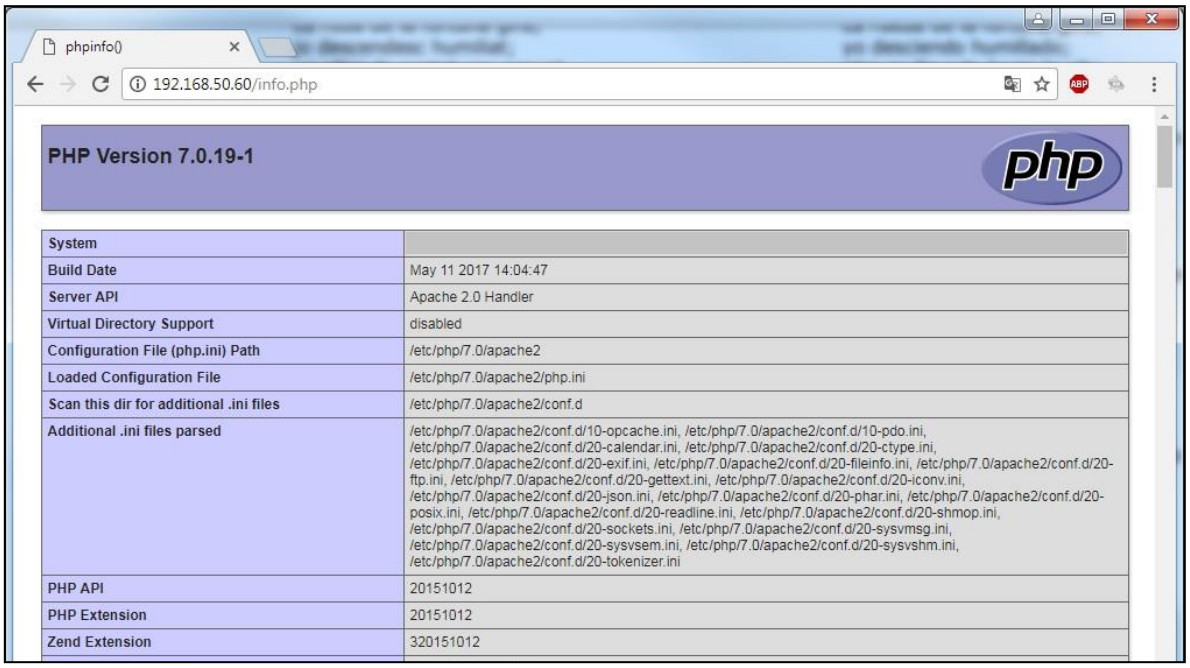
```
memory_limit = 256M
upload_max_filesize = 32M
post_max_size = 32M
```

Una vez hecho esto se crea el archivo *info.php* en el directorio */var/www/html*, el archivo quedará como se muestra en la Figura A.90.

```
<?php phpinfo(); ?>
~
~
```

Figura A.90 Archivo info.php

En un navegador de introduce la IP o el nombre del servidor y el nombre del archivo *info.php*. Si se muestra una página similar a la que aparece en la Figura A.91, el servicio de PHP funciona de manera correcta.



System	
Build Date	May 11 2017 14:04:47
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012

Figura A.91 *info.php* vista desde un navegador

Anexo B

Manual de hardening y administración del servidor web

Índice

1. Introducción

El presente manual explica, de forma detallada, las configuraciones posteriores a la instalación del sistema operativo, así como funciones clave para la administración del servidor.

El manual se encuentra dividido en secciones que detallan los puntos antes mencionados.

La primera sección, Introducción, es una breve explicación de la importancia del servidor y del contenido del "Manual de configuración post-instalación y administración del servidor web".

En la segunda sección, Hardening del servidor, se indican las configuraciones realizadas para fortalecer la seguridad del servidor, explicadas en el capítulo 4 de este trabajo de tesis.

En la tercera sección, Interfaces de red, se muestran los comandos básicos para visualizar la información de las interfaces de red y manipularlas.

En la cuarta sección, Actualización del sistema, se presenta la importancia de actualizar periódicamente el sistema operativo y las aplicaciones instaladas, así como la forma de llevarlo a cabo.

En la quinta y última sección, Administración de particiones, se presenta la forma en que se puede aumentar o reducir el volumen de particiones en caso de que se requiera para administrar así el espacio del disco duro.

2. Hardening del servidor

2.1. Acceso al BIOS

En este punto se establece una contraseña para poder realizar cambios en la configuración del BIOS, explicado en el capítulo 3, en el punto 3.2.1.

Se enciende el servidor y cuando aparezca la pantalla que se muestra en la Figura B.1 se presiona F2 para entrar al sistema de configuración del BIOS.

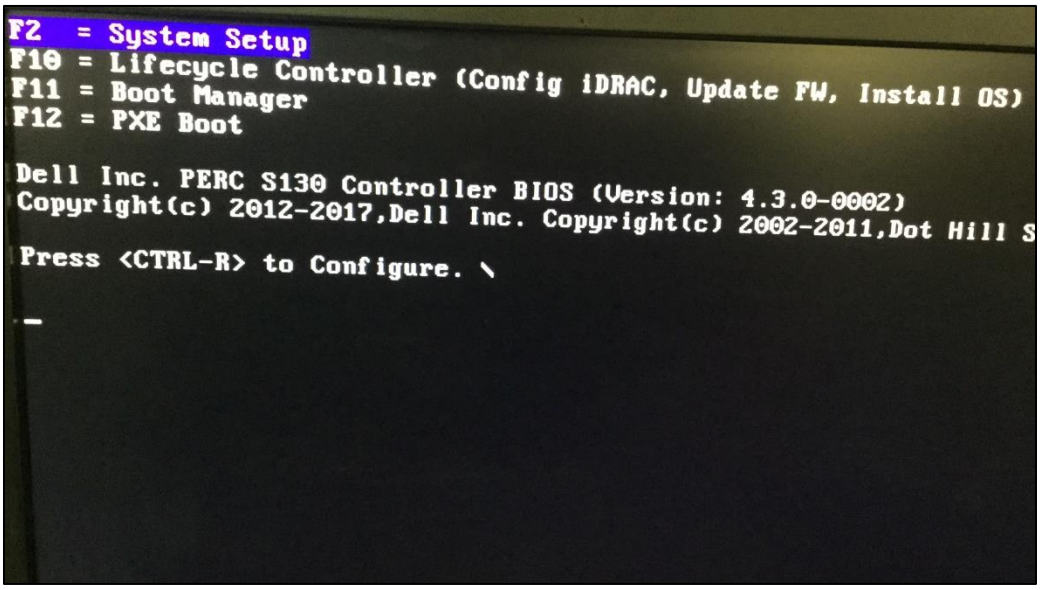


Figura B.1 Pantalla inicial

Al entrar al sistema de configuración del BIOS, aparece en pantalla menú principal que se muestra en la Figura B.2. Se da click en la opción System BIOS.

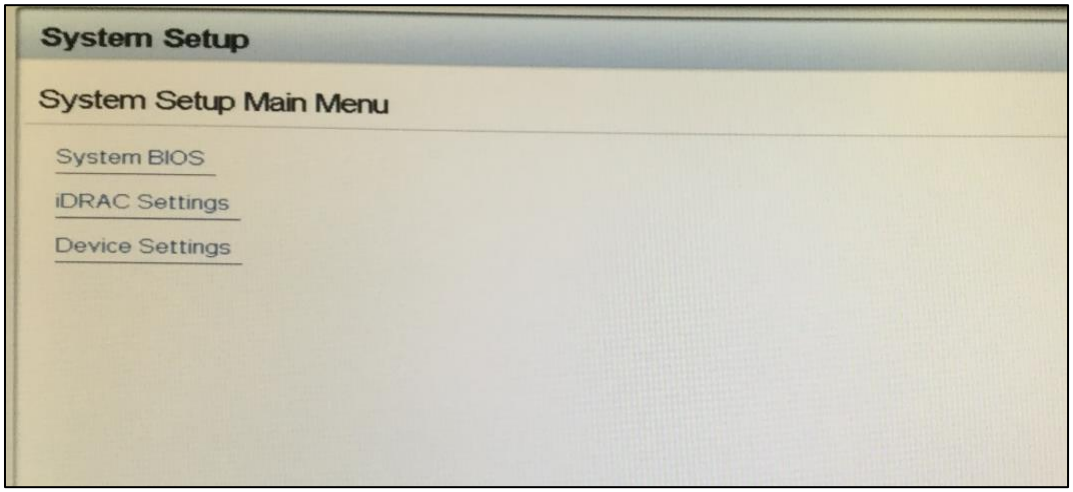


Figura B.2 Menú principal System Setup

En el menú System BIOS, se da click en la opción System Security, como se muestra en la Figura B.3.

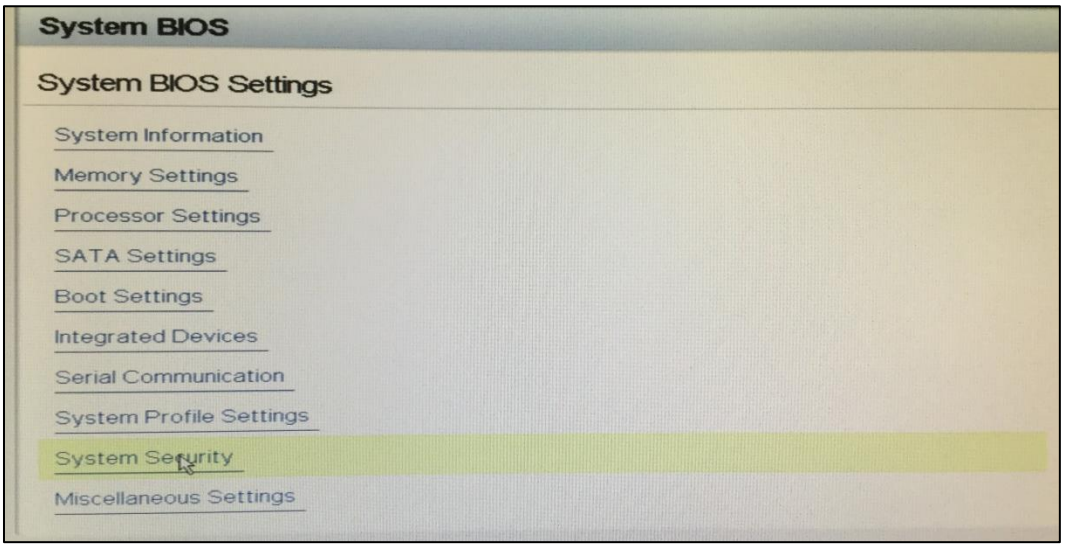


Figura B.3 Menú System BIOS

En las configuraciones de seguridad, se pueden establecer dos tipos de contraseñas.

- System Password: Es la contraseña que debe ser ingresada cada que se prende el servidor para permitir que el sistema operativo arranque.
- Setup Password: Es la contraseña que debe ser ingresada cuando se requiera hacer un cambio a la configuración del BIOS.

Para este caso, solamente se establece el Setup Password y las demás opciones se mantienen igual, quedando como se muestra en la Figura B.4. Una vez ingresada la contraseña, se despliega un cuadro de texto como el que se muestra en la Figura B.5, en el que se debe volver a ingresar la contraseña y al terminar se da click en el botón OK.

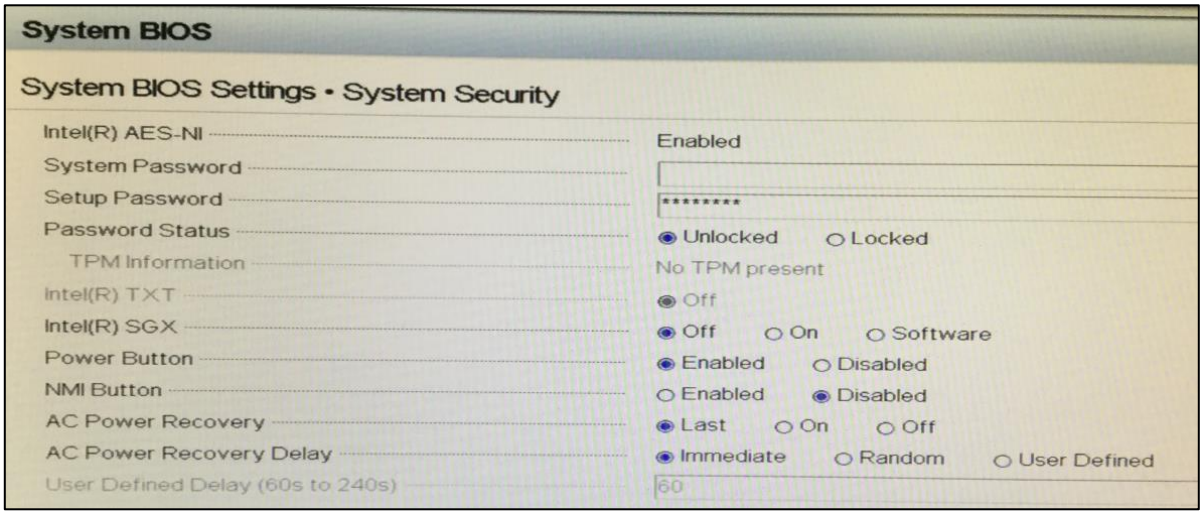


Figura B.4 System Security

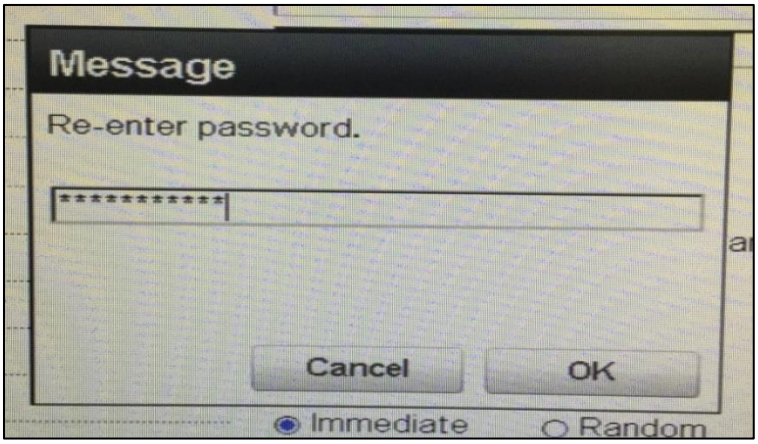


Figura B.5 Confirmación de contraseña

Para guardar los cambios, se debe salir del sistema de configuración del BIOS. Antes de salir se avisa que se han guardado los cambios exitosamente como se muestra en la Figura B.6 y se reinicia el sistema.

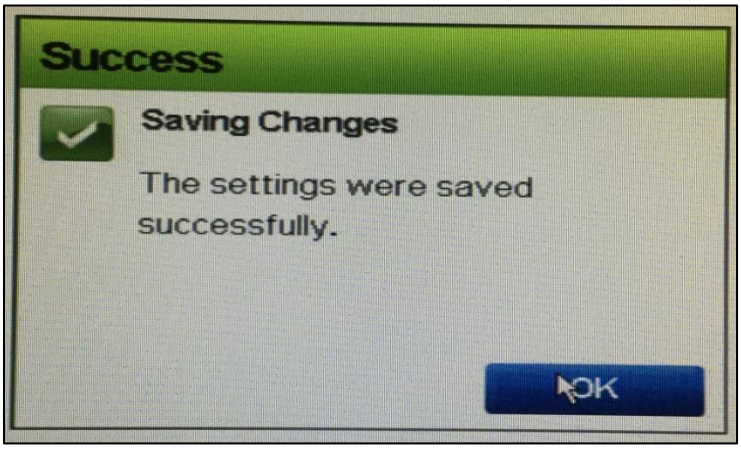


Figura B.6 Aviso de cambios guardados

Para corroborar que funcione la contraseña, se intenta acceder nuevamente al sistema de configuración del BIOS, para lo cual ahora se pide ingresar la contraseña como se muestra en la Figura B.7.

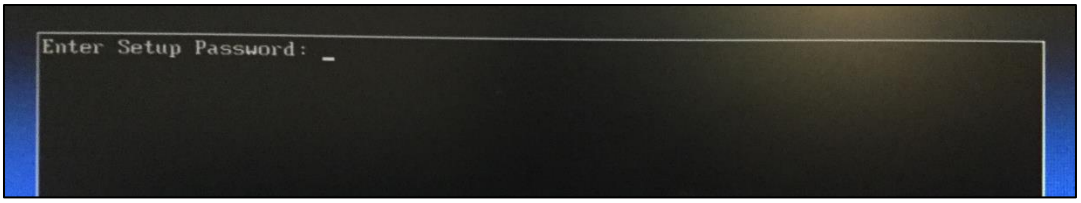


Figura B.7 Contraseña BIOS

Ahora se procede a quitar la opción de arranque por CD, para lo que entramos nuevamente al sistema de configuración del BIOS y ahora se elige la opción de Boot Settings, como se muestra en la Figura B.8.

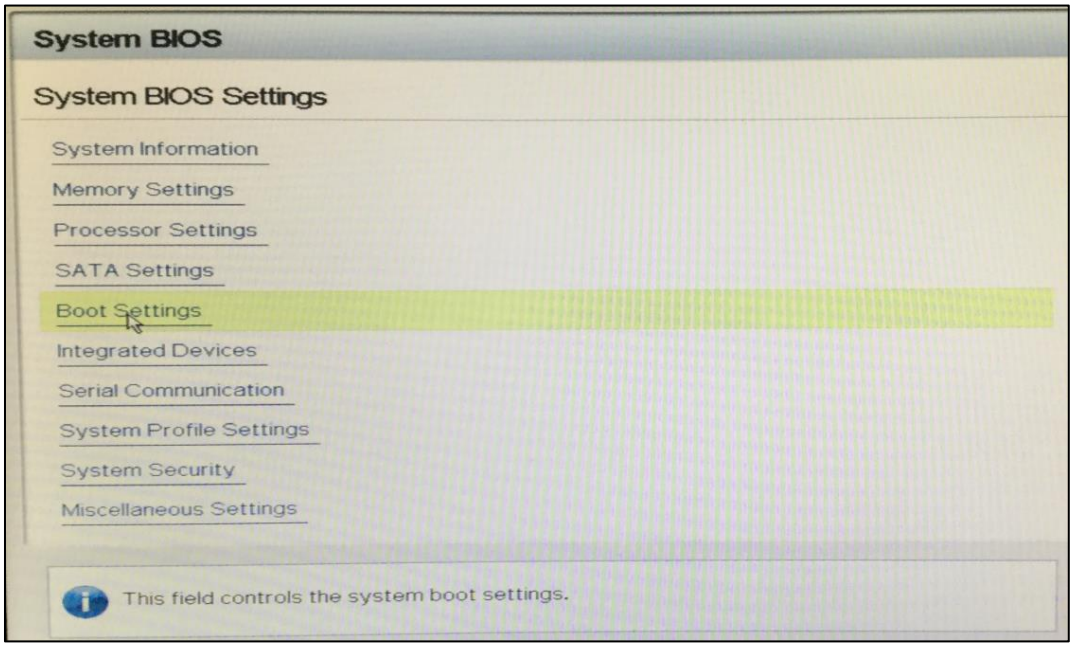


Figura B.8 Menú System BIOS

En el menú de Boot Settings se selecciona la opción BIOS Boot Settings. (véase Figura B.9)

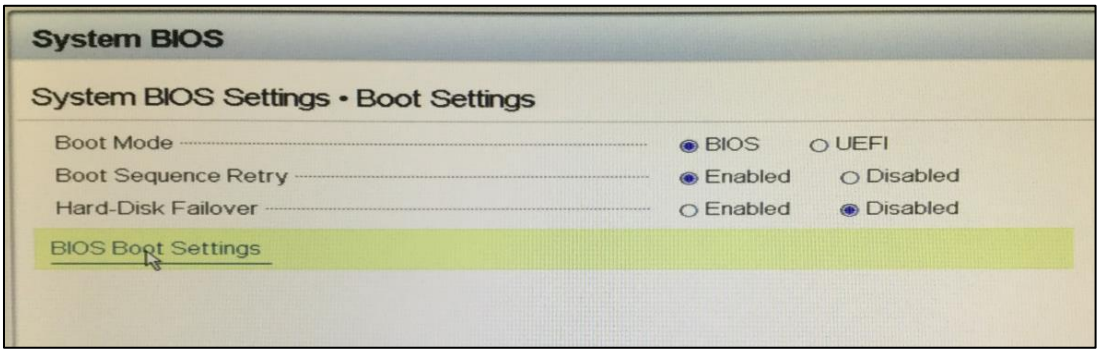


Figura B.9 Menú Boot Settings

Se muestran los dispositivos de arranque, se debe dejar habilitada solamente la opción del disco duro, deshabilitando el resto como se muestra en la Figura B.10. Al finalizar, se debe salir del sistema de configuración del BIOS para guardar los cambios.

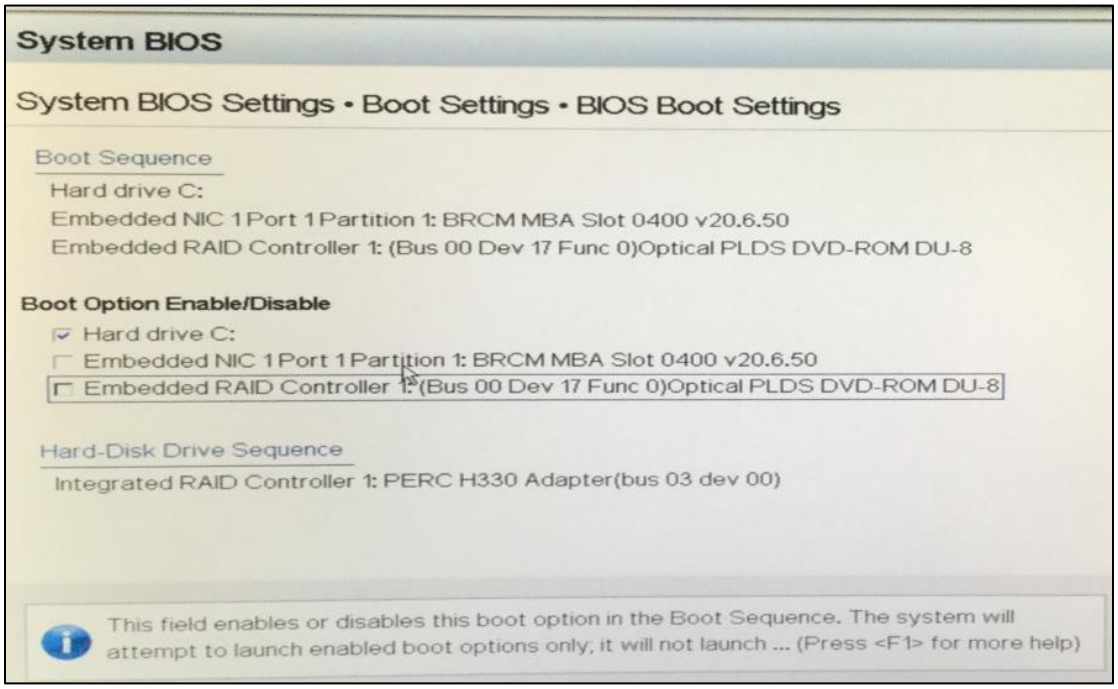


Figura B.10 Dispositivos de arranque

2.2. Colocar contraseña a GRUB

En este punto se establece una contraseña al gestor de arranque GRUB, explicado en el capítulo 3, en el punto 3.2.2.

Lo primero que se debe hacer es ingresar a una terminal como usuario root. Una vez como usuario root, se va a utilizar el comando:

```
grub-mkpasswd-pbkdf2
```

Con el comando se obtiene una contraseña encriptada en SHA512, al teclear el comando pide la contraseña y la confirmación de la misma contraseña, como se muestra en la Figura B.11. La parte resaltada es la que se va a ocupar en los pasos siguientes.

```
root@DebianLVM:~# grub-mkpasswd-pbkdf2
Introduzca la contraseña:
Reintroduzca la contraseña:
El hash PBKDF2 de su contraseña es grub.pbkdf2.sha512.10000.B65118BEE9B7EB6F873C
666F3FD896DC1A4D397E0144FB0B1074D983DDF878AAC5C496C04689BA063FF7D8EC8A0702889FAD
C6DBDB93694AEB8760EC9B5B4CFF.169BEF15666A6BEE2B58CCF9101323934A5307838BC03F5893E
BBA2F0D61D34140D27E7E6C675AB5D7DF30A7A8F39922D8724C6D5404907C2B38E823A360A5E8
root@DebianLVM:~#
```

Figura B.11 Comando grub-mkpasswd-pbkdf2

Se edita el archivo */etc/grub.d/00_header* y al final del archivo se agregan las siguientes líneas:

```
cat << EOF
set superusers=”[usuario]”
password_pbkdf2 [usuario] [contraseña]
EOF
```

En donde:

- [usuario] es el nombre del usuario GRUB
- [contraseña] es la contraseña encriptada obtenida en el paso anterior.

Quedando como se muestra en la Figura B.12.

```
# Play an initial tune
if [ "x${GRUB_INIT_TUNE}" != "x" ] ; then
  echo "play ${GRUB_INIT_TUNE}"
fi

if [ "x${GRUB_BADRAM}" != "x" ] ; then
  echo "badram ${GRUB_BADRAM}"
fi

cat << EOF
set superusers="usuario"
password_pbkdf2 usuario grub.pbkdf2.sha512.10000.B65118BEE9B7EB6F873C666F3FD896D
C1A4D397E0144FB0B1074D983DDF878AAC5C496C04689BA063FF7D8EC8A0702889FADC6DBDB93694
AEB8760EC9B5B4CFF.169BEF15666A6BEE2B58CCF9101323934A5307838BC03F5893EBBA2F0D61D3
4140D27E7E6C675AB5D7DF30A7A8F39922D8724C6D5404907C2B38E823A360A5E8
EOF
```

Figura B.12 Archivo /etc/grub.d/00_header

Una vez editado el archivo, se guarda la configuración con el siguiente comando.

```
grub-mkconfig -o /boot/grub/grub.cfg
```

como se muestra en la Figura B.13

```
root@DebianLVM:~# grub-mkconfig -o /boot/grub/grub.cfg
Generando un fichero de configuración de grub...
Found background image: /usr/share/images/desktop-base/desktop-grub.
png
Encontrada imagen de linux: /boot/vmlinuz-4.9.0-8-amd64
Encontrada imagen de memoria inicial: /boot/initrd.img-4.9.0-8-amd64
Encontrada imagen de linux: /boot/vmlinuz-4.9.0-7-amd64
Encontrada imagen de memoria inicial: /boot/initrd.img-4.9.0-7-amd64
hecho
root@DebianLVM:~#
```

Figura B.13 Comando grub-mkconfig

Ahora se edita el archivo */etc/grub.d/10_linux*, se ubica la línea

```
echo "menuentry '$(echo "$os" | grub_quote)' ${CLASS}
    \$menuentry_id_option 'gnulinux-simple-
    $boot_device_id' {" | sed "s/^/$submenu_indentation/"
```

Y se le agrega `--unrestricted`, quedando como se muestra en la Figura B.14. Una vez hecho los cambios se guarda el archivo.

```
          grub_warn "$(gettext_printf "Please don't use old title \`%s'
for GRUB_DEFAULT, use \`%s' (for versions before 2.00) or \`%s' (for 2.0
0 or later)" "$GRUB_ACTUAL_DEFAULT" "$replacement_title" "gnulinux-advan
ced-$boot_device_id>gnulinux-$version-$type-$boot_device_id")"
      fi
      echo "menuentry '$(echo "$title" | grub_quote)' ${CLASS} \$menuent
ry_id_option 'gnulinux-$version-$type-$boot_device_id' {" | sed "s/^/$su
bmenu_indentation/"
  else
      echo "menuentry '$(echo "$os" | grub_quote)' ${CLASS} \$menuentry_
id_option 'gnulinux-simple-$boot_device_id' --unrestricted {" | sed "s/^
/$submenu_indentation/"
  fi
  if [ "$quick_boot" = 1 ]; then
      echo "    recordfail" | sed "s/^/$submenu_indentation/"
  fi
  if [ x$type != xrecovery ] ; then
      save_default_entry | grub_add_tab
  fi
```

Figura B.14 Archivo /etc/grub.d/10_linux

Al finalizar para guardar la configuración, se teclea el comando

```
update-grub
```

como se muestra en la Figura B.15.

```
root@DebianLVM:~# update-grub
Searching for GRUB installation directory ... found: /boot/grub
Searching for default file ... found: /boot/grub/default
Testing for an existing GRUB menu.lst file ... found: /boot/grub/menu.lst
Searching for splash image ... none found, skipping ...
Found kernel: /vmlinuz-4.9.0-8-amd64
Found kernel: /vmlinuz-4.9.0-7-amd64
Updating /boot/grub/menu.lst ... done

root@DebianLVM:~#
```

Figura B.15 Comando uptade-grub

Para probar las configuraciones hechas, se reinicia el servidor y una vez cargado el gestor de arranque GRUB, se muestra el menú como en la Figura B.16. Con las teclas de arriba y abajo se puede seleccionar un sistema operativo (si se tiene instalado más de uno), con la tecla ‘e’ se pueden modificar las opciones de arranque y con la letra ‘c’ se puede acceder a una pequeña consola, con una serie de comandos limitados.

Figura B.16 Menú de GRUB

Si las configuraciones se hicieron correctamente, al presionar la letra ‘e’ o ‘c’, el sistema pide el nombre de usuario y la contraseña que se establecieron en los pasos anteriores, como se muestra en la Figura B.17.

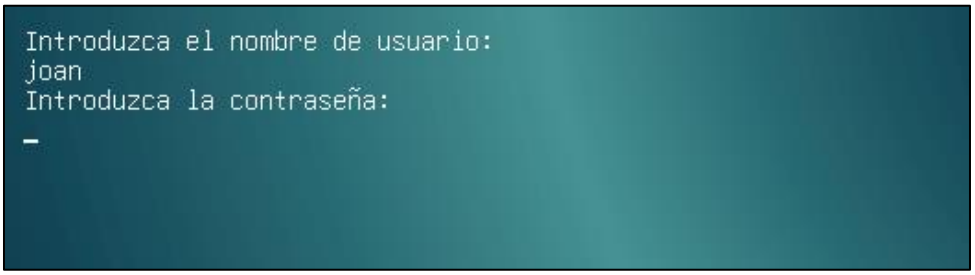


Figura B.17 Acceso a GRUB

2.3. Instalación y configuración de Secure Shell

En este punto se instala y configura Secure Shell, de acuerdo a lo descrito en el capítulo 3, en el punto 3.2.3.

Para instalar SSH se debe abrir una terminal y acceder al sistema como root, ya en el sistema se ejecuta el comando

```
apt-get install -y ssh
```

como se muestra en la Figura B.18.

```
root@DebianLVM:~# apt-get install -y ssh
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Figura B.18 Instalación de SSH

Una vez instalado SSH se inicia el servicio y se habilita para que se inicie automáticamente cuando se enciende el servidor, usando los comandos

```
systemctl start ssh
systemctl enable ssh
```

como se muestra en la Figura B.19.

```
root@DebianLVM:~# systemctl start ssh
root@DebianLVM:~# systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/s
ystemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
root@DebianLVM:~#
```

Figura B.19 Iniciar y habilitar SSH

- Limitar que el usuario root inicie sesión de forma remota y forzar el uso de una cuenta de usuario normal (véase Figura B.20). Se descomenta la línea:

  ```
  PermitRootLogin no
  ```

- Indicar la cantidad de veces que se puede ingresar erróneamente el usuario y/o la contraseña (véase Figura B.20). Se descomenta la línea:

  ```
  MaxAuthTries 2
  ```

```
# Authentication:

#LoginGraceTime 2m
#StrictModes yes
PermitRootLogin no
MaxAuthTries 3
#MaxSessions 10
```

Figura B.20 Archivo /etc/ssh/sshd_config

- Indicar la cantidad de conexiones simultáneas que permitirá SSH por IP que intente conectarse. Se descomenta la línea: (véase Figura B.21)

  `MaxStartups 3`

```
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
MaxStartups 3
#PermitTunnel no
#ChrootDirectory none
```

Figura B.21 Archivo /etc/ssh/sshd_config

- Especificar los usuarios con acceso a la conexión vía SSH. Al final del archivo se agrega la opción AllowUsers, indicando los usuarios separados por un espacio

  `AllowUsers usuario1 usuario2 usuario3`

  como se muestra en la Figura B.22.

```
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server

AllowUsers usuario1 usuario2 usuario3
```

Figura B.22 Archivo /etc/ssh/sshd_config

Una vez que se han hecho los cambios, se guarda el archivo y se reinicia el servicio de SSH, con el comando

`systemctl restart ssh`

como se muestra en la Figura B.23.

```
root@DebianLVM:~# systemctl restart ssh
root@DebianLVM:~#
```

Figura B.23 Reniciar SSH

Para configurar el mensaje de bienvenida que se muestra al acceder a Secure Shell, es necesario modificar el contenido del archivo */etc/motd*, el contenido de este archivo se muestra cuando se ha ingresado correctamente de forma remota al equipo.

Con base en los puntos descritos en el capítulo 4, se propone un mensaje de bienvenida al usuario, el cual se muestra en la Figura B.24.

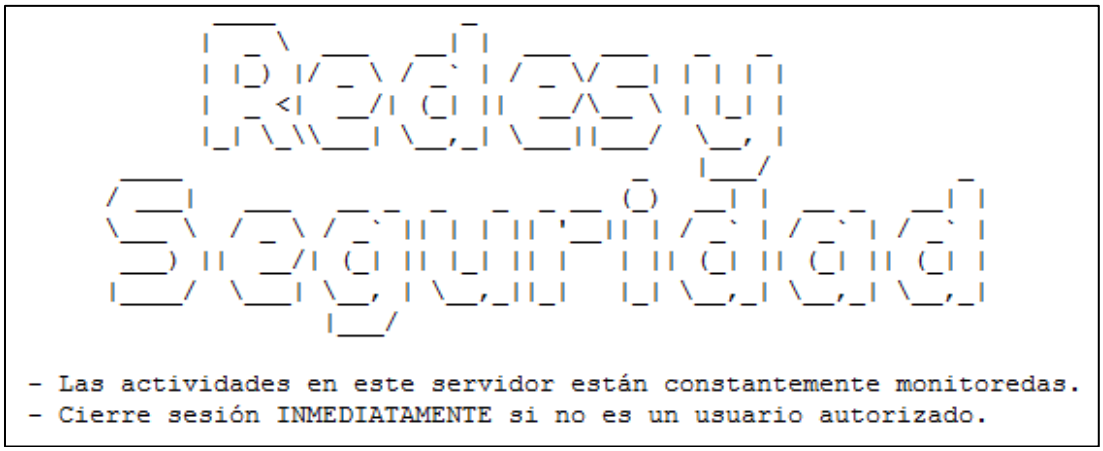


Figura B.24. Mensaje de bienvenida SSH

2.4. SUDO

En este punto se instala y configura la herramienta sudo, de acuerdo a lo descrito en el capítulo 3, en el punto 3.2.4.

Para instalar sudo se debe abrir una terminal y acceder al sistema como root, ya en el sistema se ejecuta el comando

```
apt-get install -y sudo
```

como se muestra en la Figura B.25

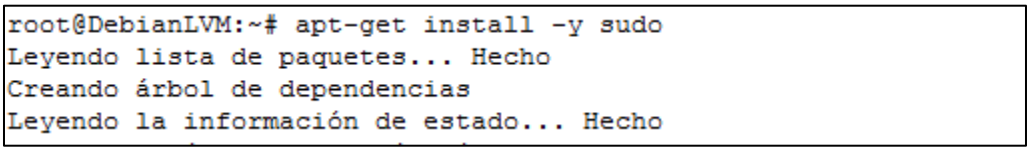


Figura B.25 Instalación de sudo

Una vez instalado, se debe editar el archivo de configuración de la herramienta sudo con el comando

```
visudo
```

con el cual se puede editar el archivo */etc/sudoers*, como se muestra en la Figura B.26.

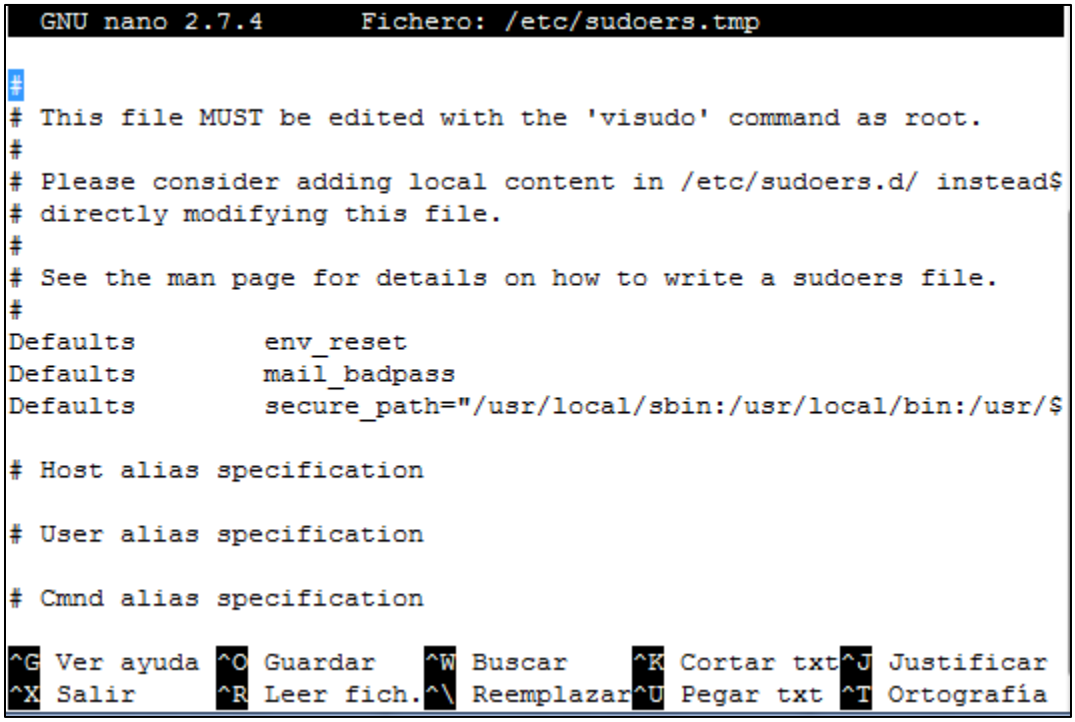


Figura B.26 Comando visudo

Cuando se instala la herramienta sudo, se crea en el sistema el grupo sudo. Por defecto, los usuarios que pertenezcan al grupo sudo pueden ejecutar comandos con permisos de root, anteponiendo el comando sudo. En la Figura B.27 se muestra la configuración por defecto del archivo */etc/sudoers*, en donde el usuario root tiene todos los permisos y se indica que los usuarios pertenecientes al grupo sudo pueden ejecutar cualquier comando.

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

Figura B.27 Archivo /etc/sudoers

Se debe cambiar el grupo sudo por defecto por uno previamente creado en el sistema, al cual pertenezcan los administradores del servidor. Quedando el archivo como se muestra en la Figura B.28.

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%grupo  ALL=(ALL:ALL) ALL
```

Figura B.28 Archivo /etc/sudoers

Si se quiere darle permiso de root a un usuario, se le agrega al usuario el grupo asignado para ese fin con el comando como grupo secundario usando el comando

```
usermod -G [nombre del grupo] [nombre de usuario]
```

como se muestra en el ejemplo de la Figura B.29.

```
root@DebianLVM:~# usermod -G grupo usuario
root@DebianLVM:~#
```

Figura B.29 Asignación de grupo secundario

Con la herramienta sudo, un usuario que se especifique en el archivo */etc/sudoers* puede cambiarse a usuario root usando el comando

```
sudo -i
```

Una vez tecleado el comando, se pedirá la contraseña del usuario, como se muestra en la Figura B.30, evitando así la divulgación de la contraseña del usuario root.

```
usuario@DebianLVM:~$ sudo -i
[sudo] password for usuario:
root@DebianLVM:~#
```

Figura B.30 Comando sudo -i

2.5. Iptables

Las reglas a establecerse en el servidor son las desarrolladas en el proyecto "Análisis, diseño y desarrollo de medidas de protección para una administración segura bajo Linux", llevado a cabo por los alumnos María Guadalupe Morales Nava y Edgar Ramón Prado.

El archivo que contiene las reglas se encuentra en el home de root, es decir, */root*. El archivo es */root/iptables.sh*, como se muestra en la Figura B.31.

```
root@DebianLVM:~# ls /root
iptables.sh
root@DebianLVM:~#
```

Figura B.31 Directorio /root

Se debe ejecutar el archivo anteponiendo con el comando `sh` e indicar la opción (`start|stop|restart`), como se muestra en la Figura B.32.

```
root@DebianLVM:~# sh /root/iptables.sh start
$Starting firewall:
$Ok! Firewall started
root@DebianLVM:~#
```

Figura B.32 Ejecución del archivo firewall.sh

Las reglas creadas con el comando `iptables` son almacenadas en memoria. Si el sistema se reinicia, estas se pierden. Para evitarlo una opción es utilizar el servicio de cron para que las reglas de iptables sean cargadas cada que se enciende el servidor.

En el sistema operativo Unix, cron es un administrador regular de procesos en segundo plano (demonio) que ejecuta procesos a intervalos regulares. El archivo de configuración de cron es */etc/crontab*, en él se especifican los procesos que deben ejecutarse y la hora en la que deben hacerlo.

Lo primero que se debe hacer es habilitar el servicio de cron para que se inicie automáticamente cuando se enciende el servidor, como se muestra en la Figura B.33

```
root@DebianLVM:~# systemctl enable cron
Synchronizing state of cron.service with SysV service script with /lib/s
ystemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable cron
root@DebianLVM:~#
```

Figura B.33 Habilitar servicio de cron

Para editar el archivo */etc/crontab* se teclea el comando que se muestra en la Figura B.34

```
root@DebianLVM:~# crontab -e
```

Figura B.34 Editar el archivo /etc/crontab

Con el comando del paso anterior se habilita la edición del archivo */etc/crontab* con el editor de texto nano. Al final del archivo se agrega la línea

```
@reboot root /bin/sh /root/iptables.sh start
```

la cual indica al servidor que se ejecute el archivo */root/iptables.sh* cada que se inicie el sistema operativo, quedando como se muestra en la Figura B.35.

```
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

@reboot root /bin/sh /root/iptables.sh start
```

Figura B.35 Archivo /etc/crontab

Al finalizar, se reinicia el servicio de cron para que se guarden los cambios, como se muestra en la Figura B.36.

```
root@DebianLVM:~# systemctl restart cron
root@DebianLVM:~#
```

Figura B.36 Reinicio de servicio cron

2.6. Certificado SSL

En este punto se instala y configura en el servidor el certificado SSL provisto por Let's Encrypt, de acuerdo a lo descrito en el capítulo 3, en el punto 3.2.6.

Let's Encrypt cuenta con el software Certbot, que automatiza la instalación del certificado SSL, sin embargo, no está disponible por defecto en los repositorios de Debian, por lo que es necesario añadir los repositorios backports de Debian en el archivo de configuración de apt. Para hacerlo se accede a una terminal como usuario root, se edita el archivo */etc/apt/sources.list* y al final de este se agrega la línea

```
deb http://ftp.debian.org/debian stretch-backports main
```

quedando como se muestra en la Figura B.37.

```
deb http://ftp.mx.debian.org/debian/ stretch main
deb-src http://ftp.mx.debian.org/debian/ stretch main

deb http://security.debian.org/debian-security stretch/updates main
deb-src http://security.debian.org/debian-security stretch/updates main

# stretch-updates, previously known as 'volatile'
deb http://ftp.mx.debian.org/debian/ stretch-updates main
deb-src http://ftp.mx.debian.org/debian/ stretch-updates main

deb http://ftp.debian.org/debian stretch-backports main
```

Figura B.37 Archivo /ect/apt/sources.list

Una vez editado el archivo de configuración, se actualizan los paquetes disponibles de los repositorios como se muestra en la Figura B.38.

```
root@DebianLVM:~# apt-get update
Obj:1 http://security.debian.org/debian-security stretch/updates
Ign:2 http://ftp.mx.debian.org/debian stretch InRelease
Obj:3 http://ftp.mx.debian.org/debian stretch-updates InRelease
Obj:4 http://ftp.mx.debian.org/debian stretch Release
Obj:5 http://ftp.debian.org/debian stretch-backports InRelease
Leyendo lista de paquetes... Hecho
root@DebianLVM:~#
```

Figura B.38 Actualización de repositorios

Posteriormente, se instala certbot con apt-get, indicando con la opción -t que busque en los repositorios backports, como se muestra en la Figura B.39.

```
root@DebianLVM:~# apt-get install python-certbot-apache -t stretch-
backports
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  augeas-lenses certbot libaugeas0 python-pyicu python3-acme
  python3-asn1crypto python3-augeas python3-certbot
  python3-certbot-apache python3-cffi-backend
  python3-configargparse python3-configobj python3-cryptography
  python3-future python3-idna python3-josepy python3-mock
  python3-openssl python3-parsedatetime python3-pbr
  python3-requests-toolbelt python3-rfc3339 python3-setuptools
  python3-tz python3-zope.component python3-zope.event
  python3-zope.hookable python3-zope.interface
```

Figura B.39 Instalación de certbot

Ya que certbot está instalado, se obtiene el certificado tecleando el comando que se muestra en la Figura B.40, en donde se indica que el servidor web utilizado es apache y con la opción -d se indica el dominio del servidor.

```
root@DebianLVM:~# certbot --apache -d redyseguridad.fi-b.unam.mx
```

Figura B.40 Obtención de certificado SSL

A continuación, certbot pide que se ingrese un correo electrónico y se acepten los términos del servicio, como se muestra en la Figura B.41. Después de hacerlo, certbot se comunica con el servidor de Let's Encrypt para verificar la autenticidad del dominio.

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Enter email address (used for urgent renewal and security notices) (Enter '
c' to
cancel): jerridhdz@hotmail.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
(A)gree/(C)ancel: A
```

Figura B.41 Términos del servicio de Let's Encrypt

Si se valida, certbot pregunta la forma en que se desea configurar los ajustes de HTTPS. Se elige la opción número 2, como se muestra en la Figura B.42, ya que de esta manera certbot modifica automáticamente los archivos de configuración para redirigir el tráfico HTTP a HTTPS.

```
Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTT
P access.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this
 for
new sites, or if you're confident your site works on HTTPS. You can undo thi
s
change by editing your web server's configuration.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 2
```

Figura B.42 Configuración de HTTPS

Para finalizar, certbot se encarga de reiniciar el servicio de apache para cargar la nueva configuración y termina con un mensaje en el que se informa que el proceso se realizó correctamente y el directorio donde se almacenan los certificados, como el que se muestra en la Figura B.43.

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/redyseguridad.fi-b.unam.mx/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/redyseguridad.fi-b.unam.mx/privkey.pem
   Your cert will expire on 2019-06-10. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

Figura B.43 Mensaje final de certbot

Hasta este punto ya se tiene descargado e instalado el certificado SSL, si se vuelve a cargar el sitio web, se observa que la dirección URL ya cuenta con las siglas https y el candado de lado izquierdo, como se muestra en la Figura B.44.

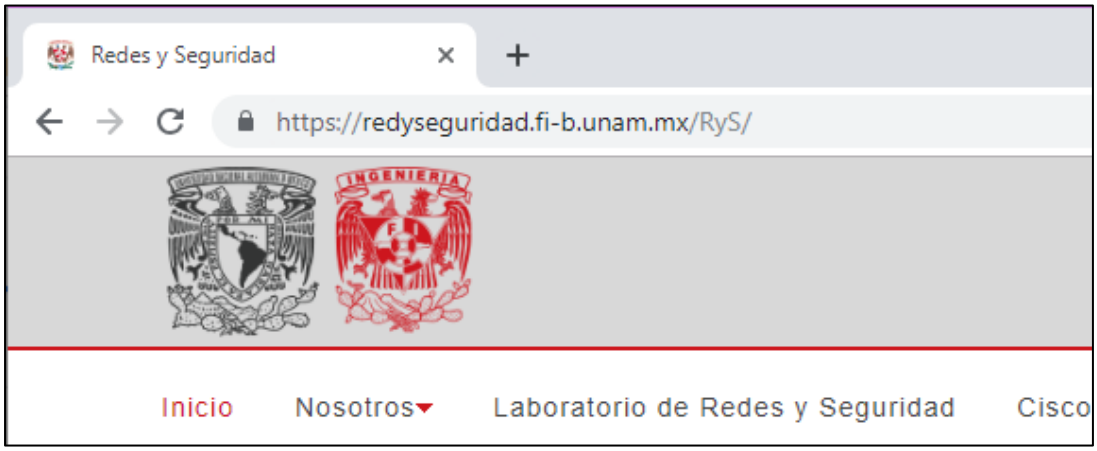


Figura B.44 Dirección URL

Los certificados de Let's Encrypt solo son válidos por noventa días. El paquete de certbot al hacer la instalación agrega un script de renovación a la carpeta */etc/cron.d,* en la Figura B.45 se observa que se crea el archivo de nombre certbot. Por defecto, este script se ejecuta dos veces al día y renueva automáticamente cualquier certificado que esté dentro de los 30 días de vencimiento.

```
root@DebianLVM:~# ls /etc/cron.d
anacron  certbot  php
root@DebianLVM:~#
```

Figura B.45 Carpeta /etc/cron.d

Se puede hacer una prueba del proceso de renovación con el comando

```
certbot renew --dry-run
```

Este proceso revisa que la renovación automática se encuentra funcionando. Si no se ven errores, como en la Figura B.46, certbot renovará los certificados y recargará Apache para guardar los cambios de manera automática cuando sea necesario.

```
root@DebianLVM:~# certbot renew --dry-run
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Processing /etc/letsencrypt/renewal/redyseguridad.fi-b.unam.mx.conf
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Cert not due for renewal, but simulating renewal for dry run
Plugins selected: Authenticator apache, Installer apache
Renewing an existing certificate
Performing the following challenges:
http-01 challenge for redyseguridad.fi-b.unam.mx
Waiting for verification...
Cleaning up challenges

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
new certificate deployed with reload of apache server; fullchain is
/etc/letsencrypt/live/redyseguridad.fi-b.unam.mx/fullchain.pem
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
** DRY RUN: simulating 'certbot renew' close to cert expiry
**          (The test certificates below have not been saved.)

Congratulations, all renewals succeeded. The following certs have been renewed
  /etc/letsencrypt/live/redyseguridad.fi-b.unam.mx/fullchain.pem (success)
** DRY RUN: simulating 'certbot renew' close to cert expiry
**          (The test certificates above have not been saved.)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Figura B.46 Prueba de renovación de certificados

3. Interfaces de red

Comúnmente se utilizó el comando `ifconfig` para realizar tareas relacionadas con la red, como verificar interfaces de red o configurarlas; sin embargo, es un comando obsoleto y ya no está presente en las nuevas distribuciones de Linux y es sustituido por la aplicación iproute2 suite.

IProute2 cuenta con el comando `ip`, el cual es similar al comando `ifconfig`, pero cuenta con más funcionalidades asociadas. En este punto se muestran los comandos básicos para visualizar la información de las interfaces de red.

3.1. Comprobación de información de interfaces de red

Para verificar la información de red relacionada con todas las interfaces disponibles en el sistema se usa el comando

```
ip addr show
```

como se muestra en la Figura B.47

```
usuario@DebianLVM:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNO
WN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s25: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfif
o_fast state UP group default qlen 1000
    link/ether 00:21:86:1e:22:3a brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.60/24 brd 192.168.50.255 scope global enp0s25
       valid_lft forever preferred_lft forever
    inet6 fe80::221:86ff:fe1e:223a/64 scope link
       valid_lft forever preferred_lft forever
usuario@DebianLVM:~$
```

Figura B.47 Consulta de todas las interfaces de red

Para ver la información asociada a una sola interfaz se utiliza el comando

```
ip addr show [nombre de la interfaz]
```

como se muestra en la Figura B.48

```
usuario@DebianLVM:~$ ip addr show enp0s25
2: enp0s25: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfif
o_fast state UP group default qlen 1000
    link/ether 00:21:86:1e:22:3a brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.60/24 brd 192.168.50.255 scope global enp0s25
       valid_lft forever preferred_lft forever
    inet6 fe80::221:86ff:fe1e:223a/64 scope link
       valid_lft forever preferred_lft forever
usuario@DebianLVM:~$
```

Figura B.48 Consulta de una interfaz de red

3.2. Reiniciar servicio de red

Para reiniciar el servicio de red se accede a una terminal como usuario root y se hace reiniciando el servicio networking como se muestra en la Figura B.49.

```
root@DebianLVM:~# service networking restart
root@DebianLVM:~#
```

Figura B.49 Reinicio del servicio de red

Otra forma de hacerlo es con el archivo del directorio /etc/init.d, como se muestra en la Figura B.50.

```
root@DebianLVM:~# /etc/init.d/networking restart
[ ok ] Restarting networking (via systemctl): networking.service.
root@DebianLVM:~#
```

Figura B.50 Reinicio del servicio de red

4. Actualización del sistema

Las actualizaciones son añadidos o modificaciones realizadas sobre los sistemas operativos o aplicaciones que se tienen instalados en un equipo y cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad.

Para actualizar el sistema se debe abrir una terminal y acceder como usuario root. Antes de actualiza, se hace una lista de las aplicaciones que requieran una actualización y sus versiones, con el comando

```
apt-get update
```

como se muestra en la Figura B.51, cabe destacar que el comando no instala o actualiza.

```
root@DebianLVM:~# apt-get update
Ign:1 http://ftp.mx.debian.org/debian stretch InRelease
Obj:2 http://ftp.mx.debian.org/debian stretch-updates InRelease
Obj:3 http://ftp.mx.debian.org/debian stretch Release
Des:4 http://security.debian.org/debian-security stretch/updates InRe
lease [94.3 kB]
Descargados 94.3 kB en 0s (207 kB/s)
Leyendo lista de paquetes... Hecho
root@DebianLVM:~#
```

Figura B.51 Actualización de repositorios

Una vez que el comando anterior ha descargado la lista de software disponible y la versión en que se encuentra, se actualizan dichas aplicaciones usando el comando

```
apt-get upgrade
```

como se muestra en la Figura B.52, con esto se instalan las nuevas versiones respetando la configuración del software.

```
root@DebianLVM:~# apt-get upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
```

Figura B.52 Actualización de aplicaciones

En el caso del sistema operativo, Debian en su página oficial *https://www.debian.org/* publica cuando ha liberado una nueva actualización o una nueva versión estable de su sistema.

El día 23 de enero de 2019 fue liberada la última versión estable 9.7, por lo que es necesario actualizar el sistema instalado de una versión estable a la siguiente, con el comando

```
apt-get dist-upgrade
```

como se muestra en la Figura B.53.

```
root@DebianLVM:~# apt-get dist-upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
```

Figura B.53 Actualización de versión

Se puede comprobar que se actualizó el sistema a la versión 9.7 con el comando

```
lsb_release -a
```

como se muestra en la Figura B.54.

```
root@DebianLVM:~# lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 9.7 (stretch)
Release:        9.7
Codename:       stretch
root@DebianLVM:~#
```

Figura B.54 Comprobación de actualización

5. Administración de particiones

Las particiones del servidor están implementadas como volúmenes lógicos como se explica en el capítulo 1. Una de la ventaja de los volúmenes lógicos es que pueden cambiar su tamaño dinámicamente, es decir, cambiar su tamaño sin necesidad de volver a instalar el sistema para modificar el particionado.

La administración de volúmenes lógicos se lleva a cabo mediante la aplicación LVM (Logical Volume Management). Para ingresar a ella se abre una terminal, se accede como usuario root y se teclea el comando lvm, para salir se teclea exit, como se muestra en la Figura B.55.

```
root@DebianLVM:~# lvm
lvm>
lvm>
lvm>
lvm> exit
  Exiting.
root@DebianLVM:~#
```

Figura B.55 Ingreso a LVM

Con el comando `vgs` se ven los grupos de volúmenes del sistema, es decir, el conjunto de volúmenes lógicos. Para este caso solo se tiene un grupo de volúmenes que ocupa el espacio total del sistema, en la Figura B.56 se ve el espacio total ocupado por los volúmenes lógicos y el espacio libre que se puede ocupar en caso de que se quiera extender uno de ellos.

```
lvm> vgs
  VG        #PV #LV #SN Attr   VSize VFree
  vg_redes    1   5   0 wz--n- 1.76t 646.66g
lvm>
```

Figura B.56 Consulta de grupos de volúmenes

Con el comando `lvs` se ven los volúmenes lógicos, se ve el grupo al que pertenecen y el tamaño que ocupan en él, como se muestra en la Figura B.57.

```
lvm> lvs
  LV        VG       Attr       LSize   Pool Origin
  lv_home   vg_redes -wi-a----- 200.00g
  lv_tmp    vg_redes -wi-a-----   2.00g
  lv_usr    vg_redes -wi-a-----  50.00g
  lv_var    vg_redes -wi-a----- 200.00g
  lv_varwww vg_redes -wi-ao---- 800.00g
lvm>
```

Figura B.57 Consulta de volúmenes lógicos

5.1. Incrementar tamaño de un volumen lógico

Para este ejemplo se va a incrementar el espacio de la partición */var/www*, la cual tiene un tamaño de 800 GB, como se muestra en la Figura B.58.

```
lvm> lvs
  LV        VG       Attr       LSize   Pool Origin
  lv_home   vg_redes -wi-a----- 200.00g
  lv_tmp    vg_redes -wi-a-----   2.00g
  lv_usr    vg_redes -wi-a-----  50.00g
  lv_var    vg_redes -wi-a----- 200.00g
  lv_varwww vg_redes -wi-ao---- 800.00g
lvm>
```

Figura B.58 Consulta de volúmenes lógicos

Para incrementar el tamaño de una partición se usa el comando `lvextend` dentro del LVM, la sintaxis del comando es:

```
lvextend -L [Tamaño nuevo] [Ruta del volumen lógico]
```

Para este caso se va a incrementar el tamaño a 900GB y cabe destacar que la ruta de los volúmenes lógicos es `/dev/vg_redes/[nombre del volumen lógico]`, quedando como se muestra en la Figura B.59

```
lvm> lvextend -L 900G /dev/vg_redes/lv_varwww
  Size of logical volume vg_redes/lv_varwww changed from 800.00 GiB
 (204800 extents) to 900.00 GiB (230400 extents).
  Logical volume vg_redes/lv_varwww successfully resized.
lvm>
```

Figura B.59 Incrementar volumen lógico

Se verifica con el comando `lvs` y se aprecia que cambió el tamaño a 900GB, como se muestra en la Figura B.60

```
lvm> lvs
  LV        VG       Attr       LSize   Pool Origin
  lv_home   vg_redes -wi-a----- 200.00g
  lv_tmp    vg_redes -wi-a-----   2.00g
  lv_usr    vg_redes -wi-a-----  50.00g
  lv_var    vg_redes -wi-a----- 200.00g
  lv_varwww vg_redes -wi-ao---- 900.00g
lvm>
```

Figura B.60 Consulta de volúmenes lógicos

5.2. Reducir tamaño de un volumen lógico

Para este ejemplo se va a reducir el espacio de la partición */var/www*, la cual tiene un tamaño de 900 GB, tal como se dejó el punto anterior.

Para reducir el tamaño de una partición se usa el comando `lvreduce` dentro del LVM, la sintaxis del comando es:

```
lvreduce -L [Tamaño nuevo] [Ruta del volumen lógico]
```

Para este caso se va a reducir el tamaño a 800GB y cabe destacar que la ruta de los volúmenes lógicos es `/dev/vg_redes/[nombre del volumen lógico]`, quedando como se muestra en la Figura B.61.

Nota: Es importante reducir el tamaño del sistema de archivos antes de reducir el volumen lógico, de lo contrario los datos podrían perderse. Al reducir el volumen lógico se libera espacio del grupo de volúmenes para que pueda ser asignado a otro volumen lógico.

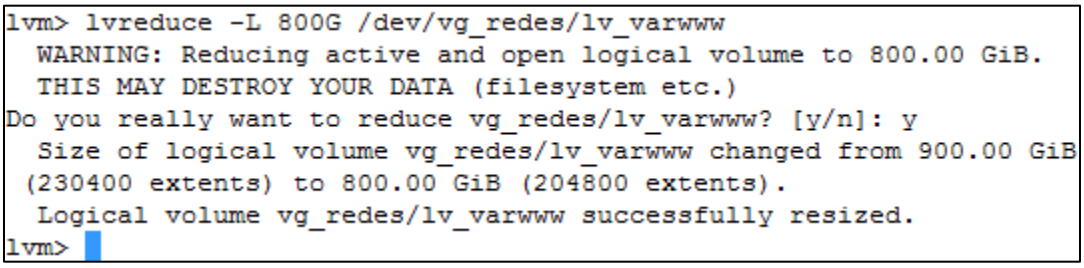


Figura B.61 Reducir volumen lógico

Se verifica con el comando `lvs` y se aprecia que cambió el tamaño a 800GB, como se muestra en la Figura B.62.

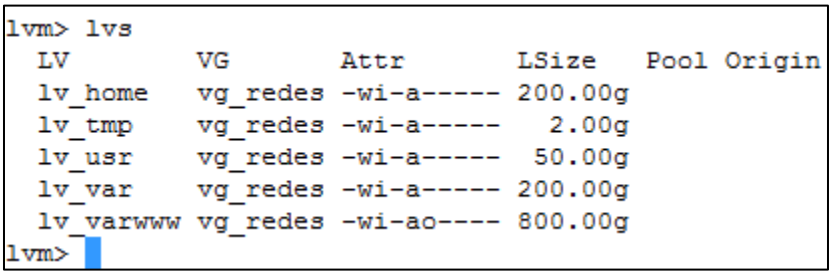


Figura B.62 Consulta de volúmenes lógicos

Anexo C

Manual de estructura y actualización del sitio web

Índice

1. Introducción

El presente manual explica, de forma detallada, la forma en que está organizada el sitio web del Área de Redes y Seguridad y el sitio web del Laboratorio de Redes y Seguridad, para que de esta forma se puedan mantener actualizados dichos sitios web.

El manual se encuentra dividido en secciones que detallan los puntos antes mencionados.

La primera sección, Introducción, es una breve explicación del contenido del "Manual de administración y actualización del sitio web".

En la segunda sección, Estructura del sitio web, se muestran las secciones que conforman las páginas principales del sitio web.

En la tercera sección, Organización del sitio web, se explica la forma en que están organizados los archivos que conforman los sitios web.

En la última sección, Actualización del sitio web, se presentan las principales partes del sitio web y la forma en hacer cambios en ellas para mantener actualizado el sitio.

2. Estructura del sitio web

El trabajo consta de dos sitios web, uno destinado al Área de Redes y Seguridad y otro al Laboratorio de Redes y Seguridad.

2.1. Sitio web del Área de Redes y Seguridad

En la Figura C.1 se muestra el sitio web del Área de Redes y Seguridad, resaltando las principales secciones, cuya modificación se explica más adelante en este manual.

Figura C.1 Sitio web del Área de Redes y Seguridad

Las secciones principales son:

1- Menú principal: Nos dirige a las diferentes páginas del sitio.
2- Slider: Carrusel de imágenes que aparece en la página principal.
3- Avisos: Sección en la que se publican avisos importantes.

2.2. Sitio web del Laboratorio de Redes y Seguridad

En la Figura C.2 se muestra el sitio web del Área de Redes y Seguridad, resaltando las principales secciones, cuya modificación se explica más adelante en este manual.

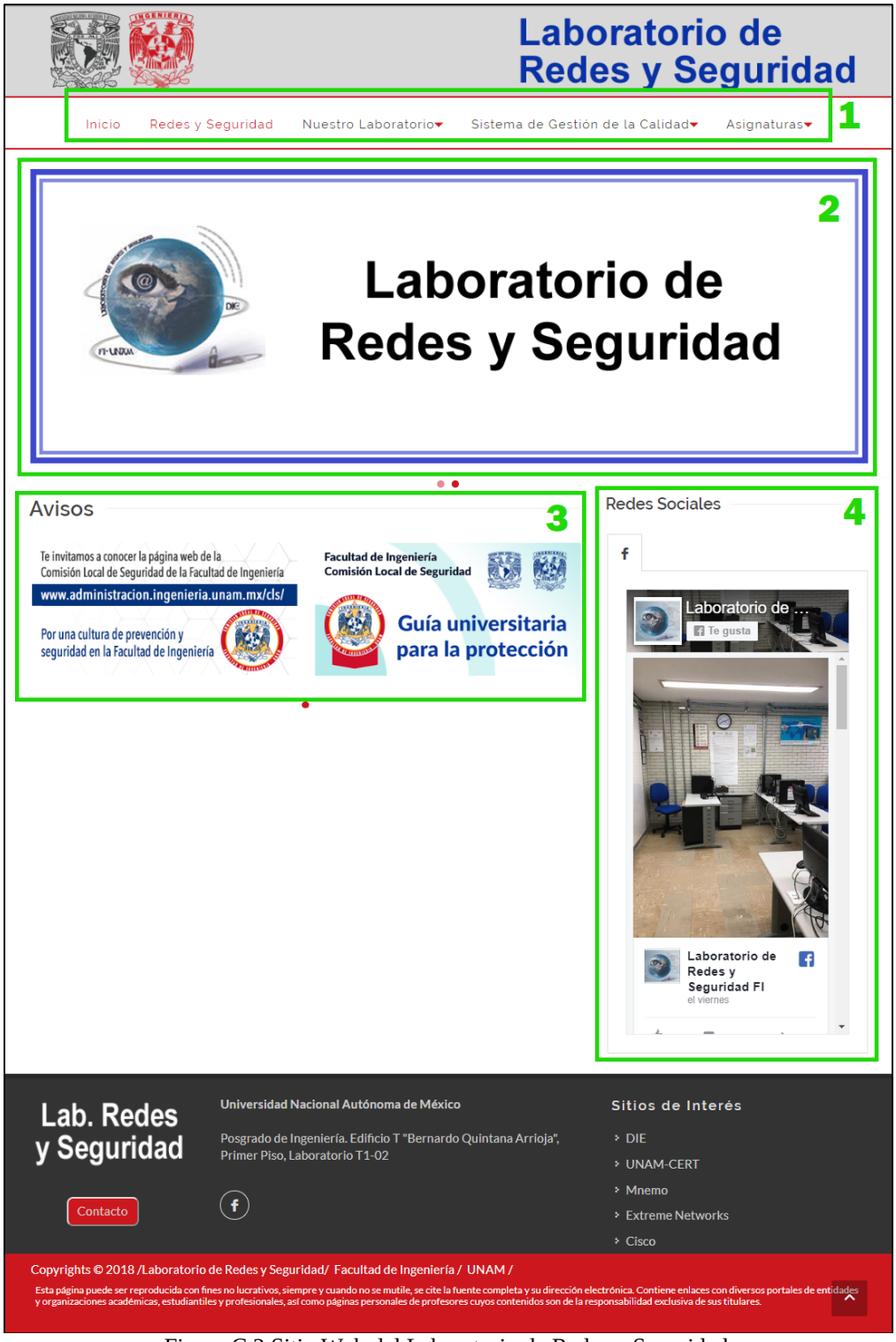


Figura C.2 Sitio Web del Laboratorio de Redes y Seguridad

Las secciones principales son:

1- Menú principal: Nos dirige a las diferentes páginas del sitio.
2- Slider: Carrusel de imágenes que aparece en la página principal.
3- Avisos: Sección en la que se publican avisos importantes.
4- Redes sociales: Sección en la que aparecen las redes sociales del Laboratorio.

3. Organización del sitio web

El sitio web está desarrollado completamente en lenguaje PHP, por lo que cada una de las páginas que conforman al sitio web es un archivo con extensión .php; además, el sitio web está conformado por imágenes, archivos PDF, entre otros, todos ellos organizados en directorios para su mejor administración.

El directorio raíz del servidor web es el directorio */var/www/html*. Todos los documentos que se encuentren dentro del directorio raíz serán accesibles vía web.

Como se muestra en la Figura C.3, en el directorio raíz se encuentran 3 carpetas, en cada una de ellas está un sitio web diferente, la carpeta Lab para el sitio web del Laboratorio de Redes y Seguridad, la carpeta RyS para el sitio web del Área de Redes y Seguridad y la carpeta Dipciber y diplomado para el sitio web del Diplomado en Ciberseguridad; además se encuentra también el archivo index.html, que para este caso redirecciona a los visitantes al sitio web del Área de Redes y Seguridad.

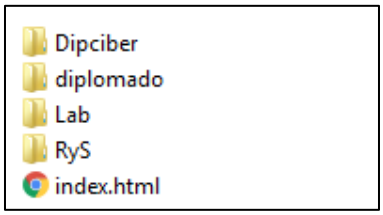


Figura C.3 Contenido de /var/www/html

3.1. Organización del sitio web del Área de Redes y Seguridad

En la Figura C.4 se muestra la forma es que está organizada la carpeta RyS.

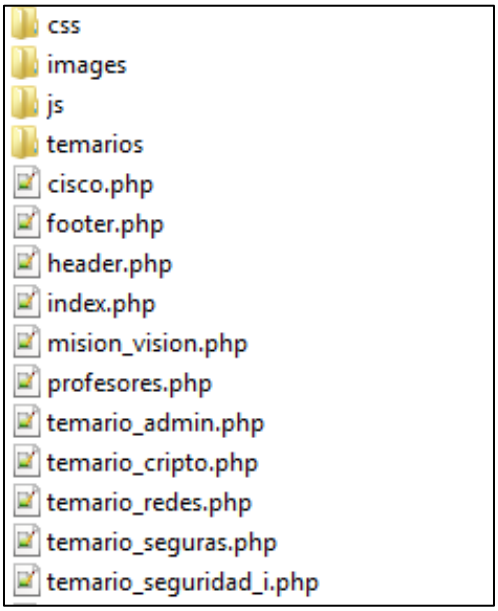


Figura C.4 Carpeta RyS

En la carpeta RyS se encuentran los archivos PHP, cada uno de ellos es una de las páginas que conforman el sitio web. Las carpetas contienen:

- Carpeta css: Hojas de estilo en archivos CSS.
- Carpeta images: Imágenes que se encuentran en el sitio web.
- Carpeta js: Archivos Javascript, que agregan funcionalidad al sitio web.
- Carpeta temarios: Los temarios de las materias en formato PDF.

3.2. Organización del sitio web del Laboratorio de Redes y Seguridad

En la Figura C.5 se muestra la forma es que está organizada la carpeta Lab.

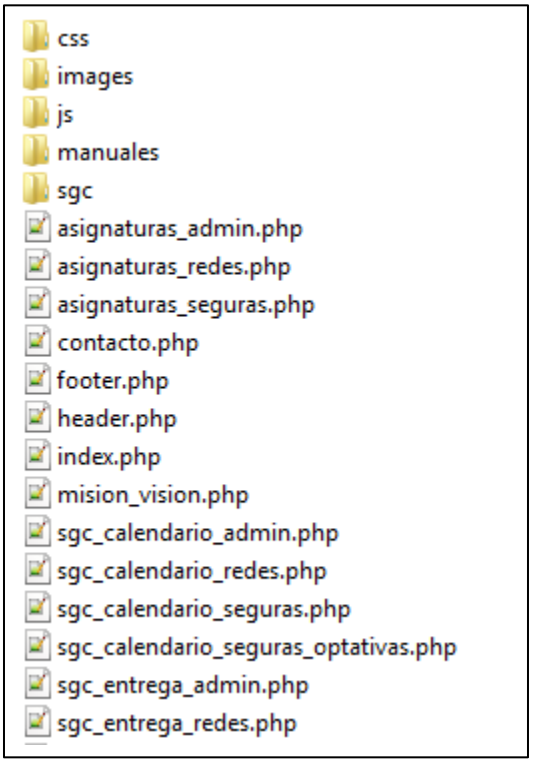


Figura C.5 Carpeta Lab

En la carpeta Lab se encuentran los archivos PHP, cada uno de ellos es una de las páginas que conforman el sitio web. Las carpetas contienen:

- Carpeta css: Hojas de estilo en archivos CSS.
- Carpeta images: Imágenes que se encuentran en el sitio web.
- Carpeta js: Archivos Javascript, que agregan funcionalidad al sitio web.
- Carpeta manuales: Manuales de prácticas y material extra de las materias del laboratorio.
- Carpeta sgc: Archivos PDF correspondientes al Sistema de Gestión de Calidad.

3.3. Organización de las imágenes de los sitios web

Las imágenes que se encuentran en los sitios web están organizadas en carpetas. Ambos sitios web tienen la misma organización que se muestra en la Figura C.6.

Figura C.6 Carpeta images

Las carpetas contienen:

- Carpeta archivos: Archivos e imágenes que se muestran al hacer click en un aviso o un slider de la página principal.
- Carpeta avisos: Imágenes que se muestran en la sección avisos de la página principal
- Carpeta fullslider: Imágenes que forman parte del slider que se encuentra en la página principal.
- Carpeta galeria: Imágenes que se encuentran en las diferentes páginas del sitio web.
- Carpeta icons: Iconos que se pueden utilizar en el sitio web.
- Carpeta logos: Logotipos de la UNAM, la Facultad de Ingeniería y el Laboratorio de Redes y Seguridad.

4. Actualización del sitio web

Para actualizar el sitio web se tienen que editar los archivos .php, para ello se puede hacer de manera local en el servidor utilizando un editor de texto, como vi o gedit.

En la Figura C.7 se muestran los comandos necesarios para editar un archivo con el editor de texto vi, se posiciona en el directorio donde está el archivo y se edita utilizando vi. Es necesario que el usuario cuente con permisos de escritura para poder editar un archivo.

```
usuario@DebianLVM:~$ cd /var/www/html/Lab/
usuario@DebianLVM:/var/www/html/Lab$ vi index.php
```

Figura C.7 Editar archivo con vi

Para cargar imágenes o archivos se puede utilizar la herramienta FileZilla, el cual es un software libre que incluye una herramienta cliente de FTP (Protocolo de Transferencia de Archivos) para poder descargar o subir archivos a un servidor.

La página oficial para descargar el software es: https://filezilla-project.org/

En la Figura C.8 se muestra la interfaz de FileZilla. En la parte superior se le indica la dirección IP del servidor a conectarse, el usuario con el que se va a conectar, la contraseña del usuario y el puerto. Se hace click en el botón “Conexión rápida”.

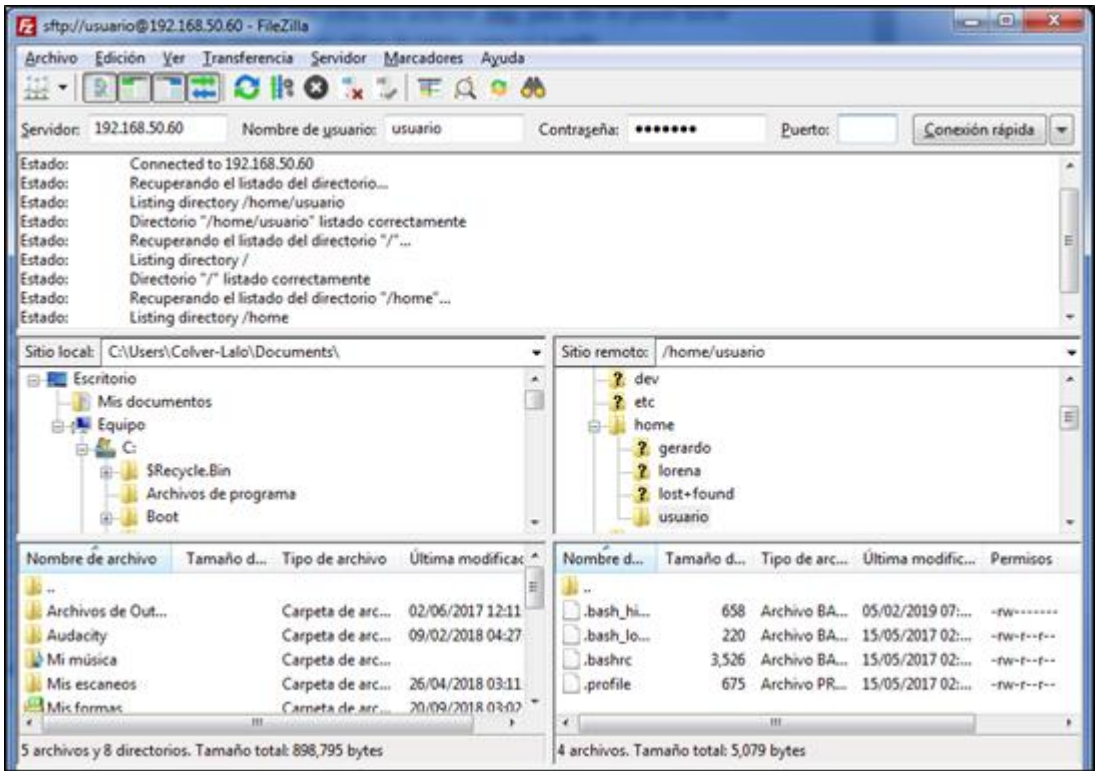


Figura C.8 FileZilla

Una vez conectado, en la parte inferior en el lado izquierdo se muestran los directorios y archivos del equipo local, de lado derecho se muestran los directorios y archivos del servidor al que se realizó la conexión. Para intercambiar archivos se pueden arrastrar los mismos de un lado a otro para hacer la transferencia.

Los sitios web del Área de Redes y Seguridad y del Laboratorio de Redes y Seguridad tienen la misma estructura, a continuación se explican las principales partes de los sitios, así como los archivos que se tienen que editar en caso de requerir modificaciones.

4.1. Header

En diseño web, el header es la parte superior de la página. Para este caso, está conformado por el menú principal y los logotipos de la UNAM y de la Facultad de Ingeniería en en lado superior izquierdo, así como de la inscripción Redes y Seguridad del lado superior derecho, como se muestra en la Figura C.9.

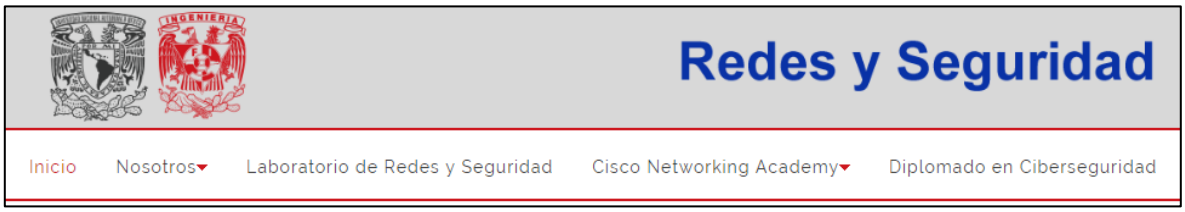


Figura C.9 Header

Los elementos antes mencionados se encuentran definidos en el archivo *header.php*. En todas las páginas del sitio web está incluido el header, con el código que se muestra en la Figura C.10, por lo que si se modifica el archivo header.php, las modificaciones se visualizan en todo el sitio web.

```
<!-- Header
============================================== -->
<?php include("header.php");?>
```

Figura C.10 Incluir el archivo header.php

4.2. Footer

El footer o pie de página es la parte inferior de un sitio web. Está conformado por la dirección del Laboratorio de Redes y Seguridad, los sitios de interés, un botón para la página de Facebook del laboratorio y la política de privacidad; además está diferenciado por los colores de fondo, como se muestra en la Figura C.11.

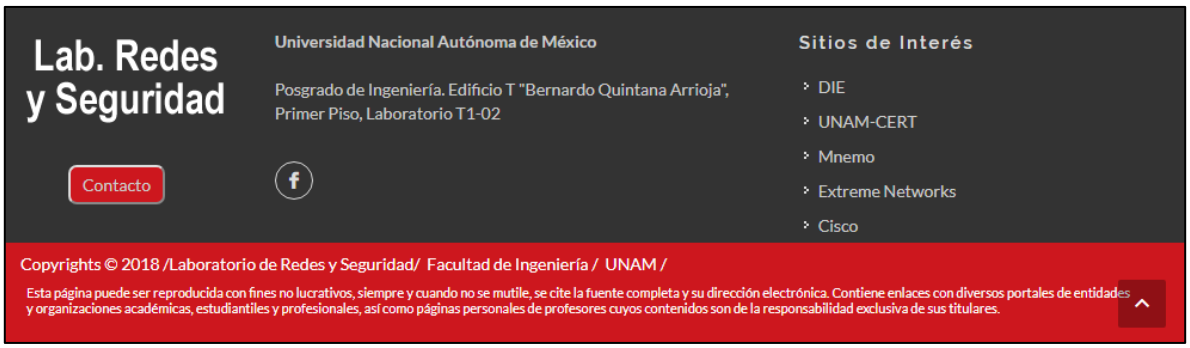


Figura C.11 Footer

Los elementos antes mencionados se encuentran definidos en el archivo *footer.php*. En todas las páginas del sitio web está incluido el pie de página, con el código que se muestra en la Figura C.10, por lo que si se modifica el archivo footer.php, las modificaciones se visualizan en todo el sitio web.

```
<!-- Footer
============================================== -->
<?php include("footer.php"); ?>
```

Figura C.12 Incluir el archivo footer.php

4.3. Slider

En la página principal se observa el slider o carrusel de imágenes que se muestra en la Figura C.13, el cual va cambiando automáticamente.

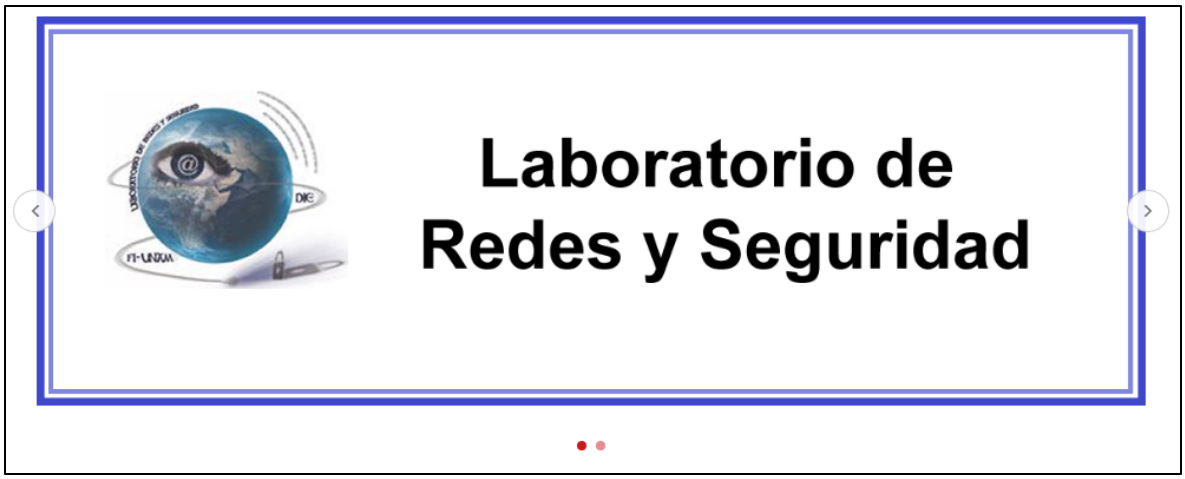


Figura C.13 Slider

El código para modificar el slider es el que se muestra en la Figura C.14 y se encuentra en el archivo *index.php*. En el código, en el campo `src` se define la imagen a mostrar y en el campo `href` se definen los archivos o imágenes que se muestran en caso de hacer click en la imagen.

```
<!--Slider Principal-->
 
<div id="oc-slider" class="owl-carousel">
    <a target="_blank"><img src="images/fullslider/redes_seguridad.png" alt="Slider"></a>
    <a target="_blank" href="images/archivos/PosterDiplomado.pdf" target="_blank">
        <img src="images/fullslider/ciberseguridad.png" alt="Slider"></a>
</div>
```

Figura C.14 Código del slider

Para una mejor administración, las imágenes que se muestran en el slider se encuentran en la carpeta llamada fullslider y los archivos e imágenes que se muestran cuando se da click en el slider se encuentran en la carpeta archivos; ambas carpetas se encuentran en la carpeta images del sitio web correspondiente.

Las imágenes que se coloquen en el slider deben tener una medida de 1140 x 400 pixeles para que se conserve el diseño del sitio web, además de tener al menos 2 imágenes para que funcione correctamente el cambio automático.

En la carpeta fullslider hay una imagen plantilla, la cual cuenta con la medida requerida y se puede editar para conservar el diseño.

4.4. Avisos

En la página principal se observa la sección de avisos que se muestra en la Figura C.15, los cuales va cambiando automáticamente.

Figura C.15 Sección de avisos

El código para modificar la sección de avisos es el que se muestra en la Figura C.16 y se encuentra en el archivo *index.php*. En el código, en el campo `src` se define la imagen a mostrar y en el campo `href` se definen los archivos o imágenes que se muestran al hacer click en la imagen.

```
<!--Avisos-->

<div class="col_full clearfix">
    <div class="fancy-title title-border">
        <h3>Avisos</h3>
    </div>

    <div class="clear"></div>

    <div id="oc-images" class="owl-carousel image-carousel">
        <div class="oc-item">
            <a target="_blank" href="http://www.administracion.ingenieria.unam.mx/CLS/">
            <img src="images/avisos/cls_ingenieria.jpg" alt="Image 1"></a>
        </div>
        <div class="oc-item">
            <a target="_blank" href="images/archivos/guia_proteccion.pdf">
            <img src="images/avisos/guia_universitaria.jpg" alt="Image 2"></a>
        </div>
    </div>
```

Figura C.16 Código de la sección de avisos

Para una mejor administración, las imágenes que se muestran en la sección de avisos se encuentran en la carpeta llamada avisos y los archivos e imágenes que se muestran cuando se da click en un aviso se encuentran en la carpeta archivos; ambas carpetas se encuentran en la carpeta images del sitio web correspondiente.

Las imágenes que de la sección de avisos deben tener una medida de 400 x 200 pixeles para que se conserve el diseño del sitio web. En la carpeta avisos hay una imagen plantilla, la cual cuenta con la medida requerida y se puede editar para conservar el diseño.

4.5. Redes sociales

En la página principal se observa la sección de redes sociales que se muestra en la Figura C.17. Esta sección solamente aparece en el sitio web del Laboratorio de Redes y Seguridad, ya que el laboratorio cuenta con su página de Facebook. Aparece un recuadro del lado derecho del sitio web en donde se muestra la página de Facebook y las publicaciones más recientes que se han hecho.

Figura C.17 Redes Sociales

Glosario

AMENAZA	Es todo aquello que intenta o pretende destruir o dañar un recurso.
API	Application Programming Interface. Es una interfaz de aplicaciones con un conjunto de rutinas que provee acceso a funciones de un determinado software.
ASP	Application Service Providers. Son una manera de adquirir externamente algunos o casi todos los aspectos de tecnologías de información que necesitan las compañías.
BIOS	Acrónimo de (Binary Input Output System), es el responsable de permitir el arranque del Sistema operativo. Para lo cual analiza a los dispositivos de entrada y salida, verifica el estado de la memoria RAM y los configura para que el sistema operativo los utilice.
COOKIE	Archivo de texto generado por el sitio web que se almacena en la computadora y contienen información relacionada con el usuario de un sitio web específico.
CPU	Unidad de Procesamiento Central es la parte central de la computadora ya que cumple con la tarea de procesar todas las funciones además de almacenar la información.
DATA CENTER	Centro de procesamiento de datos, instalación empleada para albergar sistemas de información de componentes asociados. Ofrece espacio para hardware en un ambiente controlado.
DMZ	Se refiere a una Zona Desmilitarizada o red perimetral, la cual es una red local que se ubica entre la red interna de una organización y una red externa.
FIREWALL	Dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente y resuelve si permite o bloquea el tráfico.
FORMATEAR	Operaciones realizadas con el fin de reestablecer un dispositivo que albergue datos a su estado original, borrando de forma no definitiva los datos que este contiene.
FTP	Protocolo de Transferencia de archivos entre sistemas conectadas a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

GESTOR DE ARRANQUE	Programa que carga el sistema operativo de un ordenador en la memoria. Cuando el equipo se enciende la BIOS realiza pruebas iniciales y cede el control al MBR donde se aloja el gestor de arranque.
GNU	Proyecto que promueve una manera de distribución de programas según la cual estos pueden ser copiados o modificados de forma libre o gratuita por sus usuarios.
GRUB	Programa que instala un gestor de arranque en el registro MBR lo cual permite insertar instrucciones específicas en el MBR que carga un entorno de comandos o menú de GRUB para así poder iniciar el sistema operativo que el usuario desee.
HIPERMEDIA	Conjunto de métodos o procedimientos para escribir, diseñar, o componer contenidos que tengan texto, video, audio, mapas u otros medios.
HIPERTEXTO	Herramienta de composición de textos, imágenes y videos en la que es posible en lo que es posible enlazar a un artículo que se consulte en el momento.
HOSTING	Espacio alquilado en el disco duro de un servidor, el cual tiene todos los programas necesarios para hacer funcionar cualquier servicio deseado.
HTML	Lenguaje que se utiliza para el desarrollo de páginas de internet. Es un sistema que permite ordenar y etiquetar diversos documentos dentro de una lista.
HTTP	HiperText Transfer Protocol (Protocolo de transferencia de Hipertexto) el cuál es un protocolo de red que se utiliza para publicar páginas web o HTTP. Es la base la cual se fundamenta internet o www.
HTTPS	Significa que la sesión web está usando un esquema seguro para proteger la información que está siendo transferida ya que agrega criptografía para codificar la información transmitida.
IMAP	Internet Message Access Procol el cuál es un método de acceso a correos electrónicos en un servidor sin tener que descargarlos al disco duro local.
INTERNET OF THINGS	Sistema de dispositivo o cualquier producto interconectado con cualquier otro de su alrededor. El objetivo es hacer que todos los dispositivos se comuniquen entre sí.

INTEROPERABILIDAD	Con respecto a software, se usa el término para describir la capacidad técnica de distintos programas para intercambiar los datos a través de un conjunto común de formatos de intercambio, para leer y escribir formatos de archivo, y para usar los mismos protocolos.
JSP	JavaServer Pages o Página de Servidor Java siglas en español es una tecnología que permite generar contenido dinámico en forma de documentos que incluye código en Java en páginas web, los cuales se procesan en línea para desplegar un resultado final al usuario en forma de HTML.
KERNEL	Software que consitituye una parte fundamental del sistema opertaivo, se define como la parte que se ejecuta en modo privilegiado conocido como modo núcleo. El núcleo de Linux se puede definir como el corazón del sistema operativo, es el encargado de que el software y el hardware de una computadora puedan trabajar juntos.
MEMORIA RAM	Random Access Memory es una memoria volátil, es decir, que pierde sus datos cuando deja de recibir energía, y puede acceder aleatoriamente, es decir, se puede acceder a cualquier byte de memoria sin acceder a los bytes precedentes por esta razón también se le conoce como memoria de acceso directo.
MODELO TCP/IP	Es una descripción de protocolos de red desarrollado en la década de 1970 y usado para comunicaciones en redes.
NAVEGADOR WEB	Software que permite visualizar páginas web a través de internet o en el equipo o acceder a recursos de información alojados en servidores web.
OPEN SOURCE	Código Abierto siglas en español es un término que se utiliza para denominar a cierto tipo de software que se distribuye mediante una licencia
PARTICIÓN	Nombre que recibe cada división presente en una sola unidad física de almacenamiento de datos. Cada partición tiene su propio sistema de archivos, además de que el sistema operativo interpreta, utiliza y manipula cada partición como un disco físico independiente.
PETICIÓN	Solicitud que realiza un cliente a un servidor que indica la acción que se ha de realizar para un recurso determinado.

PHP	Lenguaje de código abierto utilizado en el desarrollo web que puede ser incrustado en HTML. El código es ejecutado en el servidor y genera un HTML el cual es enviado al cliente
POP3	Post Office Protocol es el protocolo de comunicaciones extendido para leer correo electrónico. Permite descargar la información en el disco duro del cliente de forma que el servidor no retenga ninguna copia de información.
PROCESO	Instrucciones que ejecuta un microprocesador mientras lee un programa determinado, implicando a la memoria y a su contenido además de ser gestionados por el sistema operativo.
PROGRAMA	En computación es una secuencia de instrucciones escritas para realizar una tarea específica en una computadora.
PROTOCOLO	Conjunto de reglas predefinidas con el propósito de estandarizar el intercambio de información en actividades informáticas. Al seguir el mismo protocolo se garantiza la compatibilidad entre los dispositivos en los distintos puntos de un sistema.
PROXY	Equipo o software dedico que se ejecuta en un equipo de cómputo actuando como intermediario entre un dispositivo final y un servidor del cual un usuario o cliente solicita un servicio.
PUERTO	Es una interfaz a través de la cual se pueden enviar y recibir los diferentes tipos de datos.
RACK	Estructura metálica que permite sostener y almacenar un dispositivo tecnológico, este puede ser un router, un switch o cualquier clase de equipo.
REPOSITORIO	Espacio que se utiliza para almacenar información de manera digital con un software especializado en la personalización e interoperatividad.
SCRIPT	Conjunto de instrucciones escritas en código de programación donde ejecuta diversas funciones en el interior de un programa.
SERVLET	Módulos escritos en el lenguaje de programación java que se utilizan en un servidor para extender la capacidad de respuesta a los clientes y pueden ser incluidos en servidores que soporten la API de Servlet.

SHELL	Es el programa informático que provee una interfaz de usuario para acceder a los servicios del sistema operativo.
SISTEMA DE ARCHIVOS	Estructura de datos que un sistema operativo utiliza para seguir la ruta de los archivos en un disco o partición. También puede referirse a una partición o disco que se utilice para almacenamiento.
SMP	Symmetric Multi-Processing. Tipo de arquitectura de ordenadores en donde dos o más procesadores comparten una única memoria central y todos los microprocesadores compiten en igualdad por el acceso.
SSH	Secure Shell. Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente-servidor que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, el protocolo SSH cifra la sesión de conexión.
SSL	Secure Sockets Layer. Título digital que autentica la identidad de un sitio web y cifra la información que se envía al servidor, es decir establece las credenciales de una entidad en línea.
SUDO	Super User DO. Comando de los sistemas operativos Linux que permite a los usuarios ejecutar programas con los privilegios de seguridad de otro usuario.
TABLA DE PARTICIONES	Área de un disco que contiene información correspondiente a cada una de las secciones o áreas en las que esté dividido.
TELNET	Es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente con un intérprete de comandos del lado del servidor. El protocolo Tlenet se aplicaen una conexión TCP para enviar datos en formato ASCII codificados en 8 bits.
UNAM	Acrónimo de Universidad Nacional Autónoma de México
URL	Dirección específica que se asigna a cada uno de los recursos disponibles en la red con la finalidad de que estos puedan ser localizados e identificados.

VERSIÓN BETA	Periodo en donde el software está técnicamente terminado y es lo suficientemente estable para trabajar con normalidad.
VoIP	Grupo de recursos que hacen posible que la señal de voz viaje a través de internet empleando un protocolo IP, es decir se envía la voz en forma digital a través de internet.
VPS	Hosting compartido independiente con características de un hosting dedicado. Un servidor VPS es mucho más potente y flexible que un hosting compartido.
VULNERABILIDAD	Es un punto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo.
WEBMASTER	Persona que se encarga de controlar y manejar un sitio web, es el responsable del funcionamiento y que todo funcione correctamente.
WWW	Iniciales que identifican a la expresión World Wide Web, el sistema de documentos de hipertexto que se encuentran enlazados

Referencias

Artículos y libros

[1] Carretero, J. (2001). “Sistemas operativos: Una visión aplicada”. Madrid: McGraw-Hill.

[2] Comer, D. “Redes globales de información con Internet y TCP/IP”. México: Prentice-Hall.

[3] Díaz, P. & Reyes, A. (2015). “Buenas prácticas de seguridad alineadas al ISO/IEC 27002 para el aseguramiento de equipos Linux-Debian pertenecientes a un CERT” (Tesis de Licenciatura). Facultad de Ingeniería, UNAM.

[4] Kent, P. (1995) “World Wide Web: fácil”. México: Prentice Hall.

[5] López, A. & Novo, A. (2000). “Protocolos de Internet: Diseño e implementación en sistemas UNIX”. México: Alfaomega.

[6] López, M. J. & Quezada, C. (2006). “Fundamentos de seguridad informática”. México, D.F.: UNAM, Facultad de Ingeniería.

[7] Lozano, R. (diciembre 2008). “Hardening en Linux”. Revista Linux+. N° 49, p. 42.

[8] Luján, S. “Programación de aplicaciones web”. España.

[9] McFedries, P. (1996) “¡Creando una página Web con HTML fácil!”. México: Prentice Hall.

[10] Mejía, J. & Teodoro, J. (2012). “Mecanismos de seguridad para un servidor VPN en Linux en el Laboratorio de Redes y Seguridad” (Tesis de Licenciatura). Facultad de Ingeniería, UNAM.

[11] Silberschatz, Abraham. (2004). “Sistemas operativos”. México, D.F.: Limusa.

[12] Tackett, J. (2000) “Edición especial Linux”. México: Prentice Hall.

Páginas de internet

[13] “El Sistema Operativo GNU/Linux” [archivo PDF]. Recuperado el 25 de noviembre de 2018 de: http://ergodic.ugr.es/cphys/LECCIONES/linux/00.introduccion_a_linux.pdf

[14] Boral, S. (2019). “Nginx vs Apache: ¿Cuál es el mejor servidor?”. Recuperado el 28 de marzo de 2019 de: https://maslinux.es/nginx-vs-apache-cual-es-el-mejor-servidor/

[15] CATIC (octubre 2019). “Lineamientos para sitios web institucionales de la UNAM” [archivo PDF]. UNAM. Recuperado el 5 de febrero de 2018 de: https://www.visibilidadweb.unam.mx/normateca/normaunam/Lineamientos_SitiosWebInstitucionales_CATIC_Octubre2016.pdf

[16] Catoira, F. (13 diciembre 2013). “Firewall en sistemas Linux con iptables”. Recuperado el 30 de enero de 2019 de: https://www.welivesecurity.com/la-es/2013/12/13/firewall-sistemas-linux-iptables/

[17] Debian (15 septiembre 2013). “es/iptables”. Recuperado el 21 de febrero de 2019 de: https://wiki.debian.org/es/iptables

[18] Debian (2004). “Árbol de directorios”. Recuperado el 25 de noviembre de 2018 de: https://www.debian.org/releases/stable/ppc64el/apcs02.html.es

[19] Debian (9 abril 2014). “es/sudo”. Recuperado el 4 de noviembre de 2018 de: https://wiki.debian.org/es/sudo

[20] Debian. “Razones para escoger Debian”. Recuperado el 15 de julio de 2018 de: https://www.debian.org/intro/why_debian.es.html

[21] DesdeLinux (8 agosto 2016). “Cron & crontab, explicados”. Recuperado el 23 de marzo de 2019 de: https://blog.desdelinux.net/cron-crontab-explicados/

[22] Di Tommaso, L. (11 junio 2010). “Introducción a LVM”. Recuperado el 25 de enero de 2019 de: https://www.mikroways.net/2010/06/11/introduccion-a-lvm/

[23] Escalante, C. “Plan de desarrollo 2015-2019” [archivo PDF]. Facultad de Ingeniería, UNAM. Recuperado el 5 de febrero de 2018 de: http://www.ingenieria.unam.mx/planeacion/paginas/plan15_19/pdd2015-2019.pdf

[24] Geekland (18 enero 2015). “Proteger el grub con contraseña”. Recuperado el 28 de noviembre de 2018 de: https://geekland.eu/proteger-el-grub-con-contrasena/

[25] González, S. (2018). “Asegurando SSH”. Recuperado el 4 de noviembre de 2018 de: https://www.linuxtotal.com.mx/index.php?cont=info_seyre_004

[26] Gunthorpe, J. (1998). “Guía de usuario de APT”. Recuperado el 30 de enero de 2019 de: https://www.debian.org/doc/manuals/apt-guide/index.es.html http://ergodic.ugr.es/cphys/LECCIONES/linux/00.introduccion_a_linux.pdf

[27] INCIBE. “La importancia de las actualizaciones de seguridad”. Recuperado el 20 de enero de 2019 de: https://www.osi.es/es/actualizaciones-de-seguridad

[28] Juell, K., Drake, Mark. & Heidi, Erika. (5 septiembre 2018). “How to secure apache with Let’s Encrypt on Debian 9”. Recuperado el 20 de febrero de 2019 de: https://www.digitalocean.com/community/tutorials/how-to-secure-apache-with-let-s-encrypt-on-debian-9#prerequisites

[29] Let’s Encrypt. “Acerca de Let’s Encrypt”. Recuperado el 23 de marzo de 2019 de: https://letsencrypt.org/es/about/

[30] Let’s Encrypt. “Acerca de Let’s Encrypt”. Recuperado el 23 de marzo de 2019 de: https://letsencrypt.org/es/about/

[31] MasLinux (10 octubre 2018). “Las 5 distros GNU/Linux más populares”. Recuperado el 25 de abril de 2019 de: https://maslinux.es/las-5-distros-gnu-linux-mas-populares/

[32] MasLinux (23 mayo 2018). “Las 7 mejores distribuciones para servidores GNU/Linux que necesitas usar”. Recuperado el 25 de abril de 2019 de: https://maslinux.es/las-7-mejores-distribuciones-de-servidores-gnu-linux-que-necesitas-usar/

[33] NitroPC. (5 octubre 2017). “Windows vs MAC vs Linux, ¿cuál se adaptará más a lo que necesitas”. Recuperado el 30 de abril de 2019 de: https://www.nitro-pc.es/blog/windows-vs-mac-vs-linux/

[34] Qualys SSL Labs. Sitio web de SSL Labs. Recuperado el 28 de marzo de 2019 de: https://www.ssllabs.com/index.html

[35] Red Hat (2005). "Protocolo SSH". Recuperado el 4 de noviembre de 2018 de: https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html

[36] Red Hat. "Características y ventajas de Red Hat Enterprise Linux 5". Recuperado el 30 de abril de 2019 de: https://www.redhat.com/es/technologies/linux-platforms/articles/red-hat-enterprise-linux-5-features-and-benefits

[37] Red Hat "Gestión del administrador de volumen lógico". Recuperado el 21 de febrero de 2019, de: https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/logical_volume_manager_administration/ch_introduction-clvm#about_this_guide-CLVM

[38] Red Hat. "Esquema de particionamiento recomendado". Recuperado el 10 de enero de 2019 de: https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/installation_guide/s2-diskpartrecommend-x86

[39] Ruiz, P. (13 agosto 2013). "Arquitectura cliente/servidor". Recuperado el 25 de abril de 2019 de: http://somebooks.es/arquitectura-clienteservidor/

[40] Smartekh (3 abril 2012). "¿Qué es hardening?". Recuperado el 18 de octubre de 2018 de: http://blog.smartekh.com/que-es-hardening

[41] Solvetic (7 noviembre 2017). "Mejores distribuciones para servidor Linux 2018". Recuperado el 25 de abril de 2019 de: https://www.solvetic.com/page/recopilaciones/s/recopilacion/mejores-distribuciones-para-servidor-linux

[42] Symantec. "¿Qué son SSL, TLS y HTTPS?". Recuperado el 30 de enero de 2019 de: https://www.websecurity.symantec.com/es/mx/security-topics/what-is-ssl-tls-https

[43] Torres, J. (22 febrero 2017). "Maria DB". Recuperado el 28 de marzo de 2019 de: http://mariadbhistoria.blogspot.com/

[44] Vega, A. (6 abril 2017). "¿Qué es Let's Encrypt y cómo configurarlo?". Recuperado el 23 de marzo de 2019 de: https://medium.com/@alonsus91/que-es-lets-encrypt-y-como-configurarlo-dae155f62a57

[45] Velasco, R. (26 enero 2019). "Apache vs Nginx: ¿Qué servidor web debo montar este 2019?". Recuperado el 28 de marzo de 2019 de: https://www.redeszone.net/2019/01/26/apache-vs-nginx-servidor-web-2019/

[46] Villalba, B. (12 noviembre 2013). "Características y funciones del sistema operativo". Recuperado el 25 de abril de 2019 de: https://prezi.com/dlbm0nidibgy/caracteristicas-y-funciones-del-sistema-operativo/

[47] Yeraldine (19 abril 2018). "Cómo usar el comando IP". Recuperado el 30 de enero de 2019 de: https://ayudalinux.com/comando-ip/