

**POLÍTICAS DE SEGURIDAD INFORMÁTICA EN SERVIDOR LINUX PARA LA
EMPRESA ENERGIZANDO S.A.S**

**MIGUEL ANGEL MANTILLA CÓRDOBA
DANIEL FELIPE LUGO GÓMEZ
ALIX XIOMARA MEDINA**

**UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS
NEIVA
2019**



**POLÍTICAS DE SEGURIDAD INFORMÁTICA EN SERVIDOR LINUX PARA LA
EMPRESA ENERGIZANDO S.A.S**

**MIGUEL ANGEL MANTILLA CÓRDOBA
DANIEL FELIPE LUGO GÓMEZ
ALIX XIOMARA MEDINA**

**Informe final, seminario de profundización presentado como requisito de
grado para optar el título de INGENIERO DE SISTEMAS**

**Asesora
Ing. IRLESA INDIRA SÁNCHEZ MEDINA**

**UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS
NEIVA
2019**

Nota de aceptación

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Neiva, 12 de Febrero de 2019

CONTENIDO

	Pág.
1. Planteamiento del problema	12
1.1 Descripción del problema	12
1.2 Formulación del problema	12
2. Justificación	13
3. Objetivos.....	15
3.1 Objetivo general.....	15
3.2 Objetivos específicos	15
4. Estado de arte	16
5. Marco teórico	18
5.1 Iso 27000 en la seguridad informática	18
5.2 Seguridad de la información	18
5.3 Política de seguridad	20
5.4 Sistema operativo linux.....	21
6. Marco metodológico	22
6.1 Análisis de la red	22
6.2 Diseño de la red.....	23
6.1.1 Método de investigación.	23
6.1.2 Población y muestra	23

6.1.3 Instrumento.....	23
6.2 Diseño política de seguridad para el servidor linux	24
6.2.1 Compra de un equipo de cómputo.....	24
6.2.2 Ingreso del equipo de cómputo.....	24
6.2.3 Instalación del equipo de cómputo.....	24
6.2.4 Ubicación del equipo de cómputo.....	24
6.2.5 Salida de un equipo de cómputo.....	24
6.2.6 Ingreso de un usuario.....	24
6.2.7 Vacaciones de un usuario.....	25
6.2.8 Punto de red nuevo.....	25
6.2.9 Control de acceso físico o perimetral.....	25
6.3 Diseño políticas de administración de la red usuarios.....	25
6.3.1 Contraseñas.....	25
6.3.2 Contraseñas complejas.....	26
6.3.3 Varias contraseñas.....	26
6.3.4 Cuentas de usuario.....	27
6.4 Políticas de contraseña.....	27
6.5 Estado cuentas de usuario	28
6.5.1 Activos.....	28
6.5.1.1 Recursos humanos.....	28
6.5.1.2 Correo electrónico.....	28
6.6 Protección de los dispositivos	28
6.6.1 Conexión en red.....	29

6.6.2 Dispositivos extraíbles y unidades ópticas	29
6.6.2.1 Instalación de dispositivos.	29
6.7 Políticas de grupo	29
6.7.1 Equipo local.	29
6.7.2 Sitio.	29
6.7.3 Conexiones remotas.	30
6.8 Copias de seguridad	30
6.9 Diseño configuración para el servidor linux	30
6.4 Análisis de los resultados	47
6.5 Presupuesto	54
6.6 Cronograma.....	55
7. Conclusiones	56
Recomendaciones	57
Bibliografía.....	58

LISTA DE TABLAS

	Pág.
Tabla 1. La empresa Energizando cuenta con cobertura a internet	47
Tabla 2. Existe un departamento encargado de la seguridad informática	48
Tabla 3. Problemas de seguridad vinculadas a la empresa	49
Tabla 4. Problemas en los ordenadores	49
Tabla 5. Cantidad de ordenadores que se conectan	50
Tabla 6. La empresa realiza periódicamente mantenimiento	51
Tabla 7. Se realiza copias de seguridad	51
Tabla 8. La empresa capacita en la seguridad de la información.....	52
Tabla 9. La frecuencia en la preparación ante los problemas de seguridad	53
Tabla 10. Política para la seguridad de la información.....	53
Tabla 11. Presupuesto.....	54
Tabla 12. Cronograma de actividades	55

LISTA DE FIGURAS

	Pág.
Figura 1. Topología de la empresa	22
Figura 2. Diseño de la red.....	23
Figura 3. Creación máquina virtual	31
Figura 4. El tamaño de memoria.....	31
Figura 5. Disco duro	32
Figura 6. Tipo de disco	32
Figura 7. Almacenamiento del disco duro	33
Figura 8. Ubicación del archivo.....	33
Figura 9. Creación de la máquina virtual.....	34
Figura 10. Selección disco de inicio.....	34
Figura 11. Instalación ubuntu server.....	35
Figura 12. Idioma.....	35
Figura 13. Ubuntu	36
Figura 14. Interfaz.....	36
Figura 15. Interfaz y sus opciones	37
Figura 16. Continuación de la interfaz.....	37
Figura 17. Nombre en la interfaz.....	38
Figura 18. Nombre de usuario	38
Figura 19. Creación de una contraseña	39
Figura 20. Carpeta cifrada	39

Figura 21. Nueva ventana.....	40
Figura 22. Instalar sistemas.....	40
Figura 23. El SCSI3	41
Figura 24. Crear una nueva tabla	41
Figura 25. Patrocinar de forma automática el espacio libre.....	42
Figura 26. Finalizar patrocinado.....	42
Figura 27. Cambios en los discos duros	43
Figura 28. Carga la página	43
Figura 29. Opción continuar.....	44
Figura 30. Cargue y ajustes.....	44
Figura 31. Instalar actualizaciones de seguridad	45
Figura 32. Instalar DNS	45
Figura 33. Aplicación de la instalación Ubuntu server	46
Figura 34. Se continua el proceso	46
Figura 35. Instalación completa del Ubuntu Server.....	47
Figura 36. La empresa Energizando cuenta con cobertura a internet	48
Figura 37. Existe un departamento encargado de la seguridad informática	48
Figura 38. Problemas de seguridad vinculadas a la empresa	49
Figura 39. Problemas en los ordenadores	50
Figura 40. Cantidad de ordenadores que se conectan.....	50
Figura 41. La empresa realiza periódicamente mantenimiento	51
Figura 42. Se realiza copias de seguridad	52
Figura 43. La empresa capacita en la seguridad de la información.....	52

Figura 44. La frecuencia en la preparación ante los problemas de seguridad.....53

Figura 45. Política para la seguridad de la información.....54

RESUMEN

El presente proyecto pretende implementar una política de seguridad informática en servidor Linux para la empresa energizando S.A.S es una empresa que desarrolla sus actividades dentro del área de telecomunicaciones y ofrece servicios en diseño, implementación y mantenimiento de redes de telecomunicaciones, cableado estructurado e infraestructura para BTS (Base Transceiver Station) en todo el territorio Nacional Colombiano.

La metodología utilizada fue mixta, permitió analizar las preguntas propuestas en el instrumento de recolección en datos. La investigación se ejecutó en 5 personas, con diferentes cargos; analista de operación, secretaria, almacenista, auxiliares administrativos. Al concluir, la seguridad de la información es una tarea para las medianas y grandes empresas, porque es una actividad compleja, que necesita revisión oportuna.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

Ingeniería y Construcción Energizando SAS, es una empresa que desarrolla sus actividades dentro del área de telecomunicaciones y ofrece servicios en diseño, implementación y mantenimiento de redes de telecomunicaciones, cableado estructurado e infraestructura para BTS (Base Transceiver Station) en todo el territorio Nacional Colombiano. Se encuentra ubicada en la calle 1B sur # 15-25, en el municipio de Garzón, Huila. La empresa actualmente, opera en la zona sur comprendida por los departamentos de Huila, Caquetá y Putumayo. Se eligió por el motivo, que no cuenta con una política de seguridad. Tienen un servidor Linux vulnerable al robo de información, además, carece de protocolos en seguridad, que garanticen mitigar los riesgos y vulneración de la información.

Del mismo modo, los usuarios que manejan el sistema de información presentan un comportamiento inadecuado e inseguro, que vulnera los datos de todos los proyectos que están en operación. Prueba de esto, en algunas estaciones de trabajo, los usuarios tienen etiquetas adheridas sobre el escritorio o partes del equipo, con contraseña de acceso al equipo de trabajo; dejando expuesto el equipo. La información y su gestión han pasado a formar parte de la actividad cotidiana de las empresas. Los ordenadores almacenan información, la procesan y la transmiten a través de redes abriendo nuevas posibilidades, por ello cuanto mayor es el valor de la información gestionada, más importante es asegurarla.

Ante este reto, es necesario fortalecer la seguridad en las empresas con políticas y estrategias de seguridad destinadas a garantizar que toda implantación de nueva tecnología vaya acompañada de un adecuado entrenamiento y capacitación profesional y de un procedimiento de evaluación de los riesgos de seguridad para detectar vulnerabilidades y posibles amenazas de ataques.¹ Las empresas viven cada día expuesta al robo de información, asegurar los sistemas informáticos es el principal aspecto básico. En las últimas décadas del siglo XXI, las tecnologías se convierten en la técnica en seguridad. Puesto que brinda la prevención, detección de intrusos y copias de datos.

1.2 FORMULACIÓN DEL PROBLEMA

De acuerdo a esto, se formula la siguiente pregunta: ¿Cómo diseñar un protocolo de seguridad en un servidor para garantizar una adecuada confidencialidad de la información?

¹ Iniciativas Empresariales. "Seguridad Informática para Sistemas Operativos Windows y Linux en Empresas".

2. JUSTIFICACIÓN

La seguridad informática en Colombia evidencia dificultades en normas de privacidad. El estado colombiano no exige hasta ahora, una normatividad que sobreproteja la información tanto pública como privada, y esto se observa en las listas enumeradas de amenazas y acosos en internet. Por otra parte, a diferencia de las personas naturales, los sectores financieros y telecomunicaciones el apoyo es mayor. Debido a que se “supone que cuentan con un sistema optima en seguridad, que la alerta de filtraciones. Este beneficio cuenta las empresas que son conecedoras del espacio comercial, y radican en la tecnología de gama.

Sin embargo, no todas entran en esta ventaja. En un reporte por Caracol Radio, aseguran que: “(...) parece algo lejano a Colombia, los hackers y las filtraciones parecen algo del primer mundo. Sin embargo, los ataques en Latinoamérica cada día aumentan debido a la vulnerabilidad de su sistema financiero y empresarial. Fortinet, una empresa de ciberseguridad mundial, decidió realizar un estudio del panorama de la seguridad informática de Colombia, donde encontró que más del 80 por ciento de las compañías en el país poseen sistemas altamente vulnerables”.²

Las propuestas en políticas de seguridad en datos son lineamientos mínimos para controlar la divulgación de información privada. Implementar los controles requeridos previene la utilización de la misma, para fines inescrupulosos. El ministerio de trabajo en su decreto 1443 de 2014, sistema de gestión de seguridad y salud, tiene como objeto que todos los entes competentes tanto públicas como privadas, apliquen normativas en la organización, ejecución y revisión de la información.

Esta propuesta sugiere el diseño de políticas de seguridad de la información. Según la Norma ISO 27001, proporcionando oportunidad y viabilidad necesaria para que la seguridad de la información soporte y comprenda los objetivos estratégicos de la empresa, mediante la protección y fortalecimiento de su información que es primordial para garantizar la debida gestión en las distintas áreas de la empresa.

El diseño de las políticas de Seguridad demuestra el compromiso de la empresa Ingeniería y Construcción Energizando SAS hacia la seguridad de su infraestructura tecnológica y de la Información. Llevando así un autocontrol en cada una de las áreas que se manejan en la empresa y teniendo disponible un departamento en el área de las TIC.

² CONTRERAS, Nicolás. “Más del 80 por ciento de las compañías en Colombia son vulnerables a ataques informáticos”.

Con el diseño de las políticas de seguridad se logrará:

- Fomentar la cultura de seguridad, lo cual facilita la tarea de proteger sus activos tecnológicos y la información.
- Generar mayor conciencia en los funcionarios de la empresa con relación a los riesgos que pueden afectar la seguridad de la información evitando fugas de información por ataques externos.
- Promover a que los funcionarios adopten políticas, procedimientos y prácticas de seguridad definidas en la entidad, y a su vez comprendan las implicaciones, peligros y riesgos de sus acciones
- Para el buen uso de las políticas de seguridad, se debe realizar capacitaciones a los empleados para dar a conocer buenas prácticas de seguridad, durante el uso de los recursos informáticos con los que cuenta la empresa.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar políticas de seguridad informática para un servidor Linux en el sistema de información de la empresa Energizando SAS.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar el control de protocolos de seguridad que están implementados actualmente en la empresa Energizando SAS
- Diseñar un protocolo de seguridad para el servidor Linux de acuerdo a las normas de seguridad (ISO 27001)
- Capacitar pedagógicamente al personal responsable del manejo de la información, en las estaciones del trabajo. Con el fin de que manipule de forma segura la información.

4. ESTADO DE ARTE

El propósito de este apartado es acercarnos a los diversos estudios que se han realizado hacia las políticas de seguridad informática en servidor Linux. A continuación, se presentan investigaciones a nivel nacional y nivel internacional. Ya que, a nivel regional no se obtuvo datos realizados.

A nivel nacional, el proyecto titulado “Implementación de un servidor Linux”.³ De la Universidad Nacional de Colombia. Expone una investigación hacia la implementación de un servidor operativo Linux, con el ánimo de disminuir costos en el software. En un artículo titulado “Endurecimiento en el sistema operativo Linux”⁴. A través de este documento, presenta algunas maneras de endurecer a Linux desde el Kernel. Ya que, las fallas en los sistemas operativos a nivel en aplicación siguen siendo vulnerable.

En un proyecto de investigación titulado “Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, Propolsinecor”.⁵ Universidad Nacional Abierta y a Distancia, San Juan, Pasto. Presenta una investigación en una empresa que crece vertiginosamente y cada vez se hace necesario la implementación de nuevos programas de desarrollo tecnológico para el control y proyección de negocio. Por ello, el proyecto lo lleva dirigido hacia la búsqueda informativa y seguridad.

De igual forma, en una monografía de grado titulada “Diseño e implementación servidores/firewall GNU-Linux con conexión WAN”.⁶ Universidad Tecnológica de Bolívar. Cartagena de Indias, Colombia. El objetivo de este trabajo se basa en la solución hacia la red telemática que se encuentra expuesta a la inseguridad.

En una investigación, titulada “Linux: una solución de seguridad informática para pymes (pequeñas y medianas empresas)”⁷. Expresan a través de este documento, la necesidad en seguridad de red personalizada de bajo costo para las Pymes, se detectaron riesgos y por lo tanto, un servidor Firewall Linux es fundamental.

A nivel internacional, En una tesis de grado titulada “Implementación de un servidor para optimizar y administrar el uso del internet en la dirección Nacional de migración”.⁸ Ecuador. Expone la importancia que tiene el internet y el impacto que este desarrolla. Para ello, infiere en la seguridad como una problemática local.

³ CABRERA, Mario. Unidad de informática.

⁴ IBARRA, Andrea. Universidad Piloto de Colombia.

⁵ PATIÑO, Luis. UNAD.

⁶ MIRANDA, Juan y PADILLA, Wilmer. Universidad Tecnológica de Bolívar, Colombia.

⁷ MARTÍNEZ, Kelly, PACHECO, Javys y ZUÑIGA, Isaac. Universidad Tecnológica de Bolívar.

⁸ Implementación de un servidor para optimizar y administrar el uso del internet en la dirección Nacional de migración

En una investigación, titulada “Seguridad Linux”⁹. En buenos Aires. Argentina. Nos presenta un programa de estudio en forma de aprender y atacar preventivamente los sistemas en servidores Linux. Además, de definir reglas, ataques, etc. En un artículo titulado “Seguridad básica en Linux”¹⁰. España. Presenta algunas técnicas sencillas para proteger los sistemas Linux. Ya que, la seguridad en una entidad es dispensable para la confidencialidad en los datos.

9 Educación IT

10 Ministerio de Educación, Cultura y Deporte. Gobierno de España.

5. MARCO TEÓRICO

En este apartado se intentará abordar el tema de la seguridad de la información, política de seguridad, sistema operativo Linux. Esto se apoyará de autores, estudios e investigaciones con base al tema.

5.1 ISO 27000 EN LA SEGURIDAD INFORMÁTICA

El sistema de gestión en seguridad informática es un proceso sistemático, que se considera con calidad en la normatividad ISO 27000. Esta funciona con el propósito de garantizar riesgos de la seguridad en la información sea conocida y organizada. Según las ISO 27000 “La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización”.¹¹

De la misma manera, se le atribuye sus bases en la confidencialidad, integridad, y disponibilidad. Puesto que, garantiza el control de la información y realizan un control documentado de tal proceso. Con el uso de las ISO, la legalidad de la información será puntual. La protección adecuada de las empresas tendrá beneficios y herramientas de utilidad. Los alcances proporcionaran riesgos mínimos pero la organización influenciara considerablemente. En cuanto a las políticas de seguridad representativas, se encuentran:

- **Políticas de password y cuentas:** Se utiliza para el bloqueo de la información.
- **Políticas generales de seguridad** finalidades, responsabilidades.
- **Autenticación:** Los mecanismos de confianza.
- **Mantenimiento:** Relacionados a la tecnología.

5.2 SEGURIDAD DE LA INFORMACIÓN

En la información existe diversas formas de comunicación con la creación de herramientas virtuales, ha permitido a manera global interactuar por medio de las redes, como es el correo, los medios electrónicos, las imágenes impresas, entre otros. En una empresa, la seguridad informática es vital, garantiza la confidencialidad, integridad y disponibilidad en la información.

¹¹ ISO 27000. Recuperado de <http://www.iso27000.es>

Según la universidad Libre de Bogotá: “La seguridad de la información está definida como todas las medidas preventivas y de reacción del individuo, la organización y las tecnologías, para proteger la información; buscando mantener en esta la confidencialidad, la autenticidad e Integridad”¹². De acuerdo a esto, las compañías sean comerciales o no, entre sus objetivos normativos, la seguridad de la información es necesaria para salvaguarde los datos. Hoy los hackers son los principales problemas en las redes. Cuando no se protege adecuadamente la ciberseguridad ocasiona la exposición y pérdida de la información. Estos ataques no paran y las empresas viven cada día episodios de “tormento”. En cuanto a los efectos negativos los ciberataques, alteran la seguridad nacional, regional e internacional, hasta la propia empresa. Por otro lado, la competencia mundial, implica que las grandes compañías cuenten con sistemas, recursos y plataformas TIC eficaces, con alto rendimiento durante los procesos de la transformación digital.

En un estudio de la Universidad Rey Juan Carlos, expresa que: “Son muchas las áreas en las que evolucionan la sociedad y empresa, pero uno de los ámbitos en los que estos cambios se producen, de forma más rápida y constante, es, precisamente, el área tecnológica. El cambio tecnológico supone una modificación constante en la forma de hacer las cosas, las herramientas que se utilizan y el enfoque de cualquier negocio”.¹³

Desde este punto de vista, las entidades encargadas del ámbito empresarial, tiene el deber de retroalimentar las áreas de sistemas de sus empresas. Para así mismo, evitar que la información confidencial salga de los parámetros privados en la red. Por ello, es preciso que los entes comerciales conozcan el manejo de su seguridad. Los principios fundamentales que se basa toda red de seguridad informática se enfocan en la protección de la infraestructura computacional. Ocupándose del diseño en normas, procedimientos, métodos y técnicas que mantienen el sistema seguro y confiable.

El sitio web conocimiento digital, opinan que la historia de la seguridad informática comienza a partir de los años 80 con lo común que era usar un computador personal y la preocupación por conservar la integridad de los datos almacenados. De aquí en adelante se empiezan a producir los virus y gusanos más exactamente en los años 90, donde se crea una alerta para los ordenadores y la conexión a internet, empezando a identificarse ataques a sistemas informáticos, comenzándose a definir la palabra Hacker, a final de los 90 las amenazas empezaron a generalizarse, aparecen nuevos gusanos y malware generalizado, ya a partir del año 2000 los acontecimientos hacen que se tome muy en serio la seguridad informática.¹⁴ Con base en esta expresión, la seguridad informática empezó creando alternativas hacia las incertidumbres del internet, para luego llegar a ser la medida más técnica de la sociedad mundial.

¹² Universidad Libre de Bogotá. Seguridad de la información.

¹³ GÓMEZ, Jesús. “Programas de apoyo a los cambios tecnológicos”.

¹⁴ Conocimiento Digital.

5.3 POLÍTICA DE SEGURIDAD

Como se mencionaba en apartados anteriores, la seguridad de la información emplea un conjunto en controles, prácticas y procedimientos organizacionales, en función del software. Cuando este mecanismo se apoya en las políticas de seguridad, hace de la práctica más factible. Según un blog de emprendimiento: “Las políticas de seguridad son un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa. Se trata de una especie de plan realizado para combatir todos los riesgos a los que está expuesta la empresa en el mundo digital. De esta forma mantendremos nuestra organización alejada de cualquier ataque externo peligroso”.¹⁵

Desde otra perspectiva, en el sitio web Emprede pymes, definen que: “es el documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información”.¹⁶

Las políticas de seguridad es un documento único y dirigido al manual de seguridad. En él, se encuentra las normas, estamentos y entes que integra todo funcionamiento para actuar en caso de riesgos, en pérdida de confidencialidad. Además, se compone de varios pasos, como son: el desarrollo de la política (requerimientos legales, regulaciones, alcances, aplicabilidad, etc.), la revisión (documentación creada y revisión) y la aprobación (el apoyo de la administración).

En el campo de las tecnologías en Colombia, aún se encuentra deficiencias. Con la implementación de las políticas de información, los espacios en el país se fortalecerán. Las capacidades en el entorno digital, será más responsable al momento de interactuar con otras redes. El concejo nacional de política económica y social apoya de esta estrategia, porque permite que se incorpore las TIC y la participación ciudadana sea numerosa. Para el MINTC, “En esta política se establecen nuevos lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación”.¹⁷

Con los medios computacionales, las áreas de la información se han preocupado por integrar diferentes tipos de software, como es el caso del Linux. Con sistemas operativos del Linux, las funciones de las políticas de seguridad previenen la integridad de la información. Con el Linux, las computadoras intuyen a sus usuarios las páginas inseguras al momento de navegar. Dependiendo de ciertas limitaciones, las características típicas que los usuarios podrían esperar de esta aplicación serían las alertas inapropiadas y peligrosas en la web.

¹⁵ Emprede pyme.net.

¹⁶ SIGEPRE. “Manual de políticas de seguridad de la información”. p.11

¹⁷ Ministerio de Tecnologías de la Información y las Comunicaciones.

5.4 SISTEMA OPERATIVO LINUX

Se conoce directamente por ser un sistema operativo de Windows. Necesario para los ordenadores que utilizan diferentes programas y navegaciones poco seguras. Se utiliza mediante un interfaz gráfico y también por la línea de comandos. Así lo enuncia un sitio web “Linux es un sistema operativo, compatible Unix, dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado, la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado al código fuente”¹⁸.

Sus orígenes se remota ha estudios de informática en el año 1991, por el estudiante Linus Torvalds quien propuso un sistema operativo que se comporte al Unix. Pero esta propuesta implicaba que Linux funcionará sobre cualquier ordenador compatible PC. Un factor primordial en esta teoría era que Linux, expandiría el internet. Debido a ello, facilitó el trabajo en equipos y apporto a todos los programas. Para la fecha del 5 de octubre del 91, el Linux lanza su primera versión 0,02 ejecutada en dos herramientas básicas de GNU.

Hoy el Linux es clónico del UNIX, viene completo y el nivel de aceptación es enorme. La importancia del Linux predomina en las grandes empresas. La ventaja de este sistema operativo es que sus costos son menores. La mayoría de las oficinas lo ejecutan por su rápida calidad en la web y los ordenadores. Cuando un computador posee un Linux, ya sea en teléfonos mediante Android protege y asegura la información. Y de la misma forma, el software queda libre de basura.

El Linux también se caracteriza por ser un código abierto, destinado para la comunidad de desarrolladores en diseños de ordenadores. Debido a esto, existen muchos tipos diferentes de sistemas operativos Linux. Algunos de ellos son:

- **Ubuntu:** Se considera el más popular dentro de grupo Linux.
- **Kubuntu:** Es similar al Ubuntu en funcionamiento, su diferencia se caracteriza en el sistema de archivos.
- **Debian:** Es una versión más complicada del sistema operativo Linux.
- **Fedora:** Es un ejemplo de distribución Linux. Se utiliza más en computadoras antiguas.
- **Linux Mint:** Es una versión modelada después de Ubuntu. Tiene una funcionalidad limitada cuando se instala.

¹⁸ www.juntadeandalucia.es

6. MARCO METODOLÓGICO

En este capítulo se explicará la metodología utilizada en el desarrollo del presente trabajo de grado. se expondrá de forma detallada cada una de las fases que conformaron la investigación.

6.1 ANÁLISIS DE LA RED

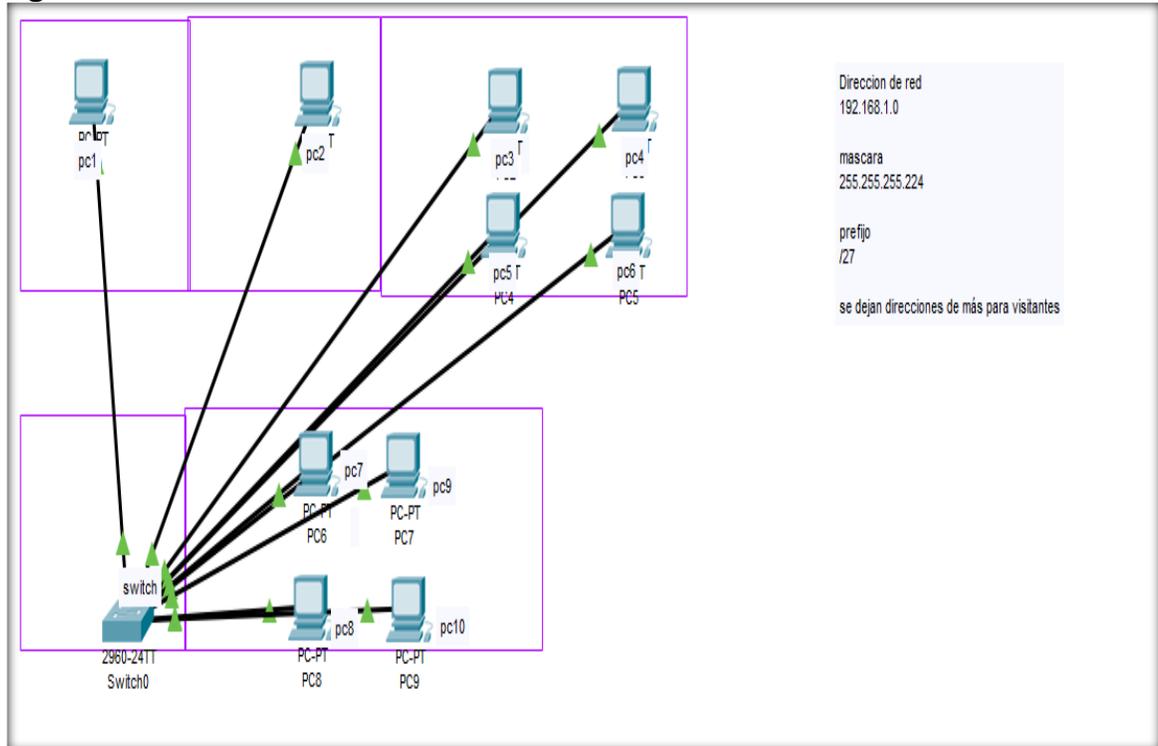
Figura 1. Topología de la empresa



Fuente: Energizando S.A.S

6.2 DISEÑO DE LA RED

Figura 2. Diseño de la red



Fuente: Energizando S.A.S

6.1.1 Método de investigación. La metodología aplicada para este proyecto fue mixta. Por qué se combinó ciertos métodos cualitativos y cuantitativos, que permitió que la investigación fuera profunda en el análisis de las preguntas propuestas en el instrumento de recolección en datos.

6.1.2 Población y muestra. La investigación se ejecutó en 5 personas, con diferentes cargos; analista de operación, secretaria, almacenista, auxiliares administrativos. Entre las edades de los 20 a 40 años. Se tuvo en cuenta las observaciones en la empresa y el análisis de la red.

6.1.3 Instrumento. En función de los objetivos planteados en la presente investigación, se diseñó una encuesta que permitió obtener la información requerida para los fines propuestos. La encuesta que sirvió como herramienta pertinente, estuvo compuesta por 10 preguntas tipo abiertas como cerradas.

6.2 DISEÑO POLÍTICA DE SEGURIDAD PARA EL SERVIDOR LINUX

6.2.1 Compra de un equipo de cómputo. Para la compra de un equipo de cómputo, se debe tener en cuenta para quien va a ser asignado el equipo, que uso le va a dar, en que área de la organización se va a instalar, con referencia a lo anterior se hace un presupuesto para presentar a la organización.

6.2.2 Ingreso del equipo de cómputo. Una vez adquirido el equipo de cómputo se lleva a activos fijos, donde se va a añadir al inventario, para esto se debe tener en cuenta las características del equipo como: Seriales, Modelo, Tipo de equipo de cómputo y el respectivo recibo de la compra del mismo.

6.2.3 Instalación del equipo de cómputo. Una vez hecho el respectivo ingreso del equipo de cómputo, el área de sistemas analiza las funciones que va a realizar el usuario quien se le va a asignar. Una vez hecho el análisis se configura el equipo y se asigna tanto el perfil del usuario y el de navegación web.

6.2.4 Ubicación del equipo de cómputo. Una vez realizado a la perfección el paso anterior, el técnico de sistemas procede a realizar el chequeo de la IP y el punto de red donde se va a dirigir el equipo. Se realiza una ficha técnica y un acta donde se responsabiliza el usuario a tener el perfecto estado el equipo. Luego de esto, el técnico realiza el traslado e instalación del mismo en el área correspondiente.

6.2.5 Salida de un equipo de cómputo. Cuando se le va a realizar la respectiva salida, los del área de sistemas son aquellos quienes realizan la eliminación de toda la información y un acta donde se da de baja al equipo de cómputo con sus respectivos motivos de la salida del mismo.

6.2.6 Ingreso de un usuario. Al ingresar un usuario a una organización, la primera área a donde debe pasar es el área de recursos humanos, donde se hace la contratación, asignación de funciones y horario que tendrá dentro de la organización. Todos estos datos recolectados por el área de recursos humanos son compartidos con el área de sistemas para la asignación del equipo de cómputo, creación de usuario y navegación web.

6.2.7 Vacaciones de un usuario. Cuando el área de recursos humanos valida el tiempo de vacaciones, informa al área de sistemas, para que el usuario quede deshabilitado por el periodo que este en vacaciones.

6.2.8 Punto de red nuevo. Se hace un chequeo de la disponibilidad de puerto libres que haya en el switch y patch panel y la cantidad de metro, además de esto el tipo de ambiente por el que pasará el cableado y se realizara la respectiva instalación del punto de red.

6.2.9 Control de acceso físico o perimetral. Como son oficinas donde constantemente ingresan usuarios, se deben cerrar, no se deben dejar solas.

- Para la entrada de los usuarios a las instalaciones, se tiene el acceso biométrico, el cual para ingresar es mediante la huella, o foto donde queda registrada la hora de ingreso y salida; para tener un mejor control.
- Además se cuenta con alarma dentro de las instalaciones en caso de que ocurra una emergencia, o infiltraciones de personas diferentes a usuarios de la empresa
- Se cuenta con un cuarto especial, de acceso biométrico donde se procede a guardar la información relevante de la empresa; solo hay una persona encargada de realizar dicha labor.

6.3 DISEÑO POLÍTICAS DE ADMINISTRACIÓN DE LA RED USUARIOS

6.3.1 Contraseñas. Políticas de contraseñas sencillas; se desea configurar una política de contraseñas con las reglas siguientes:

- Se pueden reutilizar las contraseñas. No se desea conservar un historial de contraseñas.
- Una contraseña debe contener al menos ocho caracteres con al menos un número.
- Si alguna vez se restablece la contraseña de un usuario, se desea que el usuario cambie la contraseña inmediatamente después del primer inicio de sesión.
- Si no se utiliza una contraseña durante 60 días, se desea que se suspenda la cuenta.

Para configurar esta política, establezca las siguientes reglas de contraseña:

- set password-policy = true;
- set password-min-length = 8;
- set password-numeric = 1;
- set password-force-change = true;
- set password-last-use = 60;

6.3.2 Contraseñas complejas. El arquitecto de directorio ha creado la siguiente política de contraseñas sin formato en inglés:

- Las contraseñas deben contener al menos siete caracteres, donde al menos tres caracteres deben ser caracteres alfabéticos y al menos tres caracteres deben ser caracteres numéricos.
- Ninguna contraseña puede contener el nombre de usuario.
- Las contraseñas son válidas durante un máximo de 14 días.
- Las contraseñas deben tener al menos un día de antigüedad antes de poder cambiarlas para evitar que los usuarios cambien su contraseña varias veces para llenar el historial de contraseñas.
- Después de que haya caducado la contraseña, los usuarios todavía pueden iniciar sesión dos veces, para darles la oportunidad de cambiar la contraseña.
- Después de tres intentos incorrectos en el inicio de sesión, la cuenta se suspende durante 30 minutos. Después de este período, el usuario puede intentar volver a iniciar sesión.

6.3.3 Varias contraseñas. Un único agente de sistema de directorio contiene dos tipos de usuarios: los usuarios y los administradores. Cada tipo de usuario tiene su propia política de contraseñas. La política predeterminada contiene valores de configuración que son comunes a las dos políticas. Sin embargo, algunos de estos valores se sobrescriben.

El arquitecto del directorio ha creado la siguiente política de contraseñas:

- Ninguna contraseña puede contener el nombre de usuario.
- Los dos tipos de usuarios tienen longitudes mínimas diferentes para las contraseñas.
- Administradores, al menos 12 caracteres
- Usuarios: al menos 8 caracteres
- Las contraseñas de administrador deben contener al menos dos números y al menos una letra mayúscula.
- Los usuarios deben cambiar sus contraseñas al menos cada 30 días.

6.3.4 Cuentas de usuario. Una cuenta de usuario es una colección de información que indica al sistema operativo los archivos y carpetas a los que puede tener acceso un determinado usuario del equipo, los cambios que puede realizar en él y sus preferencias personales, como el fondo de escritorio o el protector de pantalla.

Para la cuenta de usuario, esta se crea por la primera letra del primer nombre del usuario, seguidamente la primera letra del segundo nombre y el primer apellido, dado el caso la persona que no tenga segundo nombre, se pondrá la segunda letra inicial del primer apellido y seguidamente el segundo apellido. De igual manera los que coincidan, se agregara la segunda letra del primer apellido para la creación de la cuenta de usuario. Como por ejemplo:

Miguel Angel Mantilla Cordoba =mamantilla

6.4 POLÍTICAS DE CONTRASEÑA

En las políticas de las contraseñas como mínimo deben tener 8 caracteres y un máximo de 12, de igual manera debe obtener: letras mayúsculas, minúsculas, símbolo y números. Como por ejemplo:

* mamantilla =Mantill@2017

Al usuario se le solicitara hacer cambio de contraseña cada 6 meses, para ingresar al sistema y por lo tanto no podrán asignar claves anteriores.

6.5 ESTADO CUENTAS DE USUARIO

Son aquellos usuarios que no tienen accesibilidad al servidor durante un tiempo asignado como:

- **Inactivo permanente:** Es aquel usuario retirado de la empresa pueda ser por despido o finalización de contrato. Este usuario quedaría desactivado totalmente del servidor.
- **Horario laboral:** Es aquel que queda deshabilitado del servidor cuando finaliza su horario de trabajo.
- **Incapacidad o vacaciones:** El usuario queda desactivado durante el tiempo que se encuentre en incapacidad o vacaciones que le asigne recursos humanos.

6.5.1 Activos. Son cuentas de empleados que se encuentran habilitados, como:

6.5.1.1 Recursos humanos. Es encargado de informar al área de sistemas el horario establecido del empleado para así mismo designar el horario en que el usuario pueda tener acceso a funciones del servidor.

6.5.1.2 Correo electrónico. El correo electrónico que se maneja en la empresa energizando SAS, es institucional y su uso debe ser relacionado solo laboral.

- Este correo no debe ser utilizado para asuntos personales
- No se debe acceder al correo electrónico de dispositivos no registrados por la empresa.
- Se debe realizar el cambio de contraseñas periódicas.

6.6 PROTECCIÓN DE LOS DISPOSITIVOS

Estos dispositivos son nombrados por las tres primeras letras de la ciudad en donde se encuentre instalado el equipo y el grupo de trabajo, luego las dos primeras letras de la sede donde se encuentra y un número asignado de acuerdo al perfil del usuario correspondiente al equipo, estos números corresponderán del 01 al 15 para los jefes de cada área de la empresa, del 16 al 20 a funcionarios y del 21 al 50 a practicantes de la empresa.

6.6.1 Conexión en red. El usuario trabajara en el lugar asignado, ya que es donde tiene el punto de red asignado y cada punto de acceso tiene su respectiva configuración, todo esto de acuerdo al rol que ejerza el usuario del área, dado el caso que el usuario de cualquier área quiera conectarse desde otra, este no tiene acceso.

6.6.2 Dispositivos extraíbles y unidades ópticas. Los equipos de cómputos tienen deshabilitado la unidad óptica, en dado caso que algún usuario lo requiera, debe solicitarlo al área de recursos humanos para que envíe la solicitud a los de sistemas.

6.6.2.1 Instalación de dispositivos. Corregir los usuarios que requieran de instalar un dispositivo, estos no lo podrán hacer, puesto a que se tiene deshabilitado esta opción, si requieren de la instalación de alguno, deberán solicitarlo al área de recursos humanos para que informe a los de sistemas.

6.7 POLÍTICAS DE GRUPO

Las GPO permiten administrar objetos de usuarios y equipos, aplicando la más restrictiva en caso de existir más de una política. Se usa una GPO para casi cualquier cosa, como indicar qué usuario o grupo tiene acceso a una unidad de disco, o limitar el tamaño máximo que puede tener un archivo. Las GPO se pueden diferenciar dependiendo del objeto al que configuran y se pueden entender en distintos niveles:

6.7.1 Equipo local. los equipos están registrados dependiendo del área de trabajo, los usuarios no podrán acceder a la red por equipos diferentes. Los usuarios podrán acceder a las aplicaciones desde su área de trabajo.

6.7.2 Sitio. Se aplican a los equipos y/o usuarios de un sitio.

Dentro de la configuración de directiva se puede acceder a lo siguiente:

- Configuración de equipo
- Configuración de usuario

Las áreas de la empresa tienen una carpeta compartida, donde no se permite un archivo mayor a 1 GB, el espacio máximo de almacenamiento será de 50 GB por área.

6.7.3 Conexiones remotas.

- Para las conexiones remotas, se debe hacer aprobación por el personal de sistemas encargado.
- Se deberá tener códigos para realizar esta conexión.
- Solo se realizará conexiones remotas de dispositivos de la empresa los cuales estén registrados.
- Se contará con un tiempo estipulado para dichas conexiones.

6.8 COPIAS DE SEGURIDAD

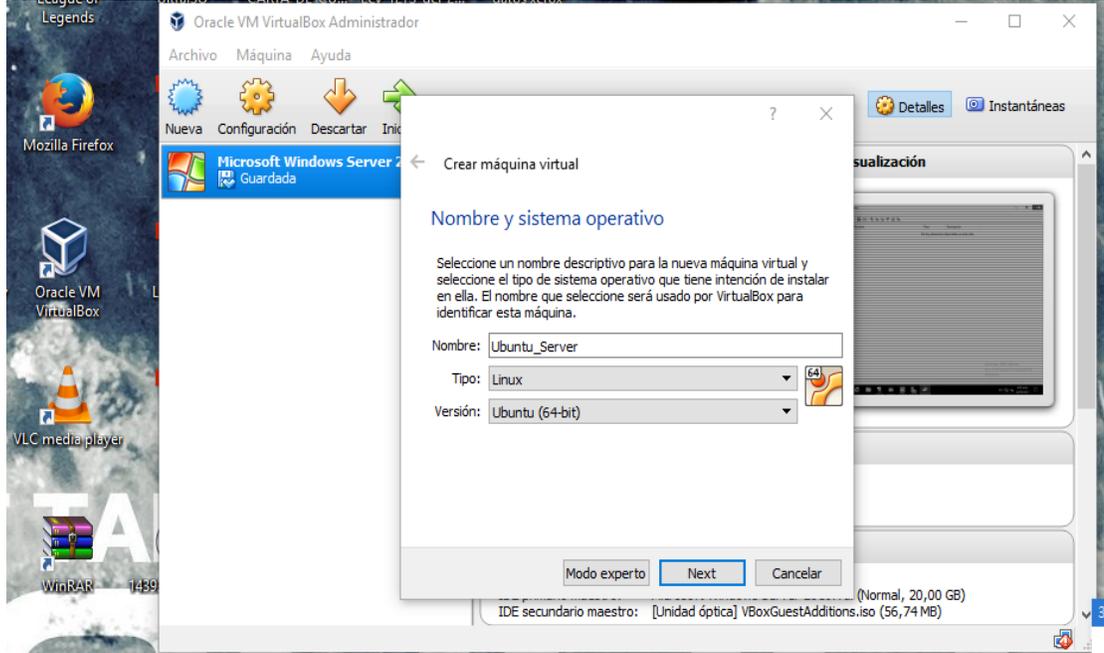
Las copias de seguridad se realizarán por cada una de las áreas, las cuales se efectuarán todos los días a las 7:00 A.M., Estas copias se almacenarán en un disco externo que se conecta por USB, los cuales se guardaran en un cuarto, donde ningún usuario diferente al encargado podrá tener acceso.

6.9 DISEÑO CONFIGURACIÓN PARA EL SERVIDOR LINUX

Como primer paso a realizar en la instalación de Ubuntu Server, es abrir la ventana máquina virtual, en este caso VirtualBox. Al tener abierto la máquina virtual damos clic en “Nueva”.

Una vez dado clic, nos arrojará una ventana llamada “Crear máquina virtual”, en el campo Nombre, pondremos nuestro servidor “Ubuntu_Server”. Luego, en Tipo pondremos Linux y en Versión Ubuntu de 64 bits según la arquitectura del computador. Una vez identificada la versión y haber llenado de forma correcta los campos, se dará clic “Next” como se muestra en la Figura 3.

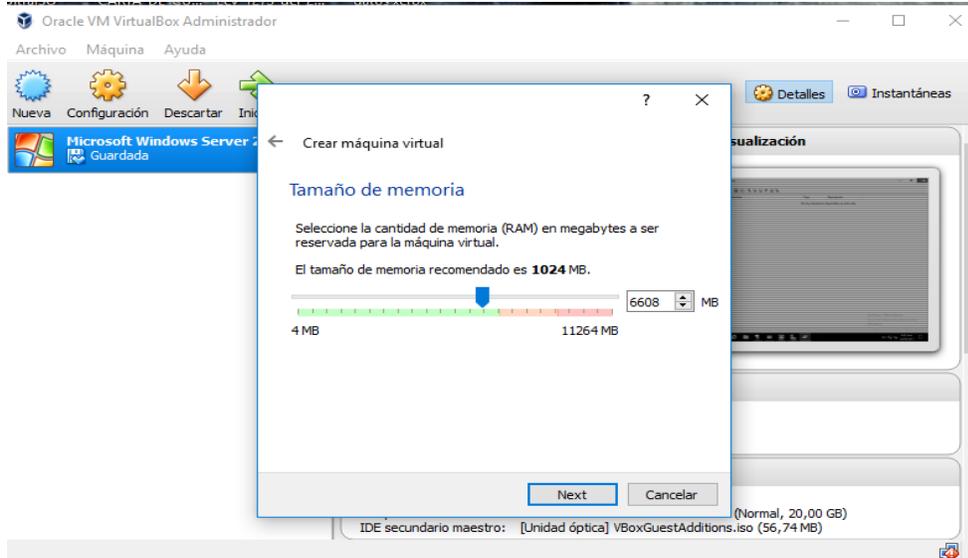
Figura 3. Creación máquina virtual



Fuente: Autores

Una vez dado clic en “next”, se pedirá el tamaño de memoria en donde se le asignará el tamaño requerido para lo que va a ser utilizado, el servidor y luego se da clic en “next”; como se muestra en la Figura 4.

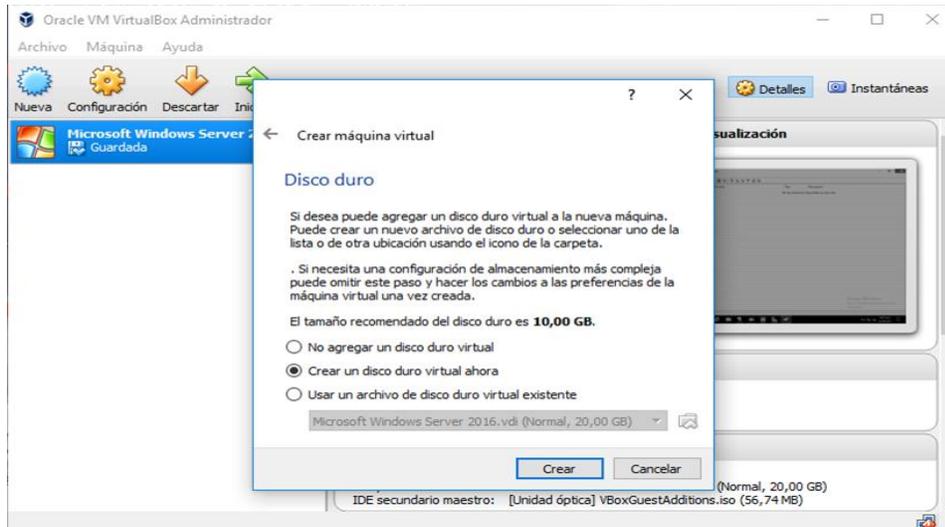
Figura 4. El tamaño de memoria



Fuente: Autores

Una vez haber culminado con el paso anterior, se da clic en la opción “crear un disco duro virtual ahora”, y nuevamente clic en “crear”. como se muestra en la Figura 5.

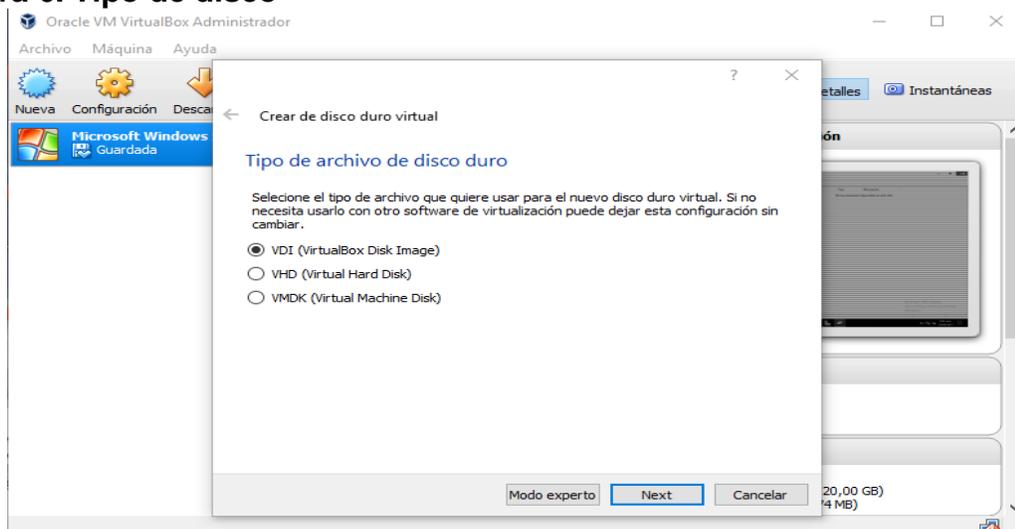
Figura 5. Disco duro



Fuente: Autores

Después del paso anterior, se selecciona el tipo de archivo de disco duro, como ya se venía mencionando, se monta un disco virtual, se escoge la opción de “vdi (virtualbox disk image)”, una vez seleccionado se da clic en “next”. como se muestra en la Figura 6.

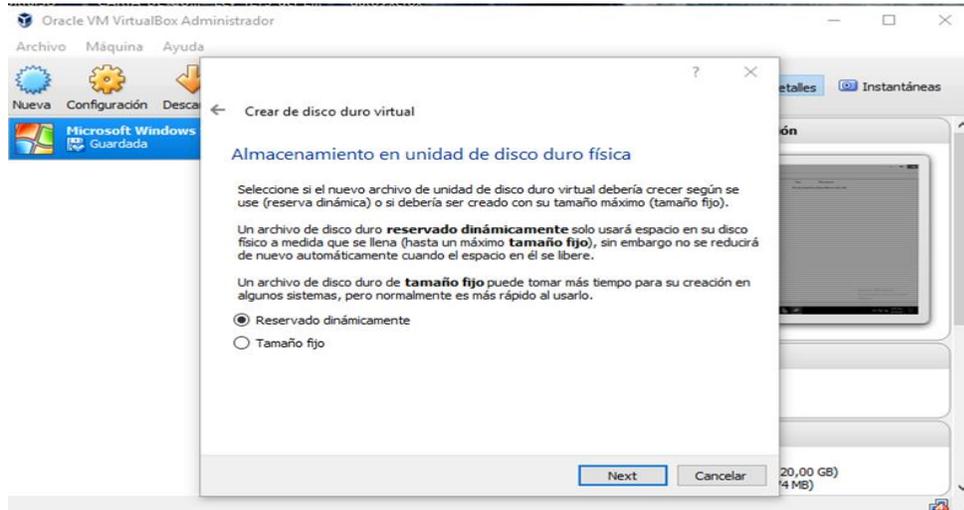
Figura 6. Tipo de disco



Fuente: Autores

A partir de lo anterior, se arrojará la siguiente ventana, en donde el almacenamiento de unidad de disco duro física, lo vamos a dejar en la opción de “reservado dinámicamente” y se da clic en “next”. como se muestra en la Figura 7.

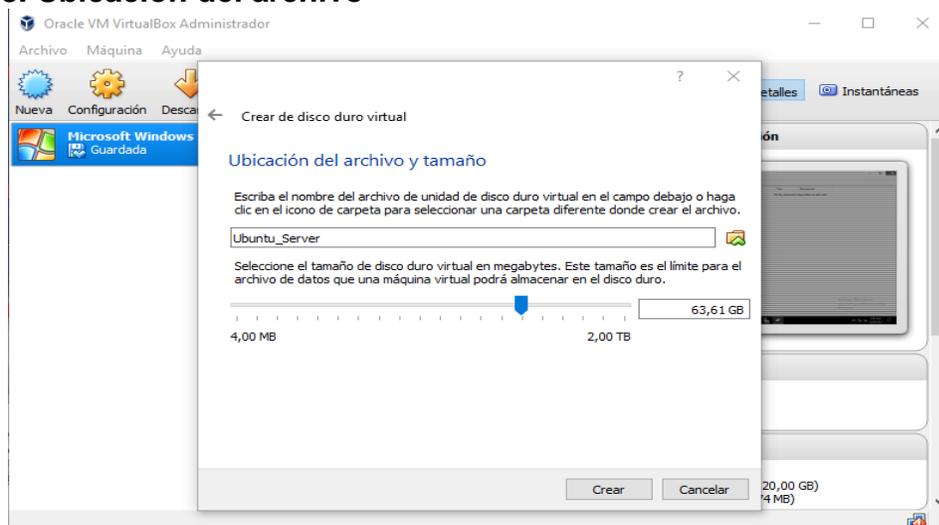
Figura 7. Almacenamiento del disco duro



Fuente: Autores

Al saltar a este paso, vamos se da clic en “crear”, y si se desea más espacio en disco duro, se asigna el tamaño que se requiera y damos clic en “crear”. como se muestra en la Figura 8.

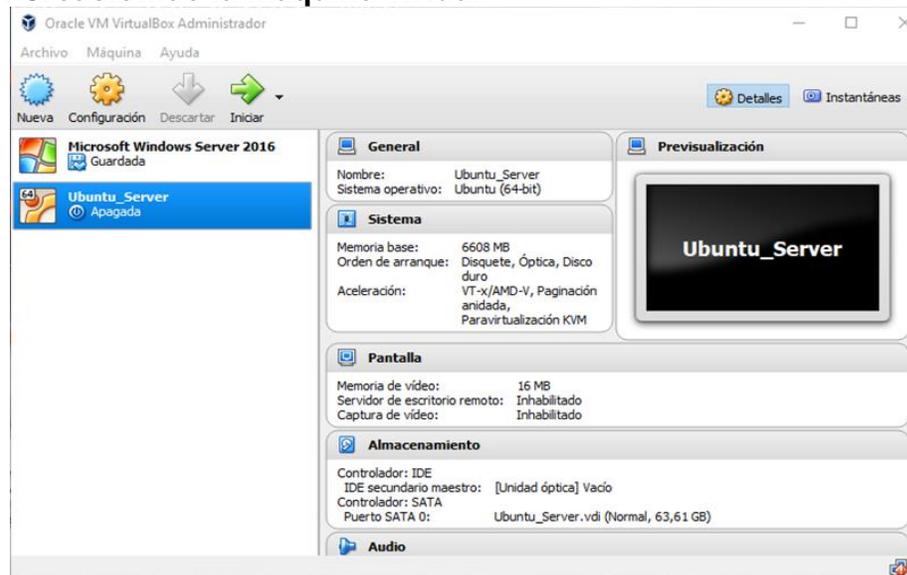
Figura 8. Ubicación del archivo



Fuente: Autores

Al dar clic en “crear”, en el paso anterior, ya nos quedara creada nuestra máquina virtual. como se muestra en la Figura 9.

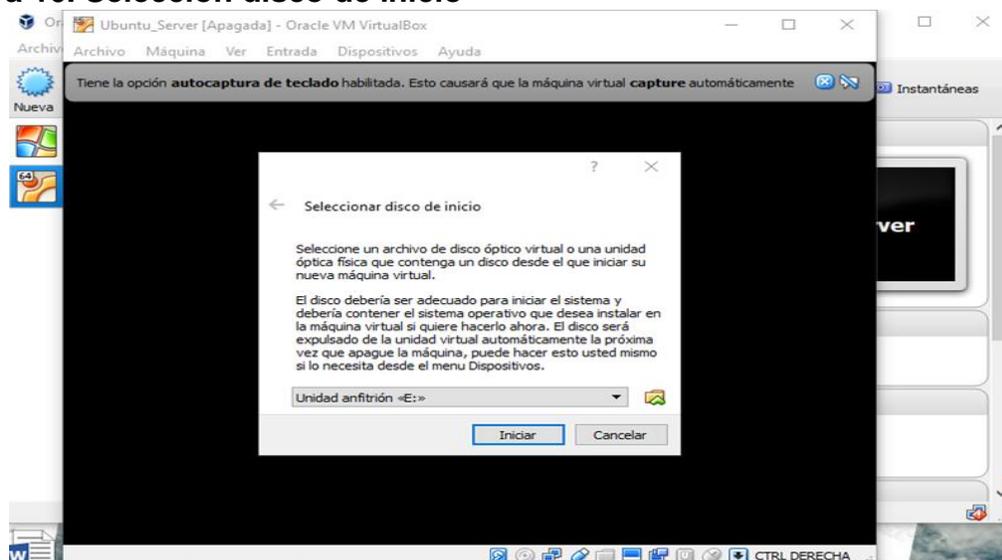
Figura 9. Creación de la máquina virtual



Fuente: Autores

Al tener creada la máquina virtual, se da clic en “Iniciar” y aparecerá lo siguiente. como se muestra en la Figura 10.

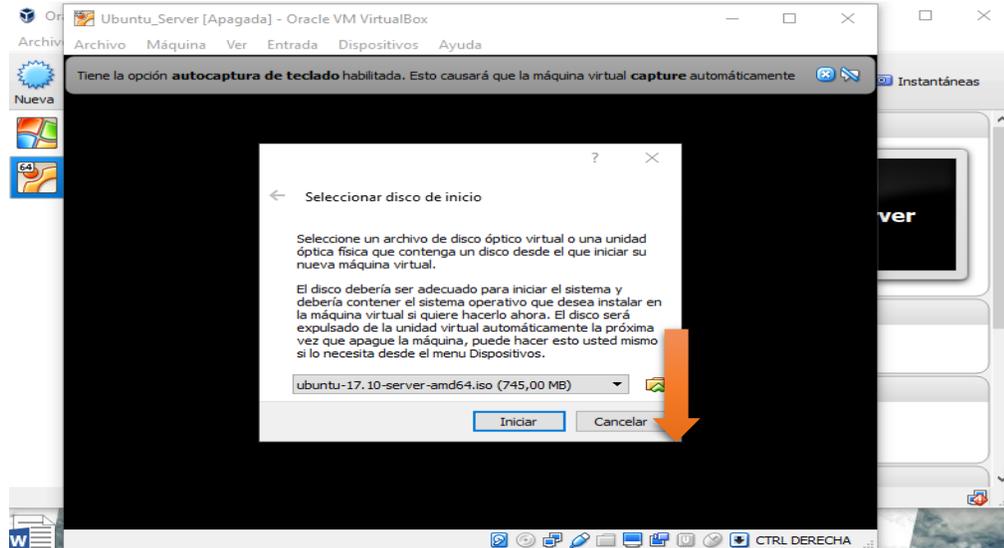
Figura 10. Selección disco de inicio



Fuente: Autores

Una vez abierta la nueva ventana, se dirige al icono de la carpeta nuestra imagen ISO, y posteriormente dar clic en “iniciar” para iniciar con la instalación de ubuntu server. como se muestra en la Figura 11.

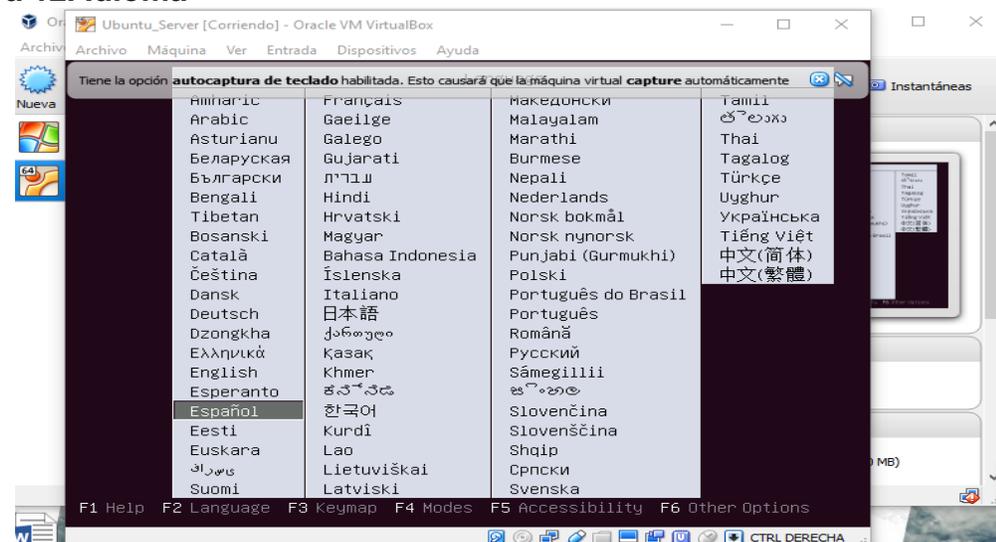
Figura 11. Instalación ubuntu server



Fuente: Autores

Una vez culminado el paso anterior, se escoge el idioma y se presiona la tecla “enter”. como se muestra en la Figura 12.

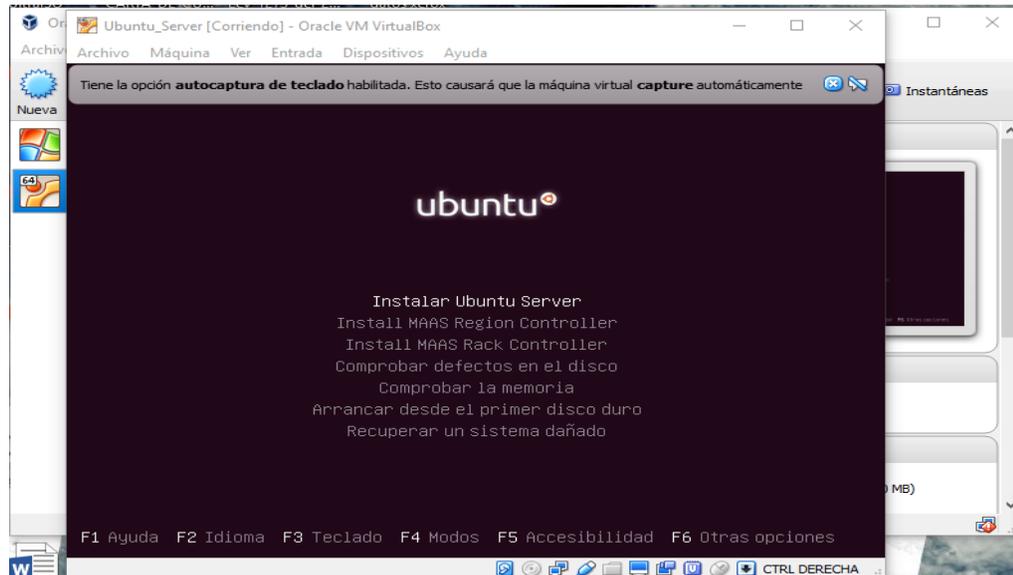
Figura 12. Idioma



Fuente: Autores

Ya realizado lo anterior, saldrá la pantalla siguiente, donde se dará “enter” en “instalar ubuntu server”, como se muestra en la Figura 13.

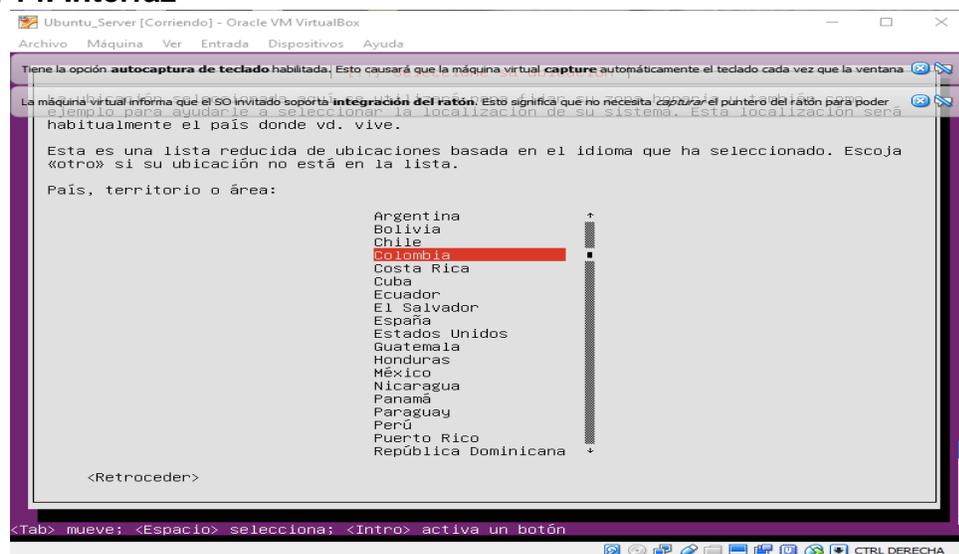
Figura 13. Ubuntu



Fuente: Autores

El siguiente paso, arrojará la siguiente interfaz, donde se escoge el país, casa “Colombia”. como se muestra en la Figura 14.

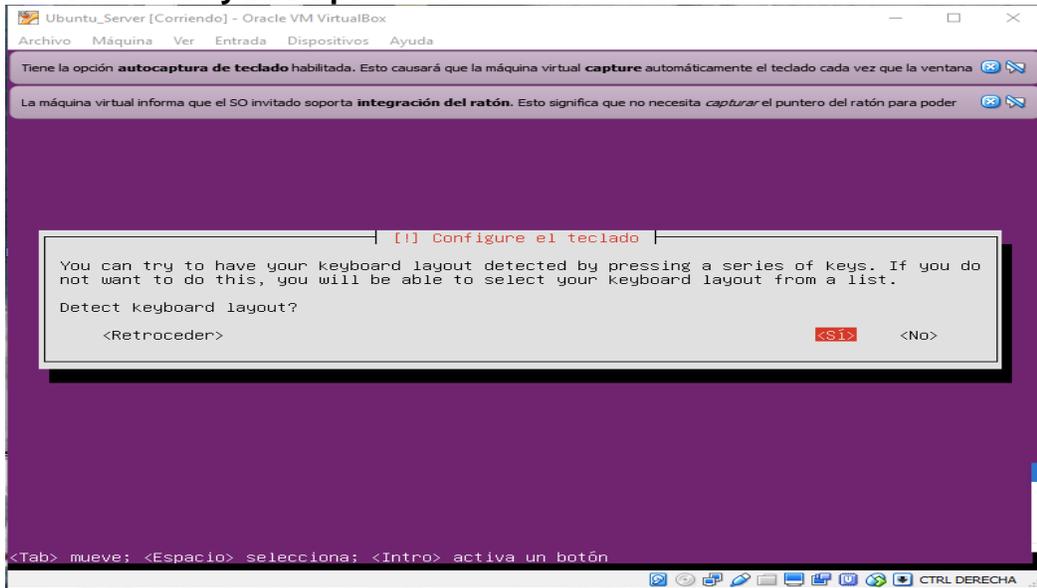
Figura 14. Interfaz



Fuente: Autores

Una vez al pasar a la siguiente interfaz, escogeremos la opción “SI” y presionamos “ENTER”. como se muestra en la Figura 15.

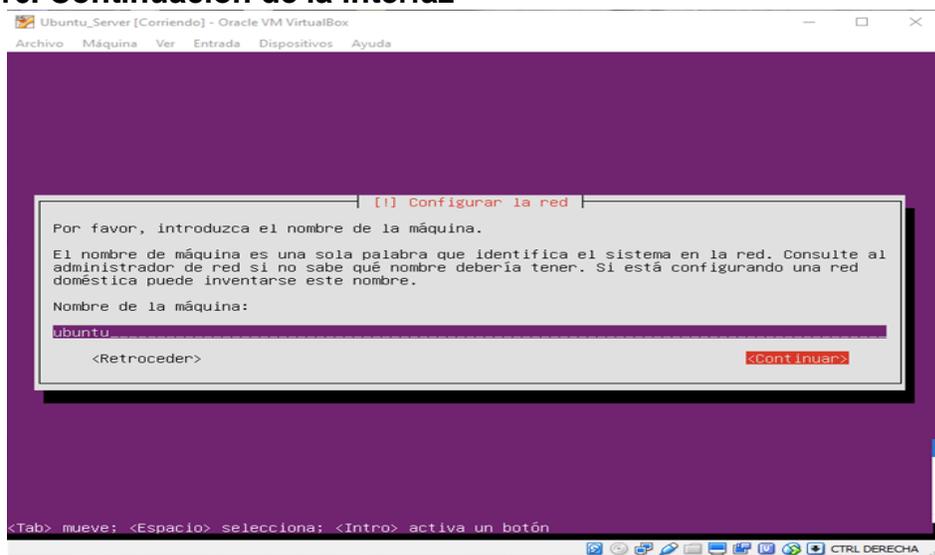
Figura 15. Interfaz y sus opciones



Fuente: Autores

Una vez realizado lo anterior, pasamos a la siguiente interfaz, en donde daremos clic en “Continuar”. como se muestra en la Figura 16.

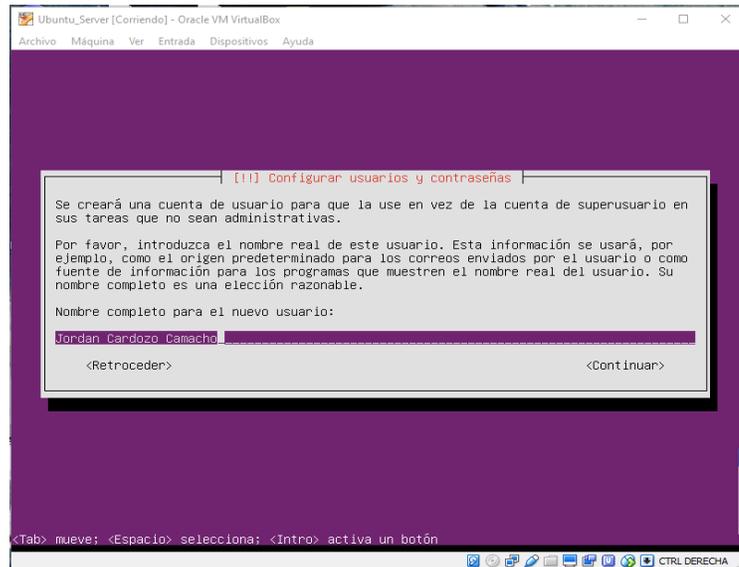
Figura 16. Continuación de la interfaz



Fuente: Autores

En la siguiente interfaz pondremos nuestro nombre y damos en “Continuar”. como se muestra en la Figura 17.

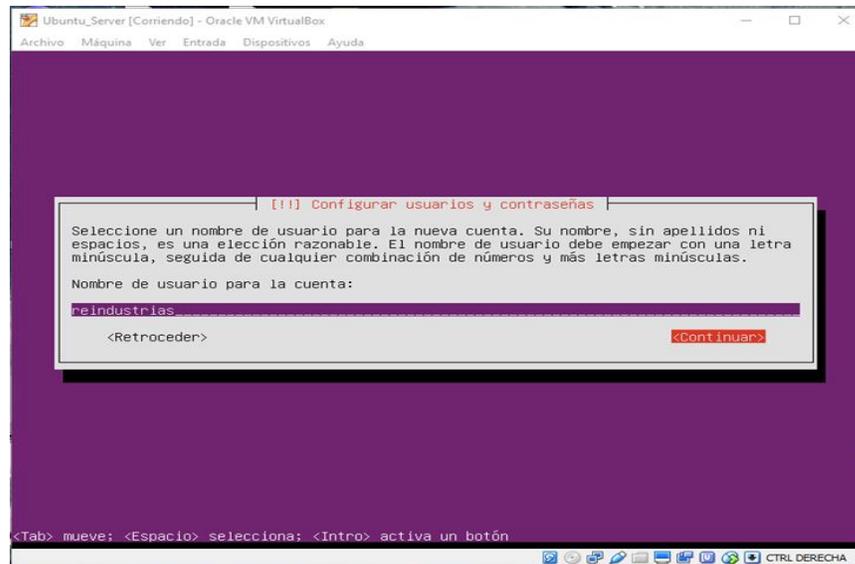
Figura 17. Nombre en la interfaz



Fuente: Autores

En este paso se pondrá un Nombre de Usuario y se da clic en “Continuar”. como se muestra en la Figura 18.

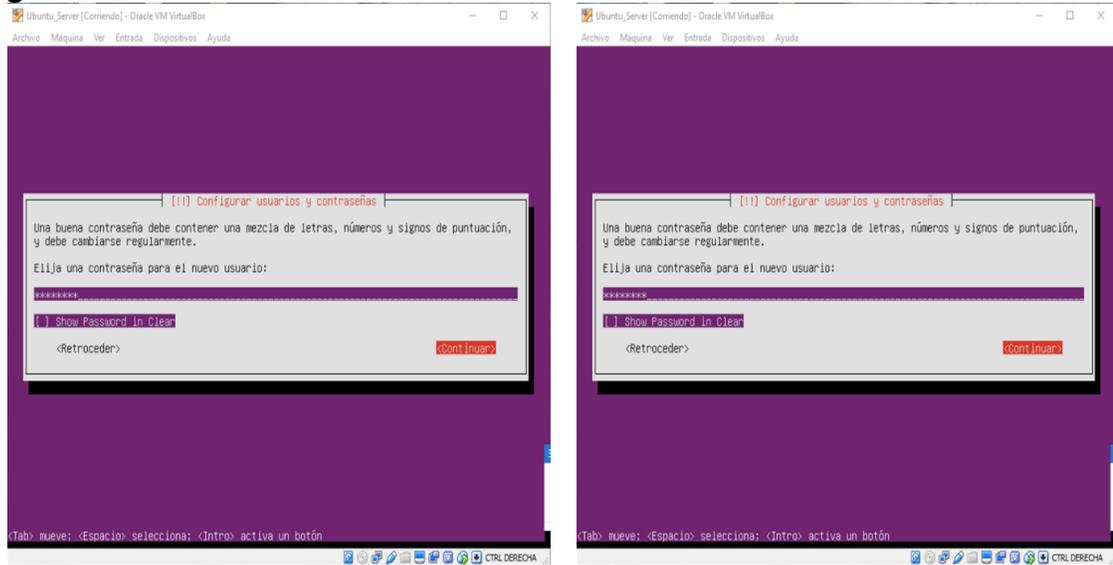
Figura 18. Nombre de usuario



Fuente: Autores

En este nuevo paso se ingres una contraseña y se pedirá nuevamente la contraseña para verificarla y damos en continuar. como se muestra en la Figura 19.

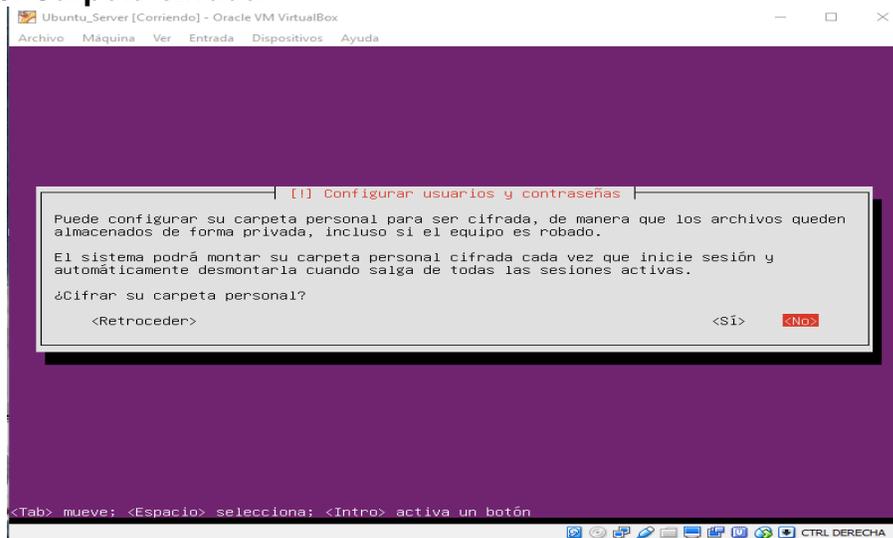
Figura 19. Creación de una contraseña



Fuente: Autores

En este nuevo paso si desea cifrar una carpeta la crifa, pero en este casi no cifraremos carpeta personal, por lo tanto, se dará clic en “Continuar”. como se muestra en la Figura 20.

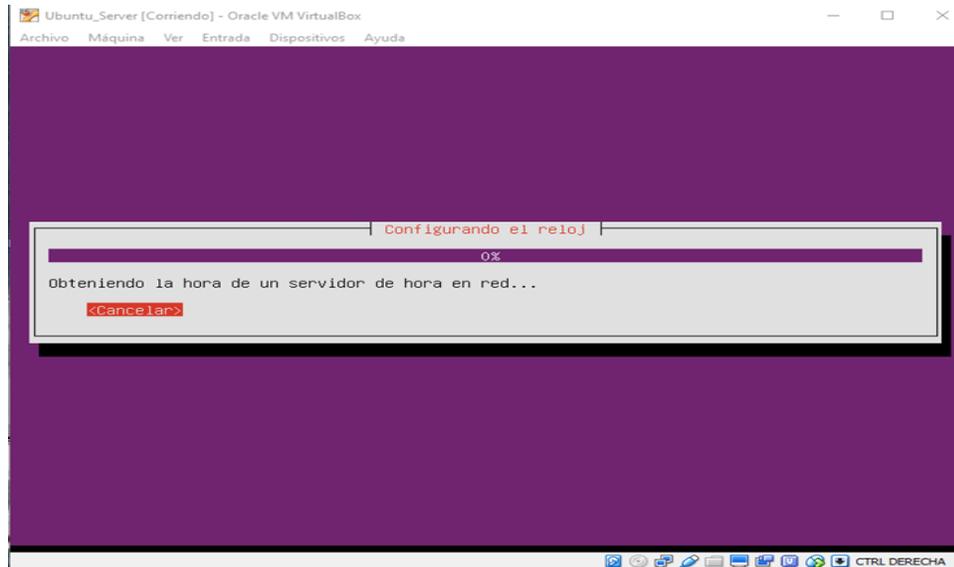
Figura 20. Carpeta cifrada



Fuente: Autores

Una vez rechazada la opción anterior, aparecerá la siguiente interfaz. como se muestra en la Figura 21.

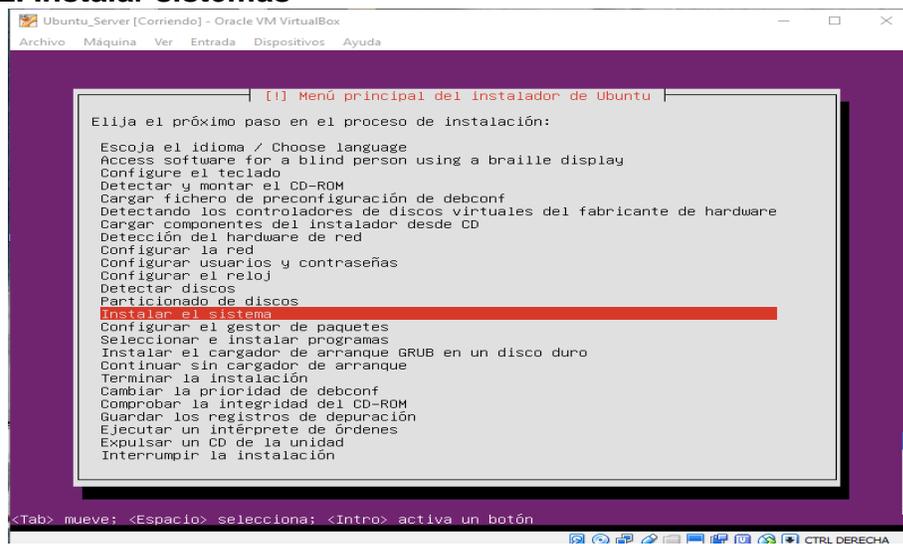
Figura 21. Nueva ventana



Fuente: Autores

Una vez termine la configuración de reloj donde se obtiene la hora de un servidor, aparece una ventana, donde se escogerá la opción “Instalar el Sistemas” y se da ENTER. como se muestra en la Figura 22.

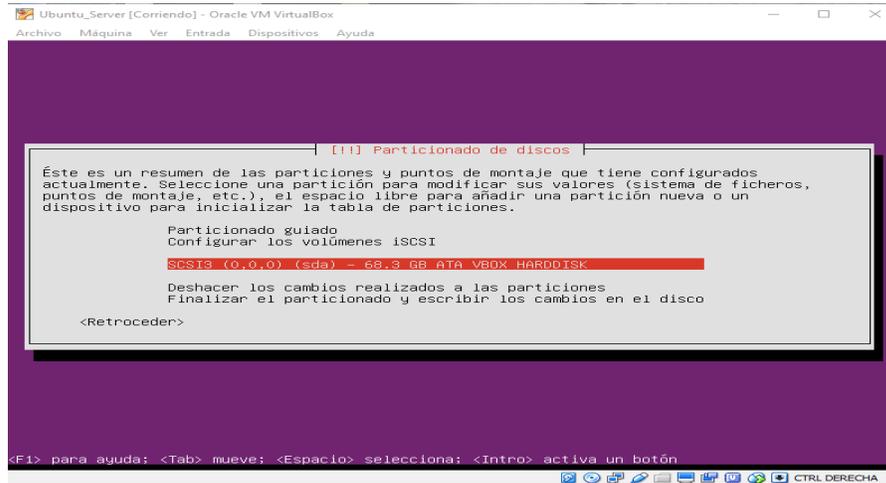
Figura 22. Instalar sistemas



Fuente: Autores

Una vez terminado el paso anterior, el sistema operativo, Ubuntu Server arrojará una ventana como la siguiente, donde se pide escoger el particionado del disco y se escogerá la opción donde dice “SCSI3 (0. 0. 0) (sda) – 68.3 GB ATA VBox HARDDISK y se da enter”. como se muestra en la Figura 23.

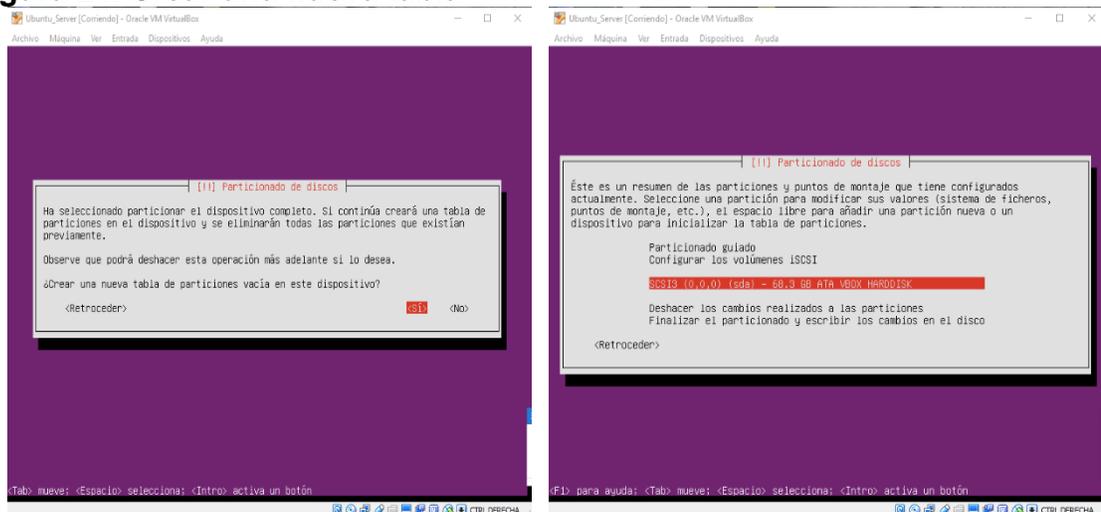
Figura 23. El SCSI3



Fuente: Autores

El siguiente paso se pregunta si se desea crear una nueva tabla de particiones vacía en el dispositivo, en donde se escogerá la opción sí, y a la opción de espacio libre y damos enter. como se muestra en la Figura 24.

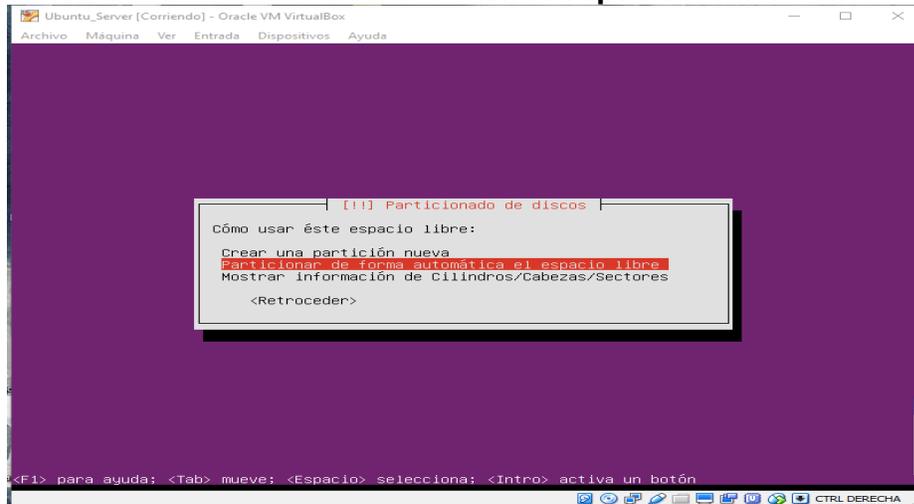
Figura 24. Crear una nueva tabla



Fuente: Autores

En el siguiente paso se escogerá la opción de “Particionar de forma automática el espacio libre” y damos enter. como se muestra en la Figura 25.

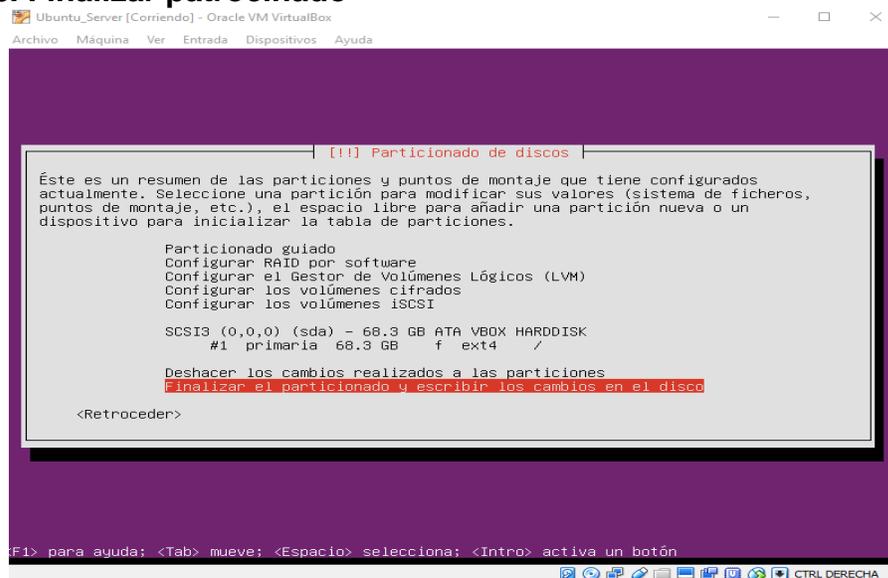
Figura 25. Patrocinar de forma automática el espacio libre



Fuente: Autores

Lo siguiente es escoger la última opción donde dice “Finalizar el particionado y escribir los cambios en el disco” y damos enter. como se muestra en la Figura 26.

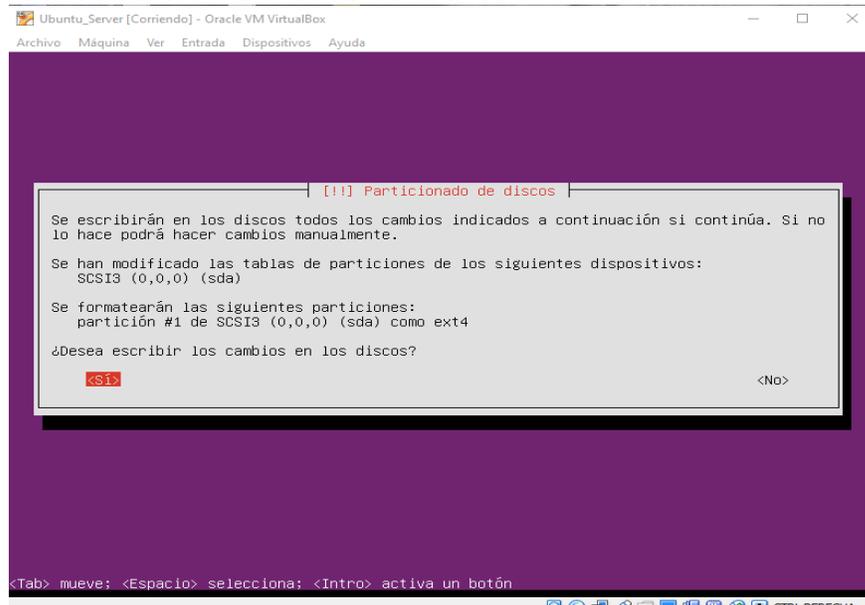
Figura 26. Finalizar particionado



Fuente: Autores

Continuación, se pregunta si deseamos escribir los cambios en los discos, escogemos la opción "SI" y damos enter. como se muestra en la Figura 27.

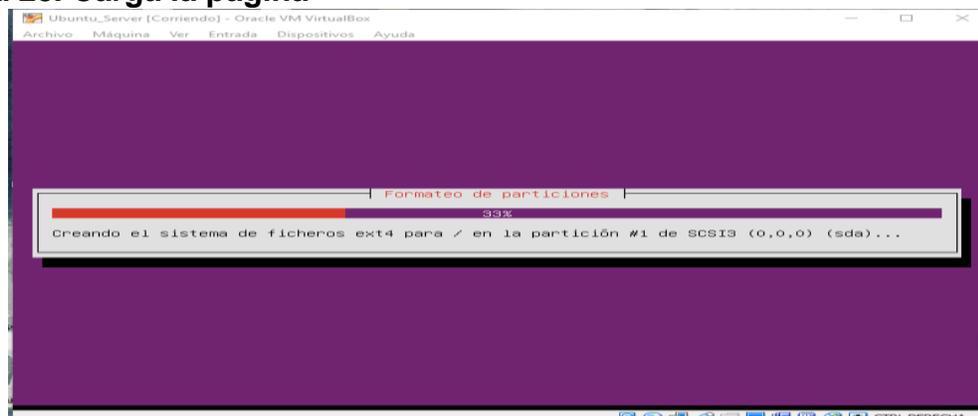
Figura 27. Cambios en los discos duros



Fuente: Autores

A continuación, se espera a que cargue todo, como se muestra en la Figura 28.

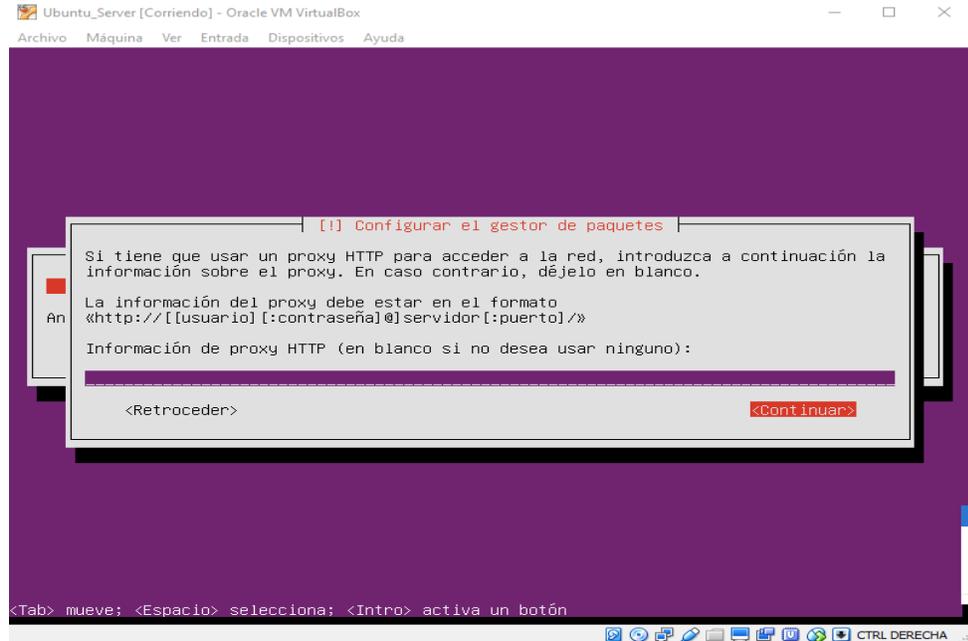
Figura 28. Carga la página



Fuente: Autores

En esta opción, se escoge continuar. como se muestra en la Figura 29.

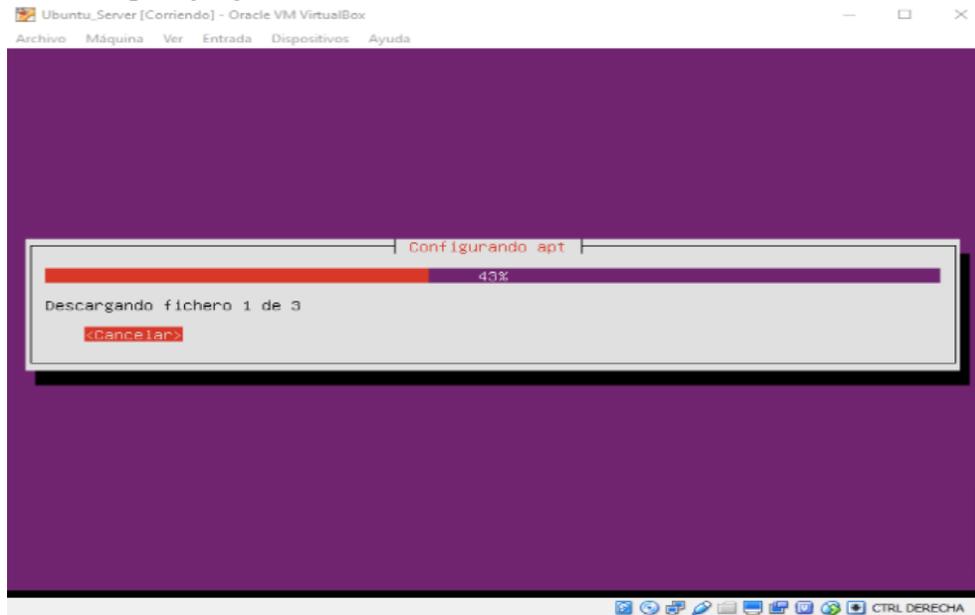
Figura 29. Opción continuar



Fuente: Autores

Se espera a que cargue todo. como se muestra en la Figura 30.

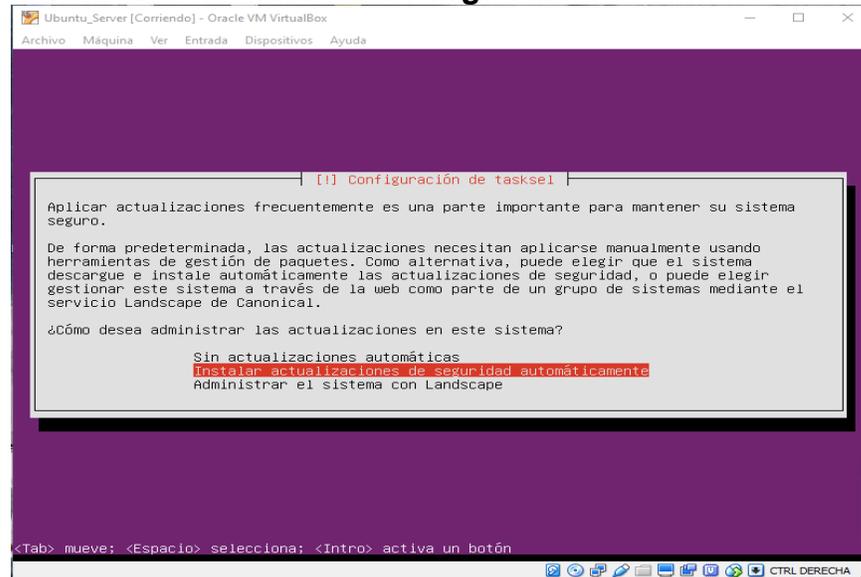
Figura 30. Cargue y ajustes



Fuente: Autores

A continuación, se escoge la opción “Instalar actualizaciones de seguridad automáticamente” y presionamos enter, como se muestra en la Figura 31.

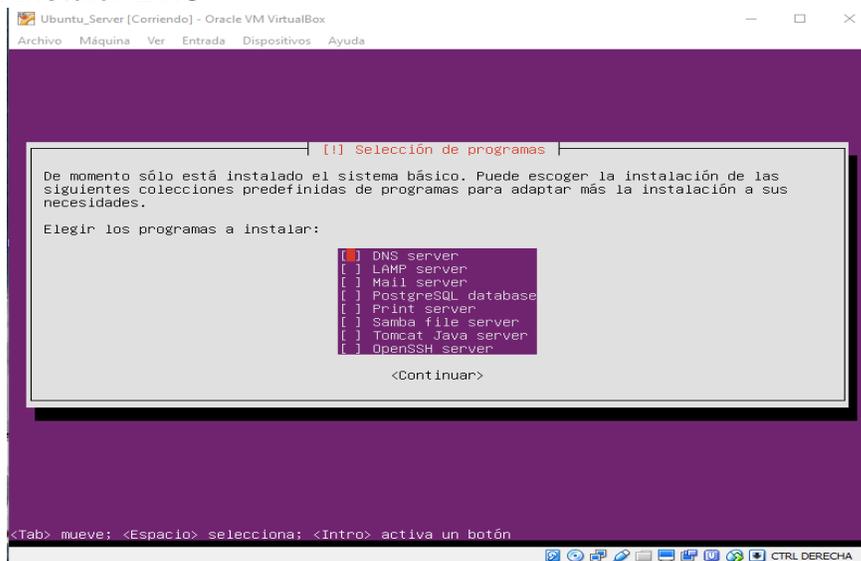
Figura 31. Instalar actualizaciones de seguridad



Fuente: Autores

Se escoge instalar DNS Server y presionamos enter, esperamos a que continúe nuestra instalación. como se muestra en la Figura 32.

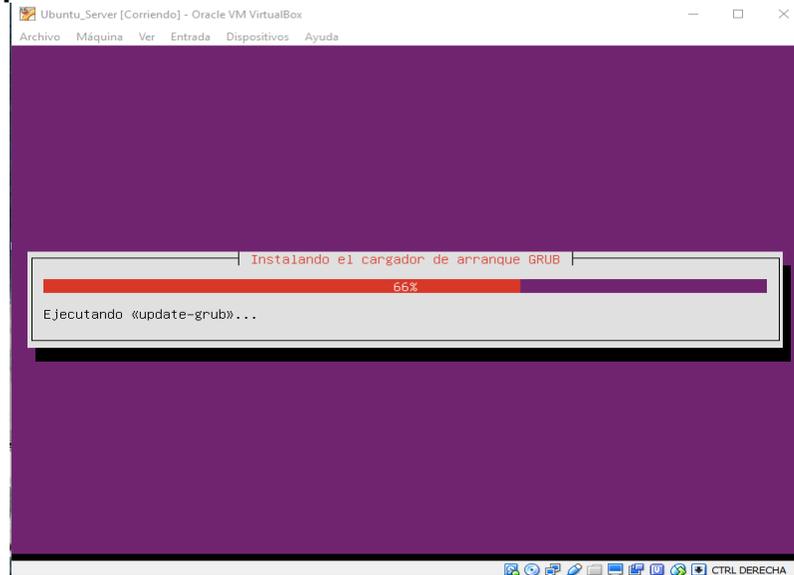
Figura 32. Instalar DNS



Fuente: Autores

Esperamos a que continúe nuestra instalación de Ubuntu Server. como se muestra en la Figura 33.

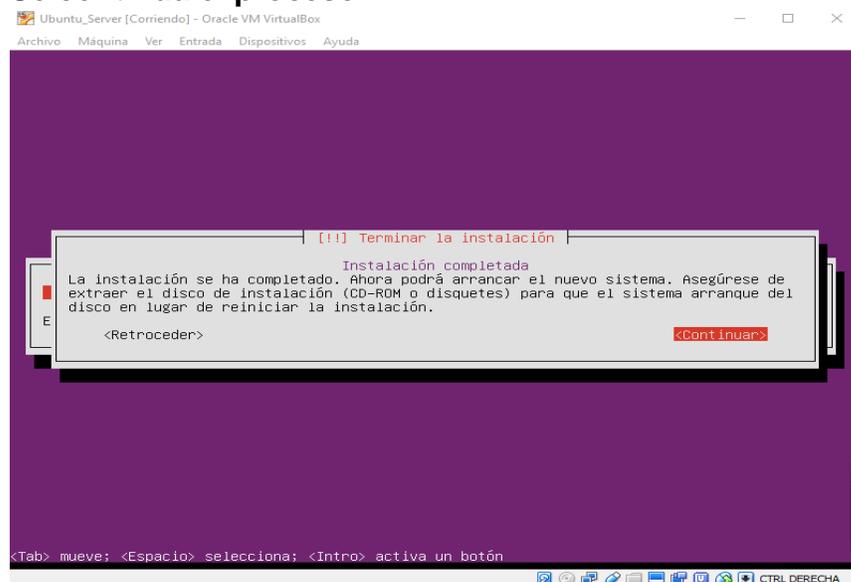
Figura 33. Aplicación de la instalación Ubuntu server



Fuente: Autores

A continuación, damos enter en "Continuar". como se muestra en la Figura 34.

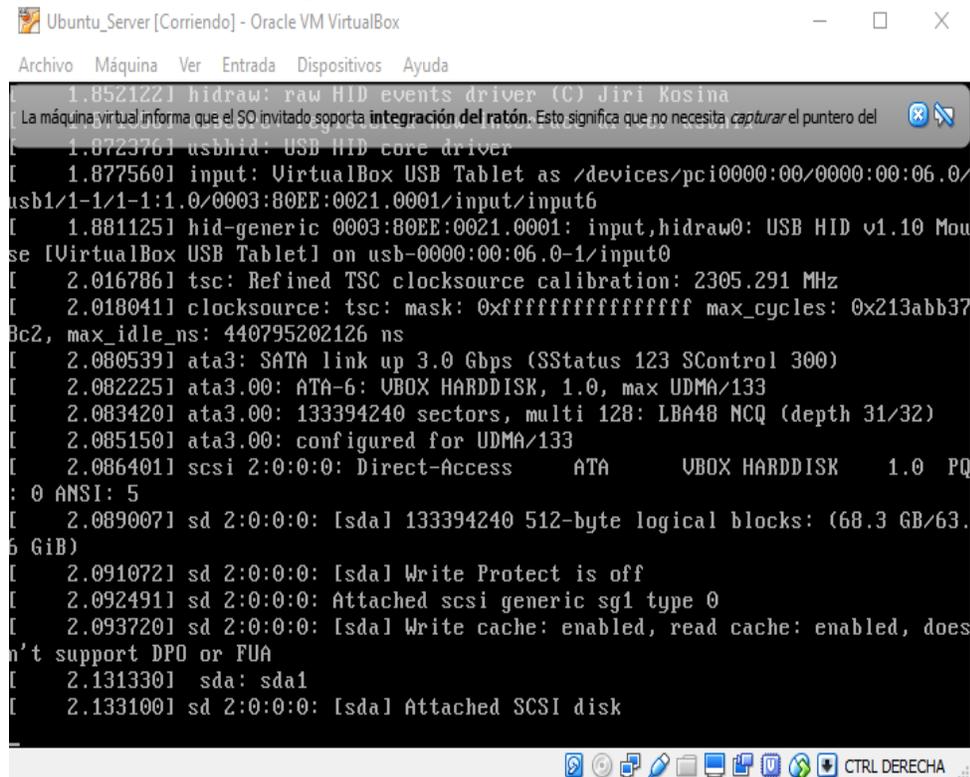
Figura 34. Se continua el proceso



Fuente: Autores

Cuando demos enter en continuar se nos reiniciara nuestro Ubuntu Server. como se muestra en la Figura 35.

Figura 35. Instalación completa del Ubuntu Server



Fuente: Autores

6.4 ANÁLISIS DE LOS RESULTADOS

Inicialmente se diseñó una encuesta proyectada y aplicada a 5 personas con diferentes cargos, pertenecientes a la empresa Energizando S.A.S. Estuvo compuesta con 10 preguntas abiertas como cerradas. A continuación, se presenta los resultados obtenidos después de su aplicación.

a. ¿La empresa Energizando S.A.S. cuenta con cobertura a internet?

Tabla 1. La empresa Energizando cuenta con cobertura a internet

Sí	5
No	0

Fuente: Autores

Figura 36. La empresa Energizando cuenta con cobertura a internet



Fuente: Autores

En la Figura 36, se presenta que el 100% de los encuestados estuvieron de acuerdo en que la empresa Energizando cuenta con cobertura a internet.

b. ¿Existe un departamento encargado de la seguridad informática?

Tabla 2. Existe un departamento encargado de la seguridad informática

Sí	0
No	5

Fuente: Autores

Figura 37. Existe un departamento encargado de la seguridad informática



Fuente: Autores

En la Figura 37, el 100% de los encuestados concordaron que la empresa Energizando, no cuenta hasta el momento, con un departamento para su seguridad informática. Además, de no tener un contrato para un personal adecuado en esta labor.

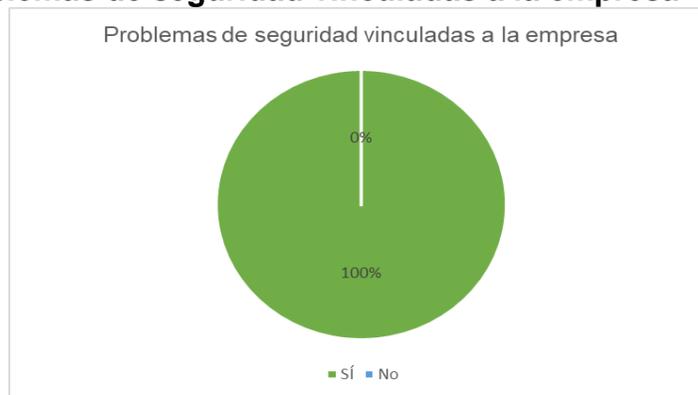
c. ¿Consideras que han tenido problemas de seguridad donde se vea comprometida la información de la empresa?

Tabla 3. Problemas de seguridad vinculadas a la empresa

Sí	5
No	0

Fuente: Autores

Figura 38. Problemas de seguridad vinculadas a la empresa



Fuente: Autores

La Figura 38 nos presenta que el 100% de los encuestados consideran que los problemas de seguridad de la empresa se vinculan a la información. Debido a que no se realiza respaldos, protocolos y cuidados en los datos.

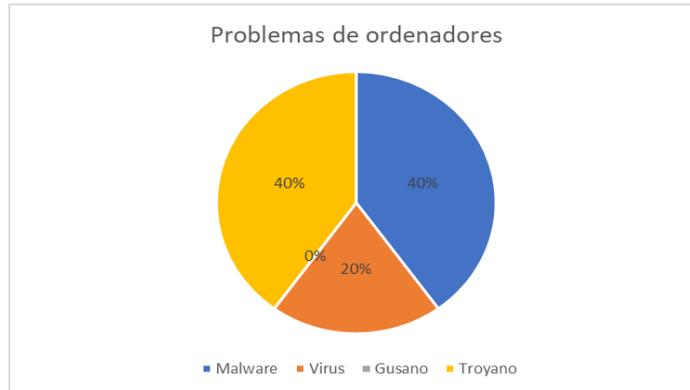
d. Has tenido algún problema de

Tabla 4. Problemas en los ordenadores

Malware	2
Virus	1
Gusano	0
Troyano	2

Fuente: Autores

Figura 39. Problemas en los ordenadores



Fuente: Autores

En la Figura 39 se presenta que los problemas más comunes en los ordenadores según los encuestados son el Malware con 40% y troyano 40%. Por lo que, la información vive cada vez más expuesta a estos tipos de virus.

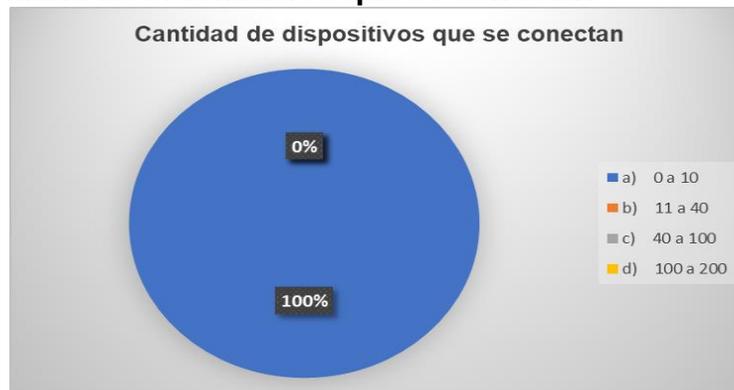
e. Actualmente en la empresa Energizando S.A.S. cuantos dispositivos aproximadamente se conectan:

Tabla 5. Cantidad de ordenadores que se conectan

0 a 10	5
11 a 40	0
40 a 100	0
100 a 200	0

Fuente: Autores

Figura 40. Cantidad de ordenadores que se conectan



Fuente: Autores

La Figura 40 expone que el 100% de los encuestados opinan que la cantidad de equipos son de 0 a 10 conectados a la red de la empresa.

f. Actualmente se realizan mantenimientos periódicos sobre las computadoras de la empresa:

Tabla 6. La empresa realiza periódicamente mantenimiento

Sí	0
No	5

Fuente: Autores

Figura 41. La empresa realiza periódicamente mantenimiento



Fuente: Autores

La Figura 41 presenta que el 100% de los encuestados opinan que la empresa no realiza mantenimiento preventivo en los equipos.

g. Generalmente realizas copias de seguridad de su información:

Tabla 7. Se realiza copias de seguridad

Sí	0
No	5

Fuente: Autores

Figura 42. Se realiza copias de seguridad



Fuente: Autores

La Figura 42 expresa que el 100% de los encuestados opinan que en la empresa no se realiza copias de seguridad que respalden la información.

h. La empresa ha capacitado a sus empleados en cuanto a seguridad informática:

Tabla 8. La empresa capacita en la seguridad de la información

Sí	0
No	5

Fuente: Autores

Figura 43. La empresa capacita en la seguridad de la información



Fuente: Autores

La Figura 43 expresa que el 100% de los encuestados concuerdan que la empresa no capacita a sus funcionarios en la seguridad de la información. Por lo que resulta vulnerable los equipos.

i. ¿Qué tan frecuentemente se preparan ante problemas de seguridad?

Tabla 9. La frecuencia en la preparación ante los problemas de seguridad

Cada mes	0
Cada semana	0
Cada año	3
Cada trimestre	1

Fuente: Autores

Figura 44. La frecuencia en la preparación ante los problemas de seguridad



Fuente: Autores

La Figura 44 presenta que los encuestados concordaron que el 75% cada año, se realiza una preparación para los problemas de seguridad. Mientras que un 25% expresaron que cada trimestre se desarrollaba.

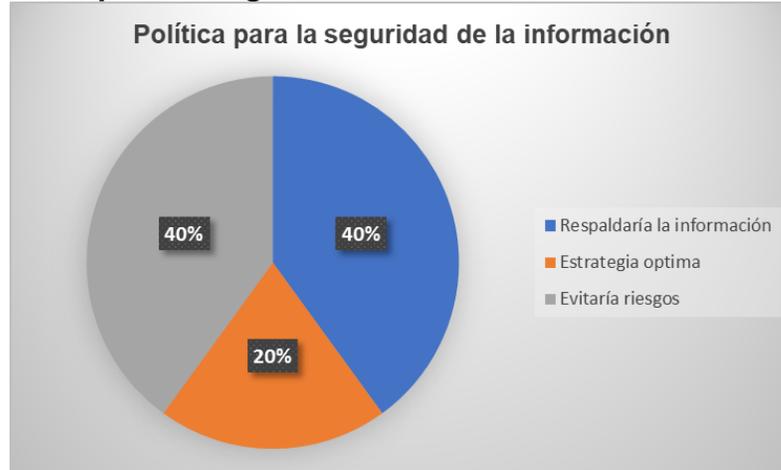
j. Qué piensa de una política para la seguridad de la información en su empresa:

Tabla 10. Política para la seguridad de la información

Respaldaría la información	2
Estrategia optima	1
Evitaría riesgos	2

Fuente: Autores

Figura 45. Política para la seguridad de la información



Fuente: Autores

La Figura 45 presenta las opiniones acerca de la propuesta del proyecto sobre una política en seguridad de la información. El 100% de los encuestados acertaron que es una estrategia necesaria para evitar daños en los equipos y salvaguardar la confidencialidad de la empresa.

6.5 PRESUPUESTO

Tabla 11. Presupuesto

ÍTEM	ACTIVIDAD O RECURSO	COSTO
1	Evaluar el riesgo, validar el estado y el grado de vulnerabilidad de la información en el servidor	\$ 100.000,0
2	Diseño de protocolos o políticas de seguridad en el servidor	\$ 450.000,0
3	Pago por concepto de transporte	\$ 80.000,0
4	Papelería	\$ 10.000,0
TOTAL		\$ 640.000,0

Fuente: Autores

6.6 CRONOGRAMA

Tabla 12. Cronograma de actividades

ACTIVIDADES	SEMANAS							
	ENERO				FEBRERO			
	1	2	3	4	1	2	3	4
Planteamiento del problema								
Objetivos								
Marco teórico								
Marco Metodológico								
Diseño de la encuesta								
Aplicación de la encuesta								
Análisis de los resultados								
Conclusiones								

Fuente: Autores

7. CONCLUSIONES

A partir de la ejecución y organización de este proyecto se concluyó:

- La seguridad de la información es una tarea para las medianas y grandes empresas, porque es una actividad compleja, que necesita revisión oportuna.
- En el análisis de las encuestas aplicadas, se encontró que la empresa Energizando S.A.S. frente a la seguridad de la información, está en riesgo de amenazas. Debido a la poca importancia que se le da y a la falta de conocimiento que se tiene frente al tema.
- No se tiene en cuenta los procesos de capacitación hacia el personal que opera en las redes. Por lo tanto, la seguridad corre riesgos.
- Se debe tener claro que la seguridad de la información es un ente importante en la empresa, y como tal habría que realizar inspecciones semanales o al mes sobre el estado de la información.
- La empresa Energizando S.A.S. no cuenta con un departamento en tecnología. Así que la tarea de revisión es escasa. Y pone en riesgo la confidencialidad.

RECOMENDACIONES

- Definir estrategias para salvaguardar la información de las empresas.
- Verificar continuamente la información de la empresa entre los envíos por redes.
- Generar políticas de control, apoyados por responsables de la materia.

BIBLIOGRAFÍA

CONTRERAS, Nicolás. “Más del 80 por ciento de las compañías en Colombia son vulnerables a ataques informáticos”. Caracol radio. Artículo. (9 junio de 2016). Disponible en <https://bit.ly/1reAFUg>

Dirección Nacional de Migración. “Sistema operativo Linux”. [anónimo]. Disponible en <https://repositorio.espe.edu.ec/bitstream/21000/347/1/T-ESPE-029761.pdf>

Educación IT. “Seguridad Linux: server hacking”. Documento web. disponible en <https://www.educacionit.com/generar-pdf-curso?toc=linux-seguridad-avanzada>

Emprende Pymes.net. “Políticas de seguridad”. Sitio web. Disponible en <https://www.emprendepyme.net/politicas-de-seguridad.html>

GOMÉZ, Jesús. “Programa de apoyo a los cambios tecnológicos”. Sitio web. (13 marzo de 2017). Disponible en <https://www.cerembs.co/blog/programas-de-apoyo-a-los-cambios-tecnologicos>

ISO 27000. “Sistema de gestión de la seguridad de la información”. sitio web. disponible en http://www.iso27000.es/download/doc_sgsi_all.pdf

IBARRA, Andrea. “Endurecimiento del sistema operativo Linux”. Artículo. Universidad Católica de Colombia. Año. 2009. Disponible en <http://polux.unipiloto.edu.co:8080/00001572.pdf>

Iniciativas Empresariales. “Seguridad Informática para Sistemas Operativos Windows y Linux en Empresas”. Sitio web. (10 julio de 2014). Disponible en <https://www.iniciativasempresariales.com/blog/seguridad-informatica-para-sistemas-operativos-windows-y-linux-en-empresas/>

Juntadeandalucia.es. “¿Qué es el Linux?”. Sitio web. Disponible en http://www.juntadeandalucia.es/empleo/recursos/material_didactico/especialidades/materialdidactico_tic_linux_basico/manuales/tema1.pdf

MIRANDA, Juan y PADILLA, Wilmer. “Diseño e implementación servidores /Firewall GNU -Linux con conexión WAN”. Trabajo de grado. Universidad tecnológica de Bolívar. Año. 2010. Disponible en <https://bit.ly/2Ed1EKd>

MARTÍNEZ, Kelly, PACHECO, Javys y ZÚÑIGA, Isaac. “Firewall – Linux: una solución de seguridad informática para pymes (pequeñas y medianas empresas)”. Revista UIS ingenierías. (2 diciembre de 2009). Vol. (8) pp.155-165, Colombia. Disponible en <https://www.redalyc.org/pdf/5537/553756879003.pdf>

Ministerio de educación, cultura y transporte. “Seguridad básica en Linux”. documento web. (25 febrero de 2008). Disponible en <https://bit.ly/2TOrBVv>

MINTIC. “Colombia cuenta con una Política Nacional de Seguridad Digital”. Sitio web. (15 abril de 2016). Disponible en <https://www.mintic.gov.co/portal/604/w3-article-15033.html>

OLMEDO, Luis. “Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, PROPOLSINECOR”. Trabajo de grado.

Presidencia de la república. “Manual de políticas de seguridad de la información”. documento web. Año. 2018. Disponible en <https://bit.ly/2rdFrUp>

Universidad nacional abierta y a distancia “unad”. Disponible en <https://repository.unad.edu.co/bitstream/10596/2742/1/12973210.pdf>

Universidad Libre. “Seguridad de la información”. sitio web. Bogotá. Disponible en <https://bit.ly/2BD98nN>

SALAZAR, Liliana. “Implementación de un servidor Linux”. Trabajo de grado. Universidad Nacional de Colombia. Disponible en <https://bit.ly/2DH67mG>