

UNIVERSIDAD DE HUÁNUCO

Facultad de Ingeniería

*PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS E
INFORMÁTICA*



TESIS:

“IMPLEMENTACIÓN DE UN SERVIDOR DE SEGURIDAD BAJO
EL S.O GNU/LINUX BASADO EN LA ISO 27002:2013 PARA
MEJORAR LA RED DE ÁREA LOCAL DEL ÁREA
ADMINISTRATIVA DEL HOSPITAL DE CONTINGENCIA
HERMILIO VALDIZÁN MEDRANO DE HUÁNUCO, 2017”

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERA DE
SISTEMAS E INFORMÁTICA

PRESENTADO POR:

PAUCAR FALCÓN, BEATRIZ HAYDEÉ

ASESOR:

ING. CRISTIAM IVAN LÓPEZ DE LA CRUZ

Huánuco- Perú

2017

DEDICATORIA

A mis padres, quienes a lo largo de mi vida han velado por mi bienestar y educación para hacer de mí una mejor persona.

BEATRIZ

AGRADECIMIENTOS

A la Universidad de Huánuco, a mi honorable Facultad de Ingeniería y a todos los Docentes que a lo largo de mi formación académica me impartieron sus conocimientos en el campo de la ingeniería y en otras áreas que corresponden a mi profesión.

Al asesor de tesis Ing. Cristiam López de la Cruz, por la acertada orientación en la realización de esta tesis.

BEATRIZ

ÍNDICE GENERAL

RESUMEN	8
ABSTRACT	9
INTRODUCCIÓN.....	10
CAPÍTULO I	12
PROBLEMA DE INVESTIGACIÓN	12
1.1. Descripción del problema.....	12
1.2. Formulación del problema.....	14
1.3. Objetivo General	14
1.4. Objetivos Específicos	15
1.5. Justificación de la investigación	15
1.6. Limitaciones de la investigación	16
1.7. Viabilidad de la investigación	16
CAPÍTULO II	18
MARCO TEÓRICO	18
2.1. Antecedentes de la Investigación	18
2.2. Bases Teóricas.....	22
2.3. Definiciones conceptuales	36
2.4. Hipótesis	39
2.5. Variables.....	39
2.5.1. Variable Dependiente.....	39
2.5.2. Variable Independiente.....	39
2.6. Operacionalización de Variables	40
CAPÍTULO III	41
METODOLOGÍA DE LA INVESTIGACIÓN	41
3.1. Tipo de Investigación	41
3.1.1. Enfoque	41
3.1.2. Alcance	41
3.1.3. Diseño.....	41
3.2. Población y Muestra.....	42
3.3. Técnicas e instrumentos de recolección de datos	42
3.4. Técnicas para el procesamiento y análisis de la información	42
CAPÍTULO IV	43
RESULTADOS	43
4.1 Procesamiento de datos	43
4.1 Contrastación de hipótesis y prueba de hipótesis.....	49
CAPÍTULO V	53

DISCUSIÓN DE RESULTADOS	53
CONCLUSIONES.....	55
RECOMENDACIONES	56
REFERENCIAS BIBLIOGRÁFICAS	57

ÍNDICE DE TABLAS

Tabla 1: Comparación Antes – Después de la cantidad de conexiones por día, en relación a los Controles de seguridad asociados a servicios de red.....	43
Tabla 2: Comparación Antes – Después de la cantidad de MB accedidos por día, en relación a los Controles de seguridad asociados a servicios de red	44
Tabla 3: Comparación Antes – Después de la cantidad de página no autorizadas visitadas por día, en relación a los Controles de seguridad asociados a servicios de red.....	45
Tabla 4: Comparación Antes - Después de la cantidad de archivos y carpetas creadas por día, en relación a los Controles de seguridad asociados a la restricción del acceso de la información	46
Tabla 5: Comparación Antes - Después de la cantidad de archivos y carpetas modificadas por día, en relación a los Controles de seguridad asociados a la restricción del acceso de la información	47
Tabla 6: Comparación Antes - Después de la cantidad de archivos y carpetas eliminados por día, en relación a los Controles de seguridad asociados a la restricción del acceso de la información	48

ÍNDICE DE ILUSTRACIONES

Ilustración 1: Comparación Antes – Después de la cantidad de conexiones por día, en relación a los Controles de seguridad asociados a servicios de red	43
Ilustración 2: Comparación Antes – Después de la cantidad de MB accedidos por día, en relación a los Controles de seguridad asociados a servicios de red	44
Ilustración 3: Comparación Antes – Después de la cantidad de página no autorizadas visitadas por día, en relación a los Controles de seguridad asociados a servicios de red.....	45
Ilustración 4: Comparación Antes - Después de la cantidad de archivos y carpetas creadas por día, en relación a los Controles de seguridad asociados a la restricción del acceso de la información.....	46
Ilustración 5: Comparación Antes - Después de la cantidad de archivos y carpetas modificadas por día, en relación a los Controles de seguridad asociados a la restricción del acceso de la información.....	47
Ilustración 6: Comparación Antes - Después de la cantidad de archivos y carpetas eliminados por día, en relación a los Controles de seguridad asociados a la restricción del acceso de la información.....	48

RESUMEN

El presente estudio de investigación tuvo como fin el de implementar un servidor de seguridad utilizando el sistema operativo GNU/Linux bajo los controles del ISO 27002:2013, en el Hospital de Contingencia Hermilio Valdizán Medrano de la ciudad de Huánuco en el año 2017.

En cuanto a la metodología se planteó bajo el enfoque cuantitativo, y el tipo aplicativo; porque se utilizó la tecnología para la solución de un problema, así mismo se empleó el diseño pre experimental de pre y post test se llevó a cabo un experimento en condiciones controladas. La población estuvo conformada por 320 trabajadores del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de la ciudad de Huánuco, y se determinó la muestra de forma no probabilística, de los cuales se permitió evaluar algunos controles técnicos en base a las actividades de los trabajadores en la red de área local. En cuanto a la recolección de datos se usó la estadística descriptiva mediante el uso del software SPSS.

Se utilizó el sistema operativo GNU/LINUX para dar soporte a la aplicación del servidor de seguridad usando los controles específicos números: 13.1.2 y 9.4 del ISO 27002:2013, se llevaron a cabo las pruebas de forma satisfactoria y cumpliendo el objetivo de dar seguridad a la red de área local del área administrativa del Hospital mediante la implementación de dicho servidor.

Palabras Clave: Seguridad Informática, GNU/Linux, ISO 27002:2013, Servidores.

ABSTRACT

The purpose of this research study was to implement a security server using the GNU / Linux operating system under the controls of ISO 27002:2013, at the Hermilio Valdizán Medrano Contingency Hospital in the city of Huánuco in 2017.

Regarding the methodology, it was proposed under the quantitative approach, and the application type; because the technology was used for the solution of a problem, likewise the pre-experimental design of pre and post test was used, an experiment was carried out under controlled conditions. The population consisted of 320 workers from the administrative area of the Hermilio Valdizán Medrano Contingency Hospital in the city of Huánuco, and the sample was determined in a non-probabilistic manner, which allowed for the evaluation of some technical controls based on the workers' activities in the local area network. In terms of data collection, descriptive statistics were used through the use of SPSS software.

The GNU / LINUX operating system was used to support the application of the security server using the specific controls numbers: 13.1.2 and 9.4 of the ISO 27002-2013, the tests were carried out satisfactorily and fulfilling the objective of giving security to the local area network of the Hospital's administrative area through the implementation of said server.

Keywords: Computer Security, GNU / Linux, ISO 27002:2013, Servers.

INTRODUCCIÓN

Actualmente con el desarrollo continuo de la tecnología, han surgido nuevas formas de comunicarnos en el mundo, quizás todo se debe a la globalización y lo pequeño que es ahora nuestro planeta; día a día estas nuevas tecnologías se imponen sobre las viejas, y con este cambio vienen circunstancias que llevan al mal uso de la información y de la informática.

El presente estudio de investigación se centra en el problema de la inexistencia de un sistema de seguridad para la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de la ciudad de Huánuco, debido a los accesos no autorizados por parte del personal a páginas y contenidos no deseados dentro de la institución, generando desperdicio de las horas de trabajo y del consumo del ancho de banda de la conexión a Internet, ante el presente problema se formula lo siguiente: ¿De qué manera la implementación de un servidor mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco?, ante la pregunta se afirma con el objetivo: Implementar y evaluar un servidor de seguridad en la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco; de esta forma la investigación se centra en la implementación de dicho servidor en el área administrativa para poder controlar las actividades en la red por parte de los trabajadores, se ha utilizado el diseño pre experimental para poder realizar las pruebas correspondientes mediante un pre y post test, con los resultados obtenidos se procedió a procesarlos en el software estadístico SPSS, si bien es cierto se utilizó la muestra del estudio a los 40 trabajadores del área administrativa pero como unidades de análisis fueron los indicadores de medición de los mismos servicios de seguridad ofrecidos por el servidor, ya que en si se midió la actividad de los usuarios de la red por medio de estas rubricas provistas por cada servicio de red.

En cuanto a la limitación principal, fue el echo del traslado temporal del Hospital al Hospital de Contingencia, esto genero desorden e inestabilidad al inicio en cuanto al acceso de la información y de las instalaciones para las respectivas pruebas, se tuvo que acomodar a la infraestructura de red con la

que se contaba para poder llevar a cabo la aplicación así mismo se realizó las pruebas previas en un servidor virtual

Finalmente como una conclusión general podemos decir que la implementación del servidor de seguridad optimizo en gran medida el control de acceso de los contenidos utilizados por parte de los trabajadores del área, así mismo se reorganizo la forma del acceso y almacenamiento de la información mediante la centralización del servicio en el servidor, cabe mencionar que dicho proyecto también se minimizo los costos debido al uso de software libre y ya de la infraestructura provista por el propio Hospital.

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1. Descripción del problema

El Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco fue creado el 20 de julio de 1963 por la junta de gobierno de los generales Nicolás Lindley, Juan Torres M. y Pedro Vargas P. quienes entregaron el mando de la construcción al arquitecto Fernando Belaunde Terry. Tiene como Misión ser un hospital comprometido socialmente en la atención integral de la salud, brindando especialidades, médico quirúrgico de calidad, practicando valores éticos y morales. Y como visión ser un hospital modelo de servicio público en salud, con cultura de amor al prójimo y aceptabilidad social. En el mencionado hospital se brinda la atención a diferentes servicios relacionados a la salud, está organizado en diferentes áreas, en la cual cada una de ellas cumple una función específica.

El área administrativa está comprendida por las siguientes oficinas: Unidad de personal, unidad de economía, unidad de logística, unidad de control patrimonial, unidad de servicios generales y mantenimiento. En dichas oficinas se realizan diferentes actividades y se utilizan algunas tecnologías de información para el procesamiento de datos y manipulación de los mismos, así mismo cada oficina de área se encuentra interconectada por una red de área local, en la cual se comparten recursos (archivos e impresoras), dicha red tiene acceso a Internet, por lo tanto, cada oficina mediante el uso de un computador se conecta a la red de área local para el uso de los diferentes servicios de Internet.

Mediante algunos testimonios y confesiones vertidas por parte de algunos jefes de las distintas áreas, así como también trabajadores de cada oficina; se recabaron algunas observaciones en relación al uso indebido de los servicios de Internet y de los recursos de la red de área local cometidos por los trabajadores de dichas áreas, a continuación,

mencionamos los problemas y dificultades suscitados: Primero, la red no cuenta con un protocolo de seguridad o un mecanismo de seguridad el cual pueda garantizar la seguridad de la información de los recursos lógicos y físicos del área; en consecuencia existe una deficiente gestión en cuanto al uso de los recursos lógicos en la red como son los directorios y archivos de cada host conectado a la red, esto se traduce en la pérdida de información, alteración, de forma intencional o no intencional, a esto se le suma la replicación y redundancia de información y la falta de sincronización en cuanto a las versiones de un archivo; en otras palabras cualquier usuario puede acceder a los archivos y carpetas compartidas de otro usuario desde cualquier host conectado a la red, ocasionando la alteración o eliminación de archivos y provocando la pérdida de tiempo y de recursos en cuanto a la elaboración de dicho archivo; así mismo un archivo puede aparecer en diferentes ubicaciones de la red desconociendo cual fue la versión última de dicho archivo. Segundo, algunos trabajadores en horas de trabajo utilizan la computadora para ingresar a páginas no permitidas durante el horario de trabajo, como por ejemplo YouTube, Facebook, Mensajería y otros, esto conlleva a la disminución de la eficiencia del trabajador en relación a las tareas asignadas. Tercero, se ha observado que en algunas máquinas de los trabajadores se han instalado programas de gestores de descarga y torrents, con la finalidad de descargar grandes volúmenes de información como por ejemplo películas y música, programas, esto ocasiona grandes demandas del ancho de banda de la conexión a internet, ocasionando así cuellos de botella, congestión, saturación en la red, perjudicando algunos servicios destinados a la labor diaria del área.

Por lo tanto se pretende solucionar mencionados problemas mediante la implementación de un servidor de seguridad bajo el sistema operativo GNU/Linux en la distribución Ubuntu Server, para la red de área local del área administrativa y así poder controlar y gestionar la seguridad de la información a nivel de la capa de red, con la aplicación de dicho servidor se podrán bloquear las páginas web no autorizadas, con el fin del buen desempeño laboral del personal, también se podrá

bloquear el acceso de algunos programas no autorizados y así no tener saturada la red, también se contara con un repositorio central de ficheros configurados con sus correspondientes niveles de seguridad. Cabe destacar que dicha implementación se basara en el ISO 27002:2013, ver anexo 02.

1.2. Formulación del problema

Formulación General

¿De qué manera la implementación de un servidor mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco?

Formulaciones Específicos

- A.** ¿De qué manera la implementación de controles de seguridad asociados a servicios de red mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco?

- B.** ¿De qué manera la implementación de los controles de seguridad asociados a la restricción del acceso de la información mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco?

1.3. Objetivo General

Implementar un servidor de seguridad para mejorar la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.

1.4. Objetivos Específicos

- A.** Evaluar los controles de seguridad asociados a servicios de red para mejorar la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.
- B.** Medir los controles de seguridad asociados a la restricción del acceso de la información red para mejorar la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.

1.5. Justificación de la investigación

1.5.1. Justificación Teórica:

La razón en cuanto a la investigación desde una perspectiva teórica es la de contar con una metodología de implementación y uso de software libre y así también la documentación necesaria en el área de la seguridad de la información a nivel de la capa de red.

1.5.2. Justificación Práctica:

Por medio del presente estudio se podrá utilizar la tecnología para poder aplicarla y solucionar el problema de investigación; la parte práctica reside en la instalación, configuración y administración del servidor de seguridad en la red de área local de la institución para así lograr una mejora en la seguridad de la información a nivel de la capa de red.

1.5.3. Justificación Metodológica:

La aplicación del servidor de seguridad en la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco, seguirá la metodología de desarrollo de proyectos ágiles, que en este caso se centra en la instalación, configuración y administración del sistema operativo

GNU/Linux con todos los servicios correspondientes para controlar y gestionar la seguridad de la información a nivel de la capa de red. También hacemos uso de la metodología empírica para el desarrollo y la aplicación del proyecto de investigación.

1.6. Limitaciones de la investigación

Las limitaciones encontradas para realizar el presente estudio de investigación son:

- ✓ Se contó con poco tiempo para la etapa de aplicación ya que el hospital se mudó al Hospital de Contingencia, generando retrasos y algunos cambios.
- ✓ La disposición inicial del servidor será limitada ya que en dicho servidor se realizan funciones de consulta de trámite de impresión mediante el uso de un sistema de información, por lo tanto, la versión beta de nuestro servidor de seguridad va a ser virtualizado para posteriormente implementarlo en el servidor físico real.

1.7. Viabilidad de la investigación

1.7.1. Viabilidad Técnica.

Es viable desde un punto de vista técnico, ya que se dispone de los recursos físicos y lógicos necesarios para el desarrollo de la investigación. Específicamente para la implementación del servidor se contará con una maquina en la cual realizaremos la virtualización de la aplicación mediante el software de virtualización bajo el sistema operativo GNU/Linux en su distribución Ubuntu Server.

1.7.2. Viabilidad económica.

La presente investigación es viable económicamente y socialmente ya que se cuenta con un presupuesto asignado para el estudio, dicho presupuesto fue costado por la propia

investigadora, también se contó con el apoyo del personal del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.

1.7.3. Viabilidad Institucional.

El estudio es viable desde el punto de vista institucional para su análisis e implementación ya que se contó con el apoyo de las autoridades del Hospital de Contingencia Hermilio Valdizán Medrano, específicamente del jefe del área administrativa, así como también los trabajadores de las diferentes unidades correspondientes a dichas áreas, la facilidad brindada en cuanto a la entrega de algunos documentos, al momento de las entrevistas, encuestas y la observación propiamente dicha.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de la Investigación

A. A nivel Internacional:

❖ **(Méndez Alvarez, Verónica Elizabeth, Jiménez Moya, Carmen Esther, 2013)**. Configuración e implementación de un servidor de internet con firewall bajo estándares de seguridad en Linux centos 5.9 en el laboratorio de redes de la carrera de ingeniería en informática y Sistemas computacionales de la universidad técnica de cotopaxi en el período marzo – agosto del 2013. Para optar el título en Ingeniería informática y Sistemas computacionales. Los puntos más resaltantes que se pueden rescatar de este trabajo de tesis son: Con el proyecto de tesis desarrollado podemos concluir que la seguridad en la actualidad tiene un rol de gran importancia en las distintas instituciones, por ello se ha hecho indispensable el uso de firewall o cortafuegos y sistemas de seguridad para defendernos de posibles ataques informáticos internos o externos. Pero como hemos podido observar el firewall no son la solución completa para la seguridad total requiriendo de otros medios para complementar y controlar las posibles infiltraciones que nuestro firewall no detecte. La conclusión es que, cada institución requiere de firewall o cortafuegos para cuidar la integridad de sus datos. La información obtenida a través de los distintos medios bibliográficos fue muy abundante pero siempre hay que tener en cuenta la confiabilidad de la fuente, la mayoría de la información obtenida fue muy útil ya que nos permitió desarrollar de la mejor manera nuestro proyecto, con esta se obtuvieron conocimientos nuevos y actualizados que fortalecieron nuestra experiencia y aportaran muchos beneficios en el desarrollo de nuestra vida profesional. En conclusión, para el desarrollo de este proyecto el internet y sus distintas fuentes

bibliográficas son útiles al momento de investigar la mejor forma de instalar nuevas tecnologías.

❖ **(Orellana Benavides, Luis Alberto, 2003)**. Seguridad en redes de datos. Para optar el título en Ingeniería Electrónica. Los puntos más resaltantes que se pueden rescatar de este trabajo de tesis son: La mayor cantidad de los ataques que se dan en la actualidad son por medio de ingeniería social que es un método basado en engaño, que usan algunos atacantes de tal manera que pueden conseguir la información directamente de los usuarios simplemente engañándolos. Razones por las cuales la creación de políticas de seguridad es parte medular de la seguridad en una red, las políticas de usuario y el entrenamiento de estos en seguridad deberá ser una etapa de alta prioridad para mantener la seguridad en la red, los cambios de contraseñas de una manera periódica, la creación de estas por medio de métodos complejos que produzcan claves difíciles de adivinar como por ejemplo el hecho de evitar palabras de diccionario o fechas, son reglas que un administrador de red debe tomar en cuenta para asegurar una red de forma radical y eficiente. Una arquitectura para que sea totalmente segura deberá contener los 4 niveles de seguridad detallados anteriormente, siendo que es posible que no todas las redes necesitan altísimos niveles de seguridad, estos se pueden considerar de tal manera que una red posea sólo un nivel podrá ser funcional para una institución de educación pero no para un banco, y de la misma manera el banco necesitará una red con los 4 niveles de seguridad mientras que una escuela no necesariamente las requiera.

B. A nivel Nacional:

❖ **(Lazo García, 2012)**. Diseño e implementación de una red Lan y Wlan con Sistema de control de acceso mediante servidores AAA. Para optar el Título de Ingeniera de las Telecomunicaciones. Los puntos más resaltantes que se pueden rescatar de este trabajo de tesis son: Se comprobó que los protocolos AAA RADIUS y TACACS+ tienen diferentes características en el manejo de autenticación y autorización. El protocolo RADIUS maneja ambos servicios de manera combinada, mientras que el protocolo TACACS+ los ofrece como servicios independientes. A pesar de ello fueron implementados en una misma red y coexisten para brindar una red con sistema de control de acceso robusto. Se demostró que con ayuda de adecuados protocolos y técnicas de red se puede optimizar el uso de recursos de la misma y hacer que esta sea más robusta frente a averías que pueda sufrir. En esta tesis usamos la técnica Etherchannel para implementar redundancia de enlace, demostrándose que el tiempo de respuesta ante una caída de enlace será menor a 1 ms. Asimismo se utilizó la técnica Etherchannel para balancear la carga entre los enlaces resultando en la ampliación del ancho de banda. También se usó el protocolo GLBP para implementar redundancia de equipos y balanceo de carga entre ellos. Al culminar con la implementación del presente proyecto se pudo concluir que, gracias al servidor RADIUS, un usuario inalámbrico puede autenticarse e ingresar a la red; asimismo, el servidor TACACS+, teniendo como base el nivel de privilegio del usuario, permite a este ingresar o no a los equipos de red para realizar configuraciones en los equipos. Se diseñó una solución teniendo en cuenta las características más valoradas por los usuarios finales: continuidad de servicio, rapidez en el intercambio de datos y seguridad de la información. Luego de finalizar el análisis económico, con ayuda de los métodos financieros: TIR y VAN, se

determinó que este proyecto es rentable y la inversión se recupera durante el primer año.

❖ **(Saavedra Mejía, 2015)**. Diseño e implementación de un sistema integrado De gestión de equipos de seguridad. Para optar el Título de Magister en Ingeniería de las Telecomunicaciones. Los puntos más resaltantes que se pueden rescatar de este trabajo de tesis son: Se integró el monitoreo de equipos de seguridad heterogéneos en la red. Se logró implementar el monitoreo de 1 cluster compuesto por 2 firewalls Check Point, 1 cluster de 2 firewalls Juniper, 1 sensor IPS McAfee, 1 proxy web Bluecoat, 1 proxy antivirus Bluecoat. Se logró el monitoreo de parámetros de funcionamiento y rangos de operación acorde con los requerimientos de gestión propios de cada equipo. Entre los cuales podemos mencionar, el monitoreo de conexiones en cada equipo, así como el detalle de consumo de recursos en cada uno de los equipos sincronizados. Se automatizó el proceso de notificación vía correo electrónico de advertencias y alertas en cada uno de los equipos sincronizados, logrando obtener un monitoreo activo a partir de la generación de notificaciones y reportes. Se demostró que se puede atender los principales requerimientos de gestión de equipos de seguridad heterogéneos en una red mediante el uso de tecnologías disponibles y de libre acceso, sin implicar mayores costos de licenciamiento o adquisición. Finalmente, en base a la implementación del sistema de gestión, se logró obtener una herramienta de monitoreo que en base a su diseño funcional nos permite anticipar posibles fallas de funcionamiento y mejorar los tiempos de respuesta frente a incidencias.

❖ **(Cohn Muroy, 2011)**. Análisis, diseño e implementación de una aplicación para la administración de las herramientas de seguridad en una red local. Para optar por el Título de Ingeniero Informático. Los puntos más resaltantes que se pueden rescatar de este trabajo de tesis son: Mientras más sencilla y fácil de utilizar sea una aplicación para los usuarios, los riesgos de llevar a cabo una inadecuada configuración son menores; asimismo, el tiempo invertido en llevar a cabo las configuraciones es menor, lo cual permite asignar dicho personal a tareas críticas. El riesgo que muchos usuarios carezcan de conocimientos en cuanto a reglas de seguridad, puede ser aminorado haciendo uso de una solución que le ayude a establecer reglas y configuraciones iniciales claras y fáciles de comprender. A pesar de las soluciones que permiten configurar y asegurar las redes y sistemas; siempre existirá un nivel de riesgo a ataques, mientras los usuarios no concienten sobre los riesgos a los que se hallan expuestos.

C. A nivel local:

❖ Se realizaron las búsquedas en los repositorios de las Universidades e Institutos de la ciudad y no se encontró trabajos de investigaciones similares al trabajo de investigación presente.

2.2. Bases Teóricas

A. Servidores: (Marchionni, 2011) Un servidor puede encontrarse en un típico local que ofrece el uso de computadoras a sus clientes. La máquina que tiene el cajero da un servicio; es un servidor, encargado de habilitar o deshabilitar una PC para que pueda ser usada para navegar o jugar. Si deja de funcionar, el negocio no factura, y ninguna de las máquinas cliente podría ser utilizada. Los servidores son equipos informáticos que brindan un servicio en la red. Dan información a otros servidores y a los usuarios. Son

equipos de mayores prestaciones y dimensiones que una PC de escritorio. Una computadora común tiene un solo procesador, a veces de varios núcleos, pero uno solo. Incluye un disco rígido para el almacenamiento de datos con una capacidad de 250 GB a 300 GB, en tanto que la memoria RAM suele ser de 2 a 16 GB. Un servidor, en cambio, suele ser más potente. Puede tener varios procesadores con varios núcleos cada uno; incluye grandes cantidades de memoria RAM, entre 16 GB a 1 TB, o más; mientras que el espacio de almacenamiento ya no se limita a un disco duro, sino que puede haber varios de ellos, con capacidad del orden del TB. Debido a sus capacidades, un servidor puede dar un solo servicio o más de uno.

B. Software Libre (Daniel, 2011) : No podemos hablar de software libre sin antes saber que existen muchos modelos para distribuir software y que éste es sólo uno de ellos, que tiene muchos beneficios y nos permitirá explotar todas nuestras cualidades como usuarios de computadoras. Este modelo fue desarrollado por Richard Stallman, quien hoy en día es un reconocido gurú de la tecnología mundial.

C. GNU/Linux: (Benchimol, 2011), es un sistema operativo que, al igual que cualquier otro (como puede ser Windows o Solaris), nos brinda operatividad sobre una computadora. En este momento, es bueno recordar que un sistema informático está constituido en forma tripartita por los recursos de hardware, los recursos de software y los usuarios, siendo cada una de sus partes tan importante como las otras dos.

Otro autor nos habla sobre Linux (**Javier García de Jalón, Iker Aguinaga, Alberto Mora, 2000**): Linux es un sistema operativo gratuito y de libre distribución inspirado en el sistema Unix, escrito por Linus Torvalds con la ayuda de miles de programadores en Internet. Unix es un sistema operativo desarrollado en 1970, una de cuyas mayores ventajas es que es fácilmente portable a diferentes

tipos de ordenadores, por lo que existen versiones de Unix para casi todos los tipos de ordenadores, desde PC y Mac hasta estaciones de trabajo y superordenadores.

¿Qué son las distribuciones?

Una de los primeros conceptos que aparecen al iniciarse en Linux es el concepto de distribución. Una distribución es un agrupamiento del núcleo del sistema operativo Linux (la parte desarrollada por Linus Torvalds) y otra serie de aplicaciones de uso general o no tan general.

Las distribuciones más conocidas son RedHat, Debian, Slackware, SuSE y Corel Linux, todas ellas incluyen el software más reciente y empleado lo cual incluye compiladores de C/C++, editores de texto, juegos, programas para el acceso a Internet, así como el entorno gráfico de Linux: X Window.

Entorno de trabajo: el shell y X Window

Al contrario que otros sistemas operativos, por defecto el trabajo con Linux no se realiza de una forma gráfica, sino introduciendo comandos de forma manual. Linux dispone de varios programas que se encargan de interpretar los comandos que introduce el usuario y realiza las acciones oportunas en respuesta.

Usuarios y grupos

Linux es un sistema operativo multitarea y multiusuario. Esto quiere decir que es capaz de ejecutar varios programas (o tareas) de forma simultánea y albergar a varios usuarios de forma simultánea. Por lo tanto, todos los usuarios de Linux deben tener una cuenta de usuario en el sistema que establezca los privilegios del mismo. A su vez Linux organiza a los usuarios en grupos de forma que se puedan establecer privilegios a un determinado grupo de trabajo, para el acceso a determinados archivos o servicios del sistema.

Distribución Ubuntu (Benchimol, 2011): Dentro del gran universo de distribuciones Linux, Ubuntu tiene hoy la gran distinción de ser la más

utilizada y elegida entre todas las opciones. Es una distribución de origen africano apadrinada por la Fundación Canonical, y su mayor representante y fundador, Mark Shuttleworth, es quien desde hace algún tiempo es la cara visible de Ubuntu en todo el mundo. Por esto, recorre el planeta difundiendo su proyecto, y dando charlas y seminarios sobre software libre y Ubuntu.

A continuación, haremos un repaso por los sabores más famosos de Ubuntu para estar informados y, por qué no, para darle también la oportunidad a alguno de estos interesantes sistemas:

Ubuntu Server: bajo el aval de Canonical, esta distribución es lanzada en conjunto con la versión desktop (cada seis meses). Se trata de una variante especialmente diseñada para servidores y es elegida por muchas empresas por su gran estabilidad y soporte.

Ubuntu Netbook Remix: es un proyecto que había sido anunciado en el año 2008, cuando se liberó su primera versión. Netbook Remix de Ubuntu tuvo mucha repercusión con su versión 9, lanzada en abril de 2009. Es un sistema operativo pensado para el mercado de netbooks y cuenta con soporte de hardware para estas computadoras.

Kubuntu: sin lugar a dudas, es la edición más importante luego de Ubuntu. Básicamente, es el mismo sistema operativo, pero utiliza otro gestor de escritorio: en lugar de hacer uso de Gnome, Kubuntu implementa KDE. Como sabemos, KDE ofrece una apariencia mucho más lujosa que Gnome, pero también requiere algo más de hardware.

Edubuntu: ésta es otra distribución famosa basada en Ubuntu. Esta solución está especialmente desarrollada para un caso muy puntual: ofrecer un completo sistema operativo para dotar de un sistema Linux a los equipos de las salas de computación de las escuelas. Para esto se realizaron varias adaptaciones; las más importantes tienen que ver con el software incluido, ya que aquí veremos muchas aplicaciones muy útiles para niños en edad escolar primaria, como la conocida suite Gcompris. Otra virtud destacable es que a nivel de diseño, la apariencia

tradicional de Gnome sobre Ubuntu ha sido altamente modificada, para ofrecer un entorno más divertido, con cambios en el escritorio y en el diseño de los iconos, entre otras cosas.

Xubuntu: como ya vimos en el capítulo anterior, existen muchas distribuciones que nos permiten reciclar nuestras viejas computadoras, volviéndolas a la vida con un sistema operativo Linux actual como Puppy. Lógicamente, el universo Ubuntu no podía dejar de participar en este rubro tan demandado por parte de los usuarios, por lo que es bueno saber que en Xubuntu encontraremos una distribución pensada para consumir pocos recursos de hardware. Básicamente, esto se debe a la inclusión del manejador de ventanas XFCE, que sustituye a Gnome como administrador de escritorio. Esto hace que Xubuntu pueda funcionar con una PC bien básica: sólo requiere un microprocesador de al menos 200 MHz y 64 MB de memoria RAM.

GNewSense: el principal inconveniente que tiene Ubuntu (dependiendo de qué punto de vista se lo observe) es que incluye algunas aplicaciones y códecs que son cerrados y propietarios. Aunque cueste crearlo, los usuarios más fundamentalistas y arraigados a la libertad de software no comparten esa ideología de desarrollo en la distribución. Es por eso que, como tenemos soluciones para todos los gustos, la Free Software Foundation puso manos en el asunto y desarrolló, para los amantes de la libertad extrema y absoluta, una distribución basada en Ubuntu que no incluye ningún paquete propietario, por lo que tenemos una distribución 100% libre.

El problema de esto es que, lamentablemente, hay algunas tareas que no podremos hacer. También existe otra distribución que forma parte del proyecto Ubuntu desarrollada bajo la misma idea, ofrecer un sistema totalmente libre. La solución lleva Gobuntu por nombre.

Sistemas de archivos

Un sistema de archivos sirve para estructurar la información en un disco rígido o en una unidad de almacenamiento. Los diferentes

sistemas de archivos que vamos a utilizar en nuestro universo libre suelen generar confusión a muchos usuarios a la hora de decidirse por uno. Por eso, a continuación, veremos una lista de los más utilizados, acompañados por una explicación concisa de cada uno, para que no nos queden dudas.

Ext2

Conocido también como Second Extended Filesystem, fue utilizado durante mucho tiempo en el sistema que estamos conociendo, e incluso en la actualidad está disponible a la hora de formatear. El principal inconveniente que trae aparejado su uso es que no permite la utilización de journaling (registros diarios), que nos posibilita tener un control en caso de que el sistema falle por alguna razón, y que tras ese fallo el sistema se recupere.

Ext3

Podemos decir, sin temor a equivocarnos, que hoy en día Ext3 es el sistema de archivos más utilizado en Linux, ya que muchas de las distribuciones actuales lo tienen y lo recomiendan por defecto. Si hace más de un año que el sistema Linux está instalado en una PC y no se ha cambiado esta opción durante la instalación, de seguramente esa partición GNU está corriendo bajo este sistema. Su principal ventaja es el registro diario incluido en él, algo que, como comentábamos antes, no se encontraba en su versión anterior

Ext4

Desde la última versión de Ubuntu que descargamos, está disponible en forma nativa esta nueva versión del sistema de archivos más conocido. En esta ocasión, todas nuestras experiencias con él han sido sumamente satisfactorias, porque tiene una gran velocidad en su desempeño. Desde ya, recomendamos su utilización cuando instalemos Ubuntu o cualquier otra distribución nueva que lo incluya.

XFS

XFS es un sistema de archivos bastante antiguo, pensado para funcionar nativamente en 64 bits, aunque también puede hacerlo en 32. Está disponible en Linux desde hace poco tiempo en el kernel y, al igual que sucede con Extended4 y Reiser, tiene soporte para journaling. Este sistema es recomendable si trabajamos con archivos de gran tamaño, por lo que, si éste no es nuestro caso, será mejor elegir otra opción como solución.

D. Seguridad en Redes: En esta sección veremos algunos mecanismos de seguridad orientado a las redes de computadoras:

Detección de intrusos

Inevitablemente, el mejor sistema de prevención contra la intrusión fallará. Una segunda línea de defensa del sistema es la detección de la intrusión, y ésta ha sido el centro de gran parte de la investigación de los últimos años. Este interés está motivado por una serie de consideraciones, que incluyen las siguientes:

1. Si se detecta una intrusión con bastante rapidez, el intruso puede ser identificado y expulsado del sistema antes de producir daños o comprometer datos. Incluso si la detección no se realiza con suficiente brevedad para evitar la intrusión, cuanto antes se detecte, menor será la gravedad de los daños y más rápidamente se podrá lograr la recuperación.
2. Un sistema efectivo de detección de la intrusión puede servir como elemento disuasivo, actuando para prevenir intrusiones.
3. La detección de intrusos facilita la recopilación de información sobre técnicas de intrusión, que se puede usar para reforzar la prevención de la intrusión. La detección de la intrusión se basa en la idea de que el comportamiento del intruso difiere del comportamiento del usuario legítimo de manera cuantificable. Es evidente que no se puede esperar que haya una distinción exacta entre un ataque realizado por

un intruso y el uso normal de las fuentes por parte de un usuario autorizado. Más bien, debemos esperar que haya un solape.

Detección estadística de anomalías

Como ya se mencionó, las técnicas de detección estadística de anomalías forman parte de dos grandes categorías: la detección de umbrales y los sistemas basados en perfiles. La detección de umbrales implica contar el número de incidencias de un tipo de evento específico en un intervalo de tiempo. La intrusión se asume si el cómputo sobrepasa lo que se considera un número razonable que se podría esperar que ocurriera.

El análisis de los umbrales, por sí mismo, es un detector ordinario y poco efectivo de ataques incluso moderadamente sofisticados. Se debe determinar tanto el límite como el intervalo de tiempo. Por la diversidad de los usuarios, es probable que dichos umbrales generen un gran número de falsos positivos o de falsos negativos. Sin embargo, los detectores simples de los umbrales pueden ser útiles en conjunción con técnicas más sofisticadas. La detección de anomalías basada en perfiles se centra en caracterizar el comportamiento pasado de usuarios individuales o grupos relacionados de usuarios y luego detectar desviaciones significativas. Un perfil puede consistir en un conjunto de parámetros, para que la desviación de un solo parámetro no pueda ser suficiente en sí misma para indicar alerta.

El fundamento de este enfoque es un análisis de los registros de auditoría. Éstos constituyen una aportación a la función de detección de la intrusión de dos formas.

Primero, el diseñador debe decidir sobre un número de métricas cuantitativas que puedan usarse para medir el comportamiento del usuario. Se puede emplear un análisis de los registros de auditoría en un período de tiempo para determinar el perfil de actividad del usuario medio. Así, los registros de auditoría sirven para definir el comportamiento típico.

En segundo lugar, los registros actuales de auditoría son la entrada que se usa para detectar la intrusión. Es decir, el modelo de detección de

intrusión analiza los registros de auditoría entrantes para determinar la desviación del comportamiento medio. Los siguientes son ejemplos de métricas útiles para la detección de la intrusión basada en perfiles:

Contador: número entero no negativo que puede ser incrementado, pero no disminuido hasta que sea inicializado por una acción de la administración. Normalmente, se guarda una cuenta de ciertos tipos de acontecimientos durante un período de tiempo concreto. Algunos ejemplos incluyen el número de accesos realizados por un solo usuario durante una hora, el número de veces que se ejecuta un comando dado durante una sola sesión de usuario y el número de fallos en la contraseña durante un minuto.

Calibre: número entero no negativo que puede ser incrementado o disminuido. Normalmente, un calibre se usa para medir el valor actual de alguna entidad. Algunos ejemplos incluyen el número de conexiones lógicas asignadas a una aplicación de usuario y el número de mensajes salientes en espera para un proceso de usuario.

Utilización de recursos: la cantidad de recursos consumidos durante un período específico. Algunos ejemplos incluyen el número de páginas impresas durante una sesión de usuario y el tiempo total consumido por la ejecución de un programa. Dadas estas métricas generales, se pueden llevar a cabo distintas pruebas para determinar si la actividad actual encaja dentro de límites aceptables se presenta los siguientes enfoques que pueden adoptarse:

- ✓ Multivariable
- ✓ Procesos de Markov
- ✓ Serie temporal
- ✓ Operativo

La prueba estadística más sencilla es medir la media y la desviación estándar de un parámetro en un período histórico. Esto da una idea del comportamiento medio y su variabilidad. El uso de la media y la

desviación estándar es aplicable a una gran variedad de contadores, temporizadores y medidas de recursos. Pero estas medidas, por sí mismas, son en general demasiado toscas para las intenciones de detección de la intrusión.

Un modelo se basa en las correlaciones entre dos o más variables. El comportamiento del intruso puede caracterizarse con mayor exactitud teniendo en cuenta dichas correlaciones (por ejemplo, el tiempo del procesador y el uso de los recursos, o la frecuencia de entrada y el tiempo transcurrido en la sesión).

Cortafuegos

Los cortafuegos pueden ser un medio eficaz de protección de un sistema o red local frente a las amenazas de seguridad provenientes de la red, mientras que al mismo tiempo proporcionan acceso al exterior mediante redes de área ancha e Internet.

Los sistemas de información de corporaciones, agencias gubernamentales y otras instituciones han experimentado una evolución constante:

- ✓ Sistemas de procesamiento de datos centralizados, con un gran computador central (mainframe) al que se conectan directamente una serie de terminales.
- ✓ Redes de área local (LAN) que conectan computadores personales y terminales entre ellos y con el computador central.
- ✓ Red del edificio de una empresa, compuesta de varias LAN, que conecta entre sí a computadores personales, servidores y quizás uno o dos computadores centrales.
- ✓ Red de toda la empresa, formada por múltiples redes corporativas distribuidas geográficamente y que se conectan entre sí mediante una red privada de área ancha (WAN).
- ✓ Conectividad con Internet, por la cual todas las redes corporativas se enganchan a Internet y también podrían o no estar conectadas por una WAN privada.

Para la mayoría de las organizaciones, la conexión a Internet ha dejado de ser una opción para convertirse en una necesidad, debido a que la información y los servicios disponibles les son esenciales. Incluso, usuarios individuales dentro de la organización quieren y necesitan acceso a Internet, y si esto no se le suministra mediante su LAN, utilizarán la capacidad de conexión telefónica de su PC con un proveedor de servicio de Internet (ISP, Internet Service Provider). Sin embargo, mientras el acceso a Internet beneficia a la organización, también constituye una amenaza, y a que permite al mundo exterior llegar hasta la red local e interactuar con ella. A pesar de que es posible equipar a cada estación de trabajo y a cada servidor de la red corporativa con fuertes características de seguridad, como por ejemplo protección de intrusos, este enfoque no es práctico.

Consideremos una red con cientos o miles de sistemas, funcionando con una mezcla de distintas versiones de UNIX, más Windows. Cuando se descubre un fallo de seguridad, cada sistema que pueda estar afectado debe ser actualizado para corregir el fallo. La alternativa, cada vez más aceptada, es el cortafuego. El cortafuego se inserta entre la red corporativa e Internet para establecer un enlace controlado y levantar un muro de seguridad exterior o perímetro. El objetivo de este perímetro es proteger la red corporativa de ataques procedentes de Internet y proporcionar un único punto de resistencia donde implantar la seguridad y la auditoría. El cortafuego puede ser un único sistema o un conjunto de dos o más sistemas que cooperan para realizar la función de cortafuegos.

Características de los cortafuegos

1. Todo el tráfico desde el interior hacia el exterior, y viceversa, debe pasar a través del cortafuego. Esto se consigue bloqueando físicamente todos los accesos a la red local excepto a través del cortafuego. Hay diferentes configuraciones, como se explicará más tarde en esta sección.
2. Se permitirá pasar solamente el tráfico autorizado, definido por la política de seguridad local. Se utilizan diferentes tipos de cortafuegos

que implementan diferentes tipos de políticas de seguridad, como se explicará más tarde en esta sección.

3. El propio cortafuego es inmune a la penetración. Esto implica que utiliza un sistema de confianza con un sistema operativo seguro.

Se presenta cuatro técnicas generales que utilizan los cortafuegos para controlar el acceso e imponer la política de seguridad del sitio. Originalmente, los cortafuegos se centraban principalmente en el control de servicios, pero han ido evolucionando para proporcionar las cuatro técnicas:

- ✓ **Control de servicio:** determina los tipos de servicios de Internet a los que se puede acceder, interna o externamente. El cortafuego puede filtrar el tráfico basándose en las direcciones IP y el número de puertos TCP; puede proporcionar software de proxy que reciba e interprete cada solicitud de servicio antes de permitir su paso; o puede alojar software del servidor como, por ejemplo, un servicio de correo o de web.
- ✓ **Control de dirección:** determina en qué dirección se pueden iniciar las solicitudes de servicios particulares y en qué dirección se les permite el paso a través del cortafuego.
- ✓ **Control de usuario:** controla el acceso a un servicio en función de qué usuario esté intentando acceder a él. Esta característica se aplica normalmente a usuarios que se hallan dentro del perímetro del cortafuego (usuarios locales). También puede aplicarse al tráfico entrante desde usuarios externos; pero esto último requiere algún tipo de tecnología de autenticación segura.
- ✓ **Control de comportamientos:** controla cómo se utilizan los servicios particulares. Por ejemplo, el cortafuego puede filtrar el correo electrónico para eliminar el «correo basura», o puede permitir el acceso externo sólo a una parte de la información de un servidor web local.

TIPOS DE CORTAFUEGOS

Router de filtrado de paquetes

Un router de filtrado de paquetes aplica un conjunto de reglas a cada paquete IP y entonces retransmite o descarta dicho paquete. El router, normalmente, se configura para filtrar paquetes que van en ambas direcciones (desde y hacia la red interna). Las reglas de filtrado se basan en la información contenida en un paquete de red.

Cortafuegos de inspección de estado

Un filtrador de paquetes tradicional toma decisiones de filtrado basadas en un paquete individual y no tiene en cuenta ningún contexto del nivel más alto. Para entender qué se entiende por contexto y por qué un filtrador de paquetes tradicional está limitado con respecto al contexto, es necesario hacer un pequeño repaso. La mayoría de las aplicaciones estandarizadas que funcionan encima de TCP siguen un modelo cliente/servidor.

Por ejemplo, para SMTP, el correo electrónico se transmite de un sistema a cliente a un sistema a servidor. El sistema a cliente genera nuevos mensajes de correo electrónico, normalmente introducidos por usuarios. El sistema servidor acepta mensajes de correo electrónico entrantes y los aloja en los buzones de usuario adecuados. SMTP funciona estableciendo una conexión TCP entre cliente y servidor, en la que el número de puerto TCP del servidor, que identifica a la aplicación servidor SMTP, es 25. El número de puerto TCP para el cliente SMTP es un número entre 1024 y 16383 generado por el cliente SMTP.

En general, cuando una aplicación que utiliza TCP crea una sesión con un computador remoto, ésta crea una conexión TCP en la que el número de puerto TCP de la aplicación remota (el servidor) es un número menor que 1024 y el número de puerto TCP de la aplicación local (el cliente) es un número entre 1024 y 16383.

Los números menores que 1024 son los números de puerto «conocidos» y están asignados permanentemente a aplicaciones particulares (por ejemplo, 25 para servidor SMTP). Los números de puerto

entre 1024 y 16383 se generan dinámicamente y tienen significado temporal solamente durante el período de tiempo en que está establecida una conexión TCP.

Pasarela del nivel de aplicación

Una pasarela del nivel de aplicación, también llamada servidor proxy; actúa como un repetidor del tráfico del nivel de aplicación. El usuario contacta con la pasarela utilizando una aplicación TCP/IP como, por ejemplo, Telnet o FTP, y la pasarela solicita al usuario el nombre del computador remoto al que desea acceder. Cuando el usuario responde y proporciona un identificador de usuario e información de autenticación válidos, la pasarela contacta con la aplicación en el computador remoto y retransmite los segmentos TCP que contienen los datos de aplicación entre los dos puntos finales. Si la pasarela no implementa el código proxy de una aplicación específica, entonces el servicio no está permitido y no puede atravesar el cortafuego. Además, la pasarela puede configurarse para permitir solamente algunas características específicas de una aplicación que el administrador de red considere aceptables mientras que deniega las otras características. Las pasarelas del nivel de aplicación tienden a ser más seguras que los filtradores de paquetes. En vez de intentar tratar con numerosas combinaciones posibles que se van a permitir y prohibir en el nivel TCP y en el IP, la pasarela del nivel de aplicación necesita solamente escrutar unas pocas aplicaciones permitidas. Además, es fácil registrar y auditar todo el tráfico entrante del nivel de aplicación.

La desventaja principal de este tipo de pasarelas es la sobrecarga de procesamiento adicional en cada conexión. En efecto, hay dos conexiones enlazadas entre los usuarios finales, con la pasarela como punto de enlace, y la pasarela debe examinar y reenviar todo el tráfico en ambas direcciones.

Pasarela del nivel de circuito

Un tercer tipo de cortafuegos es la pasarela del nivel de circuito. Ésta puede ser un sistema autónomo o puede ser una función especializada

realizada por una pasarela del nivel de aplicación para ciertas aplicaciones. Una pasarela del nivel de circuito no permite una conexión TCP extremo a extremo; en vez de eso, la pasarela establece dos conexiones TCP, una entre ella y un usuario TCP en un computador interno, y otra entre ella y un usuario TCP en un computador externo. Una vez se han establecido las dos conexiones, la pasarela normalmente retransmite segmentos TCP desde una conexión hacia la otra sin examinar los contenidos. La función de seguridad consiste en determinar qué conexiones serán permitidas.

Un uso común de una pasarela del nivel de circuito se da en una situación en la que el administrador del sistema confía en los usuarios internos. La pasarela se puede configurar para permitir servicio del nivel de aplicación o proxy para conexiones entrantes y funciones del nivel de circuito para conexiones salientes. En esta configuración, la pasarela puede incurrir en la sobrecarga del procesamiento necesario para examinar datos de aplicaciones entrantes para funciones prohibidas, pero no incurre en esa sobrecarga para los datos salientes.

Servidor Proxy (McNab, 2008): Un proxy, o servidor proxy, en una red informática, es un servidor —programa o dispositivo—, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C).

2.3. Definiciones conceptuales

- ✓ **CACHE:** En informática, la memoria caché es la memoria de acceso rápido de un microprocesador, que guarda temporalmente los datos recientes de los procesados (información).
- ✓ **DNS:** El sistema de nombres de dominio (DNS, por sus siglas en inglés, Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información

variada con nombre de dominio asignado a cada uno de los participantes.

- ✓ **FTP:** Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.
- ✓ **HTTP:** Es el protocolo de comunicación que permite las transferencias de información en la World Wide Web
- ✓ **IP:** Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizando la red.
- ✓ **ISP:** El proveedor de servicios de Internet (ISP, por la sigla en inglés de Internet service provider) es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, cablemódem, GSM, dial-up, etcétera.
- ✓ **KERNEL:** En informática, un núcleo o kernel (de la raíz germánica Kern, núcleo, hueso) es un software que constituye una parte fundamental del sistema operativo, y se define como la parte que se ejecuta en modo privilegiado (conocido también como modo núcleo).
- ✓ **RAM:** La memoria de acceso aleatorio (Random Access Memory, RAM) se utiliza como memoria de trabajo de computadoras para el sistema operativo, los programas y la mayor parte del software. En la RAM se cargan todas las instrucciones que ejecuta la unidad

central de procesamiento (procesador) y otras unidades del computador.

- ✓ **ROUTER:** Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red), y que por tanto tienen prefijos de red distintos.
- ✓ **SHELL:** En informática, el shell o intérprete de órdenes o intérprete de comandos es el programa informático que provee una interfaz de usuario para acceder a los servicios del sistema operativo.
- ✓ **TCP:** Es uno de los protocolos fundamentales en Internet.
- ✓ **UNIX:** Unix (registrado oficialmente como UNIX®) es un sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969, por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Dennis Ritchie, Ken Thompson y Douglas McIlroy.
- ✓ **WAN:** Una red de área amplia, o WAN, (Wide Area Network en inglés), es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física. Muchas WAN son construidas por organizaciones o empresas para su uso privado, otras son instaladas por los proveedores de internet (ISP) para proveer conexión a sus clientes.
- ✓ **WORKFLOW:** El flujo de trabajo (workflow en inglés) es el estudio de los aspectos operacionales de una actividad de trabajo: cómo se estructuran las tareas, cómo se realizan, cuál es su orden correlativo, cómo se sincronizan, cómo fluye la información que soporta las tareas y cómo se le hace seguimiento al cumplimiento de las tareas. Generalmente los problemas de flujo de trabajo se modelan con redes de Petri.

2.4. Hipótesis

Hipótesis General

La implementación de un servidor mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.

Hipótesis Específicas

- A.** La implementación de los controles de seguridad asociados a servicios de red mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.

- B.** La implementación los controles de seguridad asociados a la restricción del acceso de la información mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.

2.5. Variables

2.5.1. Variable Calibración

X: Servidor de Seguridad en Linux.

2.5.2. Variable Evaluativa

Y: Seguridad de la red de área local.

2.6. Operacionalización de Variables

VARIABLE	INDICADORES		TIPO DE VARIABLE
Calibración Servidor de Seguridad en Linux	<ul style="list-style-type: none"> ✓ Servidor Linux (Ubuntu server) ✓ Capacidad de almacenamiento. ✓ Copias de seguridad. ✓ Control y administración de todas las peticiones que le hagan las demás computadoras. 		Nominal Dicotómica
VARIABLE	DIMENSIONES	INDICADORES	TIPO DE VARIABLE
Evaluativa Seguridad de la red de área local	Controles de seguridad asociados a servicios de red (Proxy y Firewall)	<ul style="list-style-type: none"> ✓ Cantidad de conexiones por día. ✓ Cantidad de bytes accedidos por día. ✓ Cantidad de páginas no autorizadas visitadas 	Numérica
	Controles de seguridad asociados a la restricción del acceso de la información (Servidor de archivos)	<ul style="list-style-type: none"> ✓ Cantidad de carpetas y archivos creados. ✓ Cantidad de carpetas y archivos modificados. ✓ Cantidad de carpetas y archivos eliminados. 	Numérica

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Tipo de Investigación

El presente trabajo de investigación es de tipo aplicada, se caracteriza por su interés en la aplicación, utilización y consecuencias prácticas de los conocimientos.

3.1.1. Enfoque

El presente estudio de investigación tiene el enfoque cuantitativo (**Sampieri, 2014**), “usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías”.

3.1.2. Alcance

Esta investigación por su naturaleza es de nivel aplicativo, debido a que se implementara un servidor de seguridad para mejorar la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano.

3.1.3. Diseño

El diseño que presenta el estudio de investigación es el pre experimental (tiene una pre y post prueba en el grupo de la investigación), teniendo en cuenta la explicación de (**Sampieri, 2014**):

G: O1 X O2

Dónde:

G = Grupo de investigación (trabajadores del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco)

X = Aplicación (Servidor de seguridad)

O₁ = Pre Observación

O₂ = Post Observación

3.2. Población y Muestra

La población está conformada por **320** trabajadores de todas las áreas del Hospital de Contingencia Hermilio Valdizán Medrano de la ciudad de Huánuco, y como muestra se ha tomado solo a los trabajadores del área administrativa siendo un total de:

$$n = 40$$

Cabe aclarar en esta sección que la muestra será referencial, mejor dicho, se usará a los trabajadores para que realicen las actividades en la red, pero en si se medirá los flujos de los datos en la red en relación a la seguridad del acceso a la información y la seguridad de los servicios de red en base a las métricas brindadas por el ISO 27002:2013.

3.3. Técnicas e instrumentos de recolección de datos

En el trabajo de investigación se utilizó la observación directa como técnica y la ficha de evaluación técnica como instrumento. En la ficha de evaluación técnica se ingresarán los resultados provenientes de los sistemas de monitoreo de cada servicio de red.

Técnica:

Observación

Instrumento:

Ficha de evaluación técnica

3.4. Técnicas para el procesamiento y análisis de la información

Las técnicas para el procesamiento de la información son las que se emplearan para el correcto análisis, ordenamiento, procesamiento y presentación de la información recabada en la investigación, de las cuales contamos con el software SPSS que nos permitirá realizar la prueba de hipótesis, así como también la presentación de los resultados usando los cuadros y gráficos estadísticos.

CAPÍTULO IV

RESULTADOS

4.1 Procesamiento de datos

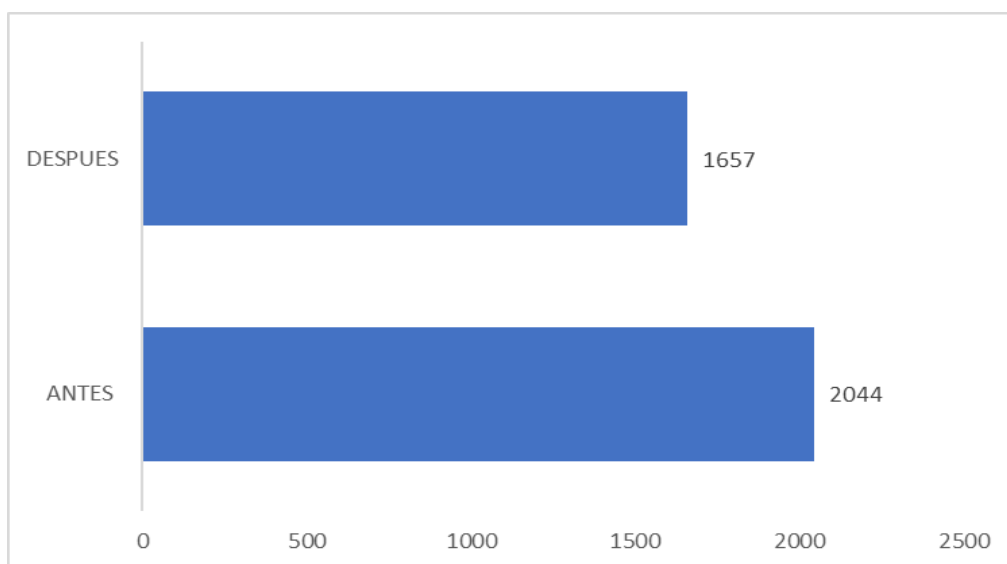
Resultados en cuanto a la dimensión: Controles de seguridad asociados a servicios de red

Tabla 1: Comparación Antes – Después de la cantidad de conexiones por día, en relación a los Controles de seguridad asociados a servicios de red.

	Antes	Después
Cantidad Conexiones	2044	1657
Total	2044	1657

Fuente: Instrumento de medición (Ficha de observación técnica)

Ilustración 1: Comparación Antes – Después de la cantidad de conexiones por día, en relación a los Controles de Seguridad asociados a servicios de red.



Fuente: Instrumento de medición (Ficha de observación técnica)

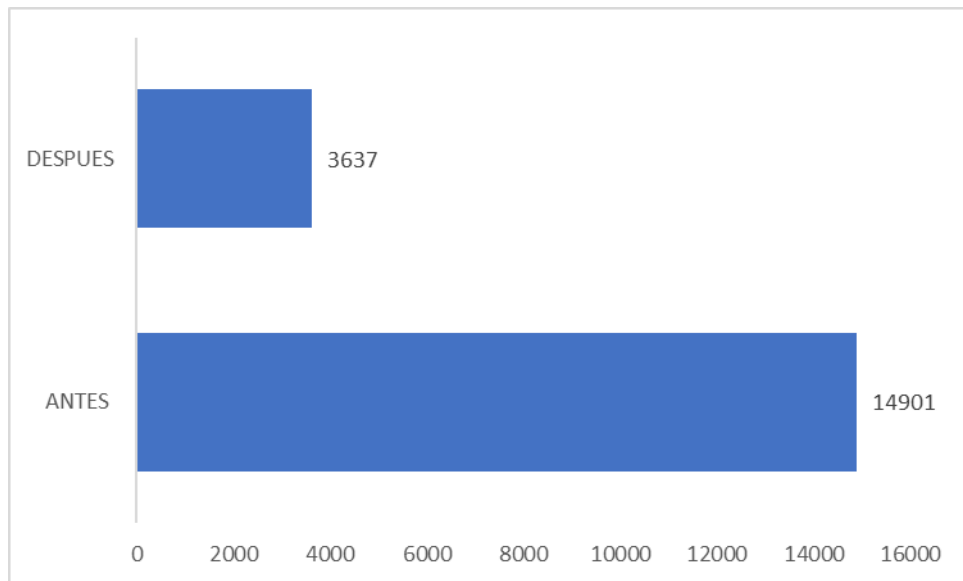
En la tabla y gráfico anterior se aprecia que hubo una disminución de la cantidad de conexiones accedidas por día, esto es por el control del servicio proxy.

Tabla 2: Comparación Antes – Después de la cantidad de MB accedidos por día, en relación a los Controles de seguridad asociados a servicios de red.

	Antes	Después
Cantidad MB	14901	3637
Total	14901	3637

Fuente: Instrumento de medición (Ficha de observación técnica)

Ilustración 2: Comparación Antes – Después de la cantidad de MB accedidos por día, en relación a los Controles de seguridad asociados a servicios de red.



Fuente: Instrumento de medición (Ficha de observación técnica)

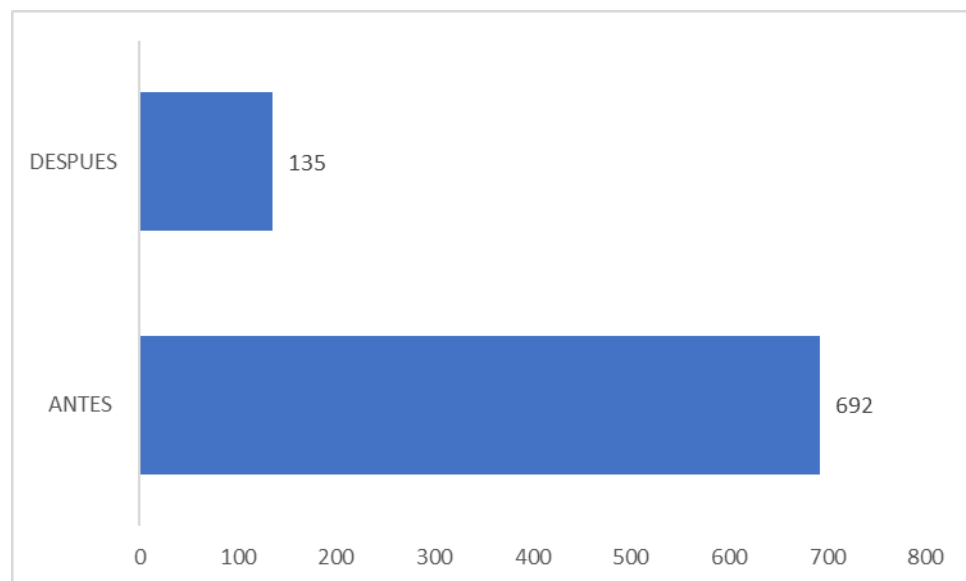
En la tabla y gráfico anterior se aprecia que hubo una disminución en la cantidad de MB accedidos por día, esto es se entiende que a menor número de conexiones también se refleja en la menor cantidad de MB consumidos.

Tabla 3: Comparación Antes – Después de la cantidad de página no autorizadas visitadas por día, en relación a los Controles de seguridad asociados a servicios de red.

	Antes	Después
Cantidad Visitas	692	135
Total	692	135

Fuente: Instrumento de medición (Ficha de observación técnica)

Ilustración 3: Comparación Antes – Después de la cantidad de página no autorizadas visitadas por día, en relación a los Controles de seguridad asociados a servicios de red.



Fuente: Instrumento de medición (Ficha de observación técnica)

En la tabla y gráfico anterior se aprecia que existe una disminución en la cantidad de páginas no autorizadas a consecuencia del filtro del proxy que evita a que se acceda a páginas bloqueadas.

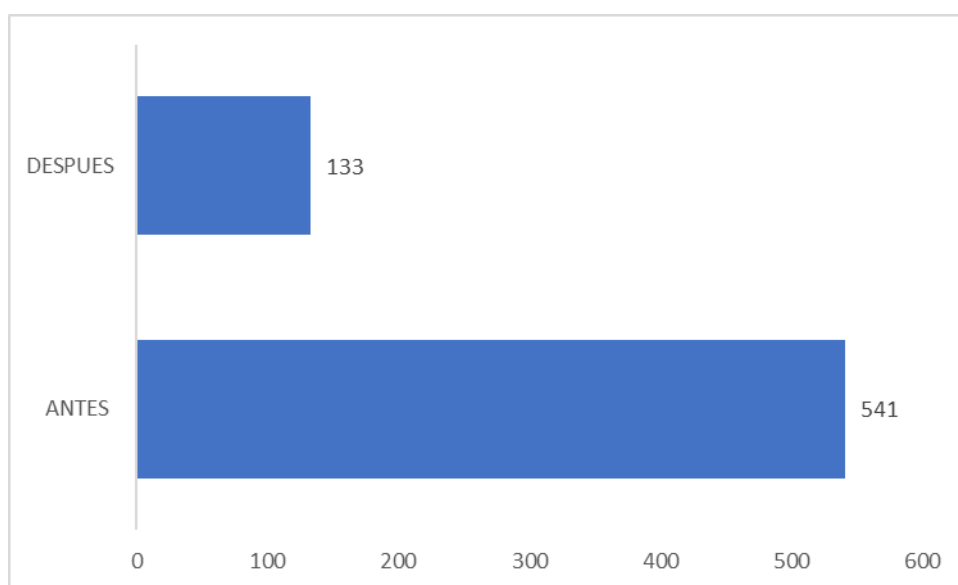
Resultados en cuanto a la dimensión: Controles de seguridad asociados a la restricción del acceso de la información.

Tabla 4: Comparación Antes - Después de la cantidad de archivos y carpetas creadas por día, en relación a los Controles de seguridad asociados a la restricción del acceso de la información.

	Antes	Después
Cantidad	541	133
Total	541	133

Fuente: Instrumento de medición (Ficha de observación técnica)

Ilustración 4: Comparación Antes - Después de la cantidad de archivos y carpetas creadas por día, en relación a los Controles de seguridad asociados a la restricción del acceso de la información.



Fuente: Instrumento de medición (Ficha de observación técnica)

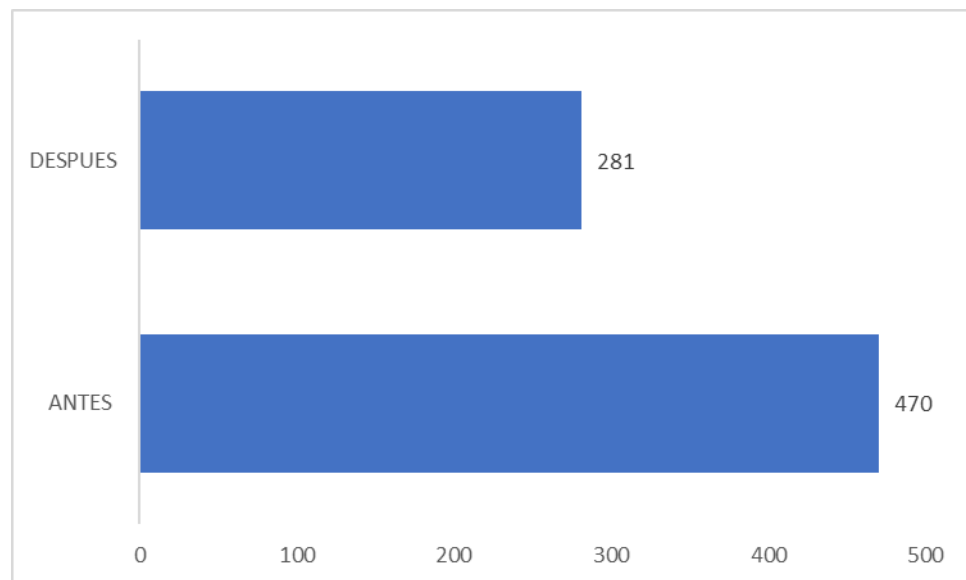
En la tabla y gráfico anterior se aprecia que existe una disminución en la cantidad de archivos y carpetas creadas, esto se debe a la restricción impuesta por el servidor de archivos.

Tabla 5: Comparación Antes - Después de la cantidad de archivos y carpetas modificadas por día, en relación a los Controles de seguridad asociados a la restricción del acceso de la información.

	Antes	Después
Cantidad	470	281
Total	470	281

Fuente: Instrumento de medición (Ficha de observación técnica)

Ilustración 5: Comparación Antes - Después de la cantidad de archivos y carpetas modificadas por día, en relación a los Controles de seguridad asociados a la restricción del acceso de la información.



Fuente: Instrumento de medición (Ficha de observación técnica)

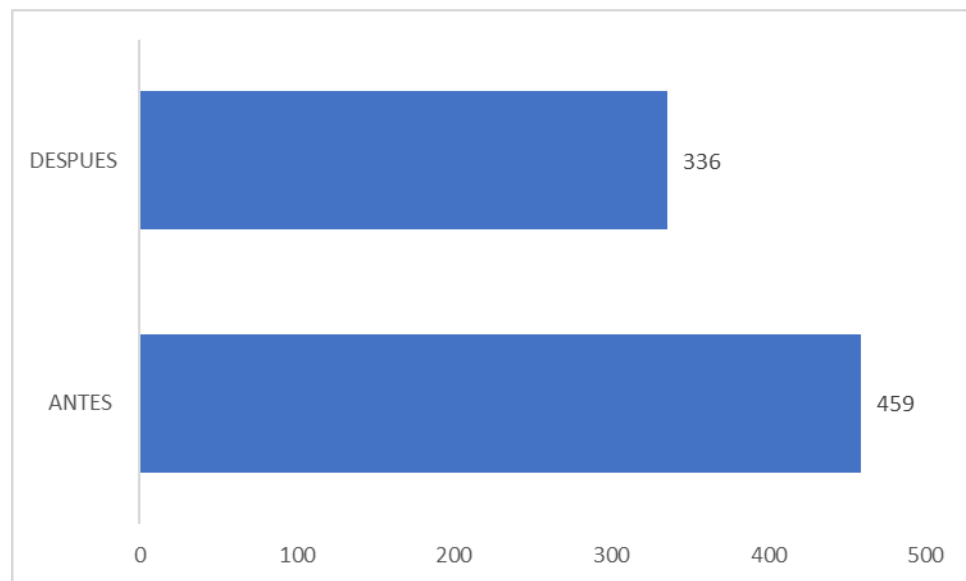
En la tabla y gráfico anterior se aprecia que existe una disminución en la cantidad de archivos y carpetas modificadas, esto se debe a la restricción impuesta por el servidor de archivos.

Tabla 6: Comparación Antes - Después de la cantidad de archivos y carpetas eliminados por día, en relación a los Controles de seguridad asociados a la restricción del acceso de la información.

	Antes	Después
Cantidad	459	336
Total	459	336

Fuente: Instrumento de medición (Ficha de observación técnica)

Ilustración 6: Comparación Antes - Después de la cantidad de archivos y carpetas eliminados por día, en relación a los Controles de seguridad asociados a la restricción del acceso de la información.



Fuente: Instrumento de medición (Ficha de observación técnica)

En la tabla y gráfico anterior se aprecia que existe una disminución en la cantidad de archivos y carpetas eliminadas, esto se debe a la restricción impuesta por el servidor de archivos.

4.2 Contrastación de hipótesis y prueba de hipótesis

Siendo las variables de tipo numérica, se optó por una prueba paramétrica: T de Student, pero antes se llevó a cabo la prueba de normalidad de los mismos, para la elección correcta del procedimiento estadístico. En virtud a ello, se obtuvieron los siguientes p-valores de cada dimensión analizada.

Tabla 7: Prueba de Kolmogorov-Smirnov para muestras relacionadas

	DIFERENCIA (PRE TEST - POST TEST) (p-valor)
Cantidad de Conexiones	0.187
Cantidad de MB	0.080
Cantidad de Páginas accedidas	0.043
Cantidad de archivos creados	0.015
Cantidad de archivos modificados	0.079
Cantidad de archivos eliminados	0.140

Fuente: Elaboración propia

Teniendo en cuenta un nivel de significancia de 5%, observamos que el p-valor nos lleva a concluir que en todos los casos los datos tienen distribución normal por lo que se considera el uso de un procedimiento paramétrico en el análisis.

Prueba de hipótesis Comparación antes – después: Cantidad de conexiones

Se ha evaluado el control de la cantidad de conexiones en la red por día antes y después de la implementación del servidor de seguridad.

Tabla 8: El ritual de la significancia Control de la cantidad de conexiones por día de la Red

1	Plantear Hipótesis Ho: El control de la seguridad de la cantidad de conexiones de la red no es mejor después de la implementación del servidor de seguridad. H1: El control de la seguridad de la cantidad de conexiones de la red es mejor después de la implementación del servidor de seguridad
2	Establecer un nivel de significancia Nivel de Significancia (alfa) $\alpha = 5\% = 0.05$
3	Seleccionar estadístico de prueba: Prueba T de Student para muestras relacionadas
4	Valor de P= 0.00187 Lectura del p-valor: Con una probabilidad de error del 0.19 % el control de la seguridad de la cantidad de conexiones de la red es mejor después de la implementación del servidor de seguridad
5	Toma de decisiones El control de la seguridad de la cantidad de conexiones de la red es mejor después de la implementación del servidor de seguridad

Interpretación

La implementación del servidor de seguridad en la red de área local del área administrativa del Hospital de Contingencia de Huánuco ha mejorado el control de las conexiones de red.

Prueba de hipótesis Comparación antes – después: Cantidad de MB consumidos por día.

Se ha evaluado el control de la cantidad de MB consumidos por día en la red antes y después de la implementación del servidor de seguridad.

Tabla 9: El ritual de la significancia Control de la cantidad de MB consumidos por día de la Red

1	<p>Plantear Hipótesis</p> <p>Ho: El control de la seguridad de la cantidad de MB consumidos por día de la red no es mejor después de la implementación del servidor de seguridad.</p> <p>H1: El control de la seguridad de cantidad de MB consumidos por día de la red es mejor después de la implementación del servidor de seguridad</p>
2	<p>Establecer un nivel de significancia</p> <p>Nivel de Significancia (alfa) $\alpha = 5\% = 0.05$</p>
3	<p>Seleccionar estadístico de prueba: Prueba T de Student para muestras relacionadas</p>
4	<p>Valor de P= 0.00080</p> <p>Lectura del p-valor:</p> <p>Con una probabilidad de error del 0.08% el control de la seguridad de la cantidad de MB consumidos por día de la red es mejor después de la implementación del servidor de seguridad</p>
5	<p>Toma de decisiones</p> <p>El control de la seguridad de cantidad de MB consumidos por día de la red es mejor después de la implementación del servidor de seguridad</p>

Interpretación

La implementación del servidor de seguridad en la red de área local del área administrativa del Hospital de Contingencia de Huánuco ha mejorado el control de consumo de MB en la red.

Prueba de hipótesis Comparación antes – después: Cantidad de páginas no autorizadas accedidas.

Se ha evaluado el control de la cantidad de páginas no autorizadas accedidas por día en la red antes y después de la implementación del servidor de seguridad.

Tabla 10: El ritual de la significancia Control de la Cantidad de páginas no autorizadas accedidas.

1	<p>Plantear Hipótesis</p> <p>Ho: El control de la seguridad de la cantidad de páginas no autorizadas accedidas por día de la red no es mejor después de la implementación del servidor de seguridad.</p> <p>H1: El control de la seguridad de cantidad de páginas no autorizadas accedidas por día por día de la red es mejor después de la implementación del servidor de seguridad</p>
2	<p>Establecer un nivel de significancia</p> <p>Nivel de Significancia (alfa) $\alpha = 5\% = 0.05$</p>
3	<p>Seleccionar estadístico de prueba: Prueba T de Student para muestras relacionadas</p>
4	<p>Valor de P= 0.000430</p> <p>Lectura del p-valor:</p> <p>Con una probabilidad de error del 0.04 % el control de la seguridad de la cantidad de páginas no autorizadas accedidas por día por día de la red es mejor después de la implementación del servidor de seguridad</p>
5	<p>Toma de decisiones</p> <p>El control de la seguridad de cantidad de páginas no autorizadas accedidas por día por día de la red es mejor después de la implementación del servidor de seguridad</p>

Interpretación

La implementación del servidor de seguridad en la red de área local del área administrativa del Hospital de Contingencia de Huánuco ha mejorado el control de consumo de MB en la red.

CAPÍTULO V

DISCUSIÓN DE RESULTADOS

En este capítulo daremos a conocer el contraste de los resultados en función a las pruebas realizadas al haber instalado un servidor de seguridad para controlar los accesos a la información por partes de los trabajadores del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de la ciudad de Huánuco.

Con respecto a los controles de seguridad asociados a servicios de red, y en relación a la cantidad de conexiones que se realizan a diario en la red externa (Internet) se aprecia que hubo una disminución de 387 conexiones, esto es debido que antes de la implantación del control de seguridad, los trabajadores realizaban accesos innecesarios a la red generando muchas conexiones y saturando la red, en una previa evaluación se determinó que se tenían un promedio de 2044 conexiones por día, mientras de después de la aplicación se obtuvo la medición de 1657 conexiones por día, esto mejoro la distribución del ancho de banda para los otros usuarios.

En cuanto a la comparación del antes y después de la cantidad de MB accedidos por día, en relación a los Controles de seguridad asociados a servicios de red hemos visto que también hubo una disminución del consumo de 11264 MB esto es debido al filtro al control de cantidad de conexiones bloqueadas por lo tanto influye en la disminución del consumo de MB de la red, dando prioridad a otras conexiones, como por ejemplo de índole laboral. Se observa que el pre test la cantidad de datos consumidos por día es de 14901 MB, mientras que después de la aplicación del servidor de seguridad y posterior evaluación, el consumo de MB se redujo a 3637 MB considerablemente una gran reducción.

Siguiendo con la discusión de resultados podemos afirmar que en relación a la cantidad de página no autorizadas visitadas por día también se logró una disminución de 557 visitas en cuanto al acceso de sitios web no autorizados, gracias al servicio del proxy que permitió bloquear aquellos sitios no deseados y que fueron recolectados en medida a las actividades de los trabajadores en la red, podemos observar en los resultados que antes de aplicar el control de

seguridad eran 692 sitios no autorizados, mientras que después de la aplicación del servidor de seguridad se redujeron a 135 visitas a paginas no autorizadas.

El acceso a la información también era un problema ya que en el servidor los usuarios podían crear grandes cantidades de archivos y así mismo eliminar y modificarlos sin control alguno, pero ya con la intervención del control de seguridad aplicado al servidor de archivos esto se mitigo y se pudo controlar mediante controles de acceso y permisos. Es así que en relación a la comparación del antes y después de la cantidad de archivos y carpetas creadas por día y los Controles de seguridad asociados a la restricción del acceso de la información se pudo observar que hubo una disminución de 408 archivos creados por día, esto se traduce que se ha evitado la creación de archivos innecesarios en el servidor, así mismo en cuanto a la modificación y eliminación de archivos también hubo una disminución: 189 y 123 respectivamente.

En conclusión, se ha optimizado la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de la ciudad de Huánuco, y por ende se ha controlado la actividad de los usuarios en la red de área local e Internet mediante la implementación de un servidor de seguridad bajo los controles asignados del ISO 27002:2013.

CONCLUSIONES

- ✓ La Implementación del servidor de seguridad para mejorar los accesos a los recursos de la red interna y externa del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco, ha sido favorable y exitosa ya que se logró minimizar la cantidad de conexiones innecesarias, la cantidad de uso de MB, y la cantidad de acceso a sitios web no autorizado y por ende se logró una mayor productividad por parte de los trabajadores ya que anteriormente a la aplicación los trabajadores usaban el tiempo de sus labores para acceder a paginas no autorizadas, descargar contenido no autorizado generando cuellos de botella en la red, también modificando y eliminando información del servidor sin autorización.

- ✓ Los controles de seguridad aplicados al área local y externa del Hospital se basaron en el ISO 27002:2013 que fue el marco de trabajo en el cual permitió escoger los controles adecuados para poder realizar las tareas de control respectivamente, se utilizó un proxy, un firewall y un servidor de archivos para controlar la actividad en la red.

- ✓ El uso de un servidor de seguridad que administra los recursos de la red, es indispensable dentro de cualquier organización por cuestiones de seguridad, facilidad de manejo de archivos, administración de cuentas de usuario y políticas de ingreso de los mismos, centralización de la información, facilidad para compartir recursos, etc.

RECOMENDACIONES

- ✓ Se recomienda a la parte administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco, brindar un presupuesto económico para el área del Centro de Cómputo e informática, para adquirir nuevos equipos (Servidores, Switch, Routers, Infraestructura adecuada)

- ✓ Se recomienda a la Institución contar con políticas de seguridad, fomentar una conciencia hacia una cultura de Seguridad de la Información con un enfoque en el cual todo el personal sea protagonista y absolutamente responsable de manejar el activo de la Institución.

- ✓ Tener en cuenta siempre, que la seguridad no es un producto, es un proceso constante que se debe ir buscando, por medio de revisiones constantes de las políticas de seguridad, de tal manera que cada día respondan favorablemente ante los nuevos retos que plantea la seguridad en redes de datos.

REFERENCIAS BIBLIOGRÁFICAS

- Benchimol, Daniel. (2011). *Linux desde cero*. Buenos aires: Fox Andina.
- Cohn Muroy, D. S. (2011). *Análisis, diseño e implementación de una aplicación para la administración de las herramientas de seguridad en una red local*. Lima.
- Javier García de Jalón, Iker Aguinaga, Alberto Mora. (2000). *Aprenda Linux como si estuviera en primero*. Madrid: San sebastian.
- Lazo García, N. A. (2012). *Diseño e implementación de una red LAN y WLAN con sistema de control de acceso mediante servidores AAA*. Lima.
- Marchionni, E. A. (2011). *Administrador de servidores*. Buenos Aires: Fox Andina.
- McNab, C. (2008). *Seguridad de redes*. Madrid: Anaya Multimedia.
- Méndez Alvarez, Verónica Elizabeth, Jiménez Moya, Carmen Esther. (2013). *Configuración e implementación de un servidor de internet con firewall bajo estándares de seguridad en linux centos 5.9 en el laboratorio de redes de la carrera de ingeniería en informática y sistemas computacionales de la universidad técnica de cotopaxi* . Ecuador.
- Orellana Benavides, Luis Alberto. (2003). *Seguridad en redes de datos*. El Salvador.
- Saavedra Mejía, R. E. (2015). *Diseño e implementación de un sistema integrado de gestión de equipos de seguridad*. Lima.
- STALLINGS, W. (2004). *FUNDAMENTOS DE SEGURIDAD EN REDES APLICACIONES Y ESTÁNDARES*. Madrid: Pearson Education.
- Dr. José Supo (2015) Como empezar una Tesis - Tu proyecto de investigación en un solo día. Edit. BIOESTADISTICO EIRL. Perú
- Dr. José Supo (2015) TÉCNICAS DE RECOLECCIÓN DE DATOS. Edit. BIOESTADISTICO EIRL. Perú.

Dr. José Supo (2015) COMO PROBAR UNA HIPÓTESIS. Edit.
BIOESTADISTICO EIRL.Perú.

Dr. José Supo (2015) LAS VARIABLES ANALÍTICAS. Edit.
BIOESTADISTICO EIRL.Perú.

Dr. José Supo (2015) CÓMO SE ELIGE UNA PRUEBA ESTADÍSTICA. Edit.
BIOESTADISTICO EIRL.Perú.

Dr. José Supo (2015) CÓMO ELEGIR UNA MUESTRA. Edit.
BIOESTADISTICO EIRL.Perú.

WEB GRAFÍA:

- ✓ <http://www.iso27000.es>
- ✓ <http://histinf.blogs.upv.es/2011/12/23/historia-de-linux/>
- ✓ <https://www.ubuntu.com/download/alternative-downloads>

ANEXOS

ANEXO 01: MATRIZ DE CONSISTENCIA

TÍTULO DEL PROYECTO: “IMPLEMENTACIÓN DE UN SERVIDOR DE SEGURIDAD BAJO EL S.O GNU/LINUX BASADO EN LA ISO 27002:2013 PARA MEJORAR LA RED DE ÁREA LOCAL DEL ÁREA ADMINISTRATIVA DEL HOSPITAL DE CONTINGENCIA HERMILIO VALDIZÁN MEDRANO DE HUÁNUCO, 2017”

PRESENTADO POR: PAUCAR FALCÓN, BEATRIZ HAYDEÉ

ASESOR: ING. EDGARDO CRISTIAM IVAN LÓPEZ DE LA CRUZ

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
<p>Problema General</p> <p>¿De qué manera la implementación de un servidor mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco?</p>	<p>Objetivo General</p> <p>Implementar un servidor de seguridad para mejorar la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.</p>	<p>Hipótesis General</p> <p>La implementación de un servidor mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.</p>	<p>Evaluativa</p> <p>Seguridad de la red de área local</p>	<p>Controles de seguridad asociados a servicios de red</p>	<ul style="list-style-type: none"> ✓ Cantidad de conexiones por día. ✓ Porcentaje de bytes accedidos por día ✓ Porcentaje del uso de la cache por día. ✓ Cantidad de páginas no autorizadas bloqueadas 	<p>Enfoque: Cuantitativo Tipo: Aplicativo Diseño: Pre-Experimental</p>
				<p>Controles de seguridad asociados a la restricción del acceso de la información</p>	<ul style="list-style-type: none"> ✓ Porcentaje de carpetas y archivos creados. ✓ Porcentaje de carpetas y archivos modificados. ✓ Porcentaje de carpetas y archivos eliminados 	
<p>Problema Específico</p> <p>A. ¿De qué manera la implementación de controles de seguridad asociados a servicios de red mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco?</p> <p>B. ¿De qué manera la implementación de los controles de seguridad asociados a la restricción del acceso de la información mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco?</p>	<p>Objetivos Específico</p> <p>A. Evaluar los controles de seguridad asociados a servicios de red para mejorar la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.</p> <p>B. Medir los controles de seguridad asociados a la restricción del acceso de la información red para mejorar la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.</p>	<p>Hipótesis Especifica</p> <p>A. La implementación de los controles de seguridad asociados a servicios de red mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.</p> <p>B. La implementación los controles de seguridad asociados a la restricción del acceso de la información mejorará la seguridad de la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco.</p>	<p>Calibración</p> <p>Servidor de Seguridad</p>	INDICADORES		<p>Esquema del Diseño:</p> <p>G: O1 X O2</p> <p>Donde:</p> <p>G= Grupo de investigación (Servicios de Seguridad Rubricas)</p> <p>X= Aplicación de la variable</p> <p>O1, O2, = Medición de Observación</p>
				<ul style="list-style-type: none"> ✓ Servidor Linux (Ubuntu server) ✓ Capacidad de almacenamiento. ✓ Copias de seguridad. ✓ Control y administración de todas las peticiones que le hagan las demás computadoras. 		

ANEXO 02: DOMINIOS Y CONTROLES DEL ISO 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.

- 5.1 Directrices de la Dirección en seguridad de la información.
- 5.1.1 Conjunto de políticas para la seguridad de la información.
- 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

- 6.1 Organización interna.
- 6.1.1 Asignación de responsabilidades para la segur. de la información.
- 6.1.2 Segregación de tareas.
- 6.1.3 Contacto con las autoridades.
- 6.1.4 Contacto con grupos de interés especial.
- 6.1.5 Seguridad de la información en la gestión de proyectos.

- 6.2 Dispositivos para movilidad y teletrabajo.
- 6.2.1 Política de uso de dispositivos para movilidad.
- 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

- 7.1 Antes de la contratación.
- 7.1.1 Investigación de antecedentes.
- 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
- 7.2.1 Responsabilidades de gestión.
- 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
- 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
- 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

- 8.1 Responsabilidad sobre los activos.
- 8.1.1 Inventario de activos.
- 8.1.2 Propiedad de los activos.
- 8.1.3 Uso aceptable de los activos.
- 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
- 8.2.1 Directrices de clasificación.
- 8.2.2 Etiquetado y manipulado de la información.
- 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
- 8.3.1 Gestión de soportes extraíbles.
- 8.3.2 Eliminación de soportes.
- 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.

- 9.1 Requisitos de negocio para el control de accesos.
- 9.1.1 Política de control de accesos.
- 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
- 9.2.1 Gestión de altas/bajas en el registro de usuarios.
- 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
- 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
- 9.2.4 Gestión de información confidencial de autenticación de usuarios.
- 9.2.5 Revisión de los derechos de acceso de los usuarios.
- 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
- 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
- 9.4.1 Restricción del acceso a la información.
- 9.4.2 Procedimientos seguros de inicio de sesión.
- 9.4.3 Gestión de contraseñas de usuario.
- 9.4.4 Uso de herramientas de administración de sistemas.
- 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

- 10.1 Controles criptográficos.
- 10.1.1 Política de uso de los controles criptográficos.
- 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.

- 11.1 Áreas seguras.
- 11.1.1 Perímetro de seguridad física.
- 11.1.2 Controles físicos de entrada.
- 11.1.3 Seguridad de oficinas, despachos y recursos.
- 11.1.4 Protección contra las amenazas externas y ambientales.
- 11.1.5 El trabajo en áreas seguras.
- 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
- 11.2.1 Emplazamiento y protección de equipos.
- 11.2.2 Instalaciones de suministro.
- 11.2.3 Seguridad del cableado.
- 11.2.4 Mantenimiento de los equipos.
- 11.2.5 Salida de activos fuera de las dependencias de la empresa.
- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
- 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- 11.2.8 Equipo informático de usuario desatendido.
- 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.

- 12.1 Responsabilidades y procedimientos de operación.
- 12.1.1 Documentación de procedimientos de operación.
- 12.1.2 Gestión de cambios.
- 12.1.3 Gestión de capacidades.
- 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
- 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
- 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
- 12.4.1 Registro y gestión de eventos de actividad.
- 12.4.2 Protección de los registros de información.
- 12.4.3 Registros de actividad del administrador y operador del sistema.
- 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
- 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
- 12.6.1 Gestión de las vulnerabilidades técnicas.
- 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
- 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

- 13.1 Gestión de la seguridad en las redes.
- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
- 13.2.1 Políticas y procedimientos de intercambio de información.
- 13.2.2 Acuerdos de intercambio.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:



14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

- 14.1 Requisitos de seguridad de los sistemas de información.
- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
- 14.2.1 Política de desarrollo seguro de software.
- 14.2.2 Procedimientos de control de cambios en los sistemas.
- 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 14.2.4 Restricciones a los cambios en los paquetes de software.
- 14.2.5 Uso de principios de ingeniería en protección de sistemas.
- 14.2.6 Seguridad en entornos de desarrollo.
- 14.2.7 Externalización del desarrollo de software.
- 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
- 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
- 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

- 15.1 Seguridad de la información en las relaciones con suministradores.
- 15.1.1 Política de seguridad de la información para suministradores.
- 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
- 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
- 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
- 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
- 16.1.1 Responsabilidades y procedimientos.
- 16.1.2 Notificación de los eventos de seguridad de la información.
- 16.1.3 Notificación de puntos débiles de la seguridad.
- 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
- 16.1.5 Respuesta a los incidentes de seguridad.
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
- 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

- 17.1 Continuidad de la seguridad de la información.
- 17.1.1 Planificación de la continuidad de la seguridad de la información.
- 17.1.2 Implantación de la continuidad de la seguridad de la información.
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

- 18.1 Cumplimiento de los requisitos legales y contractuales.
- 18.1.1 Identificación de la legislación aplicable.
- 18.1.2 Derechos de propiedad intelectual (DPI).
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de datos y privacidad de la información personal.
- 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento de las políticas y normas de seguridad.
- 18.2.3 Comprobación del cumplimiento.

ANEXO 03: FICHAS DE EVALUACIÓN TÉCNICA

FICHA DE EVALUACIÓN TÉCNICA					
N.º Ficha	01	Fecha		Hora	
Componente	Controles de seguridad asociados a servicios de red				
Medición	Pre-test				
Indicadores					valor
¿Cuál ha sido la cantidad de conexiones por día?					
¿Cuál ha sido la cantidad de MB accedidos por día?					
¿Cuál ha sido la cantidad de páginas visitadas no autorizadas por día?					

FICHA DE EVALUACIÓN TÉCNICA					
N.º Ficha	01	Fecha		Hora	
Componente	Controles de seguridad asociados a servicios de red				
Medición	Post-test				
Indicadores					valor
¿Cuál ha sido la cantidad de conexiones por día?					
¿Cuál ha sido la cantidad de MB accedidos por día?					
¿Cuál ha sido la cantidad de páginas visitadas no autorizadas por día?					

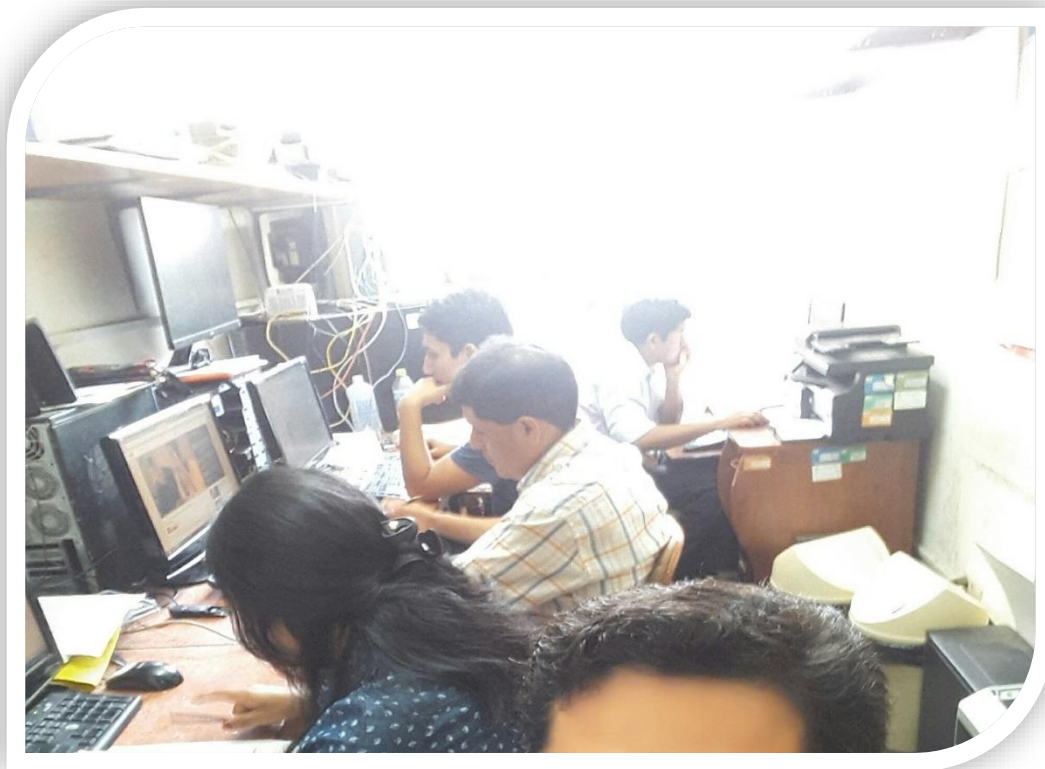
FICHA DE EVALUACIÓN TÉCNICA					
N.º Ficha	01	Fecha		Hora	
Componente	Controles de seguridad asociados a la restricción del acceso de la información				
Medición	Pre-test				
Indicadores					valor
¿Cuál ha sido la cantidad de carpetas y archivos creados por día?					
¿Cuál ha sido la cantidad de carpetas y archivos modificados por día?					
¿Cuál ha sido la cantidad de carpetas y archivos eliminados por día?					

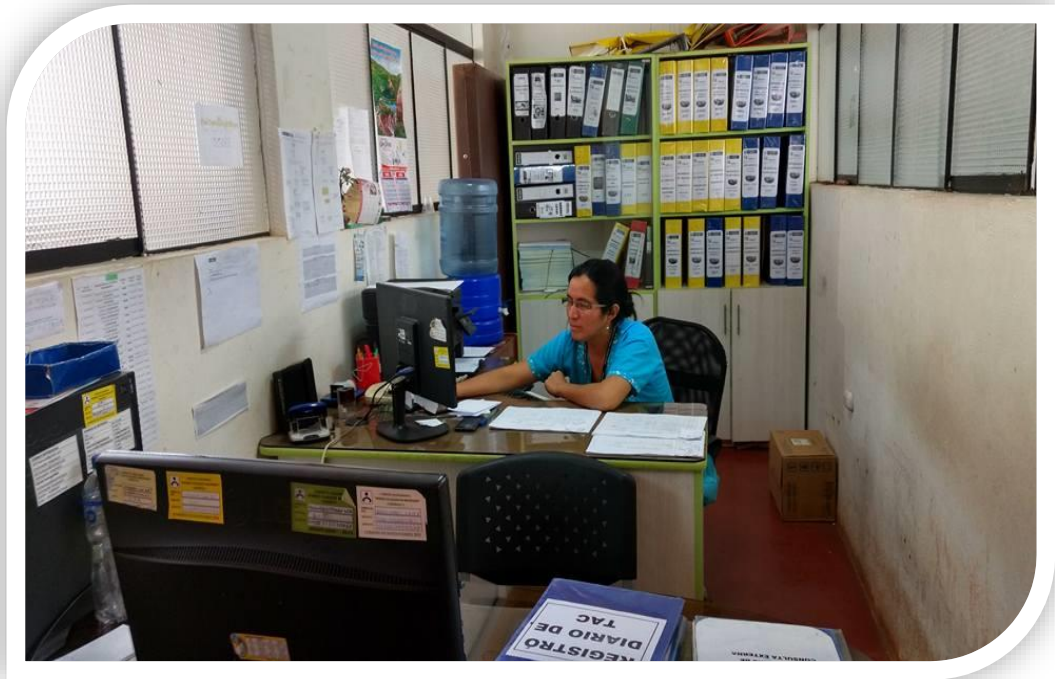
FICHA DE EVALUACIÓN TÉCNICA					
N.º Ficha	01	Fecha		Hora	
Componente	Controles de seguridad asociados a la restricción del acceso de la información				
Medición	Post-test				
Indicadores					valor
¿Cuál ha sido la cantidad de carpetas y archivos creados por día?					
¿Cuál ha sido la cantidad de carpetas y archivos modificados por día?					
¿Cuál ha sido la cantidad de carpetas y archivos eliminados por día?					

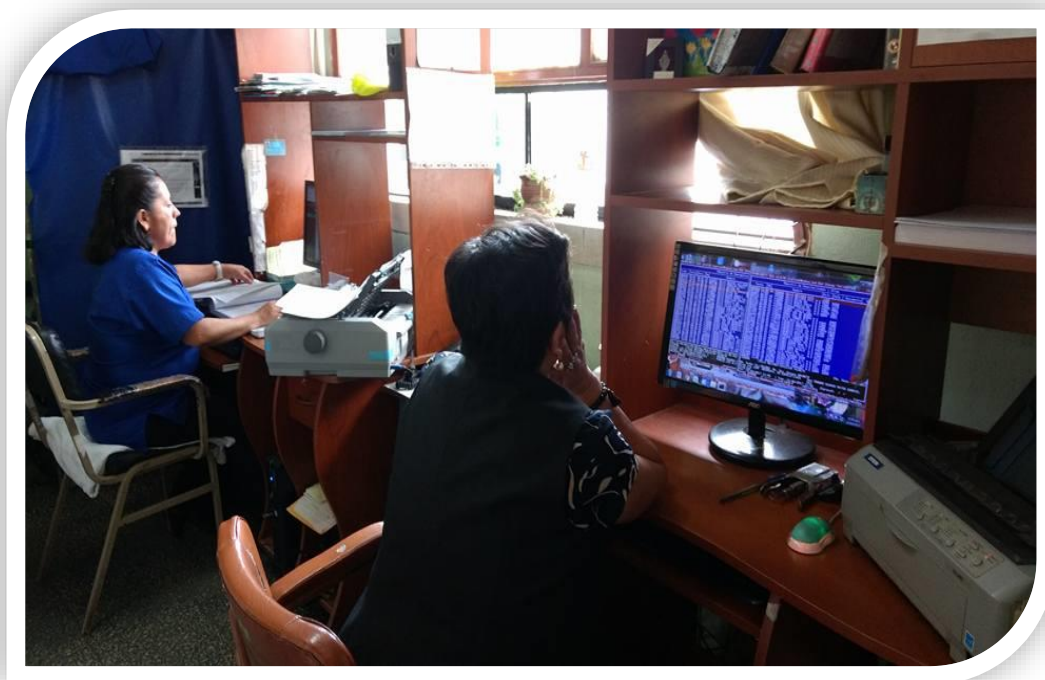
FOTOGRAFÍAS DEL HOSPITAL (Unidades de trabajo)



Centro de Computo





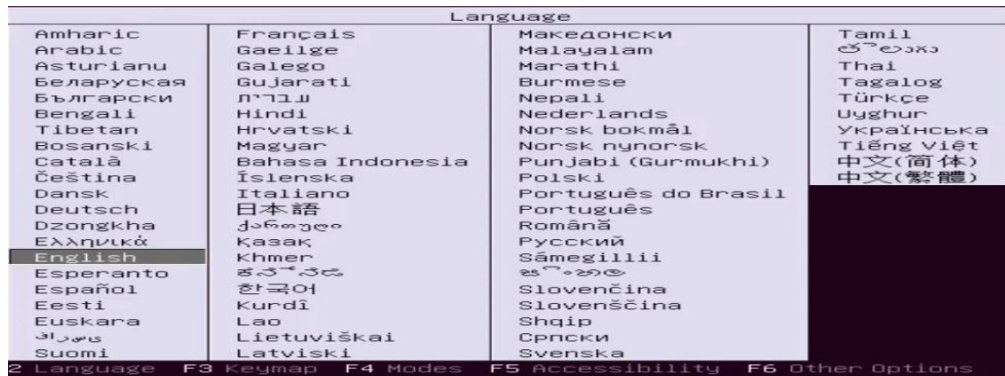


Admisión

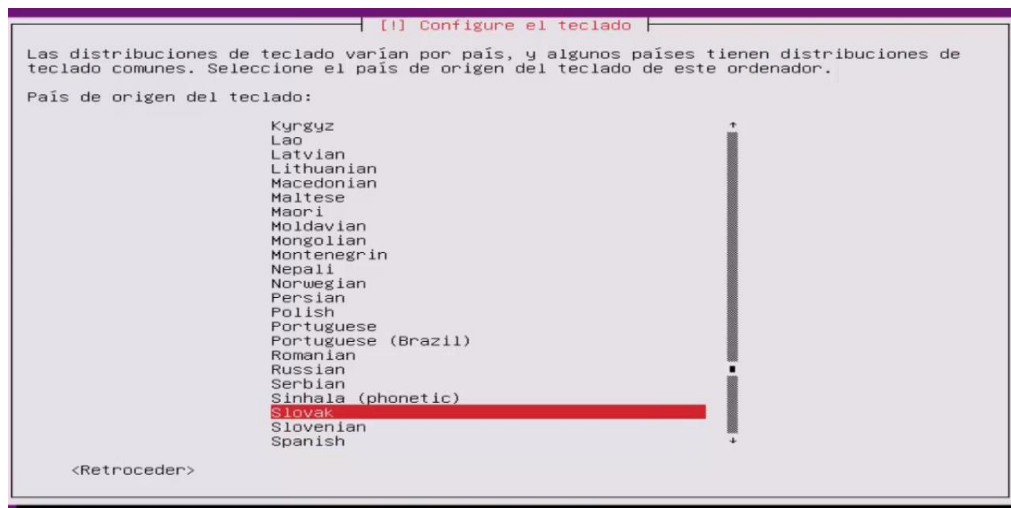
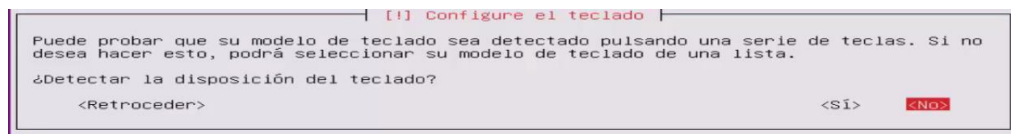


INSTALACIÓN DEL UBUNTU SERVER 10

Lo primero seleccionamos el idioma.

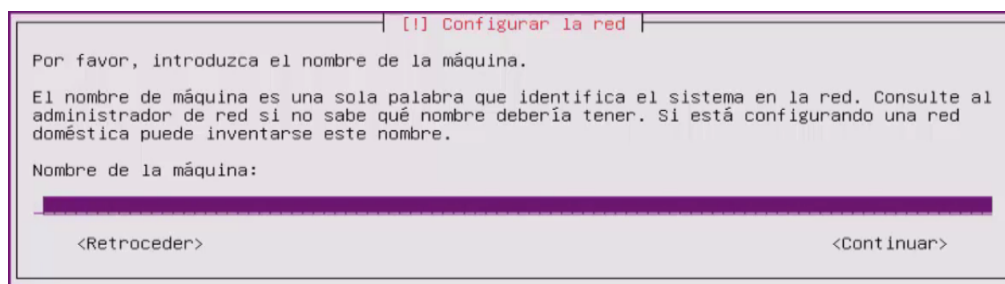


Configuramos nuestro teclado.



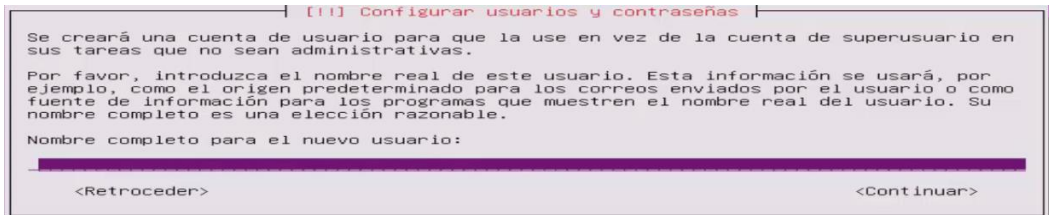
A continuación, seleccionamos el nombre de la maquina (Servidor):

- Nombre Maquina: SERVER01

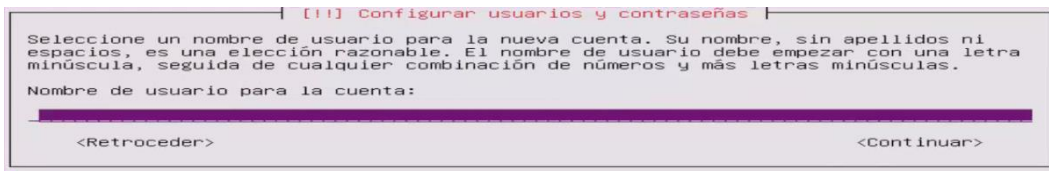


Seguidamente configuramos el usuario y la contraseña:

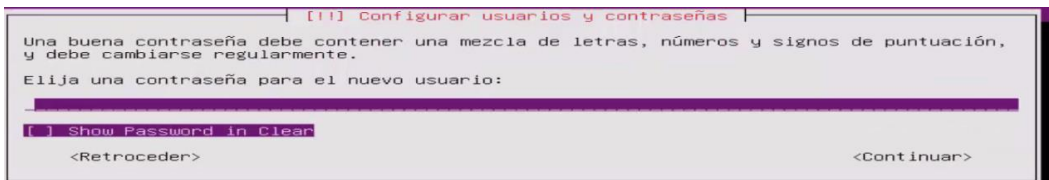
- Seleccionemos un nombre para el nuevo usuario: usuario01



- Nombre de usuario para la cuenta: usuario01

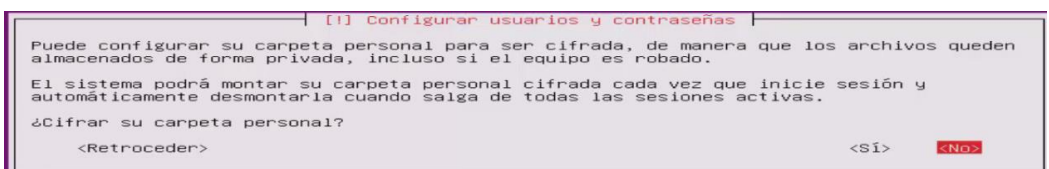


- Elegimos una contraseña para el usuario: servidores2017 (si nos sale una alerta, le damos SI).
- Volvemos a repetir CONTINUAR.

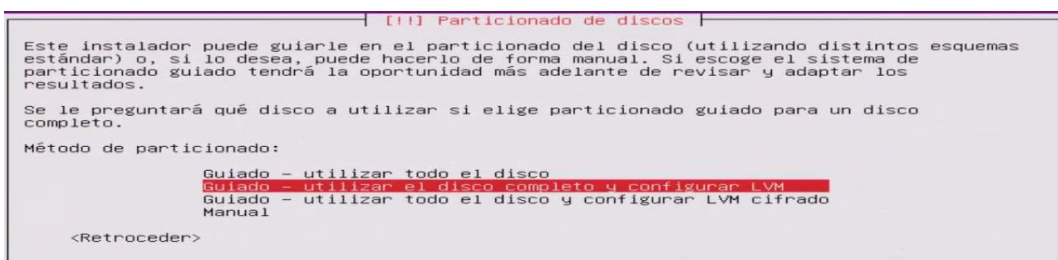


Configurar usuarios y contraseñas

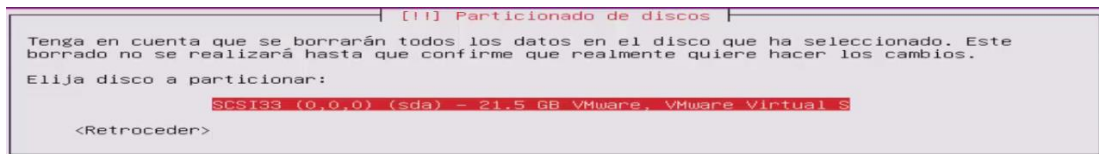
¿Cifrar su carpeta personal?, Seleccionamos NO y continuar.



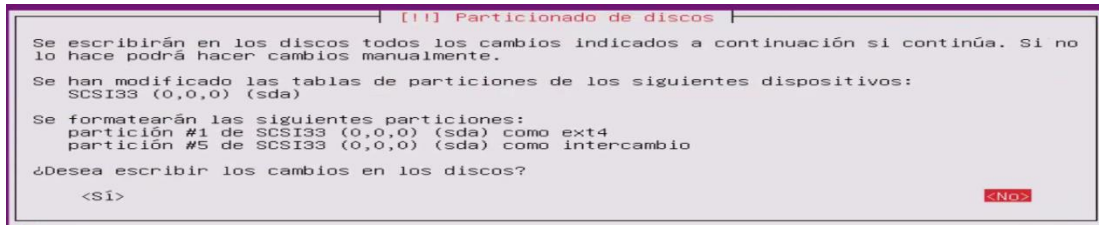
Configurar particionado de Disco, Seleccionamos **utilizar todo el Disco** y le damos ENTER.



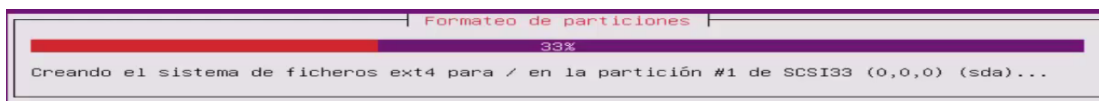
Y seleccionamos el disco que tenemos y ENTER.



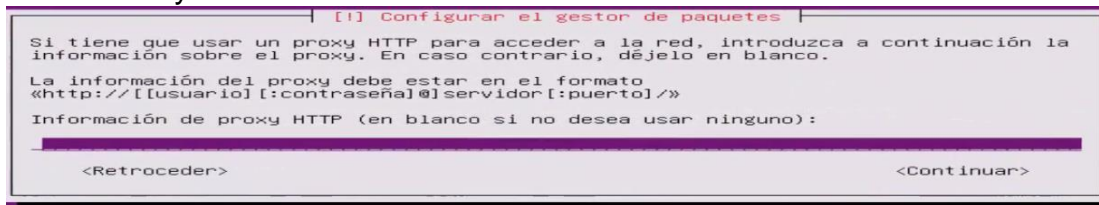
Particionado de Discos, ¿Desea Escribir los cambios en los discos?, Seleccionamos SI y ENTER.



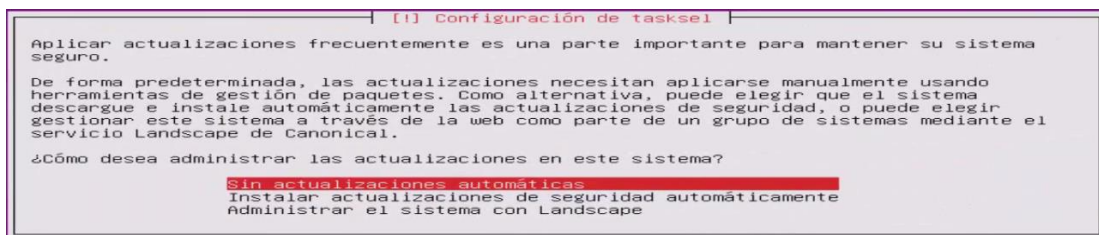
Va a empezar a formatear.



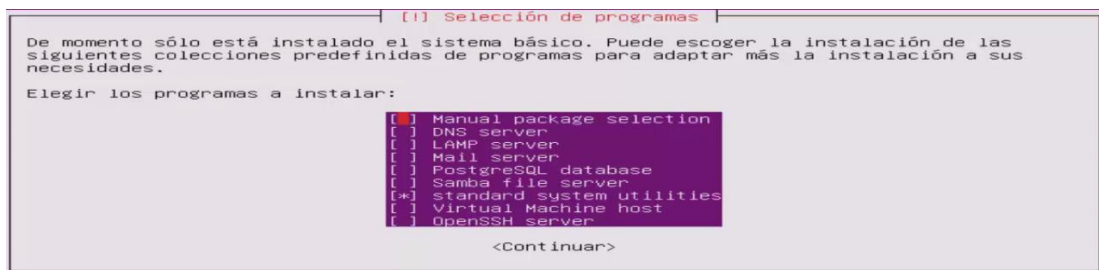
Configuramos el gestor de paquetes, si no tenemos le dejamos en blanco y CONTINUAR.



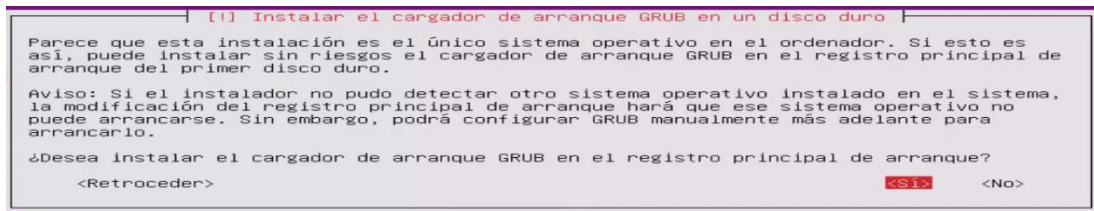
Configuración de tasksel, seleccionamos a nuestro gusto y ENTER.



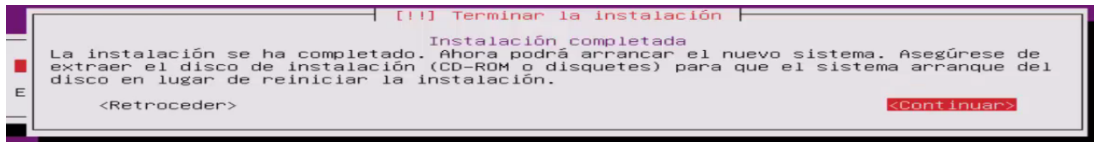
Selección de Programas, seleccionamos openSSH Server con un espacio y standard system utilites y tabulador para continuar.



Instalar el cargador de arranque GRUB en un disco duro, seleccionamos SI.



Terminar la instalación y CONTINUAR.



Pantalla de logueo de UBUNTU SERVER:



Una vez ingresado, es necesario actualizar los paquetes de los repositorios con los siguientes comandos.

- Sudo apt-get update
- Sudo apt-get upgrade.

CONFIGURACIÓN DE TARJETAS DE RED

1. CONFIGURACIÓN LADO DEL SERVIDOR.

INGRESAMOS A LA CONFIGURACIÓN CON EL COMANDO:

- **sudo nano /etc/network/interfaces** y pulsamos ENTER

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

#The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.1.254
    netmask 255.255.255.0
    network 192.168.1.0
    broacast 192.168.1.255
    gateway 192.168.1.1

auto eth1
iface eth1 inet static
    address 192.168.2.254
    netmask 255.255.255.0
    network 192.168.2.0
    broadcast 192.168.2.255
```

```
Pueden actualizarse 3 paquetes.
0 actualizaciones son de seguridad.

clopez@SERVER01:~$ ifconfig
ens33    Link encap:Ethernet direcciónHW 00:0c:29:37:04:72
        Direc. inet:192.168.1.254 Difus.:192.168.1.255 Másc:255.255.255.0
        Dirección inet6: 2001:1388:70c0:882d:20c:29ff:fe37:472/64 Alcance:Global
        Dirección inet6: fe80::20c:29ff:fe37:472/64 Alcance:Enlace
        ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
        Paquetes RX:2200 errores:0 perdidos:4 overruns:0 frame:0
        Paquetes TX:2406 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1000
        Bytes RX:226224 (226.2 KB) TX bytes:907714 (907.7 KB)
        Interrupción:19 Dirección base: 0x2000

ens34    Link encap:Ethernet direcciónHW 00:0c:29:37:04:7c
        Direc. inet:192.168.2.254 Difus.:192.168.2.255 Másc:255.255.255.0
        Dirección inet6: fe80::20c:29ff:fe37:47c/64 Alcance:Enlace
        ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
        Paquetes RX:1303 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:338 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1000
        Bytes RX:131878 (131.8 KB) TX bytes:58752 (58.7 KB)
        Interrupción:16 Dirección base: 0x2080

lo       Link encap:Bucle local
        Direc. inet:127.0.0.1 Másc:255.0.0.0
        Dirección inet6: ::1/128 Alcance:Anfitrión
        ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
        Paquetes RX:267 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:267 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1
        Bytes RX:26434 (26.4 KB) TX bytes:26434 (26.4 KB)

clopez@SERVER01:~$
```

- Una vez configurado cada puerto con su respectivo IP, guardamos con ctrl + X y seleccionamos SI y ENTER.
- Y procedemos a reiniciar el servidor.

CONFIGURAMOS UBUNTU EN SERVER

- echo > 1 /proc/sys/net/ipv4/ip_forward

PARA QUE SEA ESTABLE MODO ROUTER.

- sudo nano /etc/sysctl.conf

```

centralita@centralita-VirtualBox ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.5.3 File: /etc/sysctl.conf
#####3
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

```

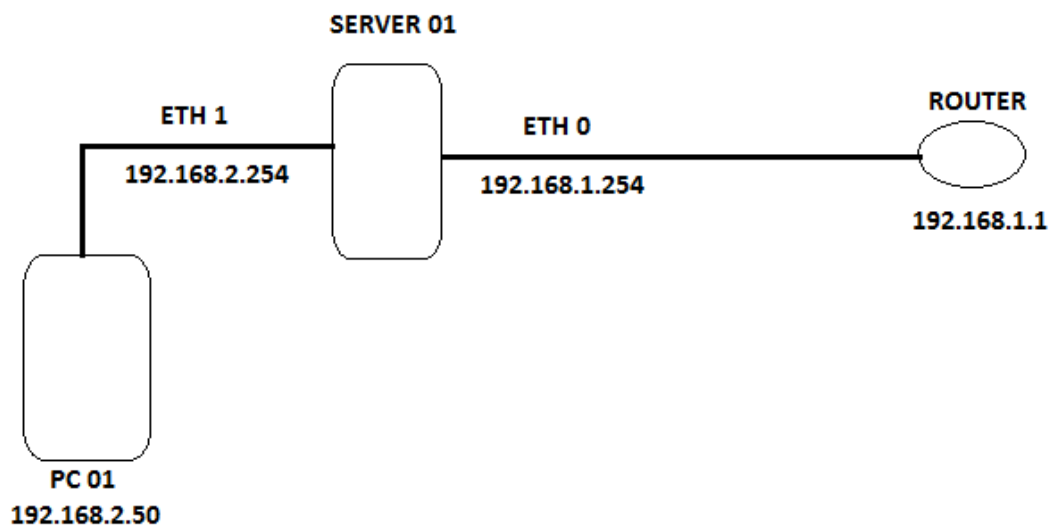
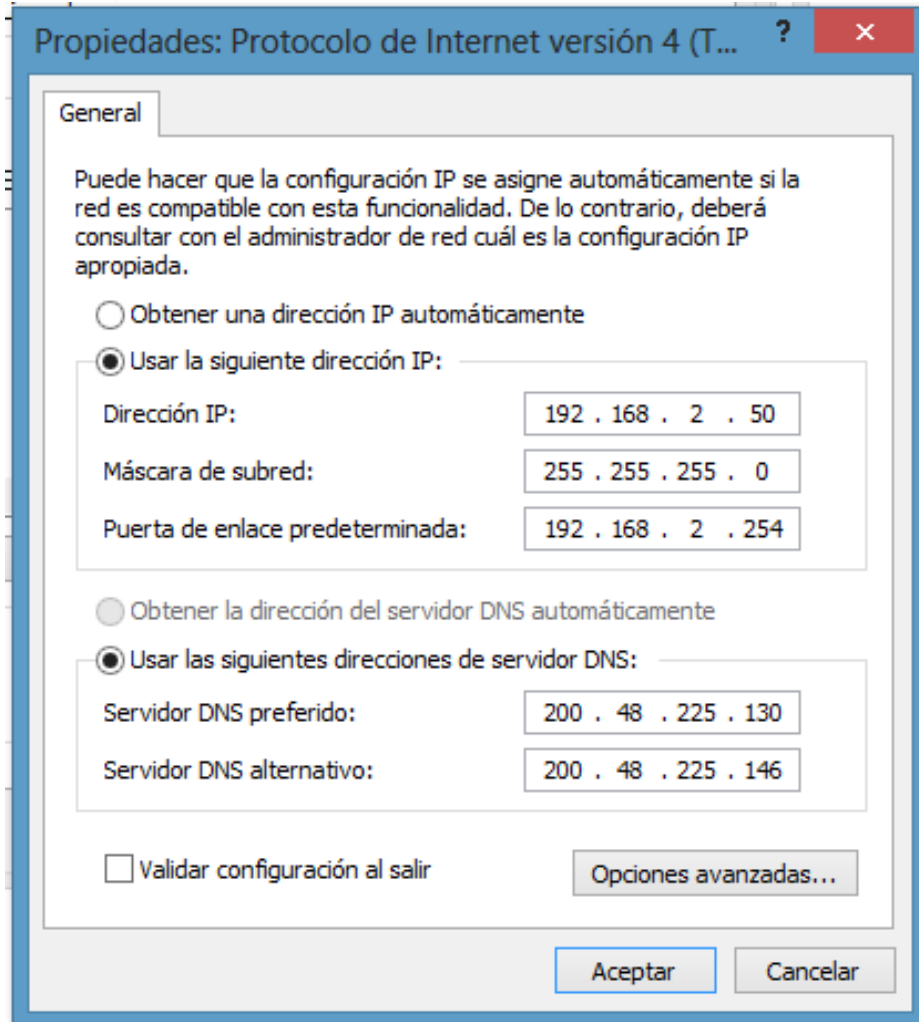
- Quitamos en # de net.ipv4.ip_forward=1
- Presionamos Control + X
- confirmamos con Y, para guardar cambios.
- Y volvemos a presionar Control + X, para salir.

PARA RECONOCER EL eth0, en las demás maquinas.

- sudo iptables -t nat -A POSTROUTING -o eth0 -J MASQUERADE

2. CONFIGURACIÓN LADO DE WINDOWS.

- Configuramos la IP del servidor del puerto de salida.



CONFIGURAR sudo iptables -t nat -A POSTROUTING -o eth0 -J MASQUERADE, PARMANENTE.

- Solución que se busco es crear un script, y se ejecute cuando arranca el sistema
- Los pasos son:
 - Crear el script con un nombre especifico con extesion .sh
 - touch prueba.sh
 - Entramos al script para poder escribir el comando.
 - sudo nano prueba.sh
 - Una vez dentro del script escribimos la línea de comando a ejecutar, en este caso es.
 - sudo iptables -t nat -A POSTROUTING -o enp0s18 -j MASQUERADE
 - Guardamos con ctrl + X, y le damos SI.
 - Le damos permiso al script con el siguiente comando.
 - Sudo chmod +x prueba.sh
 - Ingreamos sudo nano /etc/rc.local
 - Antes del exit 0 escribimos la dirección donde se ubica el script:
 - sh /home/clopez/prueba.sh
 - guardamos con ctrl + X.

INSTALACIÓN DE WEBMIN

- Necesitamos de un cliente que esté conectado al servidor para acceder a webmin.
- Verificar que esté conectado el cliente con el Servidor, con ping ambos lados, (lado del cliente y del servidor), desactivar firewall de Windows en el caso se utilice como cliente.
- Los pasos para la instalación son la siguiente:
 - Entramos al archivo sources.list
 - nano /etc/apt/sources.list
 - Añadimos los siguientes repositorios:
 - deb <http://download.webmin.com/download/repository> sarge contrib
 - deb <http://webmin.mirror.somersettechsolutions.co.uk/repository> sarge contrib
 - Descargamos la clave para la descarga
 - wget <http://www.webmin.com/jcameron-key.asc>
 - Cargamos la llave
 - apt-key add jcameron-key.asc
 - Actualizamos el Server
 - apt-get update
 - Instalar Webmin
 - Instalar Webmin
- Una vez instalado entramos por lado del cliente por un navegador (IP del servidor y el puerto 10000)
- No pedirá un logeo el cual ingresamos con el usuario del servidor.

BLOQUEAR REDES P2P CON IPTABLES.

Instalamos el paquete xtables-addons-commons, con el siguiente comando.

- **sudo apt-get install xtables-addons-common**

Una vez instalado se comprueba por medio de la siguiente sintaxis;

- **sudo iptables -m ipp2p --help**

```
lsilva@stack:~$ sudo iptables -m ipp2p --help
iptables v1.4.14

Usage: iptables -[ACD] chain rule-specification [options]
       iptables -I chain [rulenum] rule-specification [options]
       iptables -R chain rulenum rule-specification [options]
       iptables -D chain rulenum [options]
       iptables -[LS] [chain [rulenum]] [options]
       iptables -[FZ] [chain] [options]
       iptables -[NX] chain
       iptables -E old-chain-name new-chain-name
       iptables -P chain target [options]
       iptables -h (print this help information)

Commands:
Either long or short options are allowed.
--append -A chain          Append to chain
--check  -C chain          Check for the existence of a rule
--delete -D chain          Delete matching rule from chain
--delete -D chain rulenum Delete rule rulenum (1 = first) from chain
--insert -I chain [rulenum] Insert in chain as rulenum (default 1=first)
```

- Para evitarnos estar ingresando regla por regla se crea un script que nos haga todo el trabajo
 - **touch blockipp2p.sh**
- ingresamos al scscript con el comando:
 - **sudo nano blockipp2p.sh**

- El contenido del script debe verse más o menos como la siguiente imagen;

```

echo "Inicio del script....."

sudo iptables -A FORWARD -p tcp -m ipp2p --edk -j DROP
sudo iptables -A FORWARD -p udp -m ipp2p --edk -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --dc -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --kazaa -j DROP
sudo iptables -A FORWARD -p udp -m ipp2p --kazaa -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --gnu -j DROP
sudo iptables -A FORWARD -p udp -m ipp2p --gnu -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --bit -j DROP
sudo iptables -A FORWARD -p udp -m ipp2p --bit -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --apple -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --winmx -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --soul -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --ares -j DROP

echo "Fin del script....."

```

- Básicamente el script bloquea (DROP) todo tipo de tráfico **P2P**. Acá el script completo.

```

echo "Inicio del script....."
sudo iptables -A FORWARD -p tcp -m ipp2p --edk -j DROP
sudo iptables -A FORWARD -p udp -m ipp2p --edk -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --dc -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --kazaa -j DROP
sudo iptables -A FORWARD -p udp -m ipp2p --kazaa -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --gnu -j DROP
sudo iptables -A FORWARD -p udp -m ipp2p --gnu -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --bit -j DROP
sudo iptables -A FORWARD -p udp -m ipp2p --bit -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --apple -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --winmx -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --soul -j DROP
sudo iptables -A FORWARD -p tcp -m ipp2p --ares -j DROP
echo "Fin del script....."

```

- Se asigna el permiso de ejecución
 - **chmod +x blockipp2p.sh**
- Se ejecuta el script por medio de la siguiente sintaxis
 - **sh blockipp2p.sh**

- Y por último se comprueba que el cortafuego (iptables) incorporó las reglas:
 - **iptables -nL**

```
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --edk
DROP      udp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --edk
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --dc
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --kazaa
DROP      udp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --kazaa
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --gnu
DROP      udp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --gnu
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --bit
DROP      udp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --bit
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --apple
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --winmx
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --soul
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --ares
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --edk
DROP      udp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --edk
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --dc
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --kazaa
DROP      udp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --kazaa
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --gnu
DROP      udp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --gnu
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --bit
DROP      udp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --bit
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --apple
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --winmx
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --soul
DROP      tcp  --  0.0.0.0/0              0.0.0.0/0          ipp2p --ares
```

De esta manera resulta mucho más cómodo el bloqueo de las redes **P2P** en el servidor GNU/Linux Debian / Ubuntu Server.

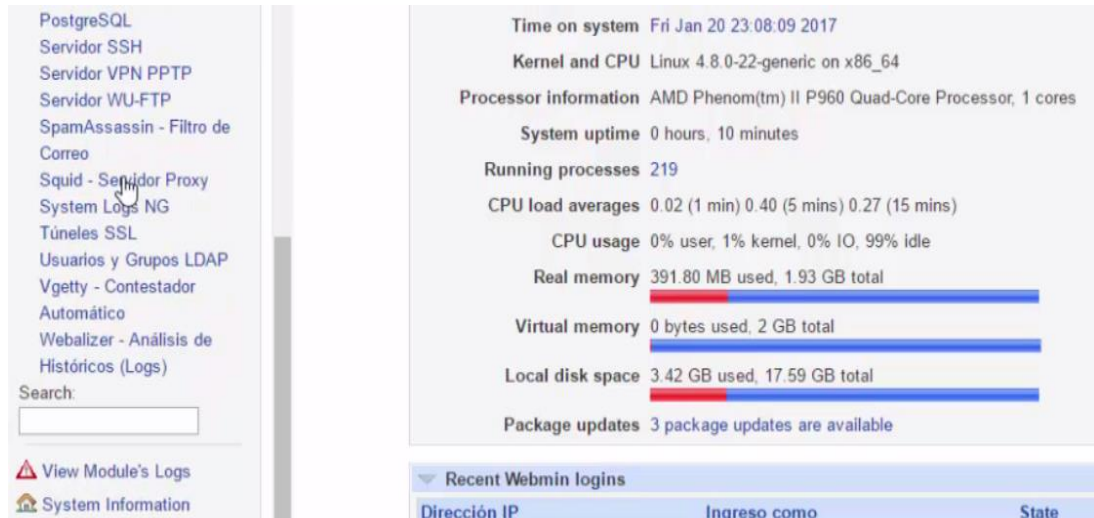
BLOQUEAR TORRENT

Agregamos al script creado los siguientes comandos

```
iptables -N DROPTORRENT > /dev/null 2> /dev/null
iptables -F DROPTORRENT
iptables -A DROPTORRENT -j LOG --log-prefix "DROPTORRENT "
iptables -A DROPTORRENT -j DROP
iptables -A FORWARD -m string --algo bm --string "BitTorrent" -j
DROPTORRENT
iptables -A FORWARD -m string --algo bm --string "BitTorrent protocol" -j
DROPTORRENT
iptables -A FORWARD -m string --algo bm --string "peer_id=" -j
DROPTORRENT
iptables -A FORWARD -m string --algo bm --string ".torrent" -j
DROPTORRENT
iptables -A FORWARD -m string --algo bm --string
"announce.php?passkey=" -j DROPTORRENT
iptables -A FORWARD -m string --algo bm --string "torrent" -j
DROPTORRENT
iptables -A FORWARD -m string --algo bm --string "announce" -j
DROPTORRENT
iptables -A FORWARD -m string --algo bm --string "info_hash" -j
DROPTORRENT
iptables -A FORWARD -m string --string "get_peers" --algo bm -j
DROPTORRENT
iptables -A FORWARD -m string --string "announce_peer" --algo bm -j
DROPTORRENT
iptables -A FORWARD -m string --string "find_node" --algo bm -
j DROPTORRENT
```

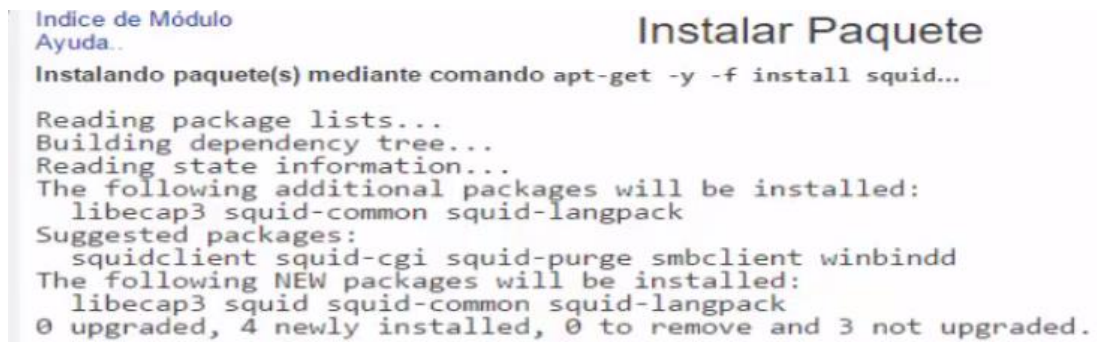
INSTALACIÓN Y CONFIGURACIÓN DE SERVIDOR PROXY (SQUID)

Entramos a Webmin, y vamos a pestaña Un-used Modules (Módulos que no están siendo usados), y entramos a Squid – Servidor Proxy.



The screenshot shows the Webmin interface. On the left, there is a sidebar with a list of modules: PostgreSQL, Servidor SSH, Servidor VPN PPTP, Servidor WU-FTP, SpamAssassin - Filtro de Correo, Squid - Servidor Proxy (highlighted with a mouse cursor), System Logs NG, Túneles SSL, Usuarios y Grupos LDAP, Vgetty - Contestador, Automático, Webalizer - Análisis de, and Históricos (Logs). Below the list is a search box and two buttons: 'View Module's Logs' and 'System Information'. On the right, there is a system information panel showing: Time on system (Fri Jan 20 23:08:09 2017), Kernel and CPU (Linux 4.8.0-22-generic on x86_64), Processor information (AMD Phenom(tm) II P960 Quad-Core Processor, 1 cores), System uptime (0 hours, 10 minutes), Running processes (219), CPU load averages (0.02 (1 min) 0.40 (5 mins) 0.27 (15 mins)), CPU usage (0% user, 1% kernel, 0% IO, 99% idle), Real memory (391.80 MB used, 1.93 GB total), Virtual memory (0 bytes used, 2 GB total), Local disk space (3.42 GB used, 17.59 GB total), and Package updates (3 package updates are available). Below this is a 'Recent Webmin logins' table with columns: Dirección IP, Ingreso como, and State.

Y ejecutamos la instalación en **Pulse Aquí**,



The screenshot shows the 'Instalar Paquete' (Install Package) page in Webmin. It displays the command `apt-get -y -f install squid...` and the output of the command. The output shows the following additional packages will be installed: libecap3 squid-common squid-langpack. Suggested packages: squidclient squid-cgi squid-purge smbclient winbindd. The following NEW packages will be installed: libecap3 squid squid-common squid-langpack. 0 upgraded, 4 newly installed, 0 to remove and 3 not upgraded.

Se va ir instalando y esperamos que termine.

El Paquete squid-common se instaló con éxito

Detalles del Paquete			
Descripción	Desconocido		
Paquete	squid-common	Clase	P-T
Versión	3.5.12-1ubuntu8	Vendedor	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Arquitectura	all	Instalado	Desconocido

El Paquete squid se instaló con éxito

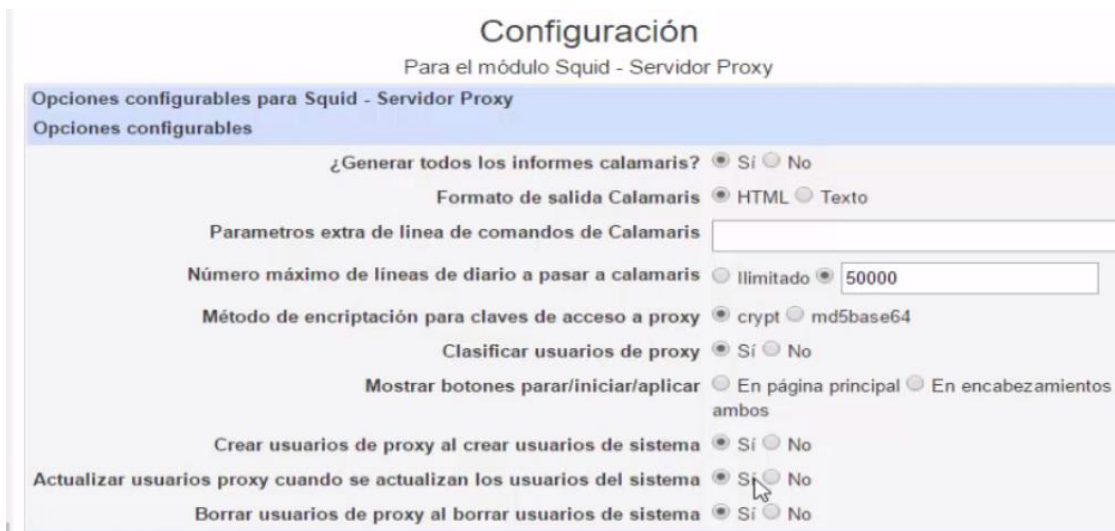
Detalles del Paquete			
Descripción	Desconocido		
Paquete	squid	Clase	P-T
Versión	3.5.12-1ubuntu8	Vendedor	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Arquitectura	amd64	Instalado	Desconocido

No se instala correctamente para corregir tenemos que hacer unos cambios de configuración manualmente.

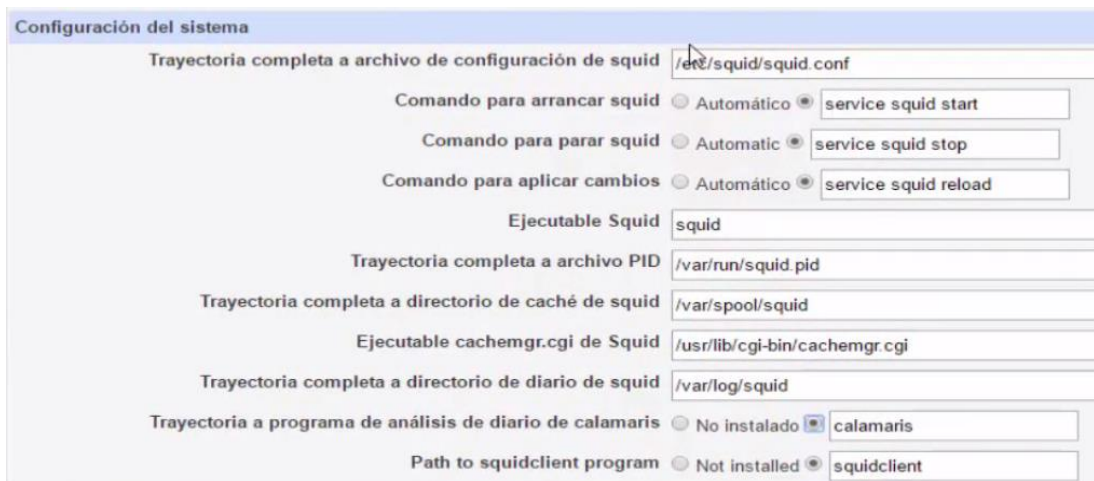
Volvemos a la pestaña de Un-used Modules (Módulos que no están siendo usados).



Hacemos click en Configuración del módulo.

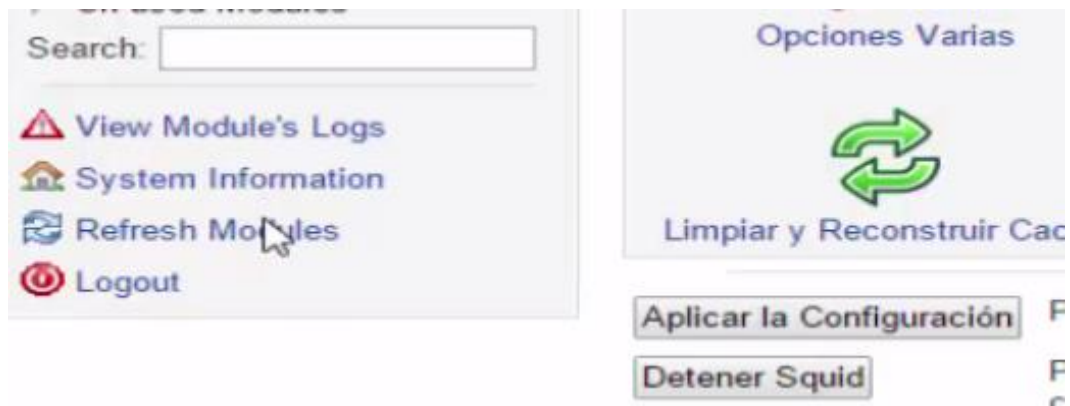


Una vez adentro de la configuración cambiamos todo lo que sale con squi3 borramos el 3 y quedaría solo squid.



Así quedaría la configuración y salvamos la configuración, para que la configuración de aplique.

Una vez salvado refrescamos los módulos para que se actualicen.



Refresh Modules

Checking for usable Webmin modules ..
.. found 64 with installed applications, 47 not installed.

Una vez terminado actualizamos la página del webmin (F5).

Después de recargar la página entramos a la pestaña **servidores** y la opción **Squid – Servidor Proxy**



Lo primero que vamos a hacer, va ser configurar **Puertos y trabajo en Red**.

Indice de Módulo Ayuda... Aplicar Cambio Parar Squi

Puertos y Trabajo en Red

Opciones de Puertos y Trabajo en Red

Direcciones y puertos de Proxy Por defecto (normalmente 3128) Listados abajo..

Puerto	Nombre de máquina/Dirección IP	Opciones de puerto
3128	<input type="radio"/> All <input type="radio"/>	<input type="text"/>
<input type="text"/>	<input type="radio"/> All <input type="radio"/>	<input type="text"/>

Direcciones y puertos SSL Por defecto (normalmente 3128) Listados abajo..

Puerto	Nombre de máquina/Dirección IP	Opciones de puerto
<input type="text"/>	<input type="radio"/> All <input type="radio"/>	<input type="text"/>

Puerto ICP Por defecto

Dirección UDP de salida Cualquiera

Grupos de multicast

Validate hostnames in URLs? Si No

Dirección TCP de salida Cualquiera

Dirección UDP de entrada Cualquiera

Búfer de recepción TCP el de por defecto del SO

Allow underscore in hostnames? Si No

Vamos a configurar nuestra dirección y los puertos que estamos utilizando.

Webmin 1.831 en sentin... x

No es seguro | https://192.168.244.151:10000

Login: root

Indice de Módulo Ayuda... Aplicar Cambios Parar Squid

Puertos y Trabajo en Red

Opciones de Puertos y Trabajo en Red

Direcciones y puertos de Proxy Por defecto (normalmente 3128) Listados abajo..

Puerto	Nombre de máquina/Dirección IP	Opciones de puerto
3128	<input type="radio"/> All <input type="radio"/> 192.168.244.151	<input type="text"/>
8080	<input type="radio"/> All <input type="radio"/> 192.168.244.151	<input type="text"/>

Direcciones y puertos SSL Por defecto (normalmente 3128) Listados abajo..

Puerto	Nombre de máquina/Dirección IP	Opciones de puerto
<input type="text"/>	<input type="radio"/> All <input type="radio"/>	<input type="text"/>

Puerto ICP Por defecto

Dirección UDP de salida Cualquiera

Grupos de multicast

Validate hostnames in URLs? Si No

¿Hacer desconexiones no limpias SSL? Activado Desactivado

Salvar

Regresar a índice de squid

Salvamos y aplicamos la configuración del servidor proxy.

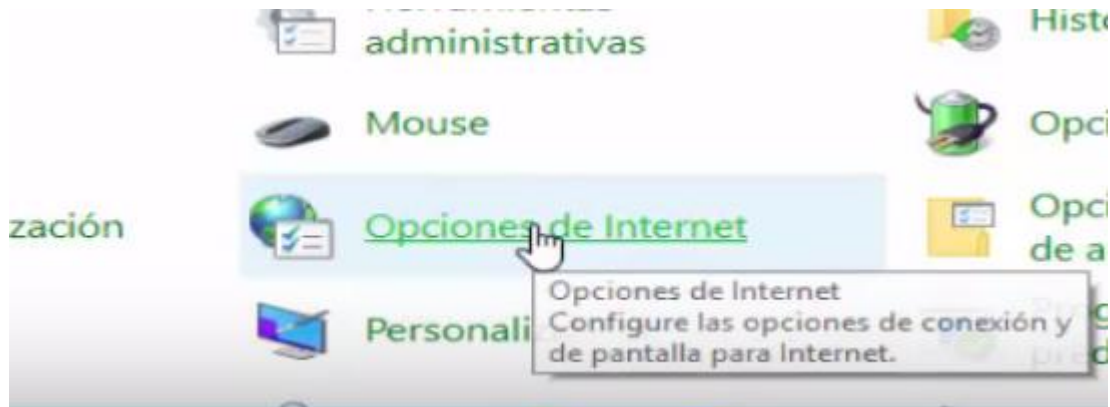
La siguiente configuración es **Opciones de Caché**.



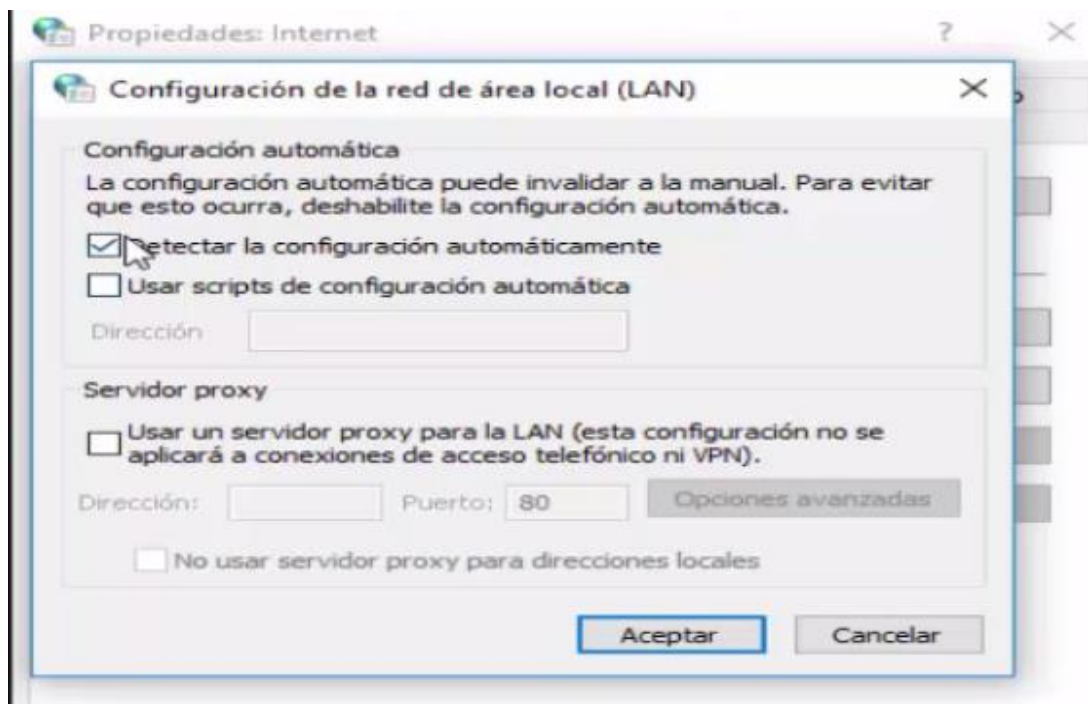
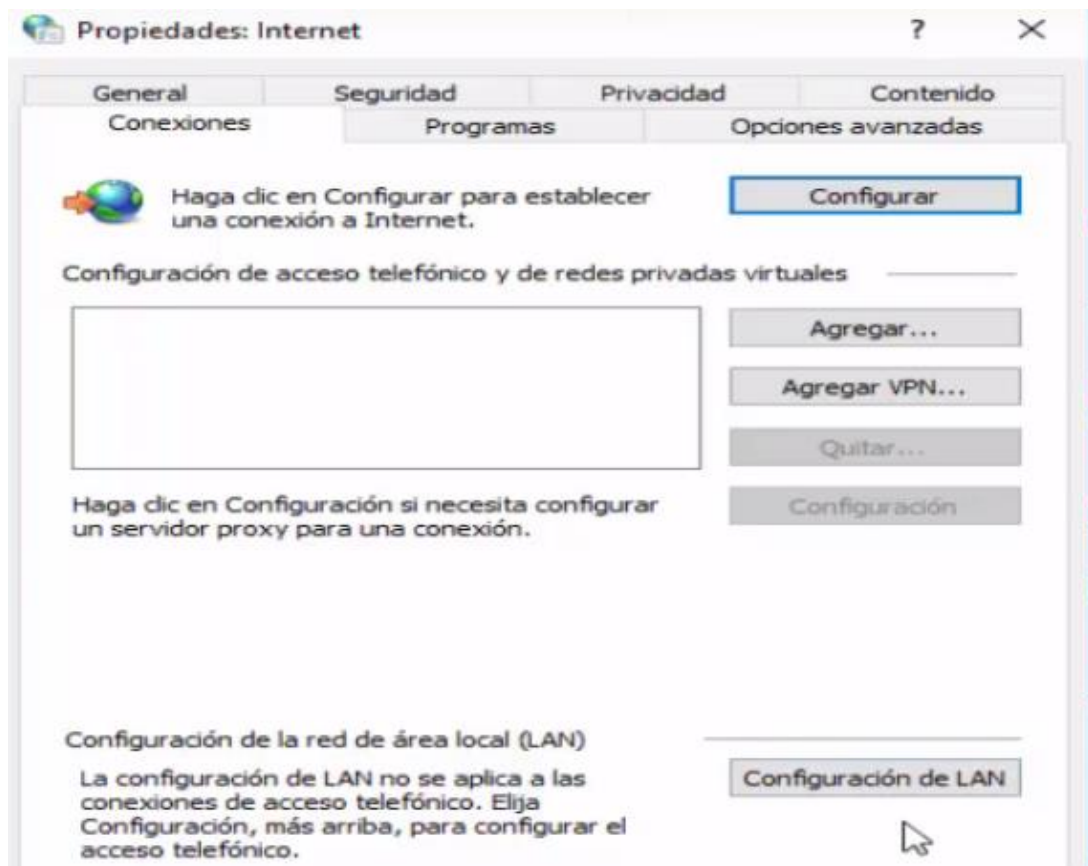
Lo dejamos por defecto y salvamos a la configuración y aplicamos cambios.

Detenemos e iniciamos el servidor en este paso.

Configuramos las propiedades de internet de los clientes que se conectan al servidor, en este caso es Windows y hacemos la siguiente configuración.

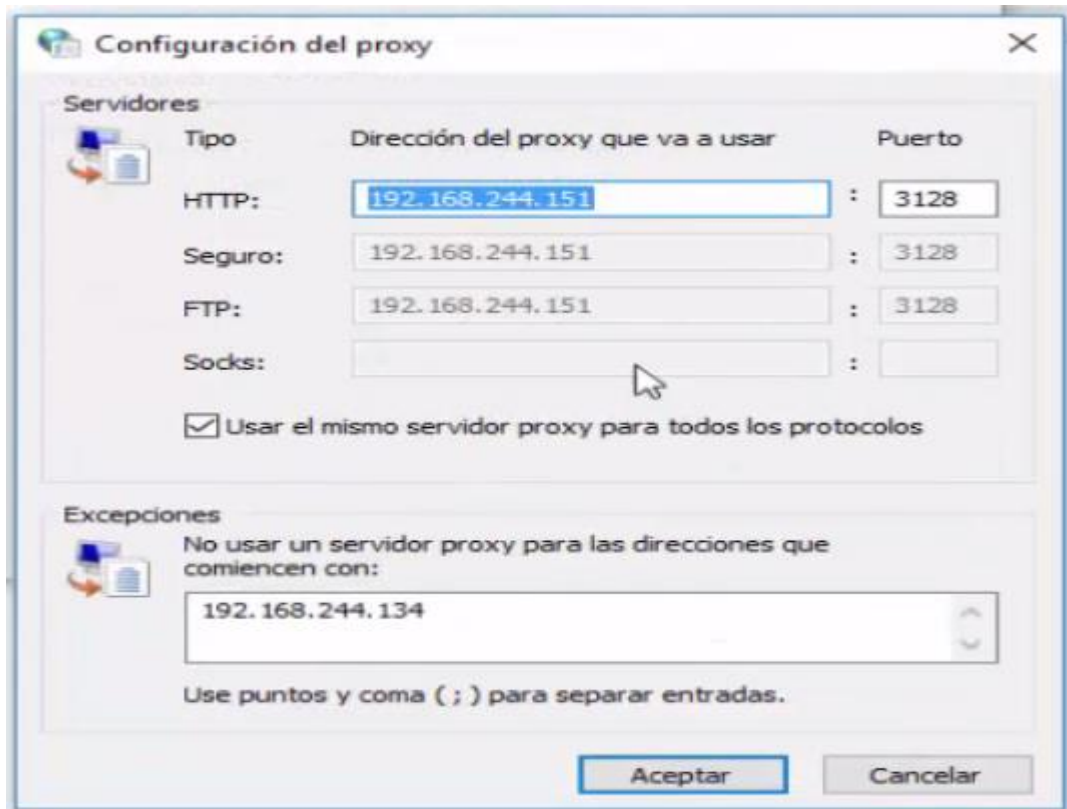


Nos dirigimos la pestaña de **conexiones** y la opción **Configuración de LAN**.



Quitamos el check de **detectar la configuración automáticamente**.

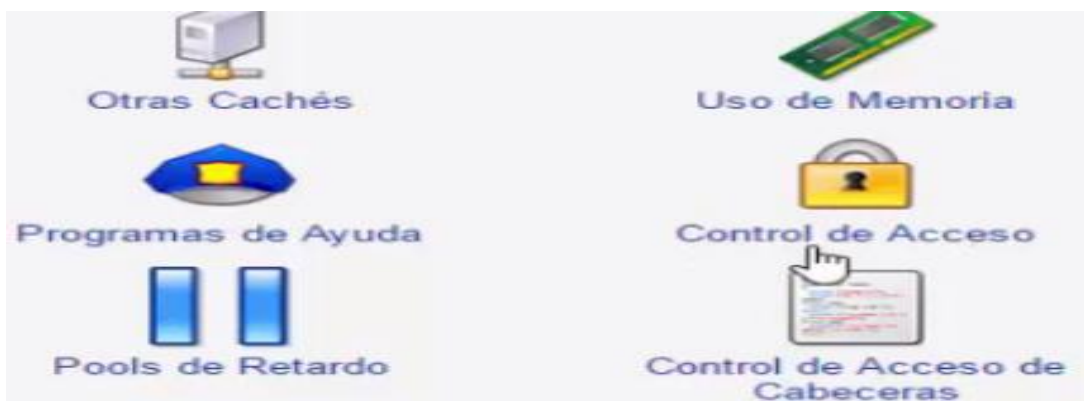
Y activamos **Usar un servidor proxy** y configuramos el Ip del servidor Proxy, cambiamos el puerto de 80, luego click **opciones avanzadas**.



Verificamos que tenga el check **Usar el mismo servidor Proxy**, y configuramos el Ip del servidor en la parte de abajo y guardamos toda la configuración (Aceptar todas las pestañas).

Lo siguiente es crear una regla para poder navegar, ya que nos bloqueó toda la navegación a internet.

Ingresamos a Control de acceso.



Nombre	Tipo	Coincidiendo con...
SSL_ports	Puerto URL	443
Safe_ports	Puerto URL	80
Safe_ports	Puerto URL	21
Safe_ports	Puerto URL	443
Safe_ports	Puerto URL	70
Safe_ports	Puerto URL	210
Safe_ports	Puerto URL	1025-65535
Safe_ports	Puerto URL	280
Safe_ports	Puerto URL	488
Safe_ports	Puerto URL	591
Safe_ports	Puerto URL	777
CONNECT	Método de Petición	CONNECT

Crear nueva ACL Dirección de Cliente

Tenemos que crear una nueva ACL (Lista de Control de Acceso), creamos una regla que permita navegar a internet, utilizamos una ACL que se llame Dirección de cliente y crear nueva.

Indice de Módulo Crear ACL

Dirección de Cliente ACL

Nombre ACL

Desde IP	A IP	Máscara de Red
<input type="text"/>	<input type="text"/>	<input type="text"/>

URL de Fallo

Almacenar ACL en archivo Configuración Squid Separate file

¿Usar sólo contenidos existentes del archivo?

Salvar

[Rearesar a Lista ACL](#) | [Rearesar a índice](#)

Escribimos un nombre referencia a la reglar en este caso navegación, el rango de IP que estamos utilizando vamos a poder 192.168.2.0 con esta configuración tomamos todas las 254 máquina que se pueden conectar al servidor por último ponemos nuestra mascara de red y salvamos la configuración.

Indice de Módulo Crear ACL Aplicar Cam
Parar S

Dirección de Cliente ACL

Nombre ACL

Desde IP	A IP	Máscara de Red
<input type="text" value="192.168.244.0"/>	<input type="text"/>	<input type="text" value="255.255.255.0"/>

URL de Fallo

Almacenar ACL en archivo Configuración Squid Separate file

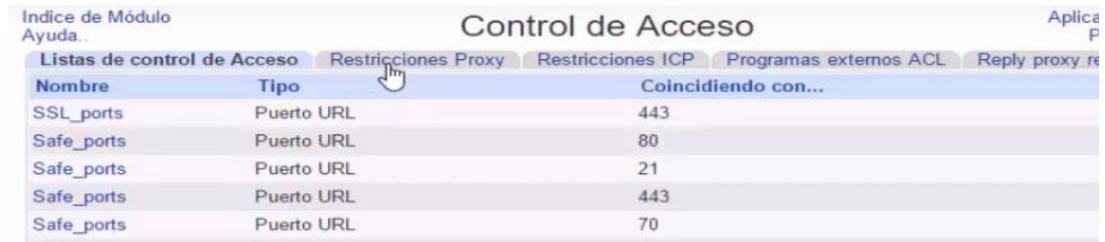
¿Usar sólo contenidos existentes del archivo?

Salvar

[Rearesar a Lista ACL](#) | [Rearesar a índice](#)

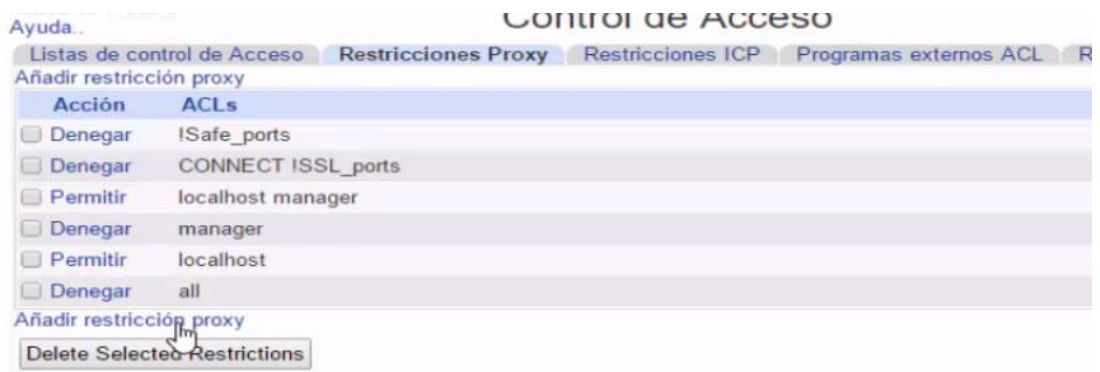
Así quedaría la configuración.

Acabamos de crear una regla que nos va a permitir navegar, tenemos que agregar la restricción para hacer efectivo el cambio, nos dirigimos a **Restricciones Proxy**.



Nombre	Tipo	Coincidiendo con...
SSL_ports	Puerto URL	443
Safe_ports	Puerto URL	80
Safe_ports	Puerto URL	21
Safe_ports	Puerto URL	443
Safe_ports	Puerto URL	70

Y Añadimos restricciones proxy, que le permita a ese grupo de máquinas navegar.



Acción	ACLs
<input type="checkbox"/> Denegar	!Safe_ports
<input type="checkbox"/> Denegar	CONNECT !SSL_ports
<input type="checkbox"/> Permitir	localhost manager
<input type="checkbox"/> Denegar	manager
<input type="checkbox"/> Permitir	localhost
<input type="checkbox"/> Denegar	all

Añadir restricción proxy

Delete Selected Restrictions



Restricción de Proxy

Acción Permitir Denegar

Coincidir con ACLs

- all (1)
- SSL_ports (1)
- Safe_ports (1)
- CONNECT (1)
- navegacion (0)

No coincidir con ACLs

- all (1)
- SSL_ports (1)
- Safe_ports (1)
- CONNECT (1)
- navegacion (0)

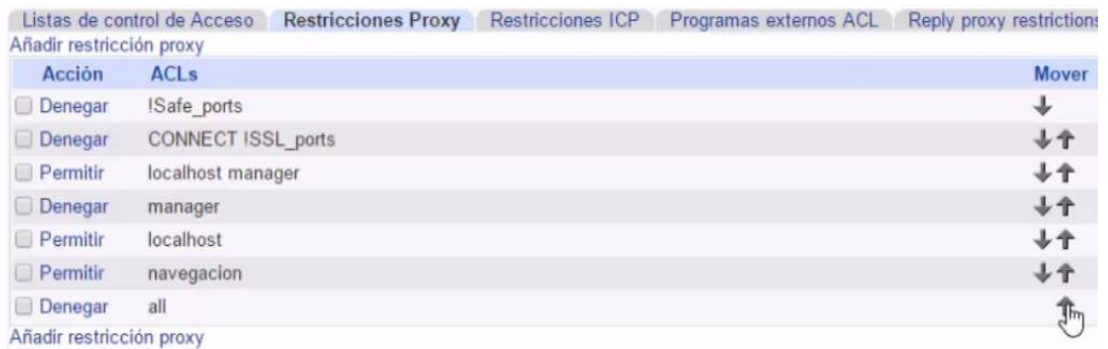
Salvar

[← Regresar a Lista de ACL](#) | [Regresar a índice](#)



Una vez seleccionado, salvamos y aplicamos cambios.

Algo bien importa que tenemos que hacer, tenemos que subir la regla que creamos y bajar la regla que deniega todo.



Así quedaría la configuración y aplicar cambios.

Con la configuración realizada ya estaríamos navegando a internet sin ningún problema.

Ahora creamos filtros para bloquear página y no pueden acceder, en este caso Facebook y YouTube.

Volvemos a panel de Control de Acceso y creamos una nueva ACL, con una configuración

Indice de Módulo Ayuda.. Control de Acceso

Nombre		Coincid
SSL_ports	Autenticación Externa	443
Safe_ports	Comunidad SNMP	80
Safe_ports	Dirección Ethernet	21
Safe_ports	Dirección IP de Proxy	443
Safe_ports	Dirección de Cliente	70
Safe_ports	Dirección de Servidor Web	210
Safe_ports	Expresión Regular URL	1025-65
Safe_ports	Expresión Regular de Autorización Externa	280
Safe_ports	Expresión Regular de Cliente	488
Safe_ports	Expresión Regular de Navegador	591
Safe_ports	Expresión Regular de Ruta URL	777
Safe_ports	Expresión Regular de Servidor Web	CONNE
Safe_ports	Expresión Regular de Usuario RFC931	192.168
Safe_ports	Fecha y Hora	
Safe_ports	Máx IP de Usuario	
Safe_ports	Máximas Conexiones	
Safe_ports	Método de Petición	
CONNECT	Número de destino AS	
navegacion	Número de fuente AS	
	Nombre de Máquina de Cliente	

Crear nueva ACL Autenticación Externa

Indice de Módulo Crear ACL Aplicar Cambios Parar Sesión

Expresión Regular URL ACL

Nombre ACL

Expresiones Regulares ¿Ignorar mayúsculas?

URL de Fallo

Almacenar ACL en archivo Configuración Squid Separate file ...

¿Usar sólo contenidos existentes del archivo?

Salvar

[← Regresar a Lista ACL](#) | [Regresar a índice](#)

Indice de Módulo Crear ACL Aplicar Cambios Parar Sesión

Expresión Regular URL ACL

Nombre ACL

Expresiones Regulares ¿Ignorar mayúsculas?

google
www.hotmail.com
hotmail
www.youtube.com
youtube
sexo

URL de Fallo

Almacenar ACL en archivo Configuración Squid Separate file ...

¿Usar sólo contenidos existentes del archivo?

Salvar

Así quedaría la configuración para sitios bloqueados, una vez creado nuestra ACL agregamos a la Restricciones.

Denegamos todo lo que coincida con ACL creada en este caso (Sitios Bloqueados).

Restricción de Proxy

Acción Permitir Denegar

Coincidir con ACLs

- all (1)
- SSL_ports (1)
- Safe_ports (1)
- CONNECT (1)
- navegacion (1)
- sitiosbloqueados (0)**

No coincidir con ACLs

- all (1)
- SSL_ports (1)
- Safe_ports (1)
- CONNECT (1)
- navegacion (1)
- sitiosbloqueados (0)

Salvar

[← Regresar a Lista de ACL](#) | [Regresar a índice](#)

Así quedaría la configuración y salvamos y aplicamos configuración.

Es importante configurar que sitios bloqueados este por encima de la restricción navegación.

Indice de Módulo
Ayuda..

Control de Acceso

Listas de control de Acceso | **Restricciones Proxy** | Restricciones ICP | Programas externos ACL | Rep

Añadir restricción proxy

Acción	ACLs
<input type="checkbox"/> Denegar	!Safe_ports
<input type="checkbox"/> Denegar	CONNECT !SSL_ports
<input type="checkbox"/> Permitir	localhost manager
<input type="checkbox"/> Denegar	manager
<input type="checkbox"/> Permitir	localhost
<input type="checkbox"/> Denegar	sitiosbloqueados
<input type="checkbox"/> Permitir	navegacion
<input type="checkbox"/> Denegar	all

Añadir restricción proxy

Delete Selected Restrictions

en esta orden es importante dejarlo.

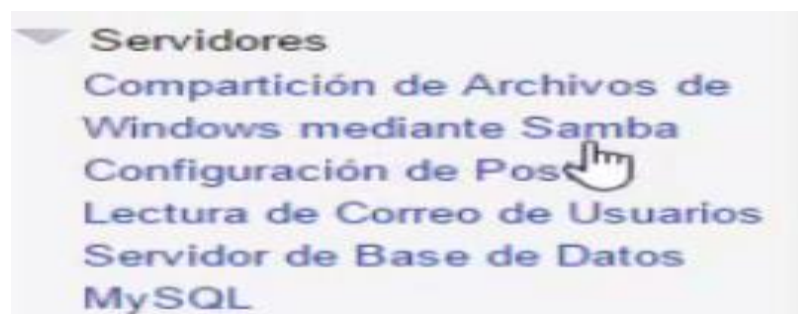
CONFIGURACIÓN DEL SERVIDOR SAMBA (Compartición de Archivos de Windows mediante Samba).

Lo primero es instalar samba mediante el terminal con el siguiente comando:

- `sudo apt-get -y -f install samba`

Una vez terminado la instalación, procedemos a Reajustar Módulos y actualizamos la página.

Entramos a la pestaña de Samba (Compartición **de Archivos de Windows mediante Samba**) para configurar.



Una vez adentro entramos a Red de Windows para configurar.

Configuración Global



Una vez adentro configuramos los siguientes campos:

- Grupo de trabajo: El nombre que vamos a conectarnos desde Windows.
- Nombre del Servidor:
- Seguridad: Seleccionamos **Nivel de Usuario**.

Salvamos la configuración.

Indice de Módulo

Opciones de Red de Windows

Opciones de Red de Windows

Grupo de Trabajo Defecto WORKGROUP

modo WINS Ser un servidor WINS Usar servidor Ninguno(a)

Descripción del servidor Defecto None %h server (Samba, Ubuntu)

Nombre del servidor

Alias del Servidor

Servicio por defecto

Configuramos Sincronización de Usuario, lo configuramos como esta en la imagen:

Indice de Módulo

Sincronización de Usuario

Se puede configurar Webmin de tal manera que los cambios en la lista de usuarios de Unix sean autom de usuarios de Samba. Esto sólo funcionará cuando el módulo de Webmin de Usuarios y Grupos sea cambiar usuarios.

Añadir usuario de Samba al crear un usuario de Unix Si No

Cambiar el usuario de Samba cuando se cambie el de Unix Si No

Borrar el usuario de Samba al borrar el de Unix Si No

Deleting the roaming profile when a Unix user is deleted Si No

Rename the roaming profile when a Unix user is renamed Si No

Group SID or RID for new users Defecto

Aplicar

Una vez configurado nos vamos a Convertir Usuario y no cambiamos nada y click en **Convertir Usuarios**.

Indice de Módulo

Convertir Usuarios

Este formulario te permite sincronizar la lista de usuarios de Unix y Samba. Cuando Samba usa claves de acceso encriptadas, se usa una lista separada de usuarios y claves de acceso en vez de la lista de usuarios del sistema. The list of users not to convert can contain usernames, UIDs, group names prefixed with an @, or UID ranges like 500-1000 or 500-.

Unix users to convert Only listed users or UID ranges All except listed users and UID ranges

Actualizar los usuarios ya existentes en Samba a partir de sus detalles en Unix Si No

Añadir nuevos usuarios de Samba a partir de la lista de usuarios de Unix Si No

Borrar los usuarios de Samba que no existen en Unix Si No

Para los recién creados usuarios, poner la clave de acceso a: Sin clave de acceso Cuenta bloqueada Usa esta clave de acceso

Convertir Usuarios

Y Creamos una Carpeta compartida.

Configuración de Módulo **Gestor de Comparticiones Samba** Versión 4.4.5-Ubuntu de Samba Buscar Documentos...

Seleccionar todo. | Invertir selección. | [Crear una nueva compartición de archivo](#) | [Crear una nueva compartición de impresora](#) | [Crear una nueva copia](#) | [Ver Todas las Conexiones](#)

Nombre de Compartición	Trayectoria	Seguridad
<input type="checkbox"/> printers	Todas las Impresoras	Imprimible para todos los usuarios conocidos
<input type="checkbox"/> print\$	/var/lib/samba/printers	Sólo lectura para todos los usuarios conocidos

Seleccionar todo. | Invertir selección. | [Crear una nueva compartición de archivo](#) | [Crear una nueva compartición de impresora](#) | [Crear una nueva copia](#) | [Ver Todas las Conexiones](#)

Ponemos nombre y seleccionamos el directorio, permisos 777 de lectura y escritura. Y **crear**.

Indice de Módulo **Crear Compartición de Archivo**

Información de Compartición

Nombre de Compartición datos Compartición de Directorios de Inicio

Directorio a compartir ...

Automatically create directory? Si No

Create with owner ...

Create with permissions

Create with group ...

¿Disponible? Si No

¿Hojeable? Si No

Comentario de Compartición

Una vez creada entramos a la carpeta para dar permisos (**Control de Seguridad y Acceso**)

Indice de Módulo **Editar Compartición de Archivo**

Información de Compartición

Nombre de Compartición datos Compartición de Directorios de Inicio

Directorio a compartir ...

¿Disponible? Si No

¿Hojeable? Si No

Comentario de Compartición

Otras opciones de Compartición

 [Control de Seguridad y Acceso](#)

 [Permisos de Archivo](#)

 [Cómo dar Nombre a Archivos](#)

 [Opciones varias](#)

Y cambiamos a la siguiente configuración:

Índice de Módulo

Editar Seguridad

Para compartición datos

Control de Seguridad y Acceso

¿Se puede escribir? Sí No

¿Acceso de Invitado? Ninguno Sí Sólo invitado

Usuario invitado de Unix ...

¿Límite a lista de posibles? Sí No

Máquinas a autorizar Todos(as) Sólo permitir:

Máquinas a denegar Ninguno Sólo denegar:

¿Revalidar usuarios? Sí No

Usuarios válidos ...

Grupos válidos ...

Usuarios inválidos ...

Grupos inválidos ...

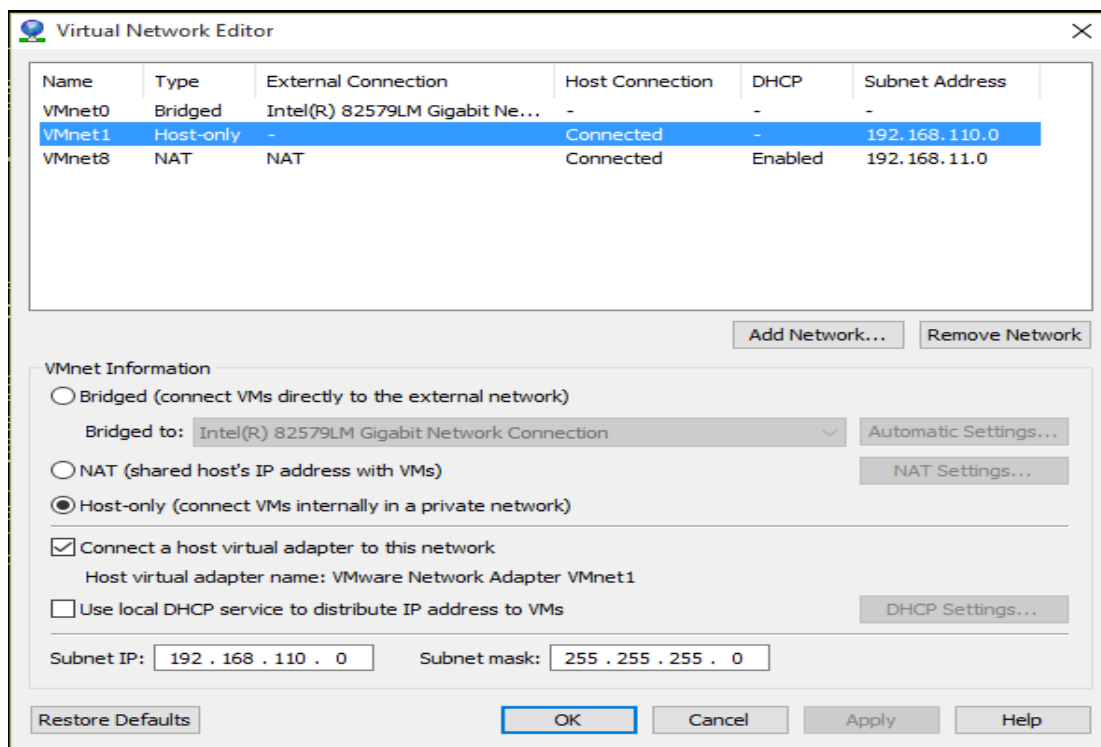
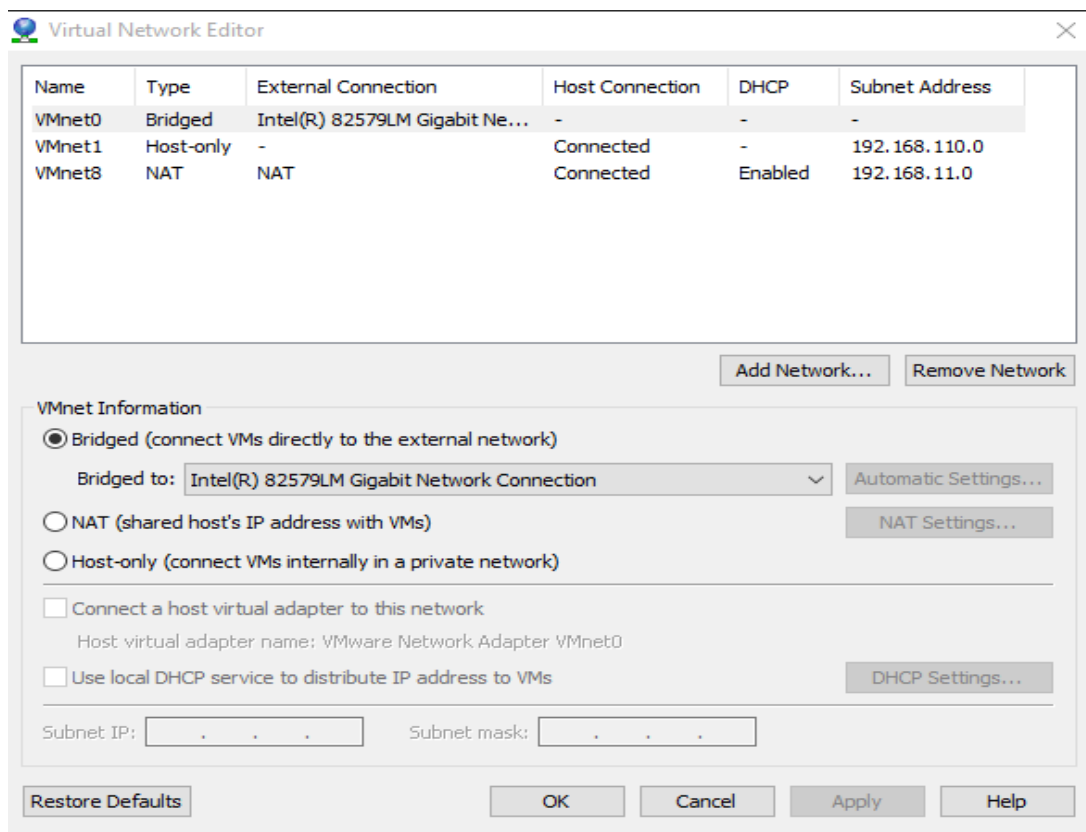
En esta parte seleccionamos a los usuarios que ven a poder ser válidos y los usuarios inválidos.

Y **salvamos** la configuración, de nuevo **salvar** y **arrancar Servidores Samba**.

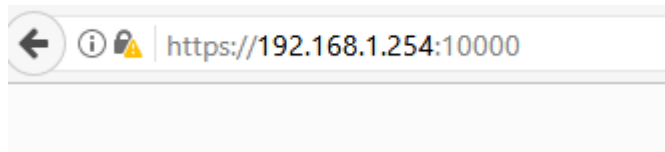
En Windows configuramos en grupo de trabajo con el que pusimos en el servidor Samba y los reiniciamos para que se configure todos los cambios.

INICIO DE SESIÓN

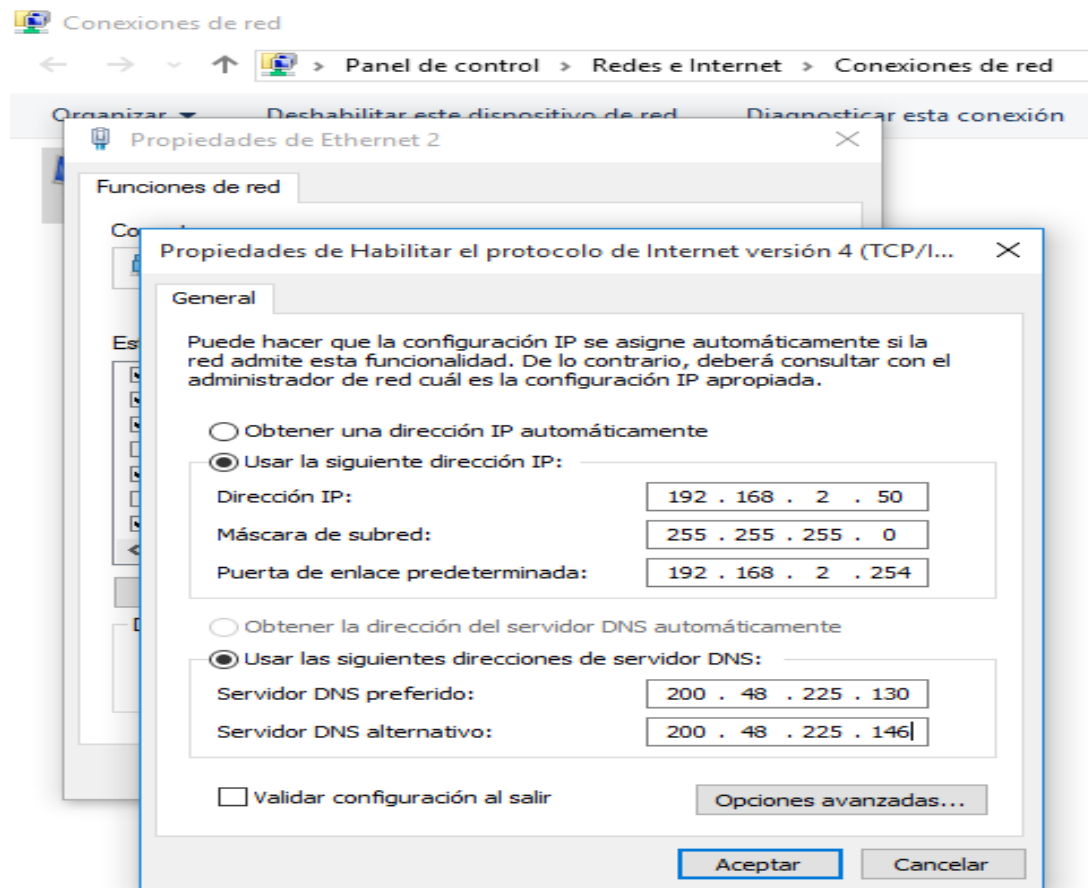
INTERFACES DE RED EN EL VMWARE



USO DEL NAVEGADOR PARA WEBMIN



CONFIGURACIÓN DEL IP PARA CONECTARSE AL SERVIDOR DESDE EL CLIENTE:



PRUEBA DEL SERVIDOR PROXY

En algunos casos se debe reiniciar el servicio proxy

Antes:

Facebook - Entra o regístrate | YouTube

https://www.youtube.com

Inicio Tendencias

Recomendados

- HAZ MANJAR DE ARROZ FACIL P/NEGOCIO O CONSUMO ROSV...
Roviv Hernández | 1,520,794 vistas · Hace 2 meses
- NASA finalmente revela la verdad sobre la misteriosa Área 51...
canal-5/telemundo | 228,674 vistas · Hace 1 año
- CNCO - Hey DJ (Letra) HD
Yohn V. Rivera | 49,920,533 vistas · Hace 3 meses
- Me voy a comer el mundo Lima Perú Full HD
PARA TODOS | 25,774 vistas · Hace 2 semanas
- BESOS DE MOZA
Cositaz Ricaz | 660,707 vistas · Hace 1 año
- Maluma, J Balvin, Shakira, Pitbull, Chayanne, CNCO, Wisin, Yandel...
Latin Club | 3,680 vistas · Hace 3 horas
- CREEPPASTA CLASH ROYALE- Creeppastas clash royale...
Kipsacr7 | 155,484 vistas · Hace 1 año
- Como prepara cachangas.
Lorena Carnero | 425,918 vistas · Hace 3 años

Subidos recientemente Videos recomendados

- REVENTAMOS CON EL GLOBO AL MÁXIMO | Clash Royale con...
TheAhorro845 - Clash Royale - Clash of Clans | 89,199 vistas · Hace 1 hora
- NADINE HEREDIA: TESTIGO HUNDE MAS A LA PRIMERA...
Mi Canal Peru | 62,683 vistas · Hace 1 día
- Fiesta Latina 2017 - Wisin, Maluma, Alex Sensation, J Balvi...
Latin ChiChigos | 189 vistas · Hace 56 minutos
- La Rosa de Guadalupe "No quiero ser mujer" Capítulo Completo
Cocho Late | 181,079 vistas · Hace 16 horas

Entretención Videos recomendados

Suscribirse 1,136,820

Facebook - Entra o regístrate | YouTube

https://www.facebook.com

facebook

Correo electrónico o teléfono Contraseña Entrar

¿Has olvidado los datos de la cuenta?

Facebook te ayuda a comunicarte y compartir con las personas que forman parte de tu vida.

Registrarte

Es gratis y lo será siempre.

Nombre Apellidos

Número de móvil o correo electrónico

Contraseña nueva

Fecha de nacimiento

17 jul 1999 ¿Por qué tengo que facilitar mi fecha de nacimiento?

Mujer Hombre

Al hacer clic en "Terminado", aceptas las Condiciones y confirmas que has leído nuestra Política de datos, incluido el Uso de cookies. Es posible que recibas notificaciones por SMS de Facebook, que puedes desactivar cuando quieras.

Terminado

Crea una página para un personaje público, un grupo de música o un negocio.

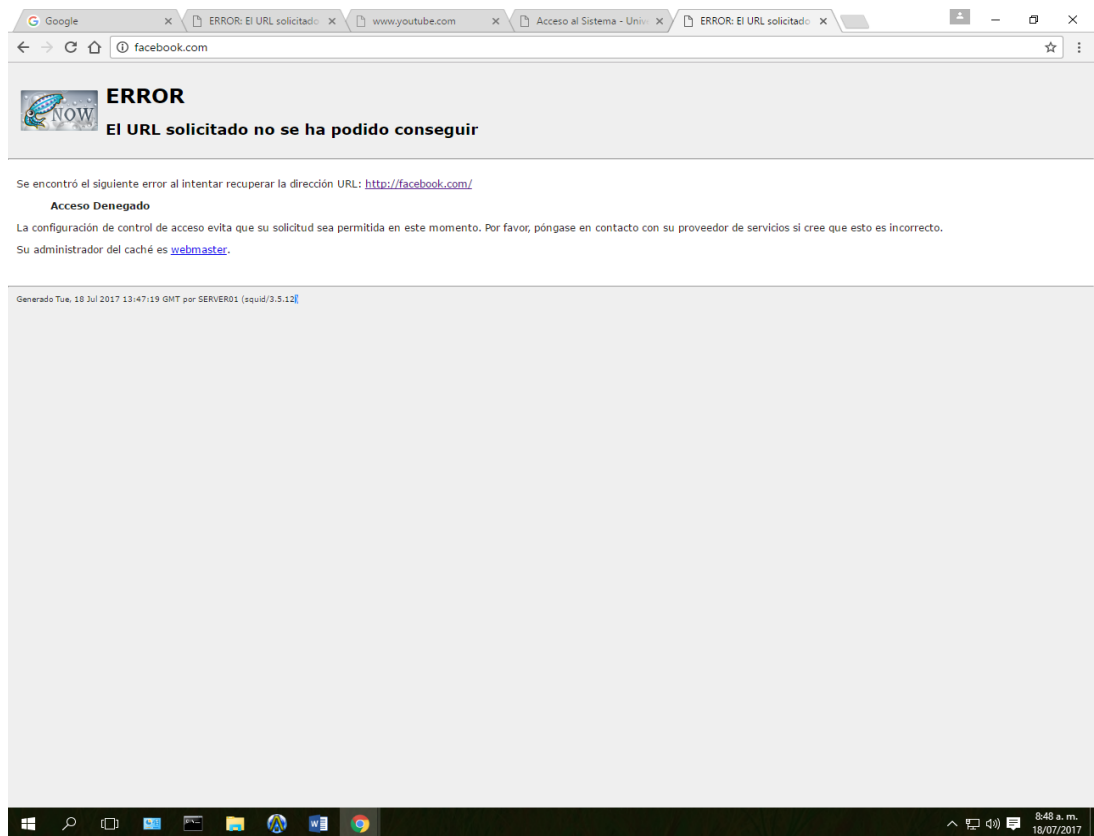
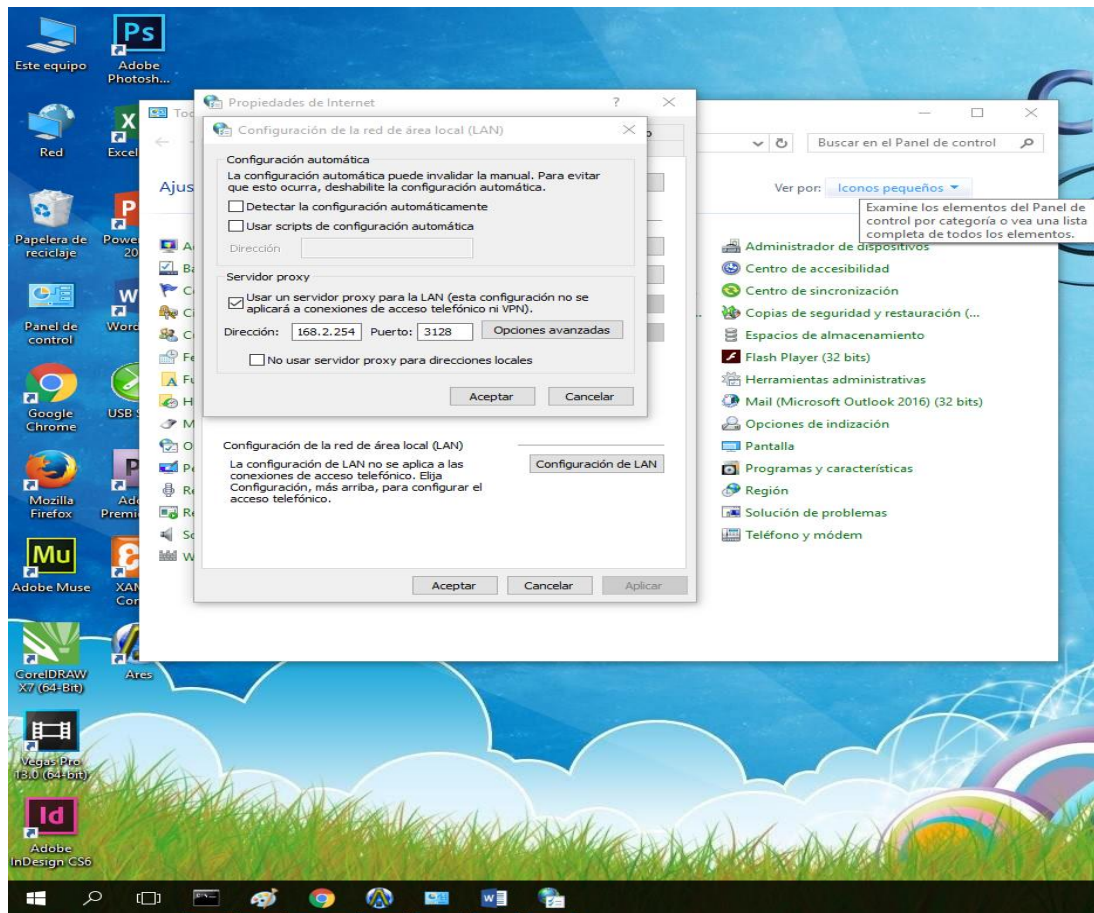
Español (España) English (US) Italiano Português (Brasil) Français (France) Deutsch 日本語 中文(简体) العربية

Registrarte Entrar Móvil Buscar amigos Páginas Ayuda

Messenger Facebook Lite Personas Lugares Juegos Lugares Famosos Mercado Grupos Recetas Moments
Instagram Información Crear anuncio Crear página Desarrolladores Empleo Privacidad Cookies Gestión de anuncios Condiciones

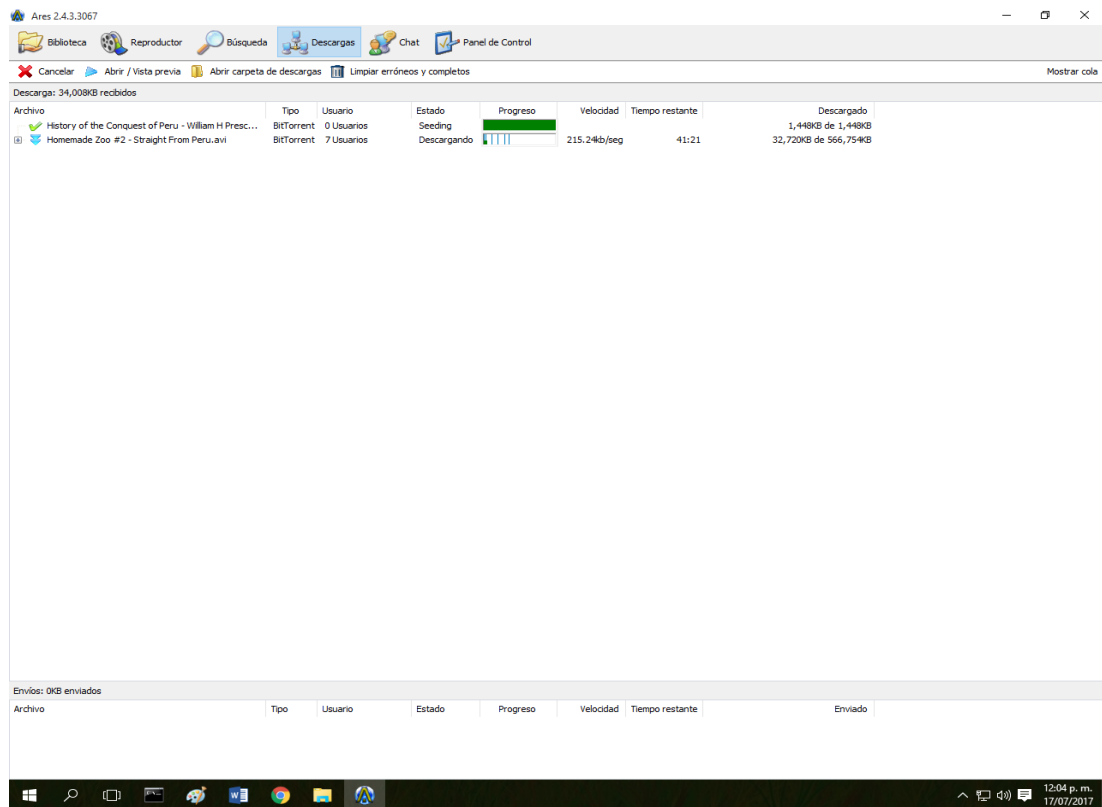
Facebook © 2017

Después:

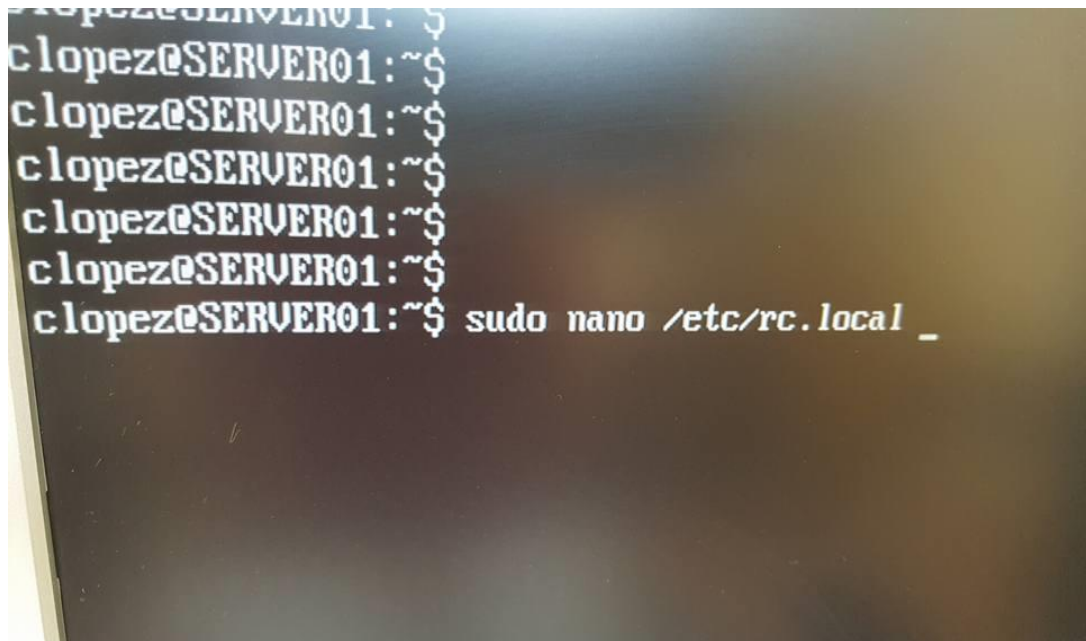


PRUEBA FIREWALL (IPTABLES):

Antes:



Después:




```
GNU nano 2.5.3 Archivo: /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

sh /home/clopez/prueba.sh
#sh /home/clopez/blockipp2p.sh
exit 0
```

SERVIDOR DE ARCHIVOS SAMBA.

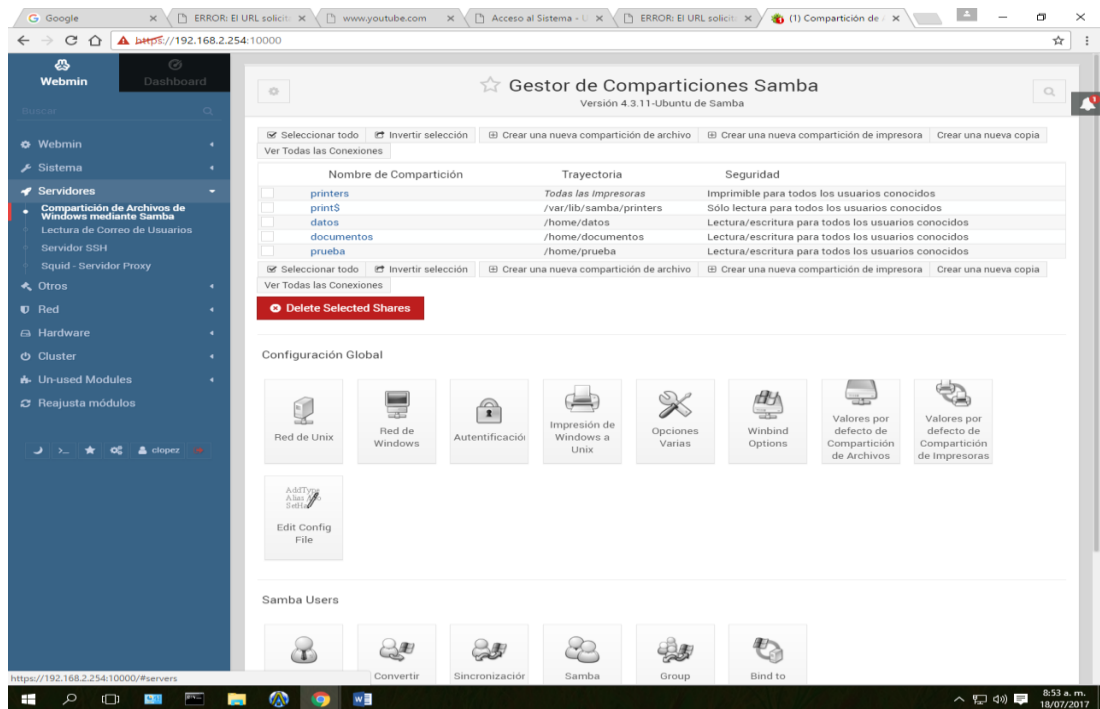
The screenshot shows the Webmin interface for managing users and groups. The page title is 'Usuarios y Grupos' and it indicates the database type is 'Regular /etc/passwd & /etc/shadow'. There are tabs for 'Usuarios Locales' and 'Grupos Locales'. A table lists various system users with columns for 'Nombre de Usuario', 'ID de Usuario', 'Grupo', 'Nombre Real', 'Directorio inicial', and 'Shell'. A 'Packages Update' notification is visible in the bottom right corner.

Nombre de Usuario	ID de Usuario	Grupo	Nombre Real	Directorio inicial	Shell
root	0	root	root	/root	/bin/bash
daemon	1	daemon	daemon	/usr/sbin	/usr/sbin/nologin
bin	2	bin	bin	/bin	/usr/sbin/nologin
sys	3	sys	sys	/dev	/usr/sbin/nologin
sync	4	nogroup	sync	/bin	/bin/sync
games	5	games	games	/usr/games	/usr/sbin/nologin
man	6	man	man	/var/cache/man	/usr/sbin/nologin
lp	7	lp	lp	/var/spool/lpd	/usr/sbin/nologin
mail	8	mail	mail	/var/mail	/usr/sbin/nologin
news	9	news	news	/var/spool/news	/usr/sbin/nologin
uucp	10	uucp	uucp	/var/spool/uucp	/usr/sbin/nologin
proxy	13	proxy	proxy	/bin	/usr/sbin/nologin
www-data	33	www-data	www-data	/usr/www	/usr/sbin/nologin
backup	34	backup	backup	/var/backups	/usr/sbin/nologin
list	38	list	Mailing List Manager	/var/list	/usr/sbin/nologin
irc	39	irc	ircd	/var/run/ircd	/usr/sbin/nologin
gnats	41	gnats	Gnats Bug-Reporting System (admin)	/var/lib/gnats	/usr/sbin/nologin
nobody	65534	nogroup	nobody	/nonexistent	/usr/sbin/nologin
system-timesync	100	system-timesync	system Time Synchronization	/run/systemd	/bin/false
system-network	101	system-network	systemd Network Management	/run/systemd/netif	/bin/false
system-resolve	102	system-resolve	systemd Resolver	/run/systemd/resolve	/bin/false
system-bus-proxy	103	system-bus-proxy	systemd Bus Proxy	/run/systemd	/bin/false
syslog	104	syslog	syslog	/home/syslog	/bin/false
_apt	105	nogroup		/nonexistent	/bin/false
lad	106	nogroup		/var/lib/ldf	/bin/false
messagebus	107	messagebus		/var/run/dbus	/bin/false
uiddd	108	uiddd			
dnsmasq	109	nogroup	dnsmasq		
sshd	110	nogroup			
clopez	1000	clopez	clopez		
sabrera	1001	users	sabrera		

- Click en nuevo usuario.

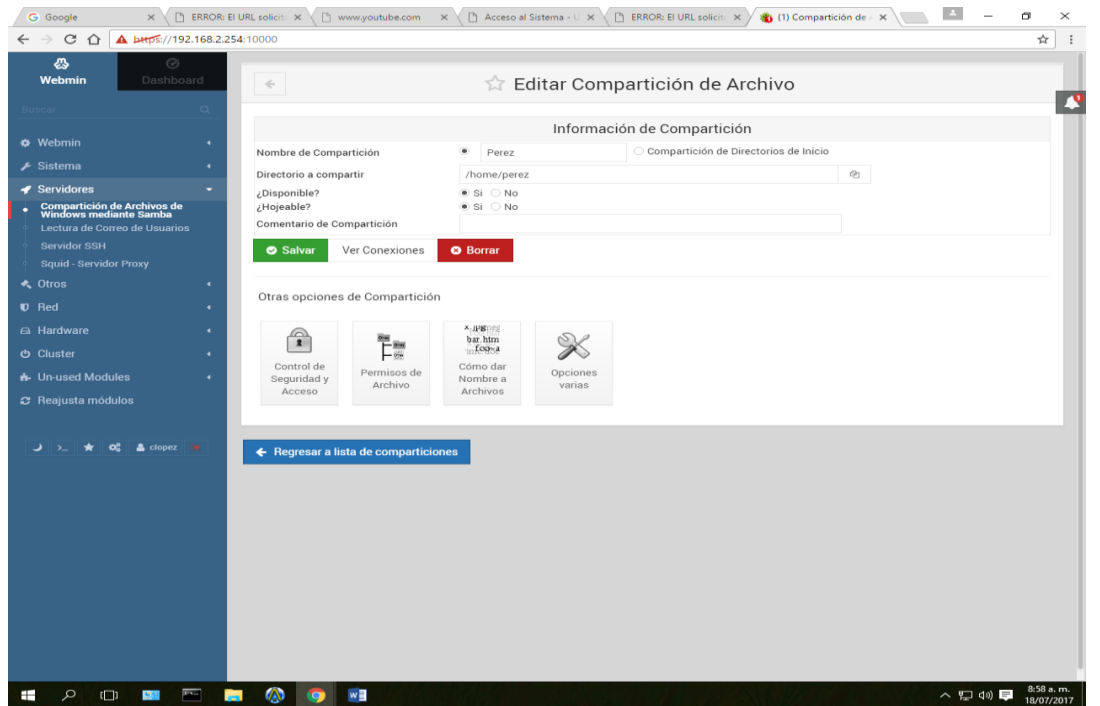
The screenshot shows the 'Crear Usuario' (Create User) page in Webmin. The 'Detalles de Usuario' section includes fields for 'Nombre de Usuario' (jperex), 'ID de Usuario' (Automatic, Calculado, 1003), 'Nombre Real' (Juan Perez), 'Directorio inicial' (Automatic, Directory), and 'Shell' (/bin/bash). The 'Contraseña' section has 'Contraseña normal' selected with the password '123456'. The 'Opciones de Contraseña' section includes 'Contraseña cambiada' (Never), 'Fecha de Expiración' (Ene), 'Días mínimos', 'Días máximos', 'Días de Aviso', 'Días inactivos', and '¿Forzar cambio en el siguiente login?' (No). The 'Afiliación del Grupo' section shows 'Grupo primario' as 'Grupo existente' (users) and 'Grupos secundarios' as root, daemon, bin, sys, adm, tty. At the bottom, there is a checkbox for '¿Crear directorio inicial?' (No).

Click en crear.



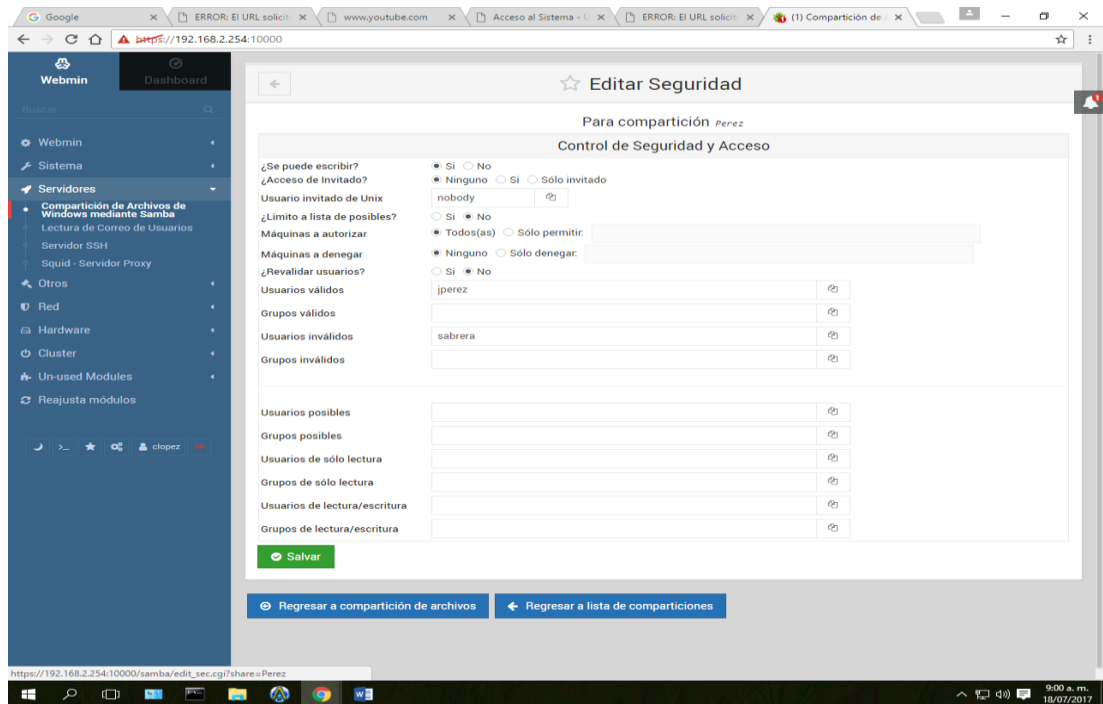
Verificar los usuarios haciendo click en Usuarios de samba y buscamos al usuario creado.

Regresar a la ventana principal del servidor Samba y hacemos Click **Crear una nueva compartición de archivos.**



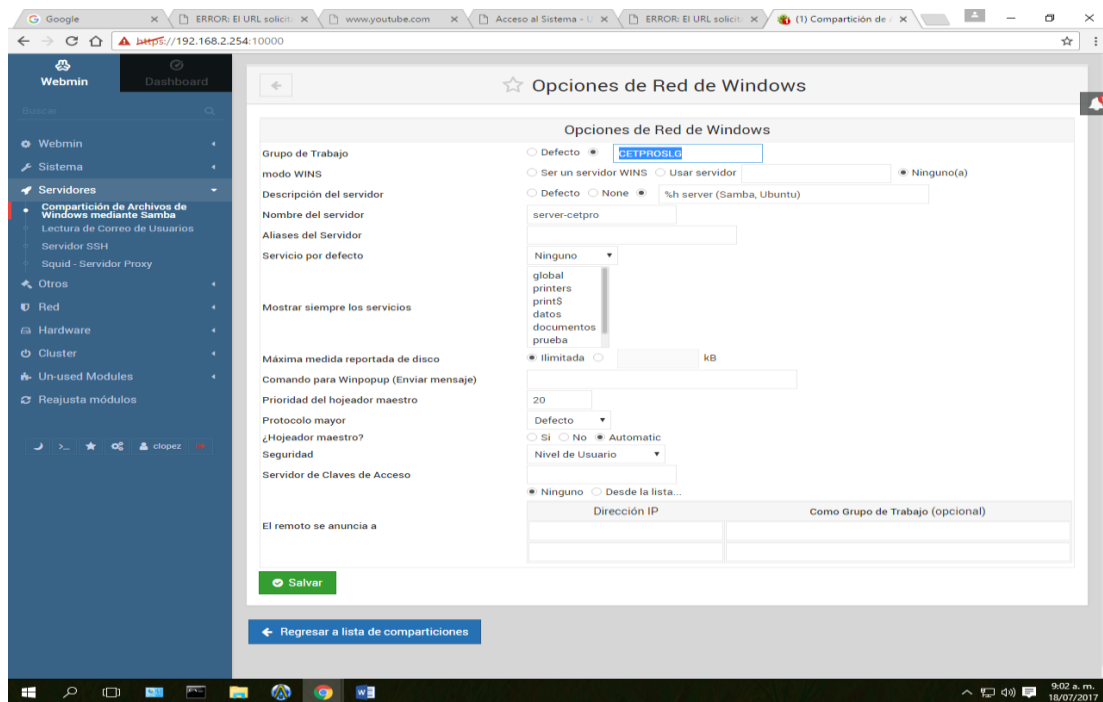
Click en crear

Después hacer click en el usuario creado y seleccionamos la opción Control de seguridad y Acceso.



Configuramos como se muestra la imagen y guardamos (salvar).

Posteriormente en el cliente se configura manualmente el grupo de trabajo que está configurado en el servidor SAMBA.



Reiniciar el cliente configurado con el grupo de trabaja que pueda adaptarse a los cambios de permiso configurado en el servidor SAMBA.