# UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

## FACULTAD DE CIENCIAS INFORMÁTICAS

**TEMA:**

ASEGURAMIENTO DE REDES Y SISTEMAS INFORMÁTICOS DE LA EMPRESA PRIVADA ALLCOMPU DE LA CIUDAD DE MANTA, BASADO EN ENTORNOS GNU/LINUX

TRABAJO DE TITULACIÓN MODALIDAD PROYECTO INTEGRADOR, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS


**AUTOR:**

MORÁN CARREÑO LEONIDAS ALBERTO

**DIRECTOR DE TEMA:**

ING. JOHNNY JAVIER LARREA PLÚA



**MANTA – ECUADOR**

2017 – 2018(1)

# TEMA:

**ASEGURAMIENTO DE REDES Y SISTEMAS INFORMÁTICOS DE LA EMPRESA PRIVADA ALLCOMPU DE LA CIUDAD DE MANTA, BASADO EN ENTORNOS GNU/LINUX.**

## CERTIFICACIÓN:

En calidad de Docente de la Facultad de Ciencias Informáticas de la Universidad Laica Eloy Alfaro de Manabí, certifico:

Haber dirigido y revisado el Trabajo de Titulación Modalidad Proyecto Integrador: "ASEGURAMIENTO DE REDES Y SISTEMAS INFORMÁTICOS DE LA EMPRESA PRIVADA ALLCOMPU DE LA CIUDAD DE MANTA, BASADO EN ENTORNOS GNU/LINUX ", proyecto que cumple con los requisitos que exige la Guía Metodológica de Titulación de la Institución y el instructivo normativo para trabajos de titulación de la carrera Ingeniería en Sistemas de la Facultad de Ciencias Informáticas y, reúne los méritos suficientes para ser sometido a la evaluación del jurado examinador que designen las autoridades.

La autoría del tema desarrollado corresponde al señor MORÁN CARREÑO LEONIDAS ALBERTO, estudiante con estudios concluidos en la carrera Ingeniería en Sistemas, período académico 2017-2018, quien se encuentra apto para la defensa.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Lo certifico:

Ing. Johnny Larrea Plúa
**Docente Facultad de Ciencias Informáticas**
**Universidad Laica "Eloy Alfaro" de Manabí**

Manta, 27 de noviembre de 2017.

TRABAJO DE TITULACIÓN MODALIDAD PROYECTO INTEGRADOR, PREVIO A LA OBTENCIÓN DEL TÍTULO DE: INGENIERO EN SISTEMAS

"ASEGURAMIENTO DE REDES Y SISTEMAS INFORMÁTICOS DE LA EMPRESA PRIVADA ALLCOMPU DE LA CIUDAD DE MANTA, BASADO EN ENTORNOS GNU/LINUX"

Tribunal examinador que declara APROBADO el Grado de INGENIERO EN SISTEMAS, al señor: MORÁN CARREÑO LEONIDAS ALBERTO

Ing. Denisse Soraya Vera Navarrete

Ing. Juan Carlos Sendón Varela

Ing. Jorge Sergio Herrera Tapia

Manta, 26 de enero de 2018

## DECLARACIÓN DE AUTORÍA

Yo, Leonidas Alberto Morán Carreño, con cédula de identidad 131363340-4, estudiante de la carrera de Ingeniería en Sistemas, libre y voluntariamente declaro que el contenido de este documento es de mi autoría y manifestó que, ante cualquier notificación de plagio, copia o falta a la fuente original, soy responsable directo y administrativo, económico y legal, sin afectar al Director de Tesis, a la Universidad y a otras entidades que hayan colaborado en este trabajo.

---

Leonidas Alberto Morán Carreño

C.I. 131363340-4

## DEDICATORIA

Dedico esta tesis en primera instancia a DIOS y a mi familia de la cual el apoyo y confianza ha sido parte fundamental para el desarrollo de este proceso de formación académica.

A la Universidad Laica Eloy Alfaro de Manabí la cual ha permitido que mi crecimiento profesional se fortalezca y me genere mejores oportunidades en diferentes ambientes laborales.

A mis Maestros, compañeros y amigos que me apoyaron y motivaron para lograr los objetivos que me propuse en el momento de tomar este reto como parte de mi vida.

Al Ing. Johnny Larrea Plua, quien como director ha sido timón y motivador para lograr hacer de este proyecto una realidad.

**Leonidas Alberto Morán Carreño**

## AGRADECIMIENTO

Agradecimiento infinito a DIOS, por oportunidades y bendiciones que me brinda a diario.

A mi familia, a mi padre quien con su ejemplo y sacrificio ha llevado a delante a la familia; a mi madre quien inculcó en mí y en mis hermanas los valores necesarios para luchar y conseguir ser personas de bien; a mis hermanas por brindarme siempre su apoyo y compartir este logro.

A mis amigos, por ser los propulsores que necesitaba para iniciar el final de esta etapa.

ALLCOMPU, empresa que me vio crecer como persona y como profesional, a todo el personal técnico y administrativo, especialmente el Ing. Aníbal Flores, que, con su experiencia y conocimientos adquirí destrezas y habilidades las cuales me desarrollaron como profesional, es por el importante aporte para la realización del fruto de esta tesis.

Al cuerpo docente y administrativo de la Facultad de Ciencias Informáticas de la Universidad Laica Eloy Alfaro de Manabí, por potenciar en ellos valores ética e integridad, por las experiencias compartidas y conocimientos, des esta manera considero que se está garantizando mi aporte a la sociedad.

# ÍNDICE DE CONTENIDO

# ÍNDICE DE ILUSTRACIONES

## INDICE DE TABLAS

# RESUMEN

Uno de los pilares fundamentales de las empresas es la información, es por ello que, debido al incremento de robo de esta, y los ataques informáticos hacia los sistemas, servidores, redes etc., los temas de seguridad van ganando importancia con el fin de asegurar la integridad, confidencialidad y disponibilidad de los datos.

El aseguramiento nace de la necesidad de precautelar y poner a prueba las medidas de seguridad que sean implementadas en las pequeñas y medianas empresas tanto en software como hardware.

Es por esto la necesidad de un modelo de defensa en profundidad que permita manejar y controlar los activos tecnológicos de la empresa ALLCOMPU, minimizando al máximo los riegos a los que puede estar sujeta dicha institución.

A demás el modelo defensa en profundidad, estará basado y desarrollado bajo entornos de tecnologías libres como lo es GNU/Linux. Lo que permitirá una estabilidad y flexibilidad a las empresas de proyectarse hacia el futuro sin verse directamente afectados en el funcionamiento de sus sistemas y la protección de los datos.

Finalmente, este trabajo busca servir de guía para que las pequeñas y medianas empresas (PYMES) decidan implementar medianas de seguridad en la información y sus sistemas informáticos, de tal forma que puedan conocer las herramientas que le serán útiles para cada nivel del modelo defensa en profundidad basado en un entorno libre.

# INTRODUCCIÓN

Hoy en día la seguridad en las empresas es cada vez un aspecto más crítico en la administración de las Tics. El robo de información confidencial por parte de usuarios que no tienen acceso a dichos datos, la suplantación de una identidad o la destrucción de información, la denegación de un servicio son solo algunos riesgos a los que se enfrentan las empresas.

Las empresas deben considerar elementos para disponer de un entorno seguro, como, sistemas adecuados tanto en versión como en configuraciones, herramientas que permitan asegurar el entorno, procedimientos de seguridad de la información, activos tecnológicos básicos necesarios, conocimiento y la capacidad de mantener lo más seguro posible el entorno tecnológico de la empresa.

En entornos empresariales o corporativos se debe tener en cuenta a los peligros a los que la empresa está expuesta. Uno de estos peligros es el software y sus continuas variantes y vertientes, en función de lo que se ejecuta.

Es por ello el aseguramiento en profundidad de los sistemas operativos toman una importancia vital para ser proactivos frente a posibles intrusiones, esto con el fin de limitar en lo posible vulnerabilidades y evitar perdida de información o manipulación de los equipos comprometidos. Por lo anterior es evidente que surge la necesidad de aplicar las técnicas de aseguramiento (Hardening) en los sistemas operativos de las empresas, con ello se minimizan riesgos y se evitan consecuencias económicas, afectación de imagen entre otras consecuencias.

El software confiable es aquel que hace lo que se supone que debe hacer, en otras palabras, es una aplicación que ejecuta procesos y realiza correctamente su tarea. El software seguro hace lo que debe hacer y ninguna otra tarea más. El software confiable puede producir inseguridad en el

entorno empresarial o corporativo. por lo cual se deben implementar procesos y realizar procedimientos para evitar la inseguridad.

Otra medida que se aplicaría para fortalecer los sistemas informáticos y el entorno empresarial sería la aplicación de políticas adecuadas de seguridad y actualización de sistemas.

En el proceso de aseguramiento o fortificación se disponen de los principios: Mínimo punto de exposición, mínimo privilegio posible y defensa en profundidad.

Como se verá a lo largo del desarrollo de esta tesis, asegurar un sistema requiere limitar características de software, muchas veces desactivar servicios y bloquear otras tantas que pueden ser fácilmente la puerta de entrada al sistema, de esta manera se está reduciendo en importante medida un gran número de vulnerabilidades. Cada organización tiene sus propias necesidades, en el desarrollo de esta investigación se pretende dar a conocer de manera unificada las características de las diferentes aplicaciones que se convierten en herramientas fundamentales y de uso imperativo en el hardening de los sistemas informáticos (Firewall, Criptografía, usos de Sniffer, entre otros). De esta manera, inicialmente se estará dando nociones básicas de qué es y en qué consiste el Hardening, así como su implementación.

GNU/Linux proporciona una base muy utilizada en el mundo de los servidores y servicios que ayudan a la protección de sistemas informáticos e información de la empresa. Pero se debe configurar y fortificar estos entornos para evitar problemas o sorpresas innecesarias.

## UBICACIÓN Y CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN

Aseguramiento de redes y sistemas informáticos mediante la implementación de un servidor HP Proliant ML150G6 con sistema operativo Debian 9 Strech GNU/Linux para la empresa privada ALLCOMPU de la ciudad de Manta.

## PLANTEAMIENTO DE PROBLEMA

La empresa ALLCOMPU, dedicada a dar soluciones tecnológicas informáticas a sectores corporativos dentro y fuera de la ciudad de Manta, tanto públicos como privados. Esta empresa a pesar de tener las características tecnológicas, evidencia una serie de problemas e inconvenientes en el área administrativa y técnica, como es, que existe inseguridad en la infraestructura de la red y en los servicios informáticos que utilizar a diario para brindar atención a sus clientes.

Esta inseguridad en la red y los sistemas es causada por una serie de inconvenientes técnicos no previsto en el momento en que se implementó la red. Entre los que podemos mencionar que existe una deficiencia en el sistema de compartición de archivos, bajo nivel de seguridad y control para conectarse a la red por medios inalámbricos (WIFI); todo esto afecta a la disponibilidad, integridad y autenticidad de la información.

Otros de los problemas que se detectó en la red de la empresa ALLCOMPU, es que los mecanismos de conexión a la red es que los usuarios que se interconectan a la red, automáticamente pasan a ser miembros de esta, teniendo acceso a toda la información de la empresa, lo que produce que algunos servicios disponibles en la red se vean comprometidos. Lo antes mencionado se debe también a que la red lógica plana sin ningún tipo de segmentación o separación de servicios dentro de la red, por lo cual se vuelve más vulnerable, afectando directamente la disponibilidad de los servicios.

Todas estas causas hacen que la red y los sistemas informáticos de la empresa ALLCOMPU sean vulnerables, ya que no constan con mecanismos de protección y seguridad por lo que representa como un real y grabe problema para el correcto funcionamiento de la empresa en los actuales momentos.

## OBJETIVO GENERAL

Implementar un modelo de defensa de seguridad informática, en la empresa ALLCOMPU usando tecnologías libres.

## OBJETIVOS ESPECÍFICOS

- Determinar los mecanismos de seguridad informática que posee la empresa ALLCOMPU en la red y sus sistemas informáticos.
- Analizar la técnica de Hardening (aseguramiento) más adecuada que permita, sus estrategias de aplicabilidad, incluyendo técnicas que se deben considerar para realizar su implementación.
- Implementar el modelo defensa en profundidad mediante el uso del sistema operativo Debían GNU/Linux y herramientas open source.
- Implementar métodos de seguridad a la red inalámbrica.

# JUSTIFICACIÓN

Las empresas vienen siendo objeto de incontables intentos a menudo por hacerse de la información de la misma, y a su vez del control de los equipos informáticos por parte de personas no autorizadas. Generalmente las empresas no tienen como prioridad la capacitación de todo su personal y la indagación respecto a las posibles medidas de seguridad que deben tomarse para prevenirlos.

Es por ello, el desarrollo del presente proyecto (Aseguramiento de redes y sistemas informáticos de la empresa ALLCOMPU, basado en entornos GNU/Linux) se convierte en una necesidad de suma importancia con la cual se pretende minimizar las vulnerabilidades de la empresa con respecto al acceso de los datos, a su vez permite poner en conocimiento las diferentes herramientas que se pueden encontrar disponibles con el fin de aumentar el nivel de seguridad de los sistemas informáticos de la empresa.

# CAPÍTULO I

# 1. MARCO TEORICO DE LA INVESTIGACIÓN

## 1.1 INTRODUCCIÓN

En este capítulo se realizará un estudio de los fundamentos de aseguramiento en redes de datos, telefonía IP (VoIP) y sistemas informáticos, partiendo de una investigación de la funcionalidad y aplicabilidad del Modelo de seguridad "Defensa en Profundidad", se resaltará la importancia de utilizar un Firewall, sin dejar a un lado los fundamentos necesarios que permitan realizar una segmentación de la red mediante VLANs.

### CONCEPTOS BÁSICOS DE SEGURIDAD EN REDES

Es muy importante aclarar terminología que llevaran a conceptualizar la seguridad de redes; términos que involucran vulnerabilidades, puertos, amenazas, direccionamiento, entre otros.

### INFORMACIÓN

La información es uno de los activos más importantes dentro de un entorno corporativo, por lo que requiere fuertes mecanismos de seguridad aplicando medidas de precautelar o asegurar una adecuada operación y continuidad de la empresa.

Daniel Cohen Karen afirma que

La información es un recurso vital para toda organización, y le buen manejo de esta puede significar la diferencia entre el éxito o el fracaso para todos los proyectos que se emprendan dentro de un organismo que busca el crecimiento y el éxito.

"La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en

consecuencia necesita ser protegido adecuadamente.” (Carlos Andrés Gil, Jonathan Martínez, Julieth Veloza & Ray Alejandro Mora, 2008)

**SEGURIDAD.**

El término seguridad posee múltiples usos. A grandes rasgos, puede afirmarse que este concepto que proviene del latín securitas hace foco en la característica de seguro, es decir, realza la propiedad de algo donde no se registran peligros, daños ni riesgos. Una cosa segura es algo firme, cierto e indubitable. La seguridad, por lo tanto, puede considerarse como una certeza.

Una de las acepciones del término es el que se utiliza en informática, un concepto moderno, pero sumamente importante para conservar los ordenadores y equipos relacionados en buen estado. La seguridad informática permite asegurarse que los recursos del sistema se utilizan de la manera en la que se espera y que quienes puedan acceder a la información que en él se encuentran sean las personas acreditadas para hacerlo.

En informática se habla de dos tipos de seguridades, la física (barreras físicas que impiden el paso al sistema de cualquier persona no acreditada. Se realiza a través de aplicaciones y procedimientos específicos que tienen el objeto de bloquear el acceso a dichos individuos) y la lógica (las formas en las que se desempeña este tipo de seguridad son a través de encriptación de códigos, de modo que no puedan ser leídos o traducidos por los intrusos que pudieran sobre pasar las barreras físicas, códigos de autenticación y antivirus o pared de fuego, en el caso de usar un sistema operativo como Windows). A la hora de elaborar un diseño, ya sea de página web o de espacio en la red de cualquier tener en cuenta ambos tipos de seguridad es fundamental. (Julián Pérez Porto y Ana Gardey. Publicado: 2008. Actualizado: 2012.)

## SEGURIDAD DE LA INFORMACIÓN

Según ISO 27001 nos dice que la…

Seguridad de la información se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser:

- Electrónicos
- En papel
- Audio y video, etc.

La concienciación de los usuarios o empleados es algo también imprescindible. Los usuarios suelen ser víctimas de numerosos engaños o ingeniería social, lo cual son un foco débil en la seguridad corporativa y de la información de la empresa. Se debe gastar recursos en concienciar a los empleados para fortificar uno de los puntos débiles de la organización.

Vale la pena recalcar que no es posible una seguridad absoluta a los sistemas de información, siempre habrá riesgos independientemente de las comidas que se tomen para contrarrestar algún tipo de amenaza.

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo

o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio. (Actualidad Tecnológica (2010). Control Interno y Auditoria Informática)

## PILARES FUNDAMENTALES DE LA SEGURIDAD DE INFORMACIÓN

La seguridad de la información según iso 27001 se caracteriza por mantener y preservar “la integridad, confidencialidad y disponibilidad de la información”.

Según la recomendación x.800 del CCITT (Comité Consultivo Internacional Telegráfico y Telefónico) conceptualiza estos términos así:

A. Integridad “propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada”.

B. Confidencialidad “propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.”

C. Disponibilidad “propiedad de ser accesible y utilizable a petición por una entidad autorizada.”

## IDENTIFICACIÓN DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN

La identificación de riesgos según Javier Areito se define como “el proceso que se encarga de identificar y cuantificar la probabilidad que se produzcan amenazas y de establecer un nivel aceptable de riesgo para la organización”

Al identificar dichos riesgos, se producen diferentes incidentes no deseados para la organización, los mismos que se presentan en la Figura 1.


*Ilustración 1: Incidentes producidos en la identificación de riesgos*

*FUENTE: (Bertolín, 2008), Pág. 8*

## AMENAZAS PARA LA SEGURIDAD DE INFORMACIÓN

Una amenaza según López en su libro Seguridad Informática, se entiende como la “presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que – de tener la oportunidad- atacarán al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad.” (Pág 13)

- Clasificación de la amenaza

Se pueden encontrar diferentes clasificaciones, de acuerdo al criterio de los autores, para este documento se ha tomado algunas de ellas y se las ha clasificado de tal manera que se muestra en la Figura 2.

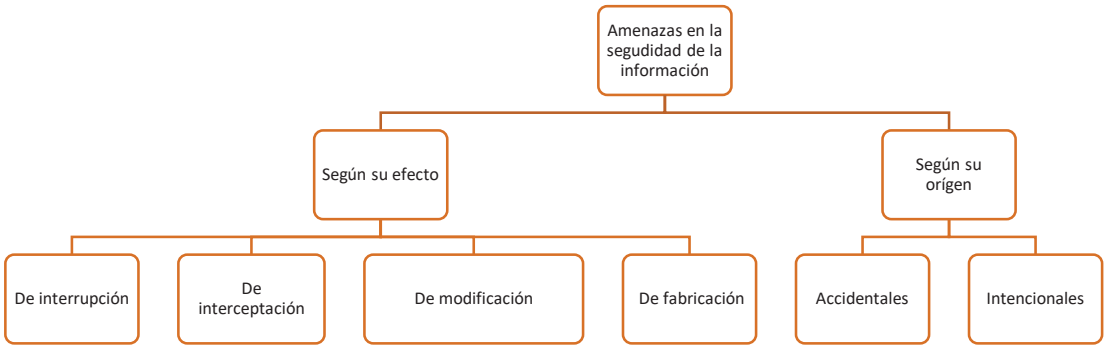


*Ilustración 2: Clasificación de las amenazas de la seguridad de información*

***FUENTE:*** *Realizado por Alberto Morán*

## VULNERABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN

Una vulnerabilidad no causa ningún daño por sí misma, pero provocan debilidades que pueden ser explotadas por una amenaza afectando algún activo de la entidad.

Es así como Bertolín, en su libro Seguridad de la información, describe a una vulnerabilidad como:

La potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo. Las vulnerabilidades asociadas a los activos incluyen las debilidades en el nivel físico sobre la organización, los procedimientos, el personal, la gestión, la administración, los equipos, el software o la información. (2008). Pág. 23.

- Clasificación de las vulnerabilidades.

Se pueden encontrar diferentes clasificaciones, de acuerdo al criterio de los autores, para este documento se ha tomado algunas de ellas y se las ha clasificado de tal manera que se muestra en la Figura 3.

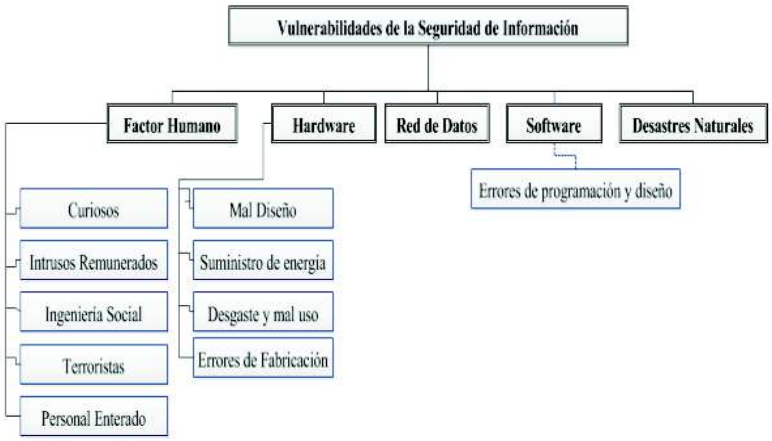


*Ilustración 3: Clasificación de las vulnerabilidades de la seguridad de información*

***FUENTE:*** *Realizada por Andrea Zura. Ibarra 2015*

## ATAQUES PRODUCIDOS EN LA SEGURIDAD DE LA INFORMACIÓN

Según Andrea Zura en su tesis “diseño del modelo de seguridad de defensa en profundidad en los niveles de usuario, red interna y red perimetral, aplicando políticas de seguridad en base a la norma iso/iec 27002 para la red de datos del Gad municipal de Otavalo”

Un ataque es la explotación de las vulnerabilidades encontradas en el diseño y configuración de un sistema dentro de una organización.

- Clasificación de los ataques.

Se pueden encontrar diferentes clasificaciones, de acuerdo al criterio de los autores, para este documento se ha tomado algunas de ellas y se las ha clasificado de tal manera que se muestra en la Figura 4.

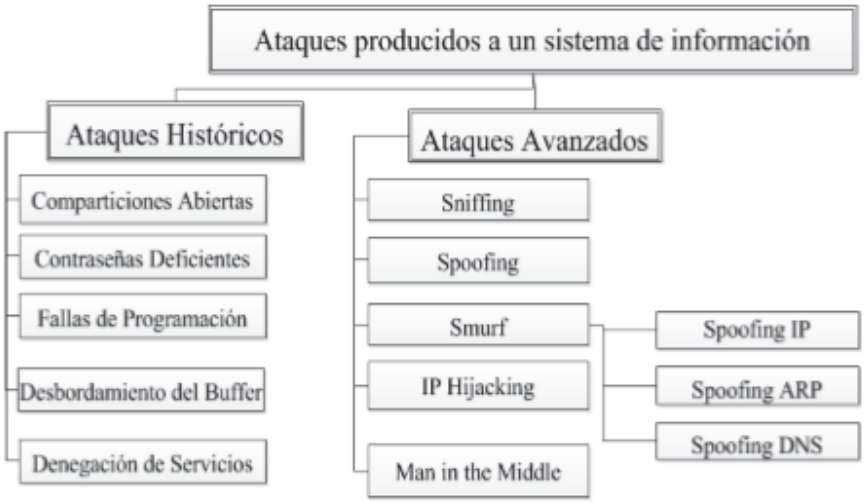


*Ilustración 4: Clasificación de los ataques producidos en la seguridad de información*

***FUENTE:*** *Realizada por Andrea Zura. Ibarra 2015*

## 1.2 ANTECEDENTES DE INVESTIGACIONES RELACIONADAS AL TEMA

## PROYECTOS A NIVEL INTERNACIONAL

**TEMA 1: ASEGURAMIENTO DE LOS SISTEMAS COMPUTACIONALES DE LA EMPRESA SITIOSDIMA.NET**

Este tema se presentó en el 2015 en la Universidad Nacional Abierta y a Distancia – UNAD, Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad Informática. BOGOTÁ D.C. – ZIPAQUIRÁ. Este proyecto consistía en implementar diferentes aplicaciones y técnicas que ayuden al aseguramiento de los sistemas operativos de la empresa sitiosdima.net. sus sistemas de información, redes de datos y la manipulación no apropiada de la información por parte de los usuarios. Y a lo largo del desarrollo del tema indica que asegurar un sistema requiere de muchas veces desactivar servicios, limitar características de software y bloquear

otras tantas que pueden ser fácilmente la puerta de entrada al sistema, de esta manera se está reduciendo en importante medida un gran número de vulnerabilidades. Y que cada organización tiene sus propias necesidades, con esto pretende dar a conocer de manera unificada las características de las diferentes aplicaciones que se convierten en herramientas fundamentales y de uso imperativo en el hardening de los sistemas informáticos (Firewall, Antivirus, IDS, Criptografía, usos de Sniffer, entre otros).

**TEMA 2: METODOLOGÍA DE ANÁLISIS DE VULNERABILIDADES PARA EMPRESAS DE MEDIA Y PEQUEÑA ESCALA**

Artículo presentado por la Pontificia Universidad Javeriana, Bogotá, Colombia. EL presente da una perspectiva global de un proceso de investigación sobre seguridad informática, específicamente en el aseguramiento de los recursos de la empresa, entre ellos, la disponibilidad de sus sistemas y recursos informáticos, la confidencialidad de los datos, y la integridad de toda la información de la empresa. Como resultado dieron a conocer pasos, que abarcan diferentes temas como lo son planeación, políticas de seguridad, aseguramiento de los recursos informáticos de la empresa. Todos estos apuntando a un mismo fin, el mejoramiento de la seguridad de la información y recursos tecnológicos, haciendo que un sistema permanezca cubierto y preparado ante eventualidades que puedan interrumpir el desarrollo normal de las actividades de la organización.

## PROYECTOS A NIVEL NACIONAL

**TEMA 1: DISEÑO DEL MODELO DE SEGURIDAD DE DEFENSA EN PROFUNDIDAD EN LOS NIVELES DE USUARIO, RED INTERNA Y RED PERIMETRAL, APLICANDO POLÍTICAS DE SEGURIDAD EN BASE A LA NORMA ISO/IEC 27002 PARA LA RED DE DATOS DEL GAD MUNICIPAL DE OTAVALO**

Este tema se presentó en el año 2015, en la Universidad Técnica del Norte, Ibarra, Ecuador. Para la obtención del Título de Ingeniería en Electrónica y Redes de Comunicación Ing. Andrea Yomaira Zura Chalá. Este

proyecto consiste en tener su infraestructura un alto grado de disponibilidad y calidad de servicios en sus distintos servicios de telecomunicaciones en beneficio de la población, que a su vez les permita poseer escalabilidad, flexibilidad y seguridad. A demás plante un diseño del modelo defensa de seguridad multicapas, conocido como defensa en profundidad; hace referencia al nivel de usuario, a nivel de red interna y a nivel perimetral.

Además, en el proyecto incluye que, mediante un presupuesto referencial demostró que es posible migrar de una solución propietaria a una solución bajo software libre; lo que permite minimizar costos y aprovechar mejor los recursos.

**TEMA 2: ASEGURAMIENTO DEL ENTORNO INFORMÁTICO EN LA DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUEZ-BIBLIAN-DÉLEG-EDUCACIÓN**

Este tema se presentó en el año 2015 en la Universidad Superior Politécnica del Litoral, Guayaquil, Ecuador. Para la obtención de Master en Seguridad Informática Aplicada Ing. Diego Esteban Izquierdo Coronel. En su proyecto nos dice que la tecnología cumple un papel importante, una de las herramientas que han revolucionado el manejo de la información, es el avance acelerado de la informática, a la par van aumentado las amenazas, vulnerabilidades y peligros. Tanto a nivel de Software como Hardware.

Empieza realizando un análisis situacional de la empresa. La auditoría en una institución en la que el desarrollo y avance depende, como factor primordial la eficiente administración de la información y del adecuado uso de la tecnología de información, en la que los sistemas de gestión han alcanzado un desarrollo tan notable, demanda la introducción muy diferente a la que fuera para esta disciplina durante su utilización.

## 1.3 DEFINICIONES CONCEPTUALES

### DEFENSA EN PROFUNDIDAD

En lo que respecta a seguridad de la información en redes corporativas, existe un concepto de mucha utilidad para todos los que están involucrados en áreas de TI, denominado defensa en profundidad (conocido como Defense in Depth). Se trata de un modelo que busca y pretende aplicar controles de seguridad para proteger los datos en diferentes capas.

Sebastián Bortnik, Analista de Seguridad afirma que

La idea de este modelo es muy sencilla: si es posible proteger a un activo de la organización con más de una medida de seguridad, hágalo. El objetivo del modelo también es claro: para que un atacante llegue a un dato o información, debe poder vulnerar más de una medida de seguridad.

En términos informáticos, este modelo propone la creación de capas de defensa con el objetivo de evitar ataques directos a la información sensible de un entorno corporativo y a la disponibilidad de los sistemas informáticos. Además, con este modelo se consigue mayor tiempo para defenderse y tomar medidas para detener cualquier anomalía que se presente y, que afecte a la disponibilidad, integridad y confidencialidad a la empresa, y utilizar planes de actuación y mayor probabilidad en detección de un ataque. (Carlos Álvarez Martín y Pablo Gonzales Pérez, Hardening de Servidores GNU/Linux).


*Ilustración 5: Esquema del modelo defense in depth o defensa en profundidad*

***Fuente:*** *Hardening de servidores GNU/Linux, Pág. 17*

## PROCEDIMIENTOS, CONCIENCIACIÓN Y POLÍTICAS

### PROCEDIMIENTOS

Los procedimientos son la mejor manera de llevar a cabo tareas rutinarias. En el ámbito informático y de seguridad es exactamente igual, es imprescindible automatizar y poder enumerar los pasos a seguir ante circunstancias que puedan ocurrir en cualquier momento de producción de la empresa. Es por ello la creación de procedimientos para la resolución de problemas o incidentes de seguridad es necesario en cada organización. (Carlos Álvarez Martín y Pablo Gonzales Pérez, Hardening de Servidores GNU/Linux).

La información y los procesos que la apoyan, los sistemas y las redes, son bienes importantes en las organizaciones, por lo que requieren ser protegidos convenientemente frente a amenazas que pongan en peligro la disponibilidad, la integridad, la confidencialidad de la información, la estabilidad de los procesos, los niveles de competitividad, la imagen

corporativa, la rentabilidad y la legalidad, aspectos necesarios para alcanzar los objetivos de la organización.

La información generalmente es procesada, intercambiada entre partes y posteriormente pasa a ser conservada en la red de datos, servidor y soportes de almacenamiento, que son parte de lo que se conoce como sistemas informáticos. Los sistemas informáticos están sometidos a continuas y potenciales amenazas, que generalmente son originadas dentro de la organización, como desde fuera del alcance de la red o perímetro de la empresa.

Es posible disminuir el nivel de riesgo significativo y con ello la materialización de las amenazas y la reducción del impacto sin necesidad de realizar elevadas inversiones ni contar con una gran estructura de personal. Para ello se hace necesario conocer y gestionar de manera ordenada los riesgos a los que está sometido el sistema informático, considerar los procedimientos adecuados enmarcados explícitamente y previamente planificados e implantar los controles de seguridad que correspondan. (Metodología para la Gestión de la Seguridad de la Información).

**CONCIENCIACIÓN**

“Ningún intruso volverá a tener acceso a mis datos, he seleccionado el password más seguro: Shadowfas…Oh no! Lo dije en voz alta”, Phillip Sutcliffe, Actuario.

Las personas son el elemento de falla más común en un sistema de seguridad. La falta de conciencia en los requerimientos de seguridad y las necesidades de control por parte de los administradores de sistemas, programadores y usuarios puede representar el riesgo más importante para la organización.

Los atacantes e intrusos pueden hacer uso de técnicas de ingeniería social y aprovecharse de la falta de conciencia de usuarios y operadores, con

el fin de obtener información confidencial. En organizaciones donde no se ha implementado campañas de o programas de concienciación, es común encontrar contraseñas escritos en papel de notas, debajo de los teclados, respaldos de información incompletos, errores de configuración de equipos, entre otros. (Secure Informations Technologies)

La concienciación es algo necesario para los empleados, técnicos o no, no ven peligros en el uso de cierta información o ciertos sistemas. Es por ello, que nacen medidas como el mínimo de privilegios posible, para contrarrestar el efecto negativo que pueden suponer las acciones de ciertos usuarios en algunos sistemas. (Carlos Álvarez Martín y Pablo Gonzales Pérez, Hardening de Servidores GNU/Linux).

**SEGURIDAD FÍSICA**

En el Libro de Hardening de servidores GNU/Linux, por Carlos Álvarez Martín y Pablo Gonzales Pérez, se refiere a la seguridad física como:

Este eslabón del modelo de defensa en profundidad se puede entender dos aspectos muy distintos. En primer lugar, se puede visualizar la seguridad física como el procedimiento mediante el uso de cámaras, guardias de seguridad, CPDs aislados y asegurados que protegen las distintas capas o el acceso a los servidores. En segundo lugar, la seguridad o protección física se podría entender como los mecanismos que son utilizados para asegurar los sistemas o la información del acceso físico a un medio digital por parte de un usuario.

Hay que recalcar que cuando un usuario dispone de acceso físico a un servidor o equipo, es la mayoría de los casos, será difícil evitar que pueda utilizar el sistema para realizar tareas de dudosa moral. Para tratar de contrarrestar esta acción es importante asegurar el inicio del sistema operativo del servidor para que el usuario no tenga acceso a la información

sino está autorizado, de esta manera se trata de proteger la información sensible mediante el uso del cifrado.

**SEGURIDAD DEL PERÍMETRO**

Alejandro Ramos Fraile (SIA company), define como

Arquitectura y elementos de red que proveen de seguridad al perímetro de una red interna frente a otra que generalmente es Internet.

- Cortafuegos.
- Sistema de Detección Y Prevención de Intrusos
- Pasarela antivirus y antispam.
- Honeypots

En el Libro de Hardening de servidores GNU/Linux, por Carlos Álvarez Martín y Pablo Gonzales Pérez, se refiere a seguridad perimetral como:

El perímetro es una de esas barreras dedicadas a proteger el entorno o capa interna de la empresa. Es el paso previo a la red interna, y es una capa que debe estar correctamente configurada y conocer profundamente.

El firewall es el mayor representante en esta capa de seguridad. Representa un mecanismo de defensa inicial y que está compuesto por reglas. Es por ello, que el conocimiento es necesario para una correcta configuración de dichos dispositivos.

*Ilustración 6: Seguridad perimetral*

*FUENTE: Multicomp*

## SEGURIDAD EN LA RED INTERNA

En el Libro de Hardening de servidores GNU/Linux, por Carlos Álvarez Martín y Pablo Gonzales Pérez, estudian a la seguridad en la red interna como:

La segmentación de redes, las virtual local network o VLAN y los IDS o Intrusión Detection System. Se debe realizar la segmentación para separar las redes en función de los usuarios que quieran acceder y, en función, de los recursos que se requieran.

En el libro de Ataques a redes de datos IPv4 e IPv6, por Juan Luis García Rambla, se refiere a la red interna como:

Las redes de datos constituyen hoy el núcleo fundamental de operaciones en las organizaciones, todo pasa por ellas. Las redes de datos hoy en día se han convertido en algo tan indispensable que un fallo en las comunicaciones puede suponer un parón significativo en la funcionalidad de una organización.

En un entorno de red debe asegurarse la privacidad de los datos sensibles. No sólo es importante asegurar la información sensible, sino

también, proteger las operaciones de la red de daños no intencionados o deliberados.

El mantenimiento de la seguridad de la red requiere un equilibrio entre facilitar un acceso fácil a los datos por parte de los usuarios autorizados y restringir el acceso a los datos por parte de los no autorizados. Es responsabilidad del administrador crear este equilibrio.

Incluso en redes que controlan datos sensibles y financieros, la seguridad a veces se considera medida tardía. Las cuatro amenazas principales que afectan a la seguridad de los datos en una red son:

- Acceso no autorizado.
- Soborno electrónico
- Robo.
- Daño intencionado o no intencionado.

La seguridad de los datos no siempre se implementa de forma apropiada, precisamente por la seriedad de estas amenazas. La tarea del administrador es asegurar que la red se mantenga fiable y segura. En definitiva, libre de estas amenazas. (Denisse Romero, 2012)

**SEGURIDAD A NIVEL DE SERVIDOR**

En el Libro de Hardening de servidores GNU/Linux, por Carlos Álvarez Martín y Pablo Gonzales Pérez, estudian a la seguridad a nivel de servidor como:

La seguridad a nivel de servidor puede ser entendida de distintas maneras, sin llegar a interceptar a la seguridad del nivel de aplicación. En esta capa se puede tener en cuenta las actualizaciones del sistema operativo

servidor que da soporte y gestiona las aplicaciones y servicios que se ejecutan en dicha máquina.

Uno de los objetivos de la defensa en profundidad en la capa del servidor es dejar a este en Zero Day Server. En otras palabras, este estado proporciona a la empresa y al administrador un sistema con el menor porcentaje de vulnerabilidades conocidas. Este es el máximo nivel de seguridad que se puede alcanzar con el software que se ejecuta en el servidor.

El Hardening es el fortalecimiento o endurecimiento de un sistema, es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades. Un sistema tiene mayor vulnerabilidad cuando más funciones o servicios brinda. (Sergio Culoccioni, septiembre 2015)

Hardening (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, entre otros; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso. (Paul Castro - Grupo Smartekh, 2012).

**SEGURIDAD EN LA APLICACIÓN**

La seguridad a nivel de aplicación es un punto importante que considerar, si las capas que soportan a esta están bien cubiertas. Generalmente se dispone de varias aplicaciones o servicios que pueden tratar con la parte pública a través de la red, y la exposición de esta debe ser controlada y segura. (Carlos Álvarez Martín y Pablo Gonzales Pérez)

La fortificación de aplicativos o servicios mediante políticas de máxima restricción es deseable en los sistemas. Los servicios deben ser lo más restrictivos posible para proporcionar un ambiente seguro de interacción con el usuario y favorecer la impresión de seguridad en la organización.

**SEGURIDAD A NIVEL DE LA INFORMACIÓN**

Irwin Valera Romero afirma que la

Seguridad de los sistemas de información consiste en la protección de los sistemas de información respecto al acceso no autorizados o modificación de la información en el almacenamiento, proceso y tránsito y contra la denegación de servicios para los usuarios autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y contrarrestar dichas amenazas.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

## 1.4 CONCLUSIONES RELACIONADAS AL MARCO TEÓRICO EN REFERENCIA AL TEMA DE INVESTIGACIÓN

Analizando y examinando cada parte del marco teórico el cual me hace referencia y fundamenta la terminología necesaria para el desarrollo del proyecto he llegado a las siguientes conclusiones.

- Es de gran importancia conocer y relacionarse con casa uno de los términos y procesos que están vinculados al aseguramiento de redes y sistemas informáticos e información. Teniendo en cuenta, que, en entornos corporativos donde el manejo de información es alto y confidencial, se debe tener en cuenta los peligros a los que la empresa se encuentra expuesta.

- El modelo de defensa en profundidad da un amplio flujo de trabajo en el aseguramiento por niveles, los cuales ayudan a la protección de

activos informáticos. Así mismo ayuda a mantener la disponibilidad, integridad y confidencialidad de los datos importantes para la organización.

- Así también para el fortalecimiento de medidas de seguridad a la organización y sus sistemas informáticos sería la aplicación de políticas adecuadas de seguridad y actualización de sistemas. Las políticas y medidas deben ser consensuadas y llevarlas a cabo cuando la seguridad de la empresa se encuentre comprometida.

- Como parte de la investigación realizada se revisó proyectos relacionados y referenciados a la temática de la tesis, lo que permitió conocer funcionalidades, protocolos, características y beneficios de uso de tecnologías libres para el aseguramiento de los sistemas informáticos.

# CAPÍTULO II

# 2. DIAGNÓSTICO

## 2.1 INTRODUCCIÓN

La presente investigación, permitirá mediante un procedimiento técnico, analítico y sistémico, conocer la actual situación de la seguridad de la información de la empresa ALLCOMPU, enmarcada en el uso de políticas y mecanismos para precautelar la disponibilidad, integridad y confidencialidad de la información de la misma. Este diagnóstico se obtiene por medio de un proceso de recolección y análisis de la información recolectada en la investigación de campo.

Los medios o fuentes que se necesitan para hacer una investigación son las fuentes primarias y secundarias, los datos primarios que contendrán información recopilada en la investigación sintética que se hará en la empresa a través de encuesta e investigaciones documentales de tesis, libros, archivos, etc.

De lo anterior se puede decir que la investigación es un procedimiento para llegar a un análisis de la situación actual de cómo las Pymes están aplicando el uso de políticas y procedimientos para el aseguramiento de sus redes de computadoras y sistemas informáticos, siendo directamente proporcional a la disponibilidad, integridad y confidencialidad de la información que la misma maneja, el grado de conocimiento y cultura sobre el tema que tienen los trabajadores.

La fuente de información primaria, pertenece a la empresa ALLCOMPU y es la que brindó la información y permitió realizar la investigación del presente proyecto integrador.

## 2.2 TIPOS DE INVESTIGACIÓN

#### 2.2.1.1.1 INVESTIGACIÓN EXPLORATORIA

La investigación explorativa ofrece una visión genérica de la información adquirida; puesto que, al adquirir información y posterior analizarla se determinan factores relevantes que ayudan a identificar los problemas en la empresa ALLCOMPU, realizando una investigación de manera general para dar una solución viable, mediante el uso de tecnologías libres óptimas.

#### 2.2.1.1.2 INVESTIGACIÓN DESCRIPTIVA

La investigación descriptiva, nos permite determinar o dimensionar los problemas presentados por la empresa, la manera que se llevan a cabo los procesos para que esta funcione, la forma como se conectan a la red tanto los colaboradores como los clientes. Todo este método de investigación ayudará a obtener un resultado con el fin de mejorar la estructura organización de la empresa en cuanto a seguridad y conectividad a sus redes de datos.

## 2.3 MÉTODOS DE INVESTIGACIÓN

### 2.3.1 MÉTODO DE INDUCTIVO

A través de este método científico se observaron los hechos, aplicando entrevistas que permitieron obtener datos que orientaran la ejecución del proyecto, así como el estudio del caso en particular para dar una solución eficaz para el aseguramiento de sistemas y redes de la empresa ALLCOMPU.

## 2.4 HERRAMIENTAS DE RECOLECCIÓN DE DATOS

Para realiza el proceso de recolección de datos en la empresa ALLCOMPU, se utilizaron dos técnicas muy efectivas, como son; la entrevista, la misma que fue aplicada a los jefes y directivos de la empresa y la observación que se la realizada in situ para conocer los procesos y mecanismos de ingreso y control a la red.

## 2.5 FUENTES DE INFORMACIÓN DE DATOS

### 2.5.1 Fuentes primarias

Para la implementación de este proyecto se obtuvo información, a través de las diferentes herramientas de recolección de datos aplicadas al personal técnico y administrativo de la empresa, logrando identificar las falencias que se tienen y llegando a la conclusión de las medidas necesarias que se deben tomar a partir de la identificación, y sustentando la solución a la misma. La cual en mutuo acuerdo entre las partes, la empresa se compromete a dar todo el apoyo correspondiente para la implementación de estas medidas de seguridad, con el fin de precautelar la integridad, disponibilidad y autenticidad de su información.

### 2.5.2 Fuentes secundarias

Se obtuvo información relaciona al caso mediante algunas publicaciones en la web, artículos que se relacionan de alguna manera con la problemática que se presenta en la empresa.

## 2.6 INSTRUMENTAL OPERACIONAL

### 2.6.1 Estructura y características de los instrumentos de recolección de datos

#### 2.6.1.1 Entrevistas

Las entrevistas fueron aplicadas a los directivos de la empresa ALLOMPU, tales como la Gerente General Ing. Andrea Ramírez y al Gerente Técnico Ing. Cristhian Puya. Así mismo se entrevistó a personal del departamento técnico y administrativo. (Ver Anexo 2)

Mediante las entrevistas obtendremos datos relevantes que permitirán determinar el estado actual en que se encuentra la empresa.

#### 2.6.1.2 Observación

Se realizó observaciones en las oficinas de la empresa lo que permitió obtener detalles y por menores de la situación actual de la misma, donde se pudo verificar que efectivamente, una vez conectado a la red wifi de la empresa se puede tener acceso a recursos compartidos, donde se había información importante y relevante para la empresa.

## 2.7 PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

El proceso de recolección de datos se lo realizó utilizando la entrevista a directivos y colaboradores de la empresa, técnicos como administrativos, los cuales coinciden en sus apreciaciones.

Sobre el modelo denominado Defensa en Profundidad, los directivos, técnicos y empleados entrevistados manifestaron no conocer nada al respecto sobre el modelo defensa en profundidad para la gestión de la seguridad de la información.

En la empresa ALLCOMPU no utilizan ningún tipo de sistema de protección a la red y por ende a los sistemas informáticos.

Es necesario la implementación de herramientas open source que ayuden y minimicen los riesgos de perdida de información, y, que a su vez permitan la disponibilidad de la misma.

Los directivos al ser entrevistados recomiendan que se deben implementar políticas y procedimientos para la seguridad de la información de la empresa y para mantener el control de los activos informáticos y medios de conexión.

Los entrevistados recomiendan la implementación de cortafuego (firewall) para el control de acceso a la red y los sistemas de la empresa, herramientas que criptográficas y aplicativos que ayuden a la protección de la información y los sistemas.

Definitivamente todos coincidieron en que la red de la empresa presenta vulnerabilidades, así como también sus sistemas informáticos por lo que se requiere a la brevedad posible implementar técnicas de seguridad para evitar el acceso de intrusos.

Los entrevistados consideran revisar la manera y la seguridad de conexión a la red mediante dispositivos inalámbricos. Coinciden en que se requiere de monitorear los accesos y restringir quienes son los que deben conectarse y el consumo de ancho de banda. Utilizar contraseñas más fuertes y utilizar mecanismo de conexión más seguros como el modo de seguridad y el cifrado de la contraseña

Los entrevistados concuerdan en que el sistema de como comparten los archivos es inseguro por lo cual no hay ninguna política que restringa o controle el acceso a este sistema y la forma en que se comparten los archivos entre los colaboradores; por lo cual es necesario la implementación del sistema de compartición de información, estableciendo políticas y restricciones de quien debe o no poder acceder a la información y de que tipo.

Todos coinciden que se presentan problemas de a nivel de red por el tráfico que se genera por los diferentes sistemas que se ejecutan para el funcionamiento de la empresa; por lo cual una correcta separación de trafico de red es lo óptimo para el desempeño de la empresa.

### 2.7.1 Informe final del análisis de los resultados

Analizada toda la información obtenida mediante el uso de las entrevistas con los colaboradores de la empresa, se puede concluir que:

- El resultado de las entrevistas indica que, la implementación del modelo defensa en profundidad, brindará un grado de seguridad alto a la empresa, yo que indica de forma directa que apunta a la disponibilidad, integridad y autenticidad de los sistemas informáticos y las redes.

- Se necesitan de políticas y concientización que ayuden y promuevan el buen uso de la información y que apunten a mantener un registro de las actividades que se realizan con la misma.

- Así mismo, la segmentación de la red en relación a los servicios que se ejecutan ayudará directamente a la disponibilidad de los sistemas y el flujo de tráfico de datos sin pérdida de los mismos.

# CAPITULO III

# 3. DISEÑO DE LA PROPUESTA

## 3.1 INTRODUCCIÓN

El aseguramiento de la red y sistemas informáticos de la empresa ALLCOMPU, requiere de la implementación de un modelo denominado "defensa en profundidad", cuyas herramientas ofrecen una gran flexibilidad en el momento de configurarlas.

En este capítulo se describirán todo el proceso de implementación del modelo defensa en profundidad. Se considerarán todos los equipos tecnológicos con los que cuenta la empresa ALLCOMPU que permitan implementar las herramientas adecuadas para el correcto funcionamiento del modelo.

## 3.2 DESCRIPCIÓN DE LA PROPUESTA

El proyecto a implementar está orientado a salvaguardar activos informáticos de la empresa ALLCOMPU, mediante aplicación del modelo *Defensa en Profundidad,* el mismo que se basa en técnicas de aplicabilidad de herramientas que reducen el riesgo significativo a las vulnerabilidades. Este modelo y sus herramientas se implementarán en el sistema operativo base Debian 9.2 Strecth, el cual estará alojado en un servidor HP ProLiant ML150G6. Como complemento del modelo se utilizará un Switch CISCO Catalys WS-C3750X-48P-S que ayudará a complementar las técnicas y el modelo en general.

Mediante la aplicación del modelo defensa en profundidad, permitirá llevar a cabo, mediante sus etapas que lo involucra de manera eficiente y flexible, lo que ayuda a la productividad de la empresa teniendo en cuenta el alto grado de seguridad que aporta a la información de la empresa ALLCOMPU.

Se vera la implementación de todas las etapas del modelo, empezando por la capa física, donde nos centraremos en asegurar el servidor desde el momento en que arranca o en el omento que este una persona no autorizada frente a él y quisiera alterar el funcionamiento. En la siguiente etapa, sobre seguridad perimetral implementaremos el firewall que permitirá o negará el tráfico que entra o sale del servidor hacia la red interna o hacia la internet, la etapa de aseguramiento a la red interna, se asegurará mediante la segmentación de red como lo son las vlans. La seguridad a nivel de servidor, veremos lo accesos remotos hacia el mismo, asegurando de que solo los usuarios autorizados puedan acceder, lo siguiente es asegurara las diferentes aplicaciones o sistemas de trabajo colaborativo en la empresa. Finalizando con el aseguramiento de la información, mediante el cifrado de la misma.

**REQUERIMIENTOS**

Para la implementación de este proyecto, la empresa ALLCOMPU apoyará con el equipamiento necesario para ejecutar el modelo defensa en profundidad, que minimizara los riesgos que pueden afectar la disponibilidad de la información y de los sistemas que la empresa utiliza.

A continuación, los equipos informáticos necesarios para la implementación del modelo y otros equipos ya existentes los cuales formaran parte del aseguramiento.

| TIPO | MARCA | MODELO | DESCRIPCIÓN | COSTO |
|---|---|---|---|---|
| Servidor | Hewlett-Packard | Proliant ML150G6 | | $1.200,00 |
| Switch | Cisco | Catalys WS-C3750X-48P-S | Utilizado para segmentación de la red | $1.100,00 |

| | | | | |
|---|---|---|---|---|
| DVR | Dahua | | Grabador de cámaras de seguridad | $80.00 |
| Central Telefónica | ZYCOO | | VoIP | $320,00 |
| Telefonos | GrandStream | GXP1615 | Extensiones telefónicas para los usuarios | $65,00 |
| Router | Tenda | | Conectividad inalámbrica | $50,00 |

*Tabla 1: Equipos a utilizar*

A continuación, algunas de las herramientas a utilizar en la implementación.

| NOMBRE | VERSION | SERVICIO | DESCRIPCIÓN |
|---|---|---|---|
| Debian GNU/Linux | 9.2 Stretch | | Sistema Operativo donde se implementará el modelo |
| GRUB | 2 | Gestor de Arranque | |
| LUKS, Cryptsetup | 2.0.0 | Cifrado de particiones | |
| GnuPG | 2.2.3 | Cifrado de Ficheros | |

| | | | |
|---|---|---|---|
| Iptables | 1.6.0 | Firewall | Filtrado de paquetes y ruteo |
| Isc-dhcpd | 4.3.5 | DHCP | |
| OpenSSH | 7.4 | SSH | Acceso remoto al servidor |
| Fail2ban | 0.9.4 | Fail2ban | |
| Samba | 4.5.12 | Samba | Sistema de archivos, compartición |
| MariaDB | 10.2.10 | MariaDB | Base de datos |

*Tabla 2: Herramientas a utilizar*

La segmentación de la red por VLANs es muy importante para el aseguramiento de los sistemas informáticos que maneja la empresa, por tal motivo se ha segmentado la red por el tipo de servicio que se ejecutan dentro de la misma.

| NOMBRE | VLAN ID | RED | MASCARA |
|---|---|---|---|
| Administrativo | 30 | 192.168.30.0 | 255.255.255.240 |
| Departamento Técnico | 40 | 192.168.40.0 | 255.255.255.224 |
| Telefonía IP | 10 | 192.168.10.0 | 255.255.255.240 |
| CCTV | 20 | 192.168.20.0 | 255.255.255.252 |
| WIFI | 50 | 192.168.50.0 | 255.255.255.252 |

*Tabla 3: Segmentación de rede por VLAN*

## 3.3 MODELO DEFENSA EN PROFUNDIDAD

Modelo que busca y pretende aplicar controles de seguridad para proteger los datos en diferentes capas. Este modelo propone la creación de capas de defensa, con el objetivo de evitar ataques directos a la información sensible de un entorno corporativo y a la disponibilidad de los sistemas informáticos.

**Estado de la situación actual**

En el análisis de la situación actual observamos que la red de la empresa ALLCOMPU es plana, es decir todos los equipos que están conectada a la misma forman parte de la misma red, por lo cual los sistemas que utiliza la empresa para compartir información entre colaboradores quedan comprometida la confidencialidad y la integridad de la misma. Podemos revisar que la conexión inalámbrica que suele ser utilizada para los clientes y los mismos colaboradores tiene acceso a ella, por lo cual conectándose pasan a formar parte de la red corporativa, tienen acceso a los sistemas y recursos compartidos.

Para la implementación de este modelo defensa en profundidad se hará bajo las siguientes fases:


*Ilustración 7: Modelo Defensa en Profundidad*

## 3.4 FASE DE PLANIFICACIÓN

### 3.4.1 Estimación del proyecto

| ACTIVIDADES | JULIO | | | | AGOSTO | | | | SEPTIEMBRE | | | | OCTUBRE | | | | NOVIEMBRE | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | HORAS DE TRABAJO |
| Presentación de la propuesta | X | | | | | | | | | | | | | | | | | | | | 10 |
| **Fase de exploración** | X | X | | | | | | | | | | | | | | | | | | | **90** |
| Observación de la situación actual | X | X | | | | | | | | | | | | | | | | | | | 30 |
| Recolección de información | | | X | X | | | | | | | | | | | | | | | | | 60 |
| **Fase de planificación** | | | | X | X | X | X | | | | | | | | | | | | | | **65** |
| Estimación de tiempo | | | | X | X | | | | | | | | | | | | | | | | 35 |
| Prioridades del proyecto | | | | | | X | X | | | | | | | | | | | | | | 30 |
| **Fases de implementación** | | | | | | | | X | X | X | X | X | X | X | X | X | X | X | X | X | **173** |
| Levantamiento de Debian GNU/Linux | | | | | | | | X | | | | | | | | | | | | | 8 |
| Procedimientos, politicas. | | | | | | | | | X | X | | | | | | | | | | | 30 |
| Seguridad Fisica | | | | | | | | | | | X | X | | | | | | | | | 25 |
| Seguridad Perimetral | | | | | | | | | | | | X | | | | | | | | | 15 |
| Seguridad a la red interna | | | | | | | | | | | | | X | | | | | | | | 35 |
| Segudidad a nivel de servidor | | | | | | | | | | | | | | X | | | | | | | 20 |
| Segudirad a nivel de aplicación | | | | | | | | | | | | | | X | X | | | | | | 30 |
| Seguridad a nivel de información | | | | | | | | | | | | | | | X | | | | | | 10 |
| **Fase de pruebas** | | | | | | | | | | | | | | | | X | X | X | X | X | **40** |
| Capacitación | | | | | | | | | | | | | | | | X | | | | | 15 |

| | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Seguimiento y monitoreo | | | | | | | | | | | | | | | | | | X | X | | | 25 |
| TOTAL, DE HORAS: | | | | | | | | | | | | | | | | | | | | | | **378** |

*Tabla 4: Cronograma de actividades*

## 3.5 IMPLEMENTACIÓN DEL MODELO DEFENSA EN PROFUNDIDAD

### 3.5.1 PROCEDIMIENTOS, CONCIENCIACIÓN Y POLÍTICAS

En esta fase se deben implementar procedimientos para la resolución de problemas o incidentes de seguridad de la empresa. La información, los sistemas y las redes informáticas son activos importantes por lo que requieren ser protegidos de manera conveniente, frente a una serie de amenazas que ponga en peligro la disponibilidad, integridad, confidencialidad, la estabilidad de los procesos, etc., de la organización.

Otro de los aspectos que hay que considerar en esta fase es la concienciación del personal técnico y administrativos, para el éxito de las políticas que se implementen.

En la empresa ALLCOMPU se implementaron las siguientes políticas:

**Políticas de seguridad de la información**

**Protección de información**

**Política:** Para el uso y mantenimiento adecuado de la información, teniendo en cuenta que es un activo de la empresa, para garantizar su integridad y confidencialidad se proceden a generar las siguientes políticas.

Aplicables a: Todos

**A. Coordinación de la seguridad de la información**

**Política:** El Departamento Técnico será el encargado, de la coordinación y el seguimiento de los procedimientos y políticas

implementadas de llevar un registro, para luego establecer los lineamientos que sean necesarios ser adecuados para que ayuden en función de mejorar la productividad y eficiencia en la empresa.

Responsable: Departamento Técnico

**B. Revisión de la política de seguridad de la información**

**Política:** El Departamento Técnico realizará seguimiento continuo de las políticas establecidas, con el fin de detectar nuevos requerimientos y necesidades; tanto en seguridad de hardware como software.

Responsable: Jefe de Departamento Técnico

**C. Proceso de autorización para nuevos medios de almacenamiento de información**

**Política:** El Departamento Técnico será el encargado de determinar los medios para almacenamiento de información y su respectiva colocación para que forme parte de la red con sus debidos permisos, bajo resguardo y responsable debe encontrarse.

Responsable: Departamento Técnico

**D. Procesos de Acuerdos de confidencialidad**

**Política:** El departamento técnico en conjunto con el administrativo deben ser los encargados de realizar actas de compromiso de confidencialidad, y uso responsable

Responsable: Todos

### E. Proceso de manejo de información y uso

**Política:** Los directivos serán los encargados de establecer el buen manejo de la información y su respectivo uso que se manejarán y darán proceso a la información. Así como las sanciones en caso de incumplimiento.

Responsable: Administrativos

### F. Proceso de intercambio de información

**Política:** Cada uno de los colaboradores son responsables directos de los activos de la información que manejan, de ser necesario el intercambio, serán los responsables de su uso, caso contrario será el Gerente Técnico quien determine responsabilidades en base a investigaciones.

Responsable: Todos

### G. Eliminación de derechos de acceso

**Política:** El departamento técnico será el encargado de ejecutar las restricciones necesarias, para evitar el acceso a la información en caso de que se termine el contrato con algún colaborador.

Responsable: Departamento Técnico

### H. Control contra software malicioso

**Política:** El Departamento Técnico se encargará de mantener las bases de datos de los antivirus actualizadas y dar mantenimiento periódicamente.

Responsable: Departamento Técnico

### I. Control contra dispositivos móviles

**Política:** El Departamento Técnico será el encargado de la seguridad de la red inalámbrica permitiendo o denegando a dispositivos que deben o no conectarse a la red.

Responsable: Departamento Técnico

**Control de accesos a la información y sistemas**

### J. Administración de accesos de los usuarios

**Política:** La administración de los activos de la información será registrada por el Departamento Técnico. Delimitando el acceso y permisos según la necesidad del usuario.

Responsable: Departamento Técnico

### K. Registro de usuarios

**Política:** El Departamento Técnico tendrá registrado todos los usuarios del sistema

Responsable: Departamento Técnico

### L. Gestión de privilegios

**Política:** El departamento técnico en base a disposiciones del Gerente Técnico dará los privilegios y servicios de información.

Responsable: Jefe Departamento Técnico

**M. Administración de controles de acceso a la red**

**Política:** El acceso a la red será determinado por el departamento técnico, quienes serán los encargados de dar los privilegios a los usuarios.

Responsable: Departamento Técnico

**N. Administración de contraseñas**

**Política:** Respecto a las contraseñas, cada usuario tendrá la facultad de establecer su propia contraseña, cumpliendo con las medidas de seguridad establecidas por departamento técnico (debe tener mínimo 8 caracteres, obligados a mayúsculas, minúsculas, números y símbolos alfa numéricos) quienes tendrán su registro, y con periodo de duración a cambio cada 6 meses.

Responsable: Todos

**O. Identificación del equipo en red**

**Política:** El departamento técnico será el encargado de ingresar cada dispositivo a la red, asignando direcciones IP para ser reconocido en el área que se coloque.

Responsable: Departamento Técnico

### 3.5.2 SEGURIDAD FÍSICA

La seguridad física de los sistemas informáticos engloba los mecanismos – generalmente prevención y detección - destinados a proteger físicamente a cualquier recurso del sistema.

En este punto se tratará una serie de técnicas para tratar de mitigará o al menos retrasar el acceso al servidor principal de la empresa estando físicamente en el emplazamiento del mismo.

#### A.- BIOS / UEFI

Lo primero que se debe hacer en el servidor una vez que se configura y forma parte de un entorno de producción, consiste en fortalecer la configuración básica del BIOS (Basic Input/Output System), o su reciente sustitución y modernización para sistemas con hardware moderno UEFI (Firmware Extensible Unificada, Unified Extensible Firmware Interface).

La fortificación en esta capa es un punto muy relativo y depende del fabricante del hardware, aunque mayoritariamente estos sistemas se manejan entre sí.

Los puntos que vamos a reforzar o fortificar en el entorno de aseguramiento de redes y sistemas informáticos de la empresa ALLCOMPU, obviamente sin dejar a un lado aquellas soluciones específicas de cada fabricante o modelo de hardware.

- Edición de opciones protegida por contraseña
- Deshabilitar la selección de medios de arranque
- Deshabilitar, si fuera posible, los siguientes medios de arranque:

- Cualquier medio de tipo extraíble del servidor. Por ejemplo, los dispositivos USB (Universal Serial Bus)
- Arranque desde todas las tarjetas de red del servidor usando sistemas PXE (Entorno de ejecución de pre arranque)

Si el atacante tuviese tener acceso al servidor físicamente, con la implementación de esta capa física ya tendría una barrera para tener acceso a los sistemas que el servidor aloja, ya que previamente deshabilitamos los posibles periféricos externos de arranque

## B.- GESTOR DE ARRANQUE GRUB Y GRUB2

Cuando se arranca el sistema operativo (Debian GNU/Linux v9) y aparece el gestor de arranque en su versión más reciente GRUB2, se sabe de antemano, que se tiene la posibilidad muy probable de saltar las credenciales del servidor. Como consecuencia de ello, disponer de acceso a la visualización de la información sensible de la empresa, y extraerlos a una unidad de almacenamiento externo, dicha extracción puede darse en soportes físicos insertados localmente (es por ello la importancia de aplicar la capa física del modelo ya que permite mitigar este tipo de eventualidades.) o bien volcándolos a servidores remotos haciendo uso de herramientas y comandos como SCP o FTP por ejemplo.

### Impacto de un gestor de arranque no protegido

Cuando no se tiene protegido el arranque del sistema operativos, y teniendo acceso al servidor físicamente, teniendo un teclado y un monitor, se puede realizar las siguientes acciones independientemente la versión del GRUB.

- Ejecución de comandos GNU/Linux

- Acceso a una Shell como root
- Arranque de un sistema editando las líneas de configuración.

En el caso de GRUB2, al momento de iniciar el servidor aparece una pantalla como la siguiente donde a priori solo es necesario para seleccionar que sistema operativo y/o kernel se desea ejecutar.

Como se observa en la descripción de funcionamiento, en la zona inferior de GRUB2, es posible editar las líneas que permitirán arrancar el sistema operativo, además de poder acceder a una terminal que proporciona el mismo GRUB. Cabe recalcar que en esta instancia aun no carga el sistema operativo y que hasta el momento no ha solicitado ningún tipo de credenciales.

**UTILIZANDO LA TERMINAL DE GRUB2**


*Ilustración 8: Pantalla principal del gestor de arranque GRUB2*

El primero de los ataques consiste en visualizar información sensible del servidor mediante la ejecución de comandos de GRUB. En el caso de GRUB2 se pulsa la “C”. Aparecerá una consola con una breve ayuda para su

uso y el prompt (Se llama prompt al carácter o conjunto de caracteres que se muestran en una línea de comandos para indicar que está a la espera de órdenes) ***grub>***

Pulsando la tecla Tab o bien escribiendo la palabra reserva help, aparecerá un listado con los comandos disponibles. De todos los comandos, son interesantes ***ls*** y ***cat.*** Con ellos se pueden volcar listados de ficheros y sus contenidos, mostrando la información de la empresa, tal cual como ocurre en las consolas o las terminales de las distribuciones de GNU/Linux.

Unos ficheros que son interesantes pueden ser ***passwd*** y ***shadow.*** Pero ¿cómo se puede visualizar el contenido de dichos ficheros? ¿cuál es su ruta? – La ruta puede ser averiguada mediante el comando ***ls -l,*** con el que se podrá obtener la partición o disco objetivo. Mediante el uso del comando anterior sabremos la ruta del disco ***(hd0,msdos1)***. En tal caso se podría volcar el contenido del fichero ejecutando ***cat (hd0,msdos1)/etc/passwd***. La salida en pantalla mostraría el contenido del fichero ***/etc/passwd***. Como se puede comprobar en esta instancia no importa el permiso que tengan los archivos ni incluso root como propietario del mismo.

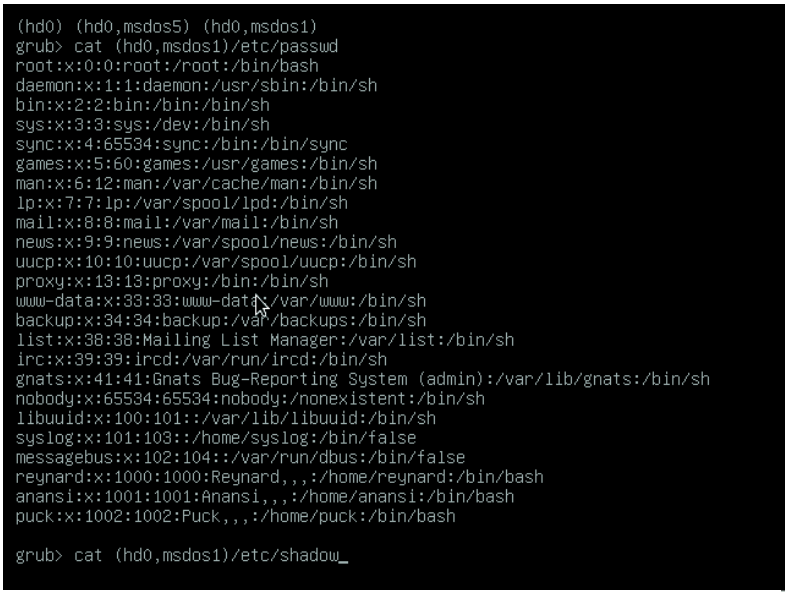


*Ilustración 9:: Contenido del fichero /etc/passwd desde la consola GRUB*

Después de haber revisado, resulta muy interesante y se puede obtener mucha información. Desde la mostrada hasta la información más sensible de la empresa, se puede comprometer la integridad, disponibilidad de la información y de los sistemas informáticos que se ejecutan en la empresa.

## OBTENIENDO ACCESO A root DESDE LA TERMINAL DE GRUB

Ahora utilizaremos el ***prompt*** de GRUB para obtener acceso como ***root*** sin conocer las credenciales o contraseñas, se ejecute una ***Shell*** con privilegios de super-usuario. Para lograr aquello, editamos la línea de arranque, estando en el menú principal de GRUB2 y situando sobre la línea desea, pulsamos la letra “E”. Dicha acción abrirá una edición de entrada de

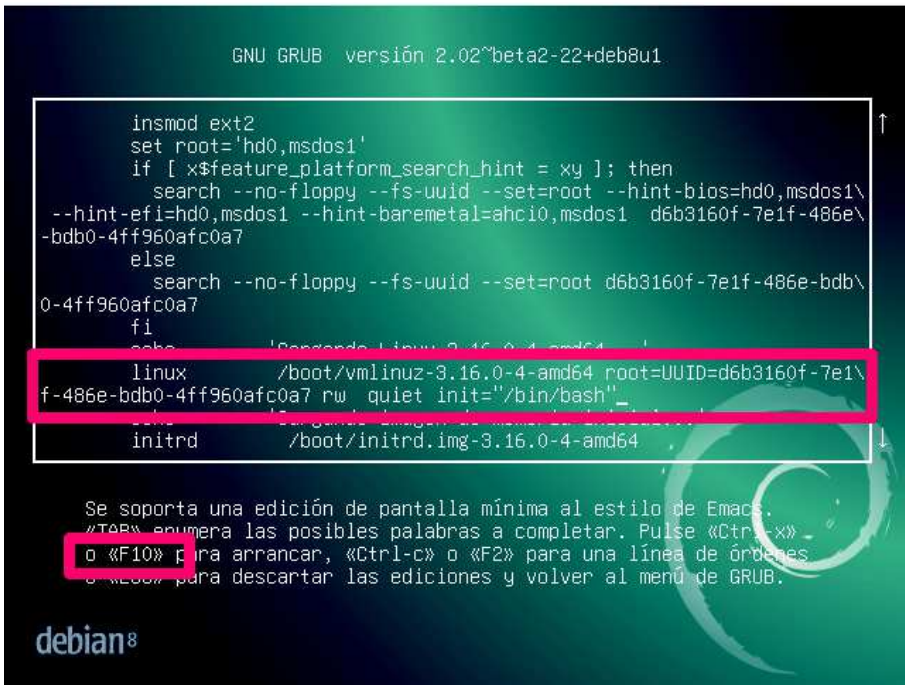


*Ilustración 10: Edición de entrada de arranque para obtener una shell como root*

GRUB. Se debe arrancar el núcleo Linux en mono-usuario y ejecutar una terminal ***sh.*** Las opciones anteriores son “***rw single init=/bin/sh”***

Una vez que el núcleo arranque mostrará el símbolo "#", que indica que se tiene a disposición un ***prompt*** como super-usuario, con las particiones montadas y con la disposición de realizar cualquier modificación sobre el sistema y todo su contenido. Una acción que se hace con normalidad es cambiar las credenciales de ***root*** y se procede a reiniciar el sistema operativo

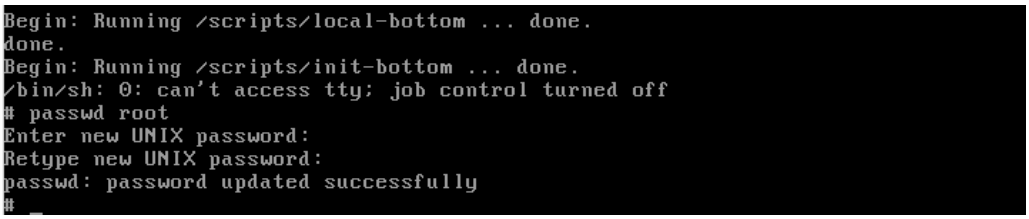


*Ilustración 11: Modificando el passwd de root*

*Ilustración 1: Modificando el passwd de root*

disponiendo de todas sus características.

## PROTECCIÓN DEL GESTOR DE ARRANQUE

Considerando los resultados obtenidos anteriormente, resulta evidente la necesidad de proteger o limitar de alguna manera el uso del GRUB. Para mitigar los ataques que pueden llegar a ser tan críticos para la empresa afectando la confidencialidad, disponibilidad e integridad de los sistemas e información es necesario establecer credenciales de acceso de entrada y a la consola del GRUB2

### Protección de GRUB2

GRUB2 es la segunda versión y la más actual del gestor de arranque, se modifican bastantes aspectos y se apuesta a una mayor flexibilidad para configurarlo. Dicha flexibilidad es gracias a la automatización con scripts de las configuraciones y nuevas directivas de configuración entre otros cambios que se dieron en comparación con GRUB, a pesar de las nuevas características el aspecto sigue siendo casi idéntico al del GRUB tradicional.

Centrados en la protección mediante password, la principal novedad radica en que es posible la creación de roles o grupos de usuarios con diferentes privilegios en GRUP2.

A la hora de establecer la contraseña, en el sistema operativo Debian GNU/Linux, lo hacemos en el fichero ***/etc/grub.d/00_header.*** Recomendación, hacer backups de los archivos de configuración de GRUB2.

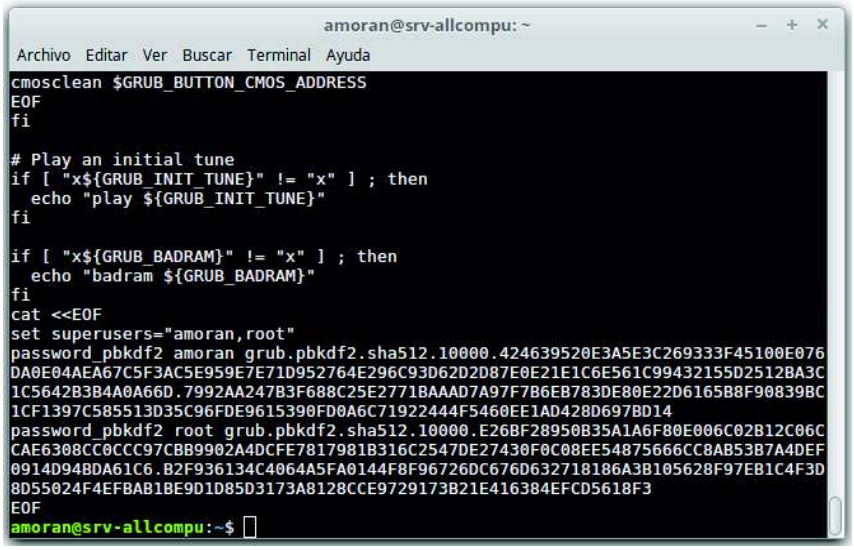


*Ilustración 12: Estableciendo un password en GRUB2*

Se ha utilizado contraseñas cifradas, cuya generación de passwords cifradas se utiliza el comando grub-mkpasswd-pbkdf2

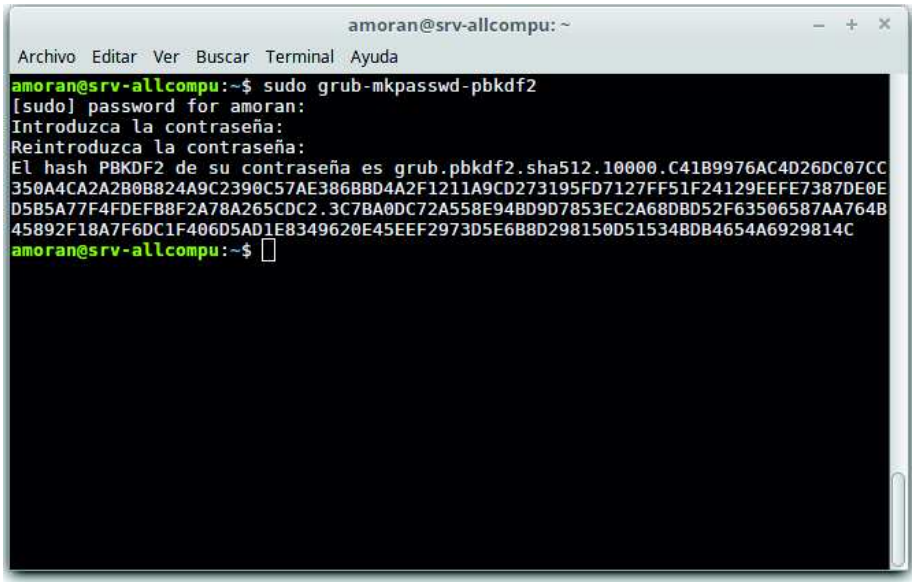


*Ilustración 13: Generando password cifrada*

Para que la configuración sea efectiva es necesario regenerar el fichero de configuración de GRUB2. Para ello se utiliza el comando ***update-grub,*** que leerá todos los scripts incluyendo el ***/etc/grub.d/00_header.*** En el momento que se reinicie el servidor se podrá verificar que la consola no es accesible a menos que se introduzcan las credenciales establecidas. De igual modo estará restringido el acceso a la edición de las líneas de arranque.

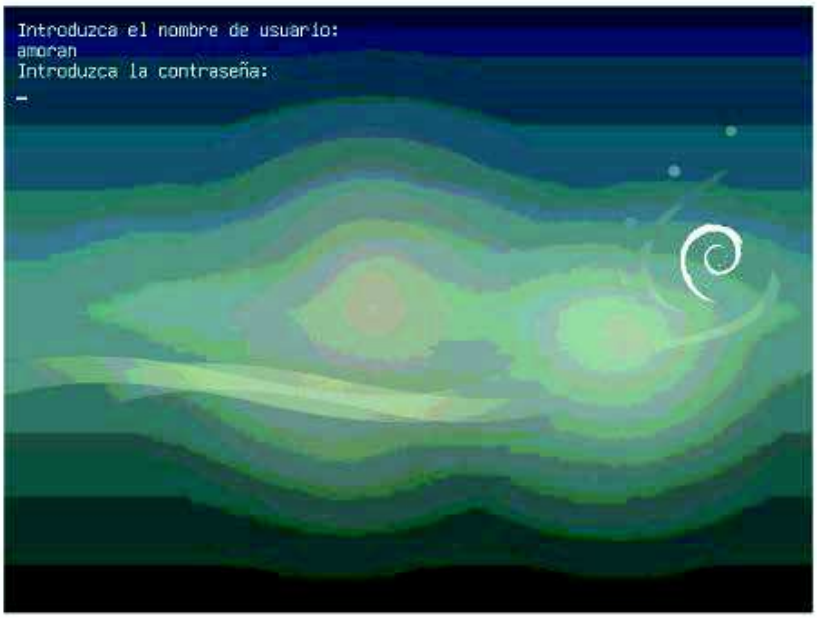


*Ilustración 14: Acceso a GRUB2*

*Fuente: Alerto Morán*

## C.- PROTECCIÓN DEL SISTEMA DE ARCHIVOS

Como se ha podido comprobar, la protección del gestor de arranque reduce la zona de impacto cuando un atacante (persona con malas intenciones) se encuentra físicamente junto al servidor.

Suponiendo que la persona atacante se encuentra físicamente junto al servidor de la empresa, es obvio que surge la pregunta. ¿Y si se apaga la máquina y se extraen los discos físicos instalados en la máquina?

### Acceso a un sistema de ficheros

Si el atacante finalmente tuvo éxito y extrajo los discos duros del servidor. Ahora el atacante inserta los discos en un sistema operativo Linux u otros capaz de abrir diversos tipos de sistemas de ficheros.

Una vez que los disco estén conectados en el sistema operativo anfitrión, que aloja los discos usurpados, hacemos uso del comando fdisk para visualizar la tabla de particiones de discos.


*Ilustración 15: Tabla de particiones con fdisk*

*Fuente: Alberto Morán*

Se puede estudiar el tipo de partición mediante el comando ***blkid /dev/sdb1,*** se procede a montar la aplicación para acceder al todo el contenido de los discos duros, para esto se utiliza el comando ***mount.***

La imagen anterior es solo una muestra de información relevante y sensible que puede llegar a conseguirse. Los directorios más interesantes que suelen ser observados son los directorios de los usuarios ***/home*** directorio de ***root,*** directorio ***/var.*** Cuyos directorios es donde por defecto suele almacenarse información y configuraciones de las aplicaciones o sistemas informáticos y el registro de las actividades que se realizan en el servidor como los ***logs***.

Considerando que en la máquina que se montaron los discos duros usurpados tiene permisos de super-usuario no habrá nada que pueda resistirse para visualizar la información. ¿Cómo podría proteger los discos

duros en caso de extravío o robo? La solución para esto es utilizar el cifrado completo de disco o particiones.

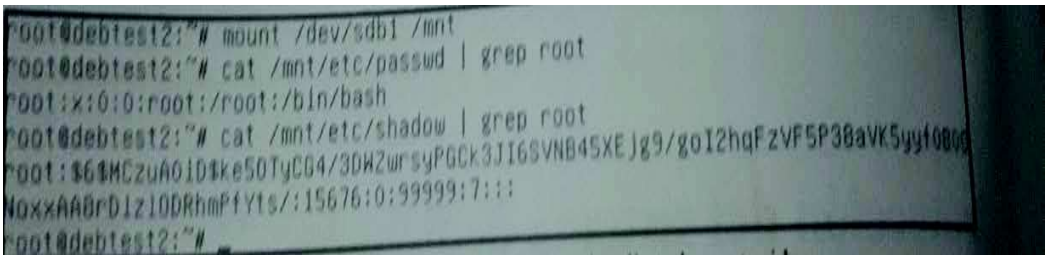


*Ilustración 16: Montando imagen con mount y visualizando contenido*

*Fuente: Alberto Morán*

### Cifrado de disco o particiones

Hay diversos métodos para poder cifrar dispositivos, los discos en sistemas operativos GNU/Linux, se implementará en este proyecto ***LUKS,*** que se ha convertido en el estándar para el cifrado de medios extraíbles.

Cabe mencionar, que otro de los sistemas de cifrado ampliamente conocido y perfectamente utilizable es ***TrueCrypt.*** Es un proyecto Open-Source y entre sus principales ventajas sobresale el poder ser utilizado con sistemas Linux, Windows y MacOS X. Todo ello sin ningún tipo de incompatibilidad.

### D.- LUKS. Linux Unified Key Setup

***LUKS*** es una especificación de cifrado que trata de definir un formato estándar de disco, ser independiente de la plataforma que utiliza y tener una amplia y clara documentación.

Además, como se comentaba anteriormente, LUKS es un estándar en cifrado, se ha optado por esta herramienta puesto que viene incluida en la mayoría de las distribuciones de GNU/Linux y Debian no es la excepción, lo que hace que la acción de cifrar los discos o particiones sea una tarea casi transparente al momento de instalar el sistema operativo.

El mundo de la criptografía es inmenso y muy técnico, por lo que se abordara el funcionamiento de LUKS no con tanta demasía, para ello es importante explicar levemente el sistema, sino de ver a grandes rasgos qué componentes entran en juego al momento de utilizarlo en Debian GNU/Linux.

- ***Device Mapper, DM.*** Se trata de un framework capaz de mapear dispositivos de bloque dentro de otro. Es decir, se pueden montar los dispositivos que se deseen dentro de otros dispositivos, habiendo siempre un último que se comunique con un dispositivo físico. Si los dispositivos ***DM*** se representasen en forma de pila, en la parte más alta podría encontrarse un sistema de ficheros.

- ***dm-crypt.*** Se trata de una de las aplicaciones o implementaciones de ***DM (Divice Mapper)***. Su cometido consiste en proporcionar cifrado transparente para un dispositivo de bloque y como actor intermediario ***DM***; ya sea un disco físico o un dispositivo de bloques virtuales.

- ***LUKS.*** Es el mecanismo utilizado para el cifrado de dispositivos de bloque. En él se especifican algoritmos de cifrado, passphrase, modos de cifrado, vectores de inicialización (IVs), etc.

Resumiendo, el funcionamiento de LUKS, teniendo una partición extendida número 5 de disco. Se dispone por lo tanto de ***/dev/sda5*** y es la partición que vamos a cifrar, puesta dicha partición va a contener información muy relevante para la empresa que nadie debería poder visualizar en caso de pérdida del disco.

Una vez que cifre la partición, no se volverá a trabajar más con ***/dev/sda5***; sino con un dispositivo de bloques virtual, esto es proporcionado gracias a ***dm-crypt*** en el que habrá usado ***LUKS*** como especificación de

cifrado. El nuevo dispositivo de trabajo, en el que habrá de crear un sistema de ficheros, pasaría a localizarse en ***/dev/mapper/<nombre>,*** en este caso ***/dev/mapper/srv—allcompu—vg-home, /dev/mapper/srv—allcompu—vg-swap_1, /dev/mapper/srv—allcompu—vg-var, /dev/mapper/srv—allcompu—vg-root, /dev/mapper/srv—allcompu-vg-tmp y /dev/mapper/sda5_crypt.*** Por supuesto, dicho dispositivo virtual estará disponible una vez que se haya desbloqueado con una frase de paso como se verá a continuación en la implantación.

**Instalar un sistema con cifrado de dato**

Como se indicó con anterioridad, la mayoría de las distribuciones disponen de soporte de cifrado de disco en sus instaladores, ya sea mediante GUI o por consola. En el caso de Debian GNU/Linux esto no es diferente, y a continuación se mostrará la implementación del cifrado de disco en el momento de la instalación del sistema operativo.

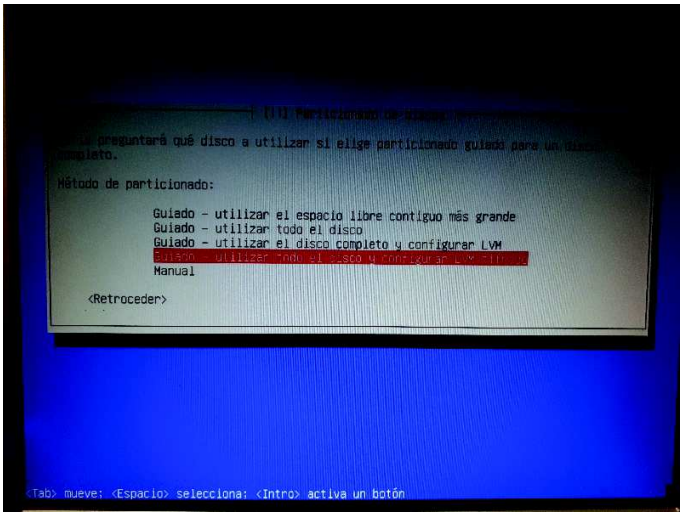


*Ilustración 18: Particionando el disco guiado y con cifrado*

*Fuente: Alberto Morán*

Cuando se generan cantidades de ***logs*** se requiere de configuraciones más complejas y separar las particiones es una recomendación muy habitual para no formen parte de un todo los archivos de configuración con la información de relevancia de la empresa y que no sea comprometida, de esta manera estamos adoptando el concepto de integridad y confidencialidad de la información de la empresa. Separaremos las particiones para ***/home, /usr, /var y /tmp.***

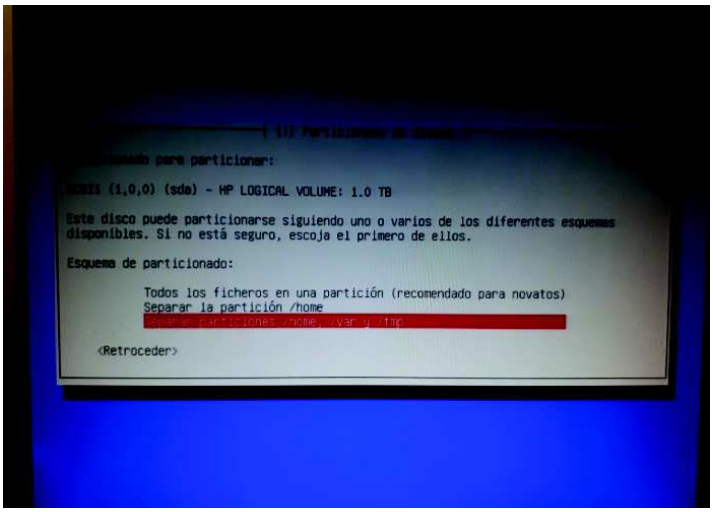


*Ilustración 17: Instalación del sistema con varias particiones y cifrado*

*Fuente: Alberto Morán*

Los sistemas de cifrado pueden configurarse de diferentes modos. Por ejemplo, se puede cifrar una partición y posteriormente formatearla como se desee, crear volúmenes lógicos y cifrar los discos lógicos necesarios, hacerlo en un raid hardware, etc.

- Partición 1, primaria, sin cifrar. Será la encargada para montar ***/boot*** y que contiene la configuración del gestor de arranque, el núcleo Linux, etc. Debe ser así, coso contrario el sistema no sería capaz de arrancar.

- Partición 5, primera partición lógica, cifrada. Esta partición será un grupo de volúmenes lógicos que contendrá dos volúmenes lógicos. Cada volumen a su vez se formatea de forma adecuada. Una partición será la destina para montar **/** y la otra será la ***swap*** del sistema. Se entiende que se usan volúmenes lógicos para proporcionar un poco de flexibilidad al sistema. Para eso se utiliza LVM (Logical Volumen Manager) que es otra de las aplicaciones de ***Device Mapper.***

Dependiendo del tamaño del disco y de la velocidad del sistema, es posible que el proceso de formateo o borrado de datos del disco ocupe un tiempo considerable. En este proceso se realiza una escritura en el disco de datos aleatorios que “sustituirá” todo lo que había con anterioridad. En el caso de Debian, la aplicación que realiza dicha acción es ***blockdev-wipe***.

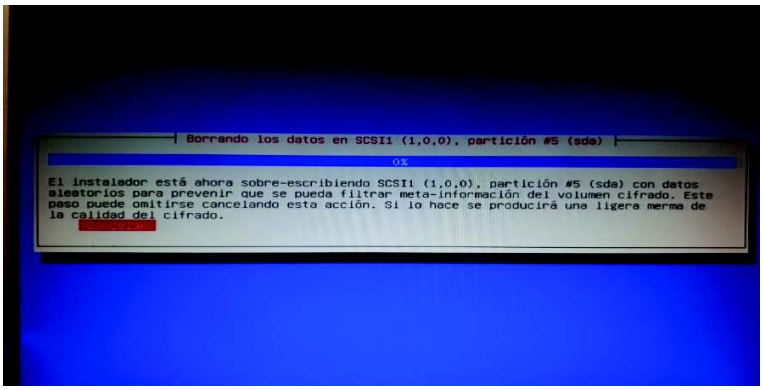


*Ilustración 19: Borrado de datos de las particiones cifradas.*

*Fuente: Alberto Morán*

Acabado el proceso de borrado el sistema solicitará al administrador o usuario la introducción de una frase de paso, ***passphrase***, que servirá para desbloquear la clave maestra del sistema de cifrado proporcionado por ***LUKS***. Como consecuencia, al introducir correctamente dicha frase de paso, la partición quedará desbloqueada y de cara al sistema y al usuario será como una partición convencional.

Al confirmar la frase de paso que desbloqueará el sistema en cada arranque, se muestra un sumario de cómo ha quedado distribuido el disco.

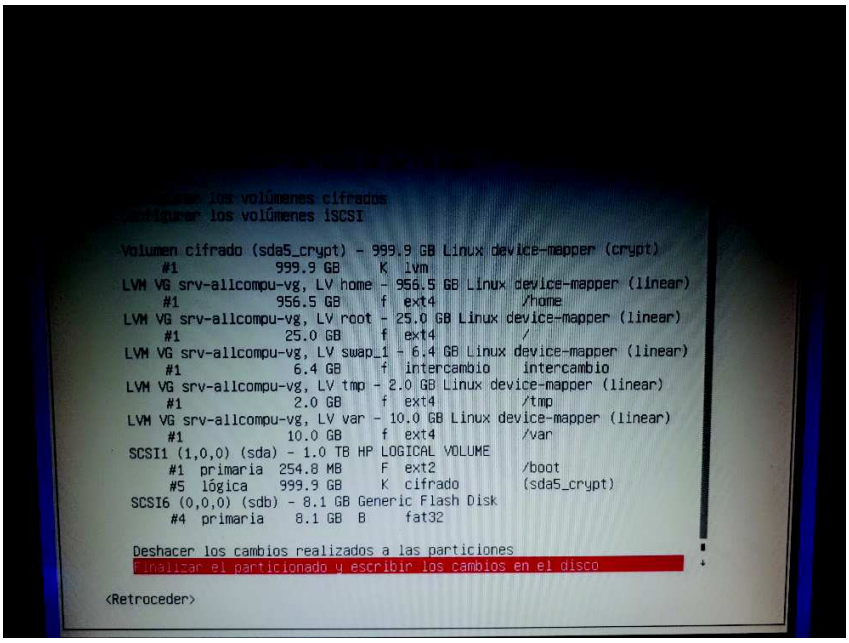

*Ilustración 20: Particionado final del disco*

*Fuente: Alberto Morán*

Todo ha quedado tal y como se había comentado con anterioridad. Se ha utilizado sobre una partición cifrada ***LVM*** para crear volúmenes lógicos que se formatearán como ***ext4 y swap.***

Acabada la instalación y el servidor arranca, aparecerá el ya conocido gestor de arranque ***GRUB2***. Al pulsar sobre la entrada del sistema operativo recién instalado con cifrado se iniciará el núcleo ***Linux*** con normalidad. Al iniciar el sistema es necesario montar la partición raíz entre otras, pero en este caso al estar cifrado aparecerá algo así:

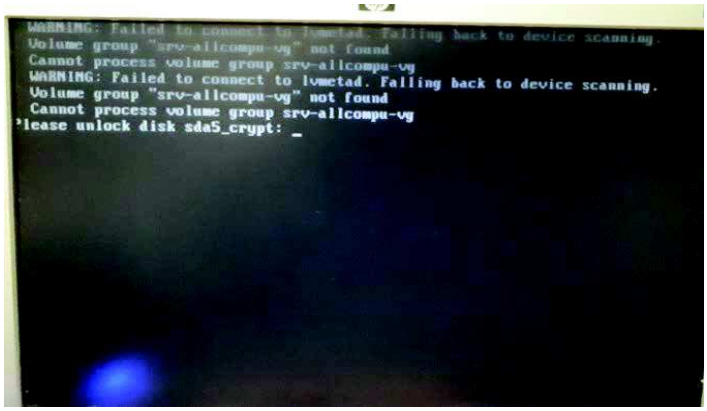


*Ilustración 21: Introducción de la passphrase en el arranque*

*Fuente: Alberto Morán*

Al introducir correctamente la frase de paso, la partición cifrada quedará desbloqueada de cara al sistema y se trabajará de forma transparente al cifrado de disco. Tanto ***DM, dm-crypt y LVM2*** en este caso estarán realizando su magia.

**Aplicaciones de gestión y administración para el cifrado con LUKS**

Después de una instalación limpia del sistema operativo sobre el disco cifrado, además de disponer de herramientas básicas para la gestión de

discos, son necesarias herramientas para poder gestionar volúmenes lógicos, volúmenes cifrados, etc.

A continuación, haciendo uso de las herramientas veremos cómo

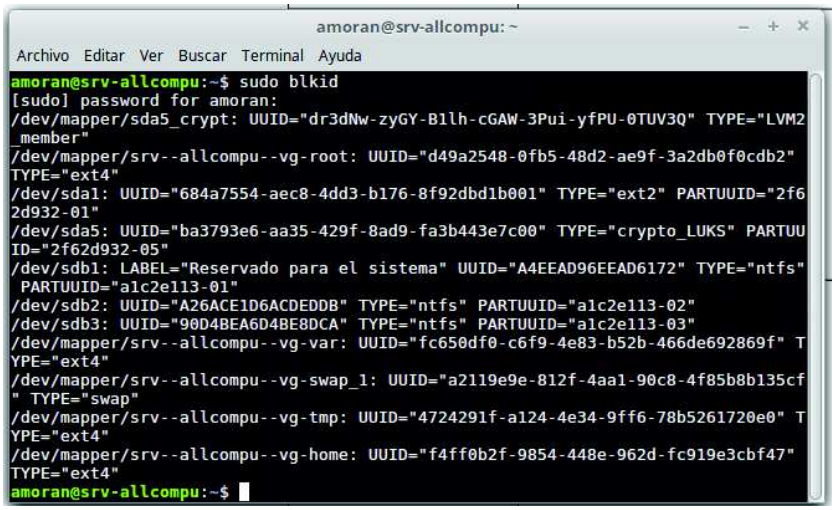


*Ilustración 22: Mostrando tipos de particiones con blkid.*

*Fuente: Alberto Morán*

detectar si efectivamente el sistema corre sobre una partición cifrada.

Como se comentó, la configuración se estableció de ese modo por defecto en la instalación de Debian cuando elegimos cifrado de datos. Tanto los volúmenes lógicos, como los volúmenes cifrados están funcionando

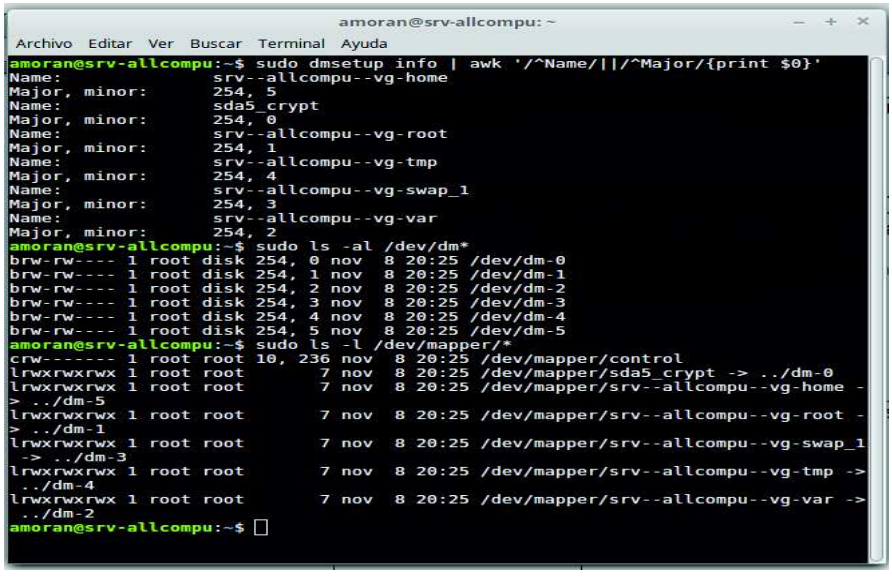

*Ilustración 23: Volúmenes generados con DM, Device Mapper.*

*Fuente: Alberto Morán*

gracias a ***Device Mapper***. Se puede visualizar el estado de los llamados dispositivos ***dm*** con los siguientes comandos.

El volumen ***/dev/mapper/sda5*** o ***/dev/dm-0*** es el correspondiente al volumen cifrado que se creó durante la instalación del sistema. Los otros volúmenes son de la partición raíz y la swap, que se tratan en realidad de volúmenes lógicos contenidos en un grupo de volúmenes usando el "disco físico" ***/dev/dm-o*** que se trata en realidad del volumen cifrado. Aquí es donde entra en juego el concepto en el que ***Device Mapper*** es capaz de mapear dispositivos de bloque dentro de otros.

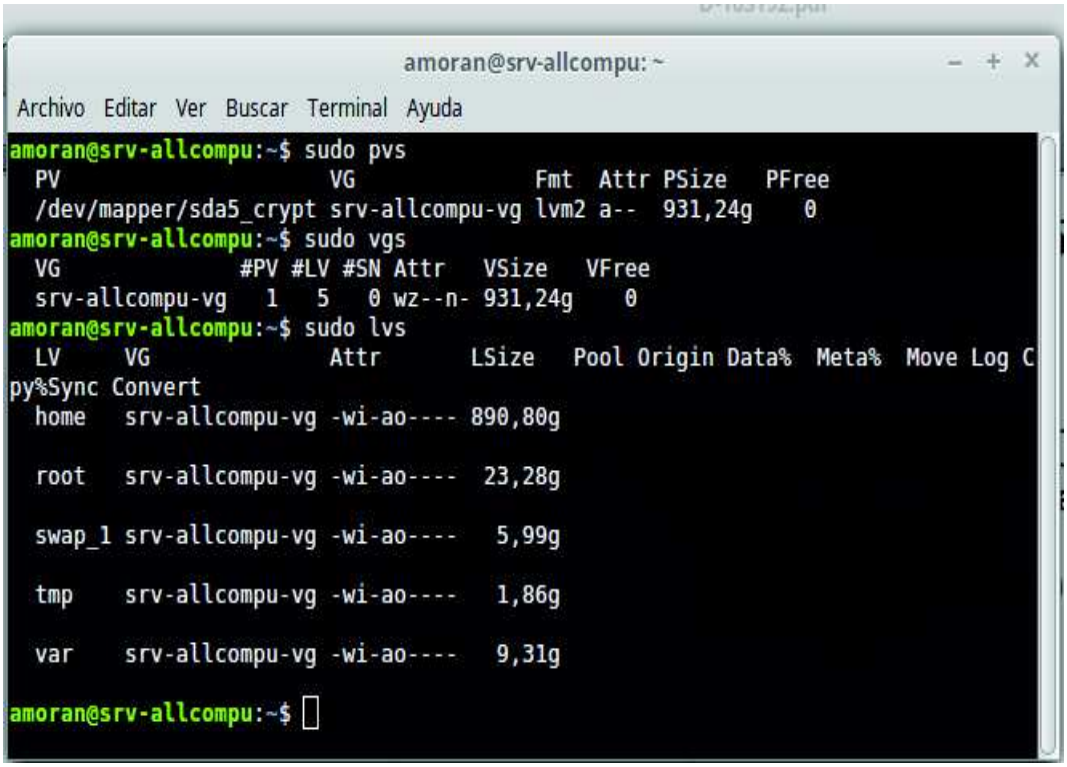


*Ilustración 24: Estado de los volúmenes lógicos*

*Fuente: Alberto Morán*

Ahora ¿qué aspecto tiene el fichero ***/etc/fstab***? – La respuesta es sencilla, se parece mucho al de un sistema sin cifrar, salvo que este caso se

usaran los dispositivos de bloques del contenido en ***/dev/mapper*** para las particiones.

El sistema raíza se encuentra cifrado con ***LUKS***, por lo que es necesario indicar de algún modo que es necesario desbloquear la partición para empezar a trabajar con normalidad. Es decir, es necesario crear los volúmenes lógicos y montar las particiones. En el archivo donde se indican qué particiones cifradas con ***dm-crypt*** deben desbloquearse es el ***/etc/crypttab.*** En dicho fichero se definen los dispositivos de bloque cifrados y bajo que nombres deben aparecer en el directorio ***/dev/mapper.***

**E.- OTRAS PROTECCIONES**

Existen algunas opciones adicionales con las que es posible proteger aún más un servidor frente a ataques físicos. A continuación, veremos algunas de ellas.

**Bloqueo y cierre automático de sesión**

Como se comentó con anterioridad, era necesario en numerosas ocasiones cifrar la información relevante para la empresa de manera individual. En varias ocasiones las sesiones permaneces desbloqueadas y cualquier persona con acceso físico al servidor o una sesión remota podrá explotar los privilegios que la sesión le conceda; en la mayoría de los casos, acceso como super-usuario.

**Variable de entorno TMOUT**

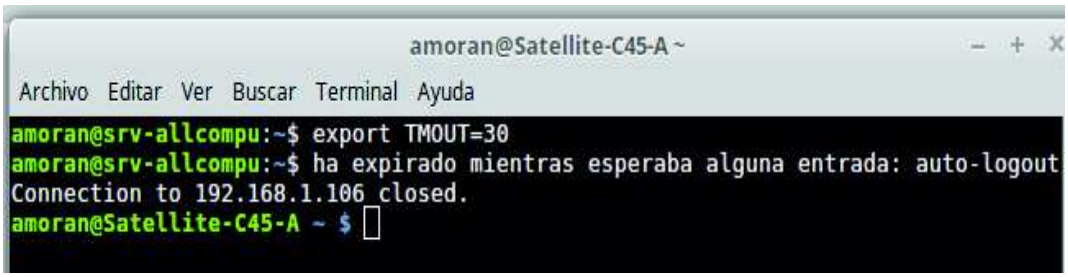


*Ilustración 25: Auto log-out con TMOUT*

*Fuente: Alberto Morán*

Por defecto, la mayoría de distribuciones Linux utilizar ***BASH*** como intérprete de comandos. Dicho intérprete dispone de una variable de entorno llamada ***TMOUT*** que esta deshabilitada inicialmente. Lo que promete es cerrar las sesiones después de un tiempo especificado de inactividad, cuyo tiempo esta expresado en segundos.

Para que el funcionamiento anterior sea aplicado de manera persistente o permanente a pesar de reinicios del sistema, es necesario establecer la variable de entorno en cada inicio de sesión. Para ello debe modificarse el fichero ***~/.bashrc*** estableciendo la línea de la imagen anterior.

**Aplicación vlock**

Si no se desea cerrar la sesión, sino, bloquear la sesión, optamos por la utilización de la aplicación ***vlock***. No está instalada por defecto en el sistema, pero puede obtenerse e instalarse fácilmente a través de los repositorios oficiales. Dispone de varios parámetros para modificar su comportamiento por defecto. Como cualquier aplicación, dispone de ayuda para entender cada modo.

En el caso de querer bloquear todas las TTY, se puede ejecutar el comando ***vlock -a*** que hará que en las terminales aparezca un mensaje indicando el bloqueo de la sesión.

**Evitando el reinicio y apagado accidental**

En la mayoría de la ocaciones, las distribuciones que eatn configuradas para responder a las señales de determinadas teclas o botones. En este caso lo que se trata de realizar consiste en inutilizar el botón de apagado y la secuencia de teclas ***Ctrl+Alt+Del.***

Para deshabilitar el apagado de debe ejecutar el siguiente comando

***Chmod a-x /lib/systemd/system/poweroff.target***

Se han eliminado los permisos de ejecución para todos los usuarios, lo que imposibilita que el script se ejecute y como consecuencia el servidor no responderá al botón de apagado.

### 3.5.3 SEGURIDAD PERIMETRAL

Tras haber implementado herramientas y ciertos métodos de protección a la capa física del modelo Defensa en Profundidad, ahora pasaremos a la siguiente capa, implementando protecciones en la capa más externa en cuanto a la red de datos o comunicaciones se refiere. En esta etapa vamos a ver herramientas que ayudaran a establecer barreras para aumentar el nivel de seguridad de la red y la información de la empresa, habilitando al mismo tiempo accesos remotos seguros. A demás se llevará a cabo como se puede monitorizar el estado de las maquinas en el entorno de red con lo que se podrá obtener información de las maquinas, si responden, sus servicios activos, entre otros.

**A.- IPTABLES**

Existen muchas formas o métodos de implementar firewalls o cortafuegos en Linux, desde el nivel de enlace como ***ebtables*** y ***arptables,*** hasta el nivel de aplicación como podría ser ***Squid*** para cachear y filtrar contenido web. En esta capa de seguridad a nivel perimetral, nos centraremos en la implementación del firewall para el filtrado y manipulación del tráfico a nivel de red y transporte mediante ***iptables.***

**¿Qué es iptables?**

***Iptables*** es una aplicación de nivel de usuario que perite la gestión, configuración y manejo del filtrado de tráfico de red en un servidor o máquina que corra bajo Linux. Para ello se utiliza ***netfilter,*** que no es más que un framework incluido en el núcleo de Linux capaz de manipular paquetes de datos de red en diferentes estados.

**Funcionamiento de iptables**

El ***kernel*** de Linux posee capacidades de direccionar o hacer una pasarela de los paquetes de red por una serie de reglas, por lo tanto, ***iptables*** es la herramienta que permite la configuración de esas reglas que el ***kernel*** ejecuta. Dichas reglas son agrupadas en cadenas y dichas cadenas están contenidas por tablas. Las reglas son un conjunto de parámetros en los que se trata de hacer que un datagrama o trama de red coincida atendiendo al protocolo, ips destino y origen, estado, etc.

Inicialmente al entrar paquetes en el servidor configurado ***iptables*** pasan por todas las tablas y cadenas configuradas por defecto.

Cuando una trama coincide con la condición de una regla, se pasa a tomar una condición de que hacer con dicho paquete. Las más comunes son dejar pasar el paquete o bien desechar el paquete. Dichas acciones, que pasarán a ser explicadas más adelante, son conocidas como ***ACCEPT*** y ***DROP*** respectivamente.

Si no existe ninguna regla que coincida con un paquete de red, a este se le aplicará la política por defecto que tenga la cadena por la que está pasando. Por defecto, como se comentaba con anterioridad, los paquetes pasan por todas las tablas ya que la política por defecto de las cadenas cuando ***iptables*** no está configurado es ***ACCEPT***. En tal caso, se entiende que se dejan pasar todos los paquetes que no coincidan con ninguna regla.

**Decisión de enrutamiento**

Se ha descrito el funcionamiento de ***iptables***. Pero ¿qué toma la decisión de por dónde deben pasar, salir o entrar los paquetes de datos?

Es ahí donde entran en juego las tablas de enrutamiento del servidor. Se atienden a las redes con las cuales se está directamente conectado, puertas de enlaces por defecto, interfaces, etc.

Dependiendo de las cadenas y las tablas, descritas a continuación, las diferentes reglas contenidas en ellas se aplicarán antes o después de la decisión de enrutamiento.

Todo esto será un poco más gráfico con el diagrama de la figura 34, mostrando al final de la siguiente sección donde abordaremos las tablas por defecto y sus respectivas cadenas.

**Tablas**

Existen cuatro tablas por defecto. Es posible cambiar esa situación mediante la carga de módulos en ***iptables***, por lo que se pueden agregar más tablas.

Las tablas por defecto son:

- ***filter.*** Es la tabla encargada del filtrado de paquetes. Es decir, en esta tabla se pueden dejar pasar o descartar paquetes dependiendo de las reglas contenidas en sus cadenas predefinidas por defecto enumeradas a continuación:
    - ***INPUT.*** Es la cadena en la que se definen las reglas para los paquetes que recibe un proceso local del servidor. Es decir, los paquetes que tengan como destino la el servidor local en la que se configura ***iptables.***
    - ***OUTPUT.*** El mismo caso que INPUT pero a la inversa. Por esta cadena pasaran todos los paquetes generados por un proceso local del servidor.

- ***FORWARD.*** Esta cadena es por la que pasan los paquetes que no van dirigidos al servidor local. Es decir, esta tabla se usa cuando el servidor configurado con ***iptables*** posee la capacidad de enrutar paquetes, o lo que es lo mismo, se comporta como un router.

- ***nat.*** En esta tabla se producen los procesos NAT que se configuren mediante ***iptables***. Contiene tres cadenas predefinidas:

  - ***PREROUTING.*** Cadena donde se realiza DNAT (Destination NAT). Por aquí pasarán los paquetes que entren en el sistema configurado con ***iptables.*** En este punto se decide a dónde se redirigen dichos paquetes. Coloquialmente hablando, es aquí donde se abren los puertos. Los paquetes pasan por esta cadena antes de la decisión de enrutado.

  - ***POSTROUTING.*** En esta cadena pasan los paquetes después de la decisión de enrutado. Se usa principalmente para hacer SNAT (Source NAT), es decir, enmascarar los paquetes con la IP de la interfaz de salida. Ejemplo: transformación de IPs privadas en IP pública.

  - ***OUTPUT.*** Cadena para realziar operaciones de ***NATeo*** para paquetes generados por un proceso local del servidor.

- ***mangle.*** Es una tabla en la que se pueden manipular determinados aspectos de los paquetes. Entre ellos se destaca la modificación del ***TimeToLive, TypeOfService*** y el marcado de paquetes. Este último proceso establece una marca a cada

paquete a nivel de kernel. Dichas marcas pueden ser usadas para tomar decisiones de enrutado dependiendo de tipos de tráficos, etc. Útil para balanceo de carga, implementaciones de QoS con ***qdisc*** configurables, etc. Las cadenas que posee la tabla ***mangle*** son:

- ***PREROUTING***
- ***INPUT***
- ***FORWARD***
- ***OUTPUT***
- ***POSTROUTING***

- ***raw.*** Se trata de una tabla relativamente nueva en la que se suele establecer una marca (***NOTRACK***) para evitar que ***netfilter*** realice un seguimiento del paquete. Se evitará que ***netfilter*** aplique ***conntrack*** al paquete. Las cadenas de las que dispone la tabla ***raw*** son:
  - ***PREROUTING***
  - ***OUTPUT***

La siguiente imagen muestra un diagrama de flujo correspondiente a los diferentes estados con lo que trabaja ***iptables.***

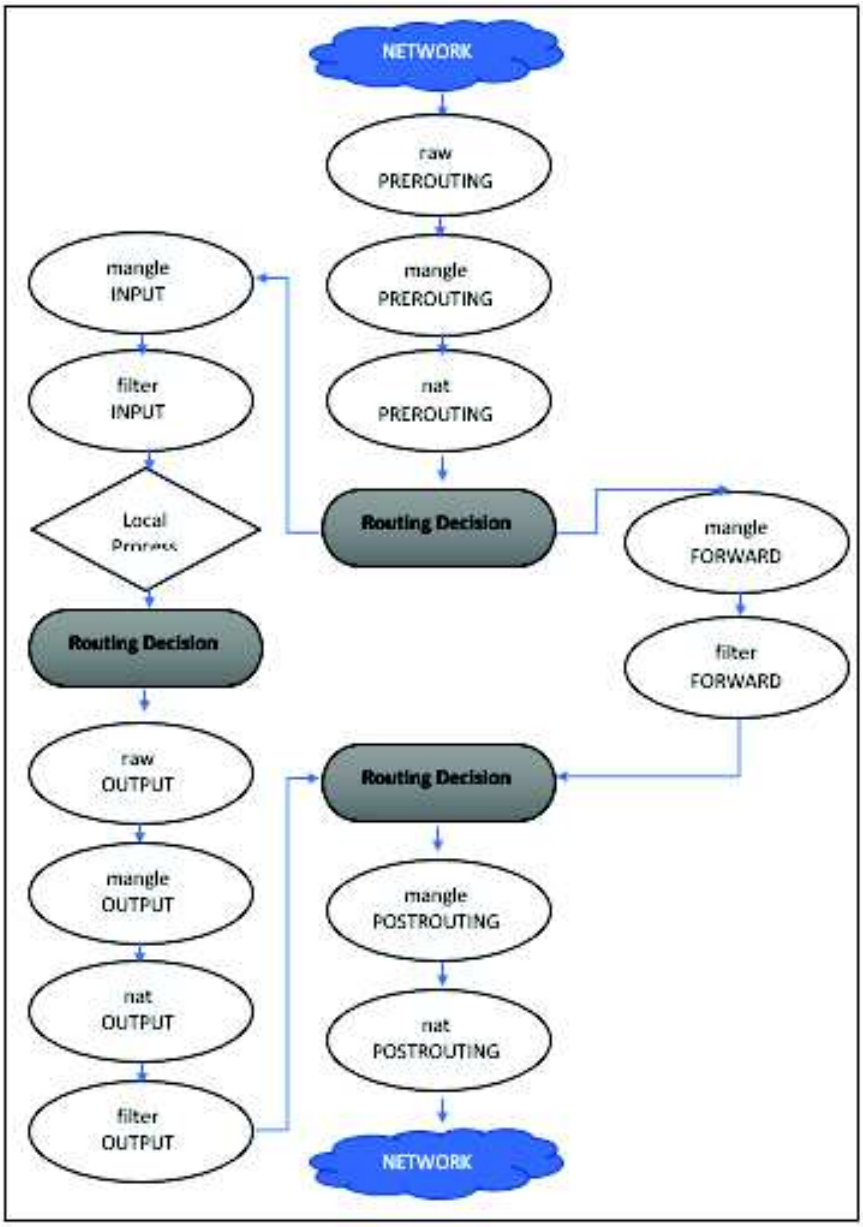


*Ilustración 26: Esquema interno de iptables*

*Fuente: Hardening de Sevidores Gnu/Linux*

### Agregando reglas con iptables

Ahora es el momento de ver cómo se crean y se eliminan reglas. También veremos cómo aplicar políticas por defecto para las cadenas. La forma genérica de hacerlo es la siguiente:

***Iptables -t <nombreTabla> -A <cadena><opciones> -j <acción>***

- ***Iptables*** es el comando en sí.
- El parámetro "***-t"*** se utiliza para indicar la tabla con la que se está trabajando en el momento de lanzar el comando ***iptables.***
- El parámetro ***"-A"*** añade ('append') una regla a la cadena indicada.
- Donde ***<opciones>*** se puede establecer diversos filtros para tratar de hacer coincidir un paquete por protocolo (***tcp, udp, icmp, http, etc.***), por puertos, IPs, etc.

**Ejemplos**

- Descartar la navegación web (sólo tráfico HTTP) por parte de las máquinas de la red local que pasen por el servidor (entrando por la interfaz interna "***enp4s0"*** y saliendo por la interfaz externa ***"enp1s4"***):

```
# iptables -t filter -A FORWARD -i enp4s0 -o enp1s4 -p tcp -dport
80 -j DROP
```

Se puede observar cómo para identificar el tráfico HTTP se ha usado la opción "-p tcp" para indicar el tipo de protocolo, así como una sub-opción denominada "--dport" para indicar el puerto destino ("destination port").

- Se realiza el mismo proceso, pero a la inversa. Denegando la respuesta de servidores HTTP.

```
# iptables -t filter -A FORWARD -i enp1s4 -o enp4s0 -p tcp -
sport 80 -j DROP
```

En caso de no especificar direcciones de origen o destino, como ocurre en esta regla y la anterior, se engloban todas las direcciones origen y destino.

- Se pasa a bloquear el tráfico ***SSH***, por lo que las máquinas de la red local no podrán conectar con el servidor ***SSH***. Denegamos tanto la petición como la respuesta.

```
# iptables -t filter -A FORWARD -i enp4s0 -o enp1s4 -p tcp –sport 22 -j DROP
# iptables -t filter -A FORWARD -i enp1s4 -o enp4s0 -p tcp –sport 22 -j DROP
```

Se puede observar cómo en la regla la respuesta de SSH se establece el parámetro "***--sport***" para indicar el puerto origen ("Source port").

- Ahora se procede a realizar ***SNAT*** para que los paquetes salientes del servidor, ya sean generados localmente o re-enviados desde otra subred, salgan con la IP pública externa.

```
# iptables -t nat -A POSTROUTING -o enp1s4 -j MASQUERADE
```

Se ha indicado que a todos los paquetes que vayan a salir por la interfaz externa ***enp1s4*** se les aplique SNAT. Así, el paquete se podrá enrutar por Internet sin problemas.

Por defecto la política de las cadenas en la tabla ***filter*** es ACCEPT. Es por eso que se han aplicado dos pares de reglas (HTTP y SSH) para tráfico de la red local con acción DROP. No tendrá sentido con la política ACCEPT establecer ACCEPT como acción de las reglas. Como norma general las acciones establecidas serán la inversa de la que se realice con la política por defecto establecida.

**Listando reglas con iptables**

Para obtener una visión de las reglas que están operativas en el sistema se puede realizar con las siguientes variantes del comando ***iptables:***

```
# iptables -t filter -nvL
```

En el comando anterior muestra las reglas aplicadas para la tabla ***filter***. En caso de omitir el parámetro ***-t*** se mostrará por defecto la tabla ***filter***.

Se realiza lo mismo, pero con la tabla ***nat***. En caso de necesitar

```
# iptables -t nat -nvL
```

obtener los números asociados a cada regla, se puede realizar con el siguiente comando:

```
# iptables -t nat -nvL -line-numbers
```

El anterior comando resulta bastante interesante para cuando se necesita eliminar una regla en concreto. Se obtiene el número de la regla de cada cadena y se procede a eliminar dicha regla utilizando el número asociado.

**Eliminado reglas aplicadas**

Cada vez que se necesita restablecer la configuración del firewall o modificar su comportamiento del mismo, será necesario eliminar reglas. A continuación, se mostrarán métodos para llevar a cabo dicha tarea.

**Método selectivo**

Cuando se desea eliminar una regla determinada de ***iptables***, previamente es necesario hacer una visualización de las reglas aplicadas en ese instante junto con sus números de regla.

Si quisiera eliminar la primera regla de la cadena ***POSTROUTING*** de la tabla ***nat*** habría que ejecutar el siguiente comando:

```
# iptables -t nat -D POSTROUTING 1
```

Se debe indicar la tabla sobre la que se desee realizar la operación con el parámetro ***-t***. acto seguido se indica de qué cadena se va a eliminar

una regla con el parámetro ***-D(delete)*** seguido del nombre de la cadena y del número de la regla a eliminar.

**Limpieza o "flush"**

Es probable que durante el proceso de pruebas con ***iptables*** puedan quedar residuos de reglas antiguas que interfieran con las que se prueben más adelante; o simplemente que se desee restablecer el estado inicial des configurado de ***iptables.*** Los siguientes comandos eliminan todas las reglas de las tablas ***nat y filter.***

```
# iptables -t nat -F
# iptables -t filter -F
```

El parámetro ***-F*** ("***flush***") dejará limpias las tablas que se hayan indicado. Cabe recalcar que al limpiar las tablas y cadenas de ***iptables*** no se restablece la política por defecto ***ACCEPT***. Habrá que establecerla en el estado deseado con el comando que implementaremos a continuación.

**Cambiando política por defecto**

Para modificar el comportamiento por defecto de ***iptables*** en ciertas cadenas se utiliza el comando ***iptables*** con los siguientes parámetros:

***Iptables -t <tables> -P <cadena> <POLÍTICA>***

Pasaremos a establecer la política por defecto de la cadena ***INPUT,*** de la tabla ***filter***, a ***DROP:***

```
# iptables -t filter -P INPUT DROP
```

Es decir, se está descantando todo el tráfico entrante que valla destinado al servidor donde tenemos configurado ***iptables.***

**Haciendo las reglas permanentes**

Cuando el servidor ya tiene configurado ***iptables*** y se procede a reiniciarlo, las reglas que se definieron desaparecen en el arranque. Volverán a existir las tablas, cadenas y políticas por defecto sin ninguna regla.

Existen varios métodos para hacer que las reglas de *iptables* se mantengan después de un reinicio. En este caso se muestra una muy sencilla

```
# sudo apt-get -y install netfilter-persistent
```

que es instalando una dependencia de *netfilter-persistent,* la cual la podemos obtener desde el repositorio oficial o ejecutando el siguiente comando:

También es posible realizar esta tarea usando los comandos *iptables-save, iptables-restore e iptables-apply.*

**Firewall ALLCOMPU**

Aplicar políticas por defecto a *DROP* en las cadenas de *filter.* Como consecuencia de ello es necesario crear reglas para permitir el tráfico necesario para la empresa.

a. Se permitirá el tráfico de *lookbak* en el servidor.

b. El servidor podrá realizar conexiones SSH

c. El servidor Debian acepta tráfico SSH

d. El servidor tendrá permitido solo el tráfico *ICMP* saliente.

e. El servidor podrá ser usado como cliente: *DNS, HHTP y HTTPS.*

A continuación, se muestran como quedarían todas las condiciones anteriores en un script *bash.*

#!/bin/bash

```
#BORRANDO REGLAS ANTERIORES
iptables -F
iptables -X
iptables -t nat -F


#SE ACTIVA EL BIT DE ENRUTAMIENTO DEL SERVIDOR
echo 1 > /proc/sys/net/ipv4/ip_forward

#CONSTANTES Y VARIABLES
VLAN10="192.168.10.0/27"
VLAN20="192.168.20.0/30"
VLAN30="192.168.30.0/27"
VLAN40="192.168.40.0/26"
VLAN50="192.168.50.0/30"
IFVLAN10="vlan10"
IFVLAN20="vlan20"
IFVLAN30="vlan30"
IFVLAN40="vlan40"
IFVLAN50="vlan50"
IFEXT="enp1s4"

#-----------------------------------------------
# TRAFICO ENTRANTE Y SALIENTE DEL SERVIDOR
#-----------------------------------------------

#RESTRIGIR ESCANEOS Y/O PAQUETES MAL FORMADOS
iptables -A INPUT -i $IFEXT -p tcp –tcp-flags ACK ACK -m state –state
NEW -j REJECT
iptables -A INPUT -i $IFEXT -p tcp –tcp-flags RST RST -m state –state
NEW -j REJECT
iptables -A INPUT -i $IFEXT -p tcp –tcp-flags PSH PSH -m state –state
NEW -j REJECT
iptables -A INPUT -i $IFEXT -p tcp –tcp-flags FIN FIN -m state –state NEW -
j REJECT
iptables -A INPUT -i $IFEXT -p tcp –tcp-flags  FIN,PSH,URG -j DROP
iptables -A INPUT -i $IFEXT -p tcp –tcp-flags ALL ACK,RST,SYN,FIN -j
DROP

#LIMITAR CONEXIONES DE TIPO TCP SYN ENTRANTES
Iptables -A INPUT -I $IFEXT -p tcp –syn -m recent –set
Iptables -A INPUT -I $IFEXT -p tcp –syn -m recent –update –seconds 5 –
hitcount 20 -j DROP

#LIMITAR A UN PING POR SEGUNDO Y DIRECCIÓN IP
```

```
Iptables -A INPUT -i $IFEXT -p icmp –icmp-type echo-request -m hashlimit
–hashlimit-name ping –hashlimit-above 1/s –hashlimit-burst 2 –hashlimit-
mode srcip -j REJECT

# SE PERMITE TODO EL TRAFICO LOOKBACK
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# SE PERMITE CONSULTAS A LA BASE DE DATOS
iptables -A INPUT -p tcp --destination-port 3306 -j ACCEPT

# SE PERMITE CONSULTAS DNS HACIA INTERNET
iptables -A INPUT -i $IFEXT -p udp --sport 53 -j ACCEPT
iptables -A OUTPUT -o $IFEXT -p udp --dport 53 -j ACCEPT

# SE PERMITEN CONSULTAS HTTP Y HTTPS HACIA INTERNET
iptables -A INPUT -i $IFEXT -p tcp --sport 80 -j ACCEPT
iptables -A OUTPUT -o $IFEXT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -i $IFEXT -p tcp --sport 443 -j ACCEPT
iptables -A OUTPUT -o $IFEXT -p tcp --dport 443 -j ACCEPT

#Se permiten consultas DHCP
iptables -A INPUT -i $IFEXT -p udp --sport 67:68 -j ACCEPT
iptables -A OUTPUT -o $IFEXT -p udp --dport 67:68 -j ACCEPT

#Se permite solo tráfico ICMP saliente y su respuesta
iptables -A INPUT -i $IFEXT -p icmp -m state --state
ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -o $IFEXT -p icmp -j ACCEPT

#Se permite el tráfico SSH por la interfaz externa
iptables -A INPUT -i $IFEXT -p tcp --sport 22 -j ACCEPT
iptables -A OUTPUT -o $IFEXT -p tcp --dport 22 -j ACCEPT

#SAMBA
iptables -A INPUT -p tcp -m multiport --dport 139,445 -j ACCEPT
iptables -A INPUT -p udp -m multiport --dport 137,138 -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#VOZ SOBRE IP
iptables -A INPUT -i $IFVLAN10 -p udp --dport 5060 -j ACCEPT
iptables -A INPUT -i $IFVLAN10 -p udp --dport 10000:20000 -j ACCEPT

#La máquina es servidor SSH (se acepta SSH por cualquier iF)
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT
```

```
#-----------------------------------------------------
# TRÁFICO FORWARD
#-----------------------------------------------------

# Se permite tráfico ICMP entre VLANS
iptables -A FORWARD -p icmp -i $IFVLAN10 -j ACCEPT
iptables -A FORWARD -p icmp -o $IFVLAN10 -j ACCEPT
iptables -A FORWARD -p icmp -i $IFVLAN20 -j ACCEPT
iptables -A FORWARD -p icmp -o $IFVLAN20 -j ACCEPT
iptables -A FORWARD -p icmp -i $IFVLAN30 -j ACCEPT
iptables -A FORWARD -p icmp -o $IFVLAN30 -j ACCEPT
iptables -A FORWARD -p icmp -i $IFVLAN40 -j ACCEPT
iptables -A FORWARD -p icmp -o $IFVLAN40 -j ACCEPT
iptables -A FORWARD -p icmp -i $IFVLAN50 -j ACCEPT
iptables -A FORWARD -p icmp -o $IFVLAN50 -j ACCEPT

# Se permite tráfico HTTP y HTTPS
iptables -A FORWARD -p tcp --dport 80 -i $IFVLAN10 -o $IFEXT -j ACCEPT
iptables -A FORWARD -p tcp --sport 80 -o $IFVLAN10 -i $IFEXT -j ACCEPT
iptables -A FORWARD -p tcp --dport 80 -i $IFVLAN20 -o $IFEXT -j ACCEPT
iptables -A FORWARD -p tcp --sport 80 -o $IFVLAN20 -i $IFEXT -j ACCEPT
iptables -A FORWARD -p tcp --dport 80 -i $IFVLAN30 -o $IFEXT -j ACCEPT
iptables -A FORWARD -p tcp --sport 80 -o $IFVLAN30 -i $IFEXT -j ACCEPT
iptables -A FORWARD -p tcp --dport 80 -i $IFVLAN40 -o $IFEXT -j ACCEPT
iptables -A FORWARD -p tcp --sport 80 -o $IFVLAN40 -i $IFEXT -j ACCEPT
iptables -A FORWARD -p tcp --dport 80 -i $IFVLAN50 -o $IFEXT -j ACCEPT
iptables -A FORWARD -p tcp --sport 80 -o $IFVLAN50 -i $IFEXT -j ACCEPT

iptables -A FORWARD -p tcp --dport 443 -i $IFVLAN10 -o $IFEXT -j
ACCEPT
iptables -A FORWARD -p tcp --sport 443 -o $IFVLAN10 -i $IFEXT -j
ACCEPT
iptables -A FORWARD -p tcp --dport 443 -i $IFVLAN20 -o $IFEXT -j
ACCEPT
iptables -A FORWARD -p tcp --sport 443 -o $IFVLAN20 -i $IFEXT -j
ACCEPT
iptables -A FORWARD -p tcp --dport 443 -i $IFVLAN30 -o $IFEXT -j
ACCEPT
iptables -A FORWARD -p tcp --sport 443 -o $IFVLAN30 -i $IFEXT -j
ACCEPT
iptables -A FORWARD -p tcp --dport 443 -i $IFVLAN40 -o $IFEXT -j
ACCEPT
iptables -A FORWARD -p tcp --sport 443 -o $IFVLAN40 -i $IFEXT -j
ACCEPT
```

```
iptables -A FORWARD -p tcp --dport 443 -i $IFVLAN50 -o $IFEXT -j
ACCEPT
iptables -A FORWARD -p tcp --sport 443 -o $IFVLAN50 -i $IFEXT -j
ACCEPT

#Se permiten consultas DNS
iptables -A FORWARD -p udp --dport 53 -i $IFVLAN10 -o $IFEXT -j
ACCEPT
iptables -A FORWARD -p udp --sport 53 -o $IFVLAN10 -i $IFEXT -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -i $IFVLAN20 -o $IFEXT -j
ACCEPT
iptables -A FORWARD -p udp --sport 53 -o $IFVLAN20 -i $IFEXT -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -i $IFVLAN30 -o $IFEXT -j
ACCEPT
iptables -A FORWARD -p udp --sport 53 -o $IFVLAN30 -i $IFEXT -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -i $IFVLAN40 -o $IFEXT -j
ACCEPT
iptables -A FORWARD -p udp --sport 53 -o $IFVLAN40 -i $IFEXT -j
ACCEPT
iptables -A FORWARD -p udp --dport 53 -i $IFVLAN50 -o $IFEXT -j
ACCEPT
iptables -A FORWARD -p udp --sport 53 -o $IFVLAN50 -i $IFEXT -j
ACCEPT

#---------------
# NAT
#---------------

# Se hace SNAT para la VLANS de la red interna
iptables -t nat -A POSTROUTING -s $VLAN30 -o $IFEXT -j MASQUERADE
iptables -t nat -A POSTROUTING -s $VLAN40 -o $IFEXT -j MASQUERADE
iptables -t nat -A POSTROUTING -s $VLAN50 -o $IFEXT -j MASQUERADE

# (2) se establecen politicas "drop" por defecto, es decir solo lo que se
autorice
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

echo "Reglas aplicadas correctamente!"
```

### 3.5.4 SEGURIDAD EN LA RED INTERNA

En la fase anterior se implementó herramientas para la protección del área perimetral mediante *iptables*. A pesar de ello, no por el hecho de haber establecido protecciones en la capa perimetral de una red significa que el servidor, puestos de usuarios y los propios usuarios estén a salvo de ataques. Ahora llega el turno de establecer algunas medidas de protección área la red interna, zona en la que la mayoría de las ocasiones las brechas de seguridad o ataques viene dados por suplantaciones de identidad.

#### A.- ICMP REDIRECT

El protocolo ICMP, *Internet Control Message Protocol,* es utilizado con diferentes finalidades para el control y notificación de error del protocolo IP. Entre los tipos de mensajes de ICMP más conocidos se encurtan los usados para completar un *ping, icmp request* e *icmp reply,* o por ejemplo el *time exceded* cuando el *TTL* de un paquete ha expirado en tránsito, etc.

Sin embargo, existe un tipo de mensaje ICMP que puede resultar muy atractivo y de gran utilidad a un atacante a la hora de desplegar un ataque. Se trata de *icmp redirect*, un mensaje ICMP de tipo 5 que permite modificar la tabla de ruta de una máquina victima con la finalidad de redirigirla hacia otros destinos en beneficio del atacante. Es posible hacerlo para una red entero o subred o a su vez dirigirlo a un host en particular. Obviamente es el uso que le daría un atacante, pero existen este tipo de mensajes ICMP para manejar la conectividad en deres congestionadas, respetar la latencia de servicios en función de *ToS o Type of Service* encontrando nuevas rutas.

**Ejemplo de ICMP Redirect malicioso**

Existen varias herramientas con las que un atacante puede realizar un ataque ICMP Redirect, pero la que veremos a continuación es ***hping3.*** Dicha herramienta está disponible en los repositorios oficiales de las distribuciones y su instalación es extremadamente sencilla.

En este escenario el atacante va a redirigir los paquetes hacia la IP destino 8.8.8.8 desde la IP origen de host victima 192.168.30.56, para que pasen por la IP asignada a la máquina del atacante que será la 192.168.30.53. Es decir, en lugar de que las peticiones hacia la dirección indicada salgan directamente por la IP de la puerta de enlace de la víctima, pasarán en su lugar por la 192.168.30.53. Para ello, el atacante lanzaría el ataque del siguiente modo:

```
# hping3 -c 1 -C 5 -K 1 -a 192.168.30.1 --icmp-ipdst 8.8.8.8 --
icmp-gw 192.168.30.53 --icmp-ipsrc 192.168.30.56 192.168.30.56
```

La IP 192.168.30.1 es la IP de la puerta de enlace que está suplantando para que la máquina victima acepte la redirección. De igual modo, el atacante debe haber configurado la máquina en modo router, incluso con una regla de salida *NAT* para enmascarar los paquetes y poder visualizar las respuestas del host destino, además de deshabilitar el envío de redirecciones. Resulta necesario realizar este último paso para que la máquina del atacante no envíe un *icmp redirect* a la víctima indicando que el mejor camino para llegar a las 8.8.8.8 es la ip 192.168.30.1

**Protección frente a ICMP Redirect**

Para proteger el servidor de este tipo de ataques, es posible configurar el servidor de forma local para evitar que los mensajes *icmp redirect* surtan efecto. Consiste en modificar un fichero con 0 ó 1:

```
# /proc/sys/net/ipv4/conf/all/accept_redirects
```

Con valor 1 se aceptarán redirecciones por ICMP y serán descartadas cuando el valor sea 0. en la mayoría de las distribuciones en la actualidad vienen con el valor en 0 por lo que las maquinas estarán protegidas por defecto. A pesar de ello es necesario conocer la configuración de este parámetro para establecer un grado más de seguridad en entornos Linux.

**B.-VLAN (Virtual Local Area Network)**

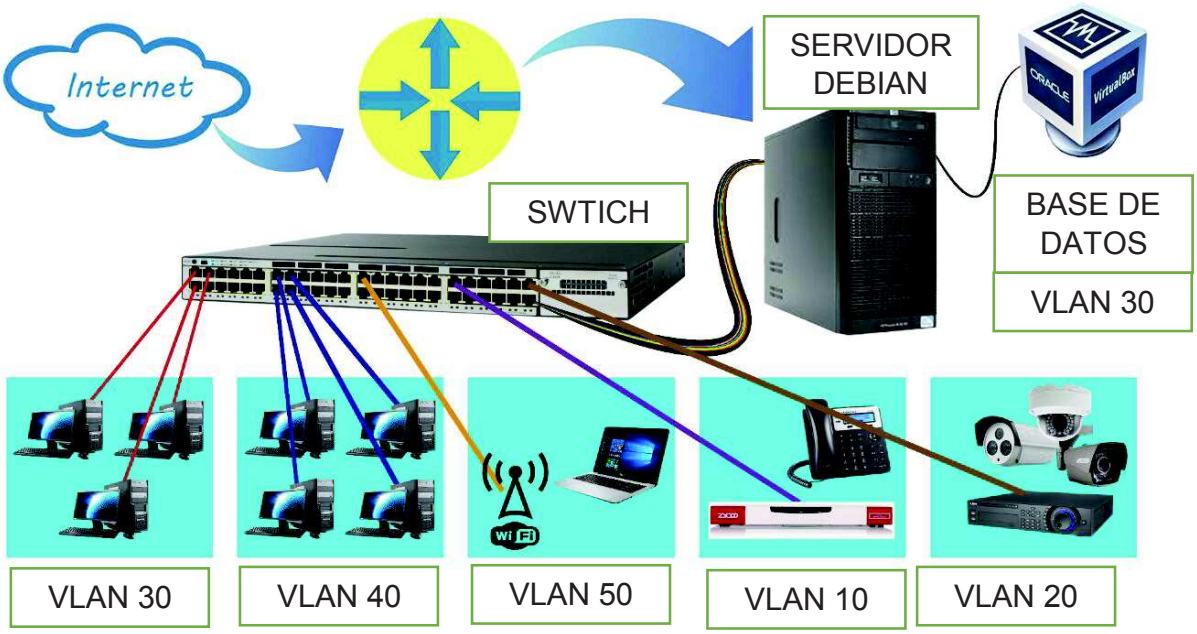


*Ilustración 27: Diseño de red ALLCOMPU*

*Fuente: Alberto Morán*

Cuando existen redes formadas por varias computadoras o máquinas resulta necesario realizar una correcta división o segmentación de la misma. Ello evitará problemas de rendimiento, seguridad y gestión de la propia red entre otros aspectos. Puede que, en la mayoría de los casos esto requiera de un elevado número de elementos o dispositivos electrónicos de red para llevarlo a cabo, router para separación de redes, firewalls, interfaces, etc.

Una *VLAN,* Virtual LAN, no es más que le concepto de una red virtual. Las VLAN se utilizan para crear diferentes redes lógicas a nivel de capa 2 (switch) en los casos que estos permitan dichas configuraciones. Exiten varios protocolos para implementar soluciones VLAN, pero el estándar es ***802.1q*** que es el más extendido y por lo tanto será el implementado en este caso. Entre algunos usos que se le pueden dar a una VLAN se encuentra:

- Agrupaciones y divisiones de equipos conectados a un mismo switch.

- Separación de telefonía IP y los datos, así como su priorización.

- Aislamiento de zonas, restricciones, etc. Esencial para reducir la zona de impacto

El ***trunking***, que no es más que hacer una boca física del switch pueda transportar tráfico de múltiples VLAN. En esos casos, para diferencias los tráficos de las diferentes VLAN se añaden 4 byts a cada trama. En esos 4 bytes se agrega la siguiente información:

- Prioridad. Define la prioridad de la trama utilizando 3 bits. Acepta valores del 0 al 7, siendo 0 el valor por defecto. Dicho valor corresponde al mecanismo de entrega ***Best Effort***. Para información sobre este aspecto puede consultarse ***CoS, Class of Service.*** No es en absoluto irrelevante teniendo en cuanta que con la técnica de ***trunking*** se comparte el mismo medio físico para el trasporte de varias VLAN.

- CFI. Se trata de un valor de un solo bit utilizado para indicar si se debe descartar la trama en caso de congestión.

- ID. Es la etiqueta que identifica a la VLAN. Su tamaño es de 12 bits y puede tener un valor comprendido entre 0 y 4095. Inicialmente, en un switch des configurado todos los puertos se encuentran en la VLAN 1 por defecto.

- Tipo. Información sobre el tipo de protocolo de red que contiene la trama. Su tamaño es de 32 bits. Un valor podría ser *0x0800* que equivale a IPv4 o bien *0x86DD* para IPv6.

Cuando se utiliza *trunking* resulta necesario utilizar determinadas herramientas y configuraciones en el servidor para interactuar con diferentes VLAN utilizando una sola interfaz física de red. Realmente se terminará trabajando con una serie de interfaces virtuales que corresponderán a cada

una de las VLAN. Es lo que recibe el nombre de interfaz *tagged,* puesto que pertenece a más de una VLAN.

**Configuración de VLAN en Debian GNU/Linux**

Para empezar a utilizar y configurar VLAN en Debian GNU/Linux es necesario averiguar si el servidor Linux es capaz de trabajar con VLAN verificando si dispone del módulo necesario.

```
# modprobe 8021q && OK
```

Como resultado tendremos un OK por parte del servidor, esto indica que el servidor esta preparado para trabajar con VLAN. Ahora solo falta que en cada arranque se cargue en memoria el módulo. Se puede editar el fichero ***/etc/modules*** y agregar el módulo o bien ejecutar la siguiente orden:

A partir de este momento se es libre de elegir cómo se desean

```
# apt-get -y install vlan
```

```
# echo 8021q >> /etc/modules
```

configurar las diferentes interfaces para VLAN. Es posible utilizar el conocido comando ***ip*** para crear interfaces de red virtuales y configurarlas. En este caso en el servidor Debian utilizaremos el paquete *vlan*, instalable desde los repositorios oficiales.

A continuación, una vez que se instalaron paquetes necesarios para vlan, es posible agregar la definición de las interfaces virtuales en el fichero ***/etc/network/interfaces*** o bien lanzar la aplicación ***vconfig*** con los parámetros adecuados. Antes de empezar es necesario saber que la nomenclatura de las interfaces virtuales se suele establecer a ***<interfazFísica>.<vlanID>*** y es como se lo realiza por defecto. Ahora pasamos a configurar las VLAN que serán implementadas en la empresa, por ende, el fichero ***/etc/network/interfaces*** quedaría así:

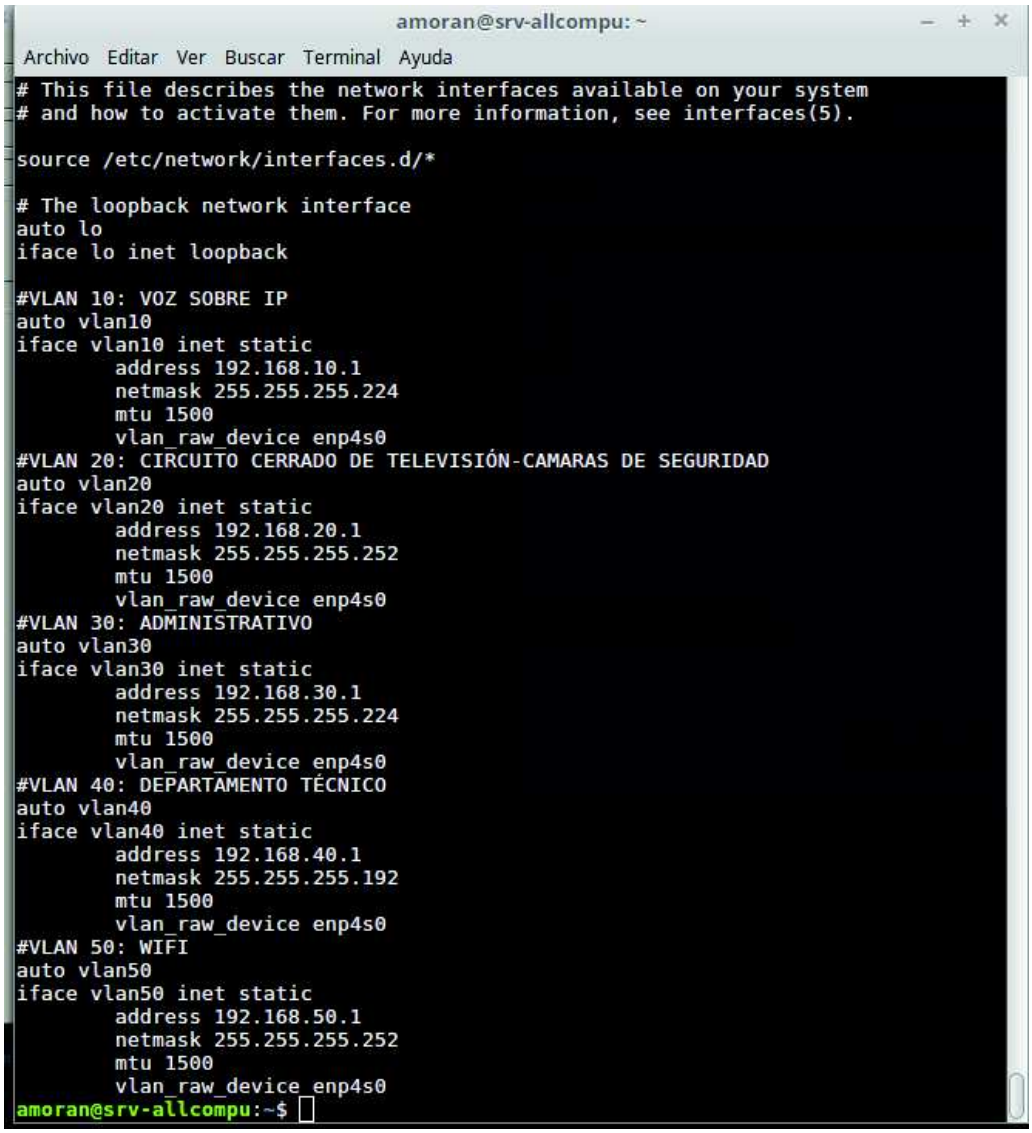


*Ilustración 28: VLANs implementadas en ALLCOMPU*

*Fuente: Alberto Morán*

Es posible visualizar el estado de las interfaces con el comando ***ip addr, ip r, ip link*** o incluso desde el fichero ***/proc/net/vlan/config.***

### C.- Configuración de VLAN en Switch Cisco Catalys WS-C3750X-48P-S

A continuación, veremos la configuración del switch para la segmentación de la red por vlan para cada servicio que se ejecutan en la empresa. Primera mente vamos a crear las vlans con su respectivo VLAN ID

```
SW_ALLCOMPU(config)# vlan 10
SW_ALLCOMPU(config-vlan)# name VOZ SOBRE IP
SW_ALLCOMPU(config-vlan)#exit
SW_ALLCOMPU(config)#vlan 20
SW_ALLCOMPU(config-vlan)# name CCTV
SW_ALLCOMPU(config-vlan)#exit
SW_ALLCOMPU(config)# vlan 30
SW_ALLCOMPU(config-vlan)# name ADMINISTRATIVO
SW_ALLCOMPU(config-vlan)#exit
SW_ALLCOMPU(config)# vlan 40
SW_ALLCOMPU(config-vlan)# name DEPARTAMENTO TÉCNICO
SW_ALLCOMPU(config-vlan)#exit
SW_ALLCOMPU(config)# vlan 50
SW_ALLCOMPU(config-vlan)# name WIFI
SW_ALLCOMPU(config-vlan)#exit
```

Seguidamente pasaremos a configurar el puerto troncal para el enlace entre el switch y el servidor Debian teniendo en cuenta que en el servidor se habilito el estándar IEEE 802.1q

```
SW_ALLCOMPU(config)#interface GigabitEthernet 0/48
SW_ALLCOMPU(config-if)#description PUERTO TRONCAL
SW_ALLCOMPU(config-if)#switchport mode trunk
SW_ALLCOMPU(config-if)#switchport trunk allowed vlan 10,20,30,40,50
SW_ALLCOMPU(config-if)#exit
```

Ahora pasamos a configurar los puertos para cada vlan respectiva, y configuraremos los puertos para que se establezca la conexión enseguida y no pase por el proceso de aprendizaje de Spanning-Tree

```
SW_ALLCOMPU(config)#interface range GigabitEthernet 0/1-10
SW_ALLCOMPU(config-if-range)#description Puerto para vlan 30 Administracion
SW_ALLCOMPU(config-if-range)#switchport mode access
SW_ALLCOMPU(config-if-range)#switchport Access vlan 30
SW_ALLCOMPU(config-if-range)#spanning-tree portfast
SW_ALLCOMPU(config-if-range)# exit

SW_ALLCOMPU(config)#interface range GigabitEthernet 0/11-22
SW_ALLCOMPU(config-if-range)#description Puerto para vlan 40 -Departamento
Técnico
SW_ALLCOMPU(config-if-range)#switchport mode access
SW_ALLCOMPU(config-if-range)#switchport access vlan 40
SW_ALLCOMPU(config-if-range)#spanning-tree portfast
SW_ALLCOMPU(config-if-range)# exit

SW_ALLCOMPU(config)#interface range GigabitEthernet 0/23-30
SW_ALLCOMPU(config-if-range)#description Puerto para vlan 10-Voz sobre IP
SW_ALLCOMPU(config-if-range)#switchport mode access
SW_ALLCOMPU(config-if-range)#switchport access vlan 10
SW_ALLCOMPU(config-if-range)#spanning-tree portfast
SW_ALLCOMPU(config-if-range)# exit
```

```
SW_ALLCOMPU(config)#interface range GigabitEthernet 0/31-33
SW_ALLCOMPU(config-if-range)#description Puerto para vlan 50 - WIFI
SW_ALLCOMPU(config-if-range)#switchport mode access
SW_ALLCOMPU(config-if-range)#switchport access vlan 50
SW_ALLCOMPU(config-if-range)#spanning-tree portfast
SW_ALLCOMPU(config-if-range)# exit

SW_ALLCOMPU(config)#interface range GigabitEthernet 0/35-37
SW_ALLCOMPU(config-if-range)#description Puerto para vlan 20 - CCTV
SW_ALLCOMPU(config-if-range)#switchport mode access
SW_ALLCOMPU(config-if-range)#switchport access vlan 20
SW_ALLCOMPU(config-if-range)#spanning-tree portfast
SW_ALLCOMPU(config-if-range)# exit

SW_ALLCOMPU(config)#interface range GigabitEthernet 0/11-22
SW_ALLCOMPU(config-if-range)#description Puerto para vlan 40 -
Departamento Técnico
SW_ALLCOMPU(config-if-range)#switchport mode access
SW_ALLCOMPU(config-if-range)#switchport access vlan 40
SW_ALLCOMPU(config-if-range)#spanning-tree portfast
SW_ALLCOMPU(config-if-range)# exit
```

**D.- Configuración de router Tenda Current System Version: V11.13.01.06_en**

Veremos configuración de seguridad para la red inalámbrica.

En la siguiente imagen veremos la configuración de la ip que hará de WAN ara la conexión inalámbrica, la cual es proveída por la vlan 50 que se creó anteriormente.

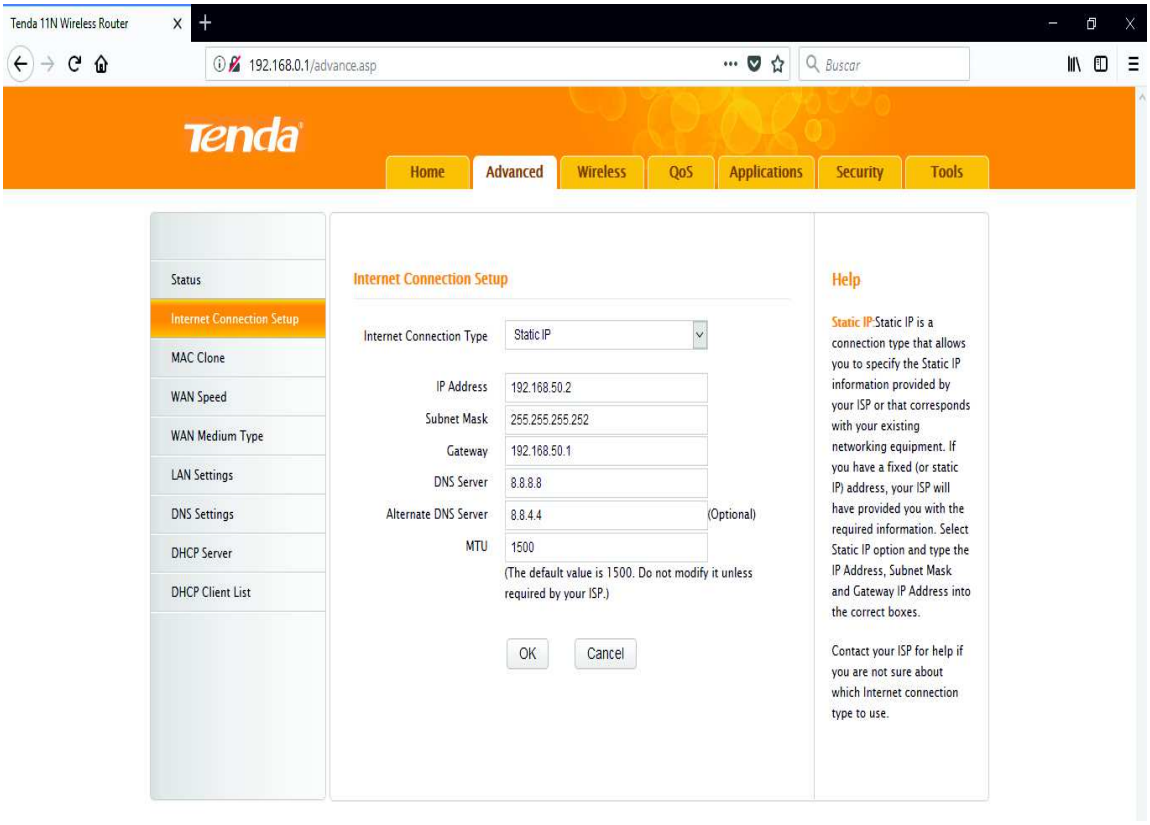


*Ilustración 29: Configuración de la WAN*

*Fuente: Router Tenda*

A continuación, establecemos el SSID (nombre a mostrar en el espectro) de la empresa, siguiente es establecer en modo de Access Point. Luego establecemos los estándares con los cuales va trabajar, El estándar IEEE 802.11 define el uso de los dos niveles inferiores de la arquitectura o modelo OSI (capa física y capa de enlace de datos), especificando las normas de funcionamiento de una red de área local inalámbrica (WLAN). La

primera versión de la norma se publicó en 1997 por el Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos) o IEEE, el cual actualmente se encarga de su mantenimiento. Las especificaciones de este estándar proporcionan la base para los productos con redes inalámbricas que hacen uso de la marca Wi-Fi.

Luego habilitamos el parámetro de propagación en el espacio el SSID previamente configurado, luego establecemos el canal en el cual va a trabajar la WLAN, se estableció el Channel 11 debido a que en los alrededores de la empresa hay mas de dos redes inalámbricas cercas y están en canales 1 y 6 por lo cual para no solapar el radio de propagación de las ondas radioeléctricas emitidas por el equipo.

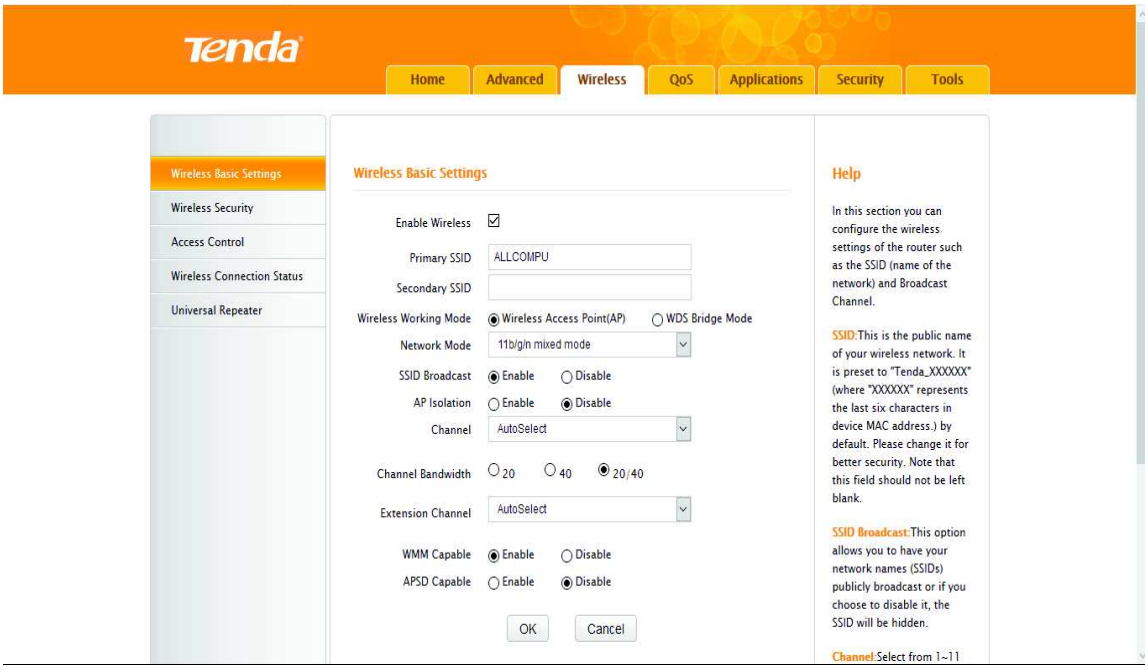


*Ilustración 30: Parametros generales del WLAN*

*Fuente: Router Tenda*

Si queremos aumentar la seguridad de nuestra red wifi podemos usar WPA2-PSK, que es un protocolo de encriptación más robusto que WEP. Básicamente, la diferencia entre un protocolo y otro es que WPA2-PSK soporta una clave de hasta 63 caracteres alfanuméricos, y además, a partir

de la pre-shared key que le introducimos, el sistema va generando nuevas claves que transmite al resto de equipos, lo cual dificulta la acción de descifrado. Hay programas capaces de esnifar el tráfico generado en una red encriptada con WEP y a partir de un volumen de datos (sobre los 4 gb) son capaces de descifrar nuestra clave.

Si sustituimos WEP por WPA2-PSK lo que hacemos es cambiar de clave automáticamente cada poco minuto, lo que supone un plus de seguridad importante.

Para configurar estas opciones, vamos a la parte de Wireless->Wireless Security y establecemos el modo de seguridad y seleccionamos el algoritmo de encriptación para la contraseña. Seguidamente establecemos la contraseña que permitirá la autenticación entre dispositivos. Y para finalizar esta configuración deshabilitamos WPS (Wifi Protected Setup) ya que esta reduce el riesgo de que pueda ser vulnerada la seguridad que hemos empleado, wps es un método de conexión inalámbrico inseguro ya que es por medio de PIN de 8 dígitos que puede ser averiguado de varias formas, por lo cual desactivar este parámetro nos da un plus de seguridad a la red.

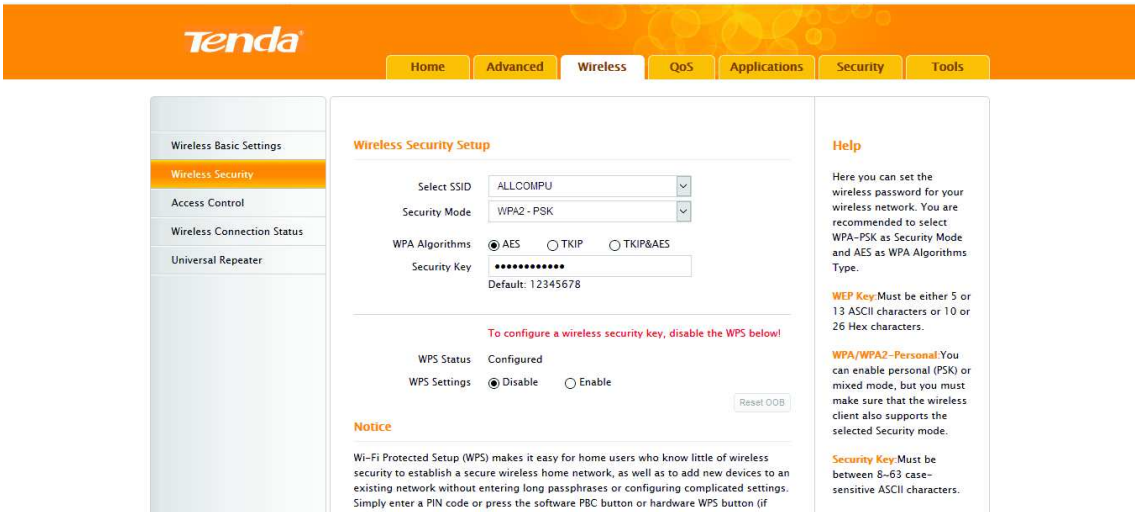


*Ilustración 31: Seguridad de conexión a red WIFI*

*Fuente: Router Tenda*

Asegurando más el acceso a la red mediante el medio inalámbrico estableceremos el acceso el filtrado por MAC, que permitirá mayor seguridad a la red.

En Wireless->Access Control, seguidamente, permitimos solo las MAC address que establecemos.

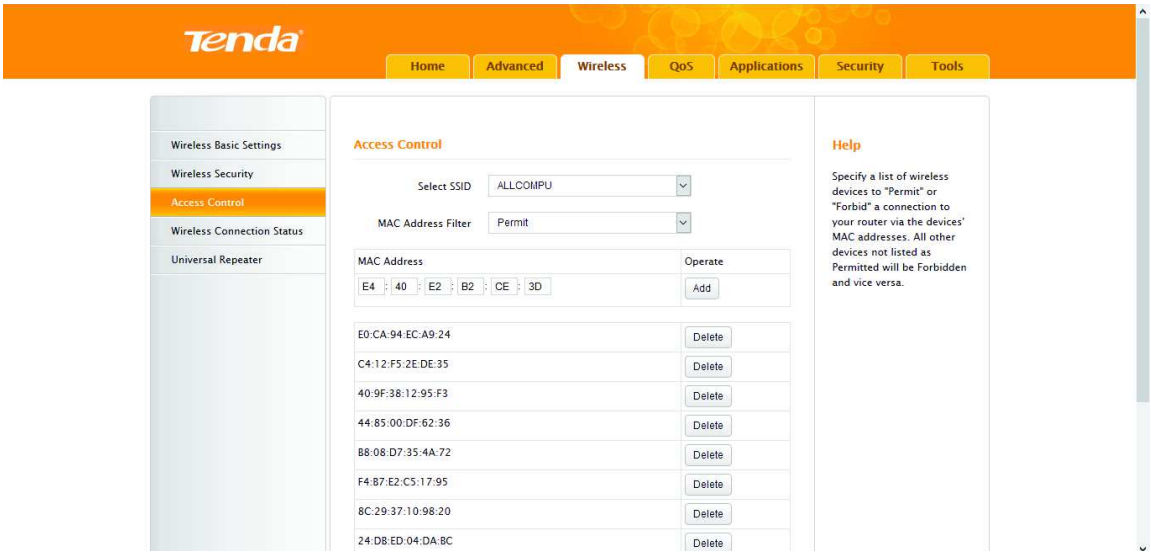


*Ilustración 32: Reserva de MAC*

*Fuente: Router Tenda*

A continuación, estableceremos anchos de bandas para un rango de direcciones IPs, de tal manera que ayudara a la fluidez del tráfico interno y el direccionado hacia la internet.

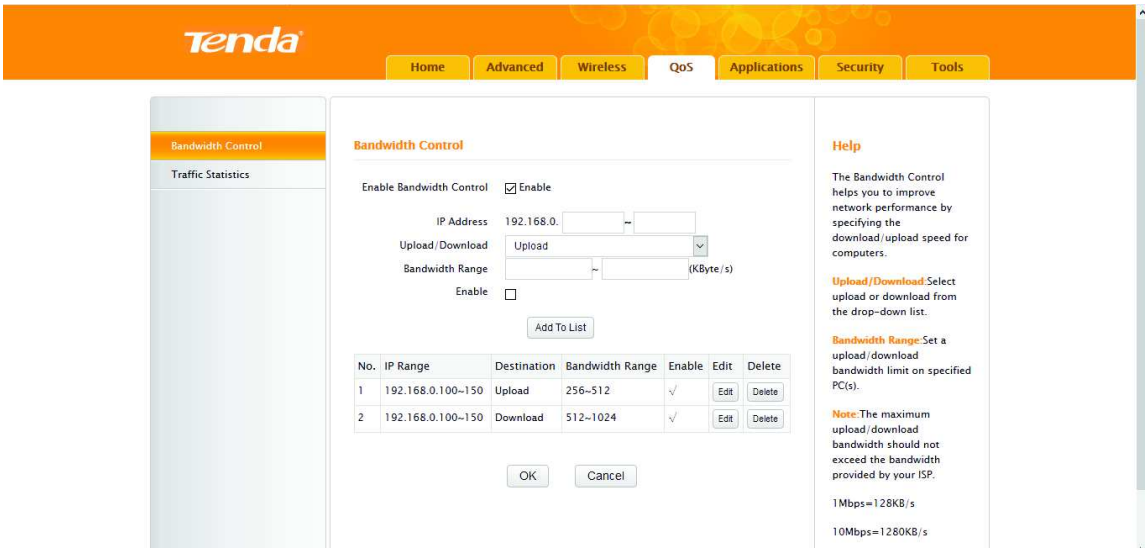


*Ilustración 34: Estableciendo ancho de banda*

Ahora configuraremos el acceso a la configuración del equipo de manera remota, mediante una dirección ip y un puerto específico. En este caso la dirección ip que va a poder hacer cualquier configuración de manera remota es 192.168.30.22 y el puerto que esta a la escucha es el 8789.

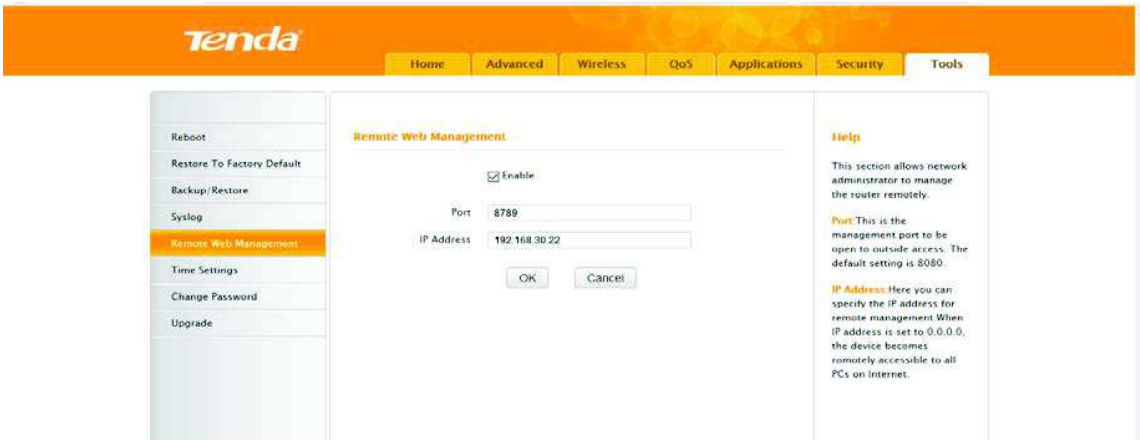


*Ilustración 35: Acceso remoto vía web*

*Fuente: Router Tenda*

**E.- ZYCOO CooVox IP Phone System**

El sistema de teléfono IP de la serie CooVox es la solución más innovadora para telecomunicaciones VoIP en el mercado SMB (pequeñas y medianas empresas). Proporcionan no solo las funciones PBX (Private Branch Exchange) tradicionales como asistente automático y correo de voz, sino que también ofrecen muchas funciones avanzadas de telefonía, incluyendo extensiones remotas, conexión de oficina remota, IVR, grabación de llamadas, registros de detalles de llamadas (CDR) ... Todo esto puede servir para mejorar operaciones comerciales con menos costo de operación.

A continuación, pasaremos a configurar algunos parámetros que ayuden al aseguramiento de la central y de la comunicación.

Cabe decir, que en este proyecto no se verá la configuración de la PBX como tal, extensiones, rutas de llamadas, etc. Será únicamente parámetros de seguridad.

Para acceder a la PBX lo haremos mediante una dirección IP establecida en el segmento de la VLAN de Voz Sobre IP 192.168.10.0/26. Recordando esto, la dirección ip de la PBX es 192.168.10.2 y para acceder vía HTTP el puerto de escucha es el 5687 por lo tanto para ingresar lo hacemos de la siguiente manera. http://192.168.10.2:5687.

El usuario y contraseña por defecto es admin para ambos campos, aquí cambiaremos esos parámetros.

Dentro del apartado de Security, encontraremos el parámetro Service, en el cual estableceremos un puerto de escucha para HTTP, el puerto es 5687, ya que el puerto por defecto es 9999. A su vez deshabiltaremos los servicios SSH y FTP para acceder a la PBX y cargar archivos de configuración respectivamente.

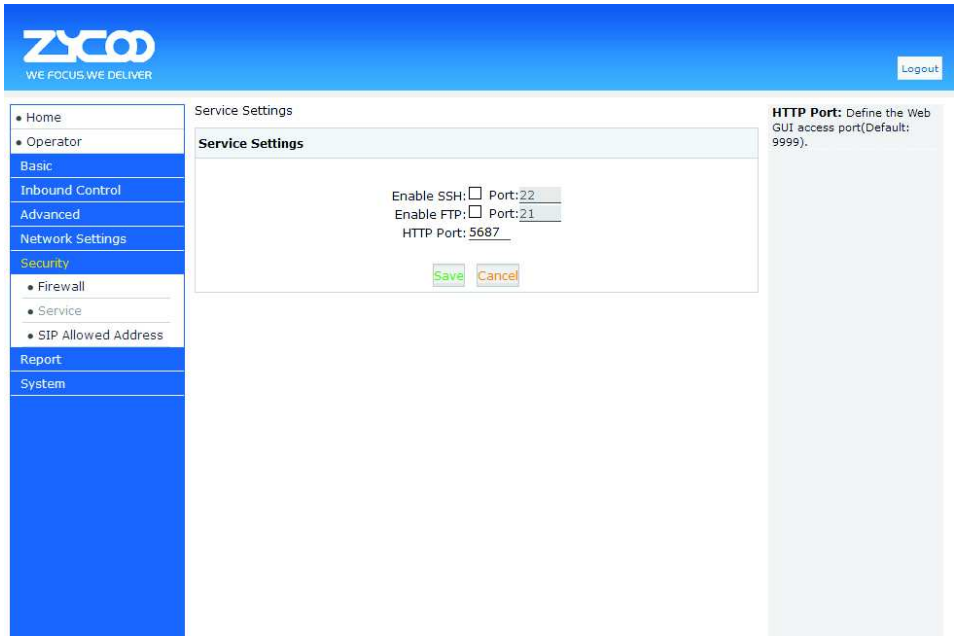


*Ilustración 36: Cambiando puerto HTTP para la PBX*

*Fuente: PBX Zycoo*

Siguiendo con medidas de seguridad, pasaremos a configurar el Firewall interno de la PBX. Configuraremos reglas que permitan asegurar los puertos de comunicación entre las extensiones y la PBX. Deshabilitaremos las respuestas la protocolo icmp para cualquier dirección que quiera hacer algún tipo de prueba de actividad con la PBX.

Así mismo, protegeremos los puertos de registro de las extensiones hacia la PBX, el puerto 5060 con el protocolo udp permitirá un máximo de paquetes de 100 y un intervalo de tiempo de 60 segundos, el puerto 5061 con el protocolo TCP permitirá un máximo de paquetes de 80 y un intervalo de tiempo de 2 segundos.

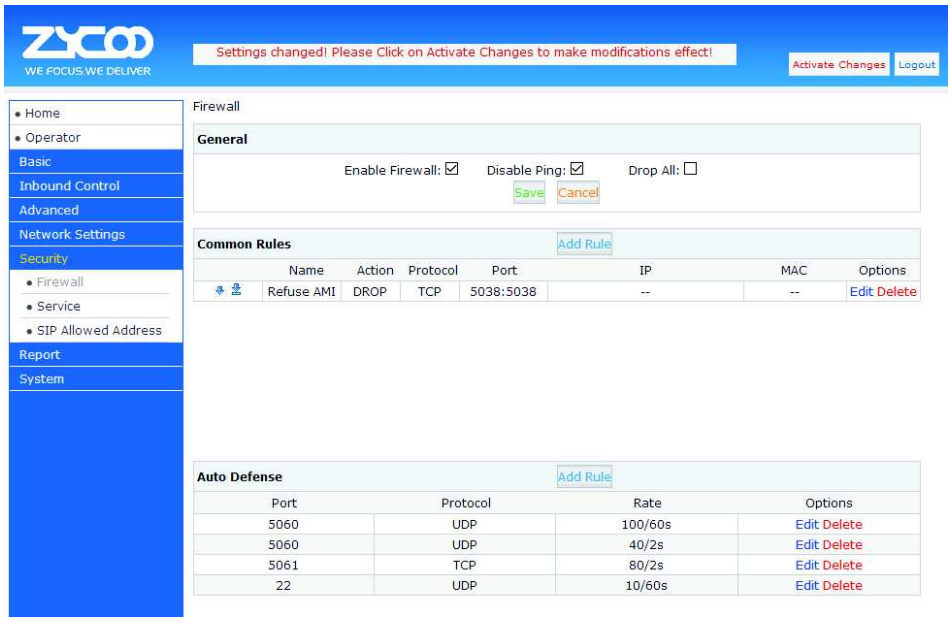


*Ilustración 38: Firewall interno de la PBX*

*Fuente: PBX Zycoo*

Ahora pasaremos a establecer las IPs permitidas para establecer comunicación con la PBX.

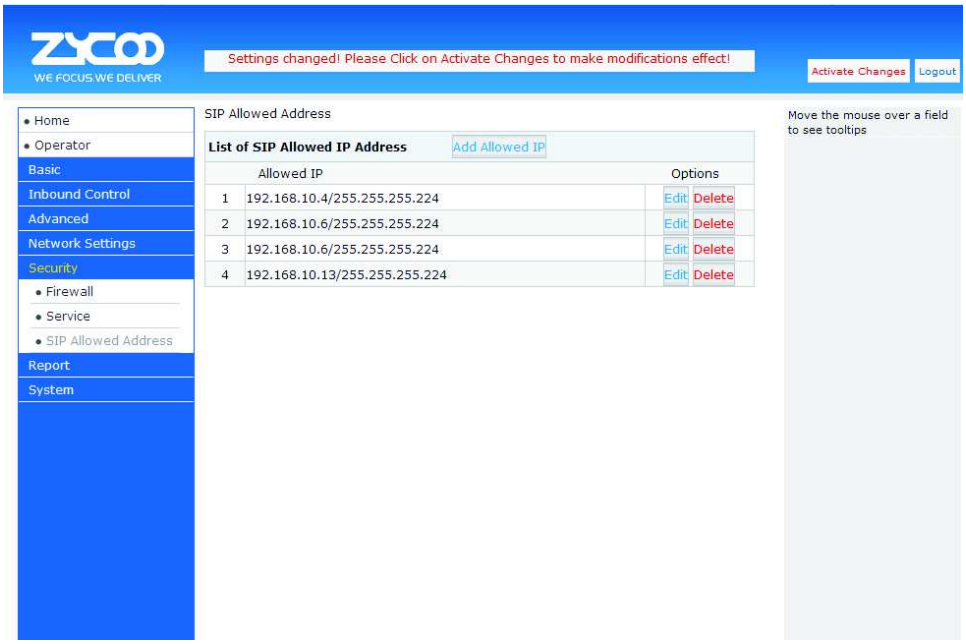


*Ilustración 37: Ips permitidas por la PBX*

*Fuente: PBX Zycoo*

### 3.5.5 SEGURIDAD A NIVEL DE SERVIDOR

#### A.- FORTIFICACIÓN Y SEGURIDAD EN SSH

SSH, Secure Shell, es uno de los protocolos más interesantes que se dispone para la administración del servidor de manera remota, y además de manera segura. SSH es el nombre que recibe tanto el protocolo como la aplicación que lo implementa. Su principal función es acceder a máquinas remotas a través de las redes, proporcionando al administrador una gestión completa de los equipos remotos mediante túneles SSH, es decir, seguros.

SSH utiliza un intercambio de claves basado en el protocolo criptográfico de *Diffie-Hellman.* Este protocolo es imprescindible para la construcción de la capa de transporte segura. SSH es un protocolo que proporciona una capa importante de seguridad para los administradores, pero en función de la configuración del servicio puede llevar al sistema a un estado de inseguridad. Es importante entender el funcionamiento del protocolo, las funcionalidades que presenta y la configuración óptima en función de las necesidades de la empresa.

**Funcionamiento del protocolo**

En la siguiente figura se puede visualizar como en primer lugar se realiza la conexión mediante TCP, realizando el ***three-way handshke*** o saludo de tres vías (***SYN, SYN+ACK, ACK***). Después de abrir la conexión, cliente y servidor se envían la versión disponible del protocolo. Actualmente existen dos versiones del protocolo SSH, la versión 1 y la 2. La versión 1 es totalmente desaconsejable, ya que se han encontrado fallos de seguridad. Después de enviarse la versión del protocolo disponible, se utiliza la clave pública y privada ***RSA***, ***Rivest Shamiry Adleman.*** El servidor envía la clave pública de host al cliente para que este pueda cifrar lo que necesite enviar al servidor en un instante posterior. El cliente comparará la clave pública de

host con la que tenga almacenada del servidor en archivo ***known_hosts,*** en la ruta ***$HOME/.ssh***.

Una vez que el cliente dispone de la clave pública de *host* del servidor, este generará una clave de sesión aleatoria y seleccionará un algoritmo de cifrado simétrico. Con esta clave de sesión, la cual por defecto se regenerará cada 3600 segundos, se cifrará el túnel. El cliente enviará un mensaje conteniendo la clave de sesión y el algoritmo seleccionado, esta información viajará cifrada con la clave pública de *host* al servidor usando el algoritmo *RSA.* En este instante, el resto de la comunicación se utilizará el algoritmo de cifrado simétrico y la clave compartida de sesión, ya que este método es más rápido para cifrar y descifrar, pero debe ser usado primero el protocolo

*Diffie-Hellman* para poder enviar de manera segura la clave compartida de sesión.**Implementando SSH, primera conexión**

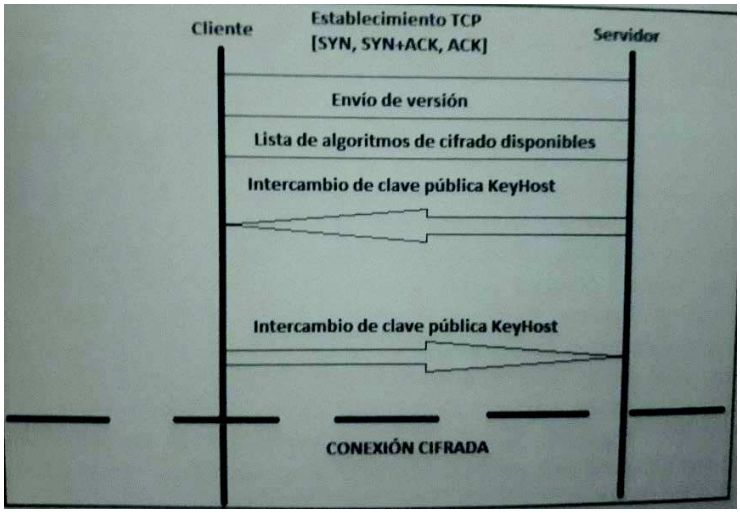


*Ilustración 39: Estableciendo la conexión mediante el protocolo SSH*

*Fuente: Hardening de servidores GNU/linux*

Para instalar en el servidor Debian GNU/Linux el protocolo SSH y realizar la primera conexión, es necesario ejecutar la siguiente instrucción al servidor **[*sudo*] apt-get install openssh-server** *y la configuración del servicio se llevará a cabo en los archivos alojados en la ruta /***etc/ssh.**

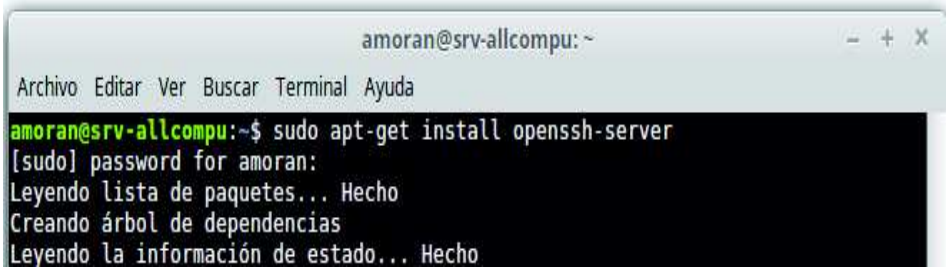


*Ilustración 40: Instalación de servicio SSH*

*Fuente: Alberto Morán*

Para poder iniciar una sesión remota se debe disponer de una cuenta de usuario en el sistema con el cual que va a trabajar. Para realizar la conexión se ejecutará la siguiente sintaxis ***ssh usuario@ip-o-dominio.***

Por defecto el servicio SSH se ejecuta por defecto en el puerto 22 del servidor. Pero en esta implementación por seguridad cambiaremos el puerto a uno por encima del puerto 2048, entonces para iniciar la sesión habiendo cambiado el puerto se utilizará el *flag -p* de la siguiente manera ***ssh -p <puerto> usuario@ip***

**Configuración del servicio**

Existen, principalmente, dos conjuntos de archivos de configuración. Todos se encuentran en la ruta */etc/ssh*, pero el primer conjunto corresponde a la configuración de las aplicaciones cliente como son *ssh, scp, sftp,* y el segundo corresponde a la configuración del servicio o demonio *sshd.*

El servidor o demonio dispone de un archivo de configuración principal /etc(ssh/sshd_config. El cliente dispone de un archivo de configuración el cual se encuentra en /etc/ssh/ssh_config. Es importante notar la diferencia entre ambos, ya que se diferencia en una sola letra. Hay que destacar que, en el caso del cliente, si un usuario dispone de un archivo de configuración en su home, como por ejemplo $HOME/.ssh/ssh_config, será este último archivo del que se cargue la configuración para el cliente y no la que se encuentra en la ruta del servidor /etc/ssh/ssh_config.

**Archivos del servicio**

Antes de empezar a configurar SSH, sobre todo *sshd_config*, veremos una serie de archivos que se debe conocer para el correcto funcionamiento y configuración del servicio.

El primer archivo a tener en cuenta es *moduli*, situado en la ruta */etc/ssh*. Contiene grupos de Diffie-Hellman los cuales son usados para el intercambio de claves, como se mencionó atrás, cuyo procedimiento es imprescindible para la creación de una capa segura de transporte.

Los siguientes archivos referencian a las claves privadas y públicas de host, las cuales son utilizadas para el intercambio de claves. Estas claves se encuentran en el directorio */etc/ssh.*

- **ssh_host_dsa_key** y ***ssh_host_dsa_key.pub.*** el archivo con extensión *pub* se refiere a la clave pública y el archivo sin extensión es la clave privada del *host*. Seutiliza *DSA* por el demonio *sshd.*

- ***ssh_host_rsa_key*** y ***ssh_host_rsa_key.pub.*** clave pública y privada de *RSA* utilizada por el demonio *sshd* en la versión 2 o *SSHv2.*

- ***ssh_host_key*** y ***ssh_host_key.pub.*** Clave pública y privada utilizada por *sshd* en la versión 1 o *SSHv1.*

Cada usuario dispone en su directorio ***$HOME/.ssh*** de una serie de archivos que, después de generarse en alguno caso, se deben conocer.

- ***Authorized_keys.*** Este archivo contiene un listado de claves públicas, para la autenticación contra el servidor de un cliente. Este listado refleja las claves públicas autorizadas por el usuario para ser usadas en su cuenta. Cuando un usuario se

conecta al servidor mediante SSH, y la autenticación elegida es mediante clave pública y privada, se chequea el valor de la clave pública en este listado, si el cliente dispone de la clave privada se autenticará en el sistema.

- ***Known_hosts.*** Este archivo contiene las claves públicas de *host* del servidor de quienes se han conectado al mismo. Este fichero es importante para asegurarse de que el cliente SSH se está conectado al servidor correcto y no a uno suplantado.

- ***id_dsa*** e ***id_dsa.pub.*** clave privada y pública DSA de usuario.

- ***id_rsa*** e ***id_rsa.pub.*** clave privada y pública RSA de usuario para la versión SSHv2.

- ***Identity*** e ***identity.pub.*** calve privada y pública RSA de usuario para SSHv1.

A continuación, pasaremos a configurar el servicio SSH mediante el archivo *sshd_config,* el cual permite configurar el comportamiento del servidor. Este archivo se puede editar mediante cualquier editor de texto y su formato es sencillo.

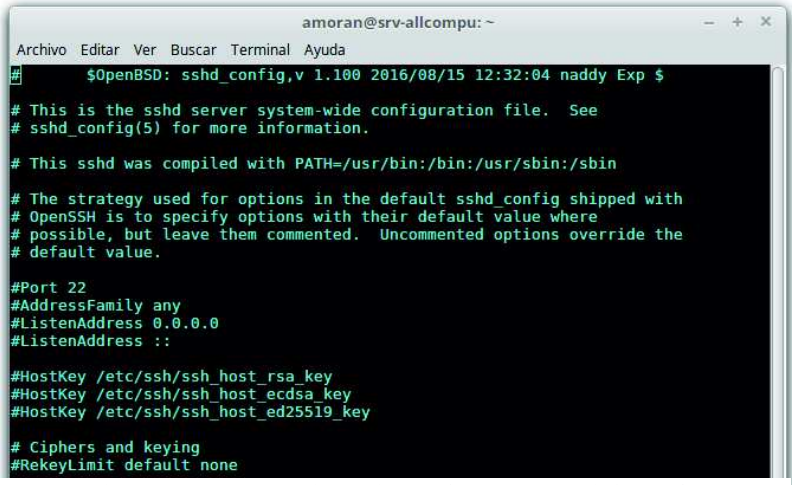


*Ilustración 41: Archivo de configuración sshd_config*

*Fuente: sshd_conf*

El fichero de configuración del cliente es similar al del servidor, aunque dispone de otras directivas. La versión del protocolo, el puerto de conexión por defecto, el listado de algoritmos de cifrado disponible, entre otras opciones.

**Directivas básicas**

En este apartado se especifican las directivas para la configuración y mejora de seguridad en el servidor. A demás, veremos unas directivas interesantes para forzar una mejor de seguridad tanto para el cliente como el servidor.

En primer lugar, veremos el archivo */sshd_config* con este listado de directivas cuya configuración puede provocar la mejora de seguridad del servicio:

- ***Port.*** La directiva *port* indica en que puerto se colocará o está a la escucha el servicio SSH. Por defecto está configurado en el puerto 22, pero esta directiva se puede cambiar por otro puerto. Hay que tener en cuenta que si se comenta la directiva se utilizará el valor por defecto, es decir, el 22. En esta configuración cambiaremos el puerto de escucha por motivos de seguridad interna para evitar escaneos simples por parte de un potencial atacante, cuyo puerto será el 2828.

- ***PermitRootLogin.*** Con esta directiva se prohíbe que un usuario pueda iniciar sesión en el servidor con el usuario *root.* De este modo se evita ataques de *fuerza bruta* al usuario *root*, así por otro método se consigue la clave de *root* no pueda ser utilizada vía SSH.

- ***MaxAuthTries.*** Con esta directiva se evita que los ataques de *fuerza fruta* puedan estar probando indefinidamente

credenciales. Limitar los intentos a un número establecido ayuda a mejorar la seguridad y evitar lo comentado anteriormente. Si una vez superado el número de intentos la conexión se abordará. Para habilitar la directiva se debe especificar o descomentar la siguiente línea ***MaxAuthTries <número intentos>.***

- ***LoginGraceTime.*** Esta directiva indica el tiempo máximo, en segundos, para introducir las credenciales en la autenticación. Por seguridad los tiempos recomendados y que se utilizará será entre 30 o 45 segundos. La sintaxis de la directiva es ***LoginGraceTime <valor segundos>.***

- ***AllowGroups.*** Esta directiva especifica el nombre de los grupos a los que pertenecen los usuarios que pueden iniciar sesión de manera remota hacia el servidor. Los grupos se deben separar por espacios en blanco del siguiente modo ***allowGroups <grupo1> <grupo2> … <grupo N>.***

- ***AllowUsers.*** Esta directiva es similar a la anterior, se puede especificar en el archivo una lista de los usuarios permitidos a iniciar sesión remotamente. Se puede usar metacaracteres, como "*" o "?", lo cual permite la construcción de patrones.

- ***Ciphers.*** Esta directiva especifica que cifrado admitirá la versión del protocolo. Si se especifican varios algoritmos, estos deben ser separados por comas. ***Aes128-cbc,3des-cbc,blowfish-cbs,cast128-cbc,arcfour.***

- ***ClientAliveInterval.*** Esta directiva envía un mensaje al cliente a través del canal, en caso que durante un tiempo X el servidor no recibe datos su sintaxis es ***ClientAliveInterval <tiempo segundos>.***

- ***ClientAliveCountMax.*** Esta directiva tiene relación con la anterior. Se especificará el número de mensajes que el servidor enviará al cliente solicitando respuesta antes de cerrar las conexiones.

- ***TCPKeepAlive.*** Deshabilitar esta directiva permite prevenir ataques de suplantación, ataques de tipo *spoofing.*

- ***DenyUsers.*** Contraria a la directiva de *AllowUsers*, todo usuario que sea especificado en esta directiva no podrá iniciar sesión de manera remota.

- ***LogLevel.*** Esta directiva es interesante para depurar y registrar las acciones que ocurren en el servicio. Los posibles valores son ***QUIET, FATAL, ERROR, INFO, VERBOSE Y DEBUG.*** El predeterminado es *INFO* y se ha de tener cuidado con *DEBUG* ya que viola la privacidad de los usuarios, por lo que no lo implementaremos en esta ocación.

- ***HostKey.*** Esta directiva indica la ruta donde se encutra la clave privada *RSA o DSA* del *host*.

- ***UsePrivilegeSeparation.*** Esta directiva permite la separación de privilegios activada, es decir, divide los procesos del servidor para prevenir la explotación y la posible escala de privilegios.

- ***Protocol.*** En esta directiva especificamos la versión del protocolo que se utiliza, en este caso solo estará activa la versión 2 del protocolo. Existen configuraciones que reflejan la siguiente directiva ***protocol 2,1*** indicando que si el cliente no dispone de la versión 2 se utilizará la 1. Esto no es nada recomendable por motivos de seguridad ya que la versión 1 se han reportado muchas vulnerabilidades.

- ***PubkeyAuthentication.*** Esta directiva activada con *yes* quiere decir que el servidor permitirá conexiones remotas mediante el método de autenticación mediante el uso de clave pública.

- ***AuthorizedKeysFile.*** Esta directiva indica al servidor donde se encuentran almacenadas las claves públicas de los usuarios. Por defecto, las claves se alamcenan en *$HOME/.ssh/authorized_keys, es decir en %h/.ssh/authorized_keys,* pudiendo ser cambiada esta ruta en el valor de esta directiva.

- ***PasswordAuthentication.*** Por defecto esta directiva viene con valor *yes* entonces el servidor permitirá la autenticación de usuarios mediante contraseña. No es recomendable para entornos bastante críticos, por lo cual para darle mayor grado de seguridad de establecerá como valor *no.*

- ***ListenAddress.*** Esta directiva indica por cual dirección se debe escuchar las peticiones. En esta implementación se dispone de interfaces virtuales VLAN por lo cual se definirán los segmentos de red por los cuales debe escuchar las peticiones. La sintaxis es la siguiente ***ListenAddress <vlan1> … <vlan N>.***

- ***ServerKeyBits.*** Esta directiva indica el tamaño de la clave de sesión. Como recomendación vamos a utilizar un tamaño de clave mayor de 768 bits, que es el valor que se dispone en gran cantidad de versiones de la aplicación. Cambiaremos por un valor como 1024 o 2048 bits.

- ***KeyRegenerationInterval.*** Esta directiva indica el tiempo, en segundos, que transcurrirá hasta que se genere una nueva clave de sesión. Por defecto, se utiliza un valor de 3600

segundo. Este valor es bastante seguro, pero si queremos más seguridad, podemos reducir ese tiempo.

- ***PrintLastLog.*** Con esta directiva habilitada se registra el último inicio de sesión del usuario al servidor.

Una vez las directivas están configuradas se debe reiniciar el servicio mediante el comando ***/etc/init.d/sshd restart***.

A continuación, veremos las directivas a nivel de cliente para mejorar la fortificación del servicio de parte del cliente.

- ***Host.*** En esta directiva se especifica las direcciones del servidor que tiene corriendo SSH.
- ***Port.*** Esta directiva es similar que, en la configuración del servidor, salvo que ahora se indica a que puerto se conectara el cliente por defecto.
- ***Protocol.*** Indica la versión del protocolo SSH, como recomendación especificar la versión 2.
- ***IdentifyFile.*** Indica la ruta y el fichero donde se encuentra almacenada la clave.
- ***PubkeyAuthentication.*** Indica al cliente si se puede autenticar contra el servidor mediante clave pública.
- ***StrictHostKeyChecking.*** Esta directiva define que realizará el cliente al conectarse al servidor del cual no se dispone su clave pública. El valor *yes* hace que se acepte automáticamente la clave recibida, el valor *no* hace que se rechace la clave del servidor, lo que significa que se cierra la conexión, mientras que el valor *ask* hace que se pida confirmación del usuario.

- ***Ciphers.*** Lista de algoritmos de cifrado simétrico que puede utilizar el cliente.

- ***PasswordAuthentication.*** Indica si el cliente puede autenticarse mediante contraseña al servidor.

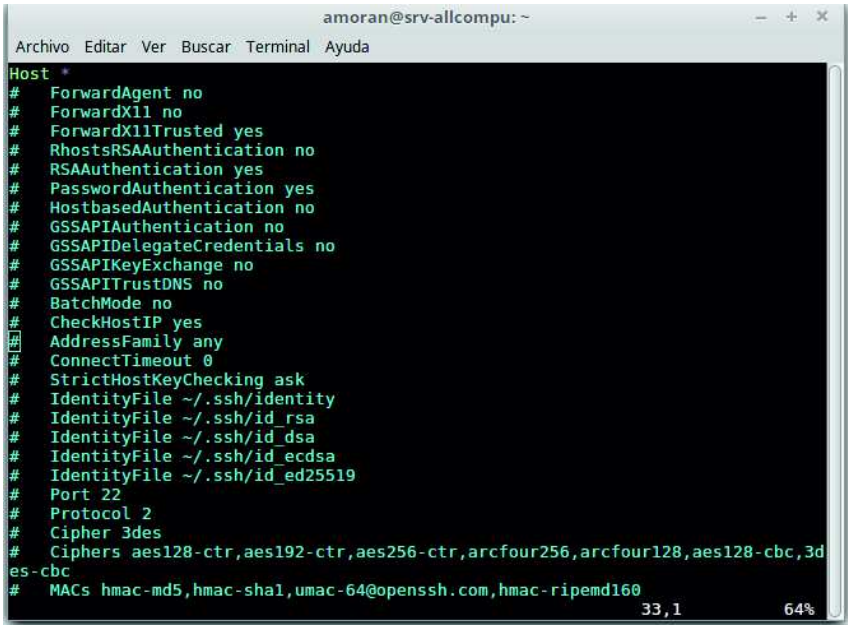


*Ilustración 42: Archivo de configuración del cliente ssh*

**Autenticación con contraseña**

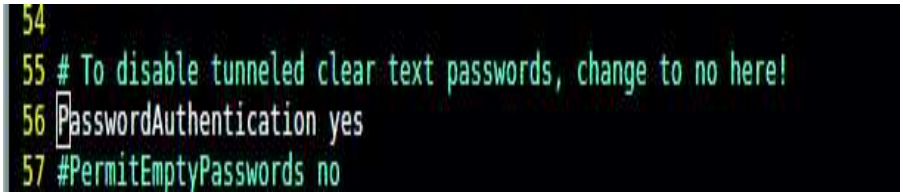


*Ilustración 44: Autenticación por contraseña*

*Fuente: sshd_conf*

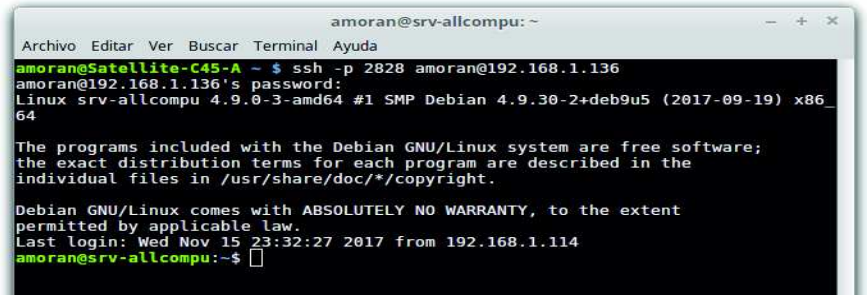


*Ilustración 43: Inicio de sesión por contraseña*

**Clave pública y clave privada**

Este tipo de autenticación es una de las más seguras a la hora de configurar el acceso de los usuarios y permite obtener el máximo partido al servicio SSH. El usuario debe generar su par de claves, privada y pública, compartiendo la clave pública con el servidor para tener acceso mediante este tipo de autenticación. Hay que recordar que un mensaje cifrado mediante clave pública solo podrá ser descifrado con su clave privada.

La clave privada puede tener un segundo mecanismo de seguridad, autenticación multifactor, denominado PIN. Cada vez que se requiera el uso de la clave privada para descifrar el desafío del servidor se solicitará al usuario que posee la clave privada que introduzca el PIN para verificar que posee dicha clave y conoce su PIN para poder utilizarla.

**Generación y autenticación con clave pública**

A continuación, se generará las claves pública y privada de tipo RSA con 4096 bits, para ello ejecutamos el comando ***ssh-keygen -b 4096 -t rsa.*** Se indica el directorio por defecto donde se almacenarán las claves y si se quiere incluir una contraseña o PIN para proteger el uso de la clave privada.

Una vez que se dispone de las clave pública y privada para autenticación del usuario creada, se debe copiar la clave pública en el servidor. La clave se subirá al servidor, y en función de la ruta que se indique en el fichero */etc/ssh/sshd_config* en la directiva *AuthorizedKeysFile*.

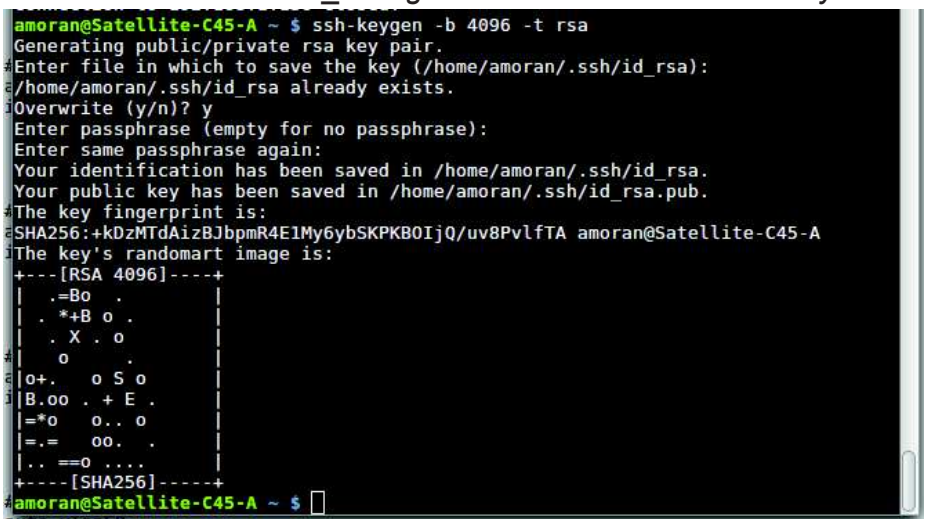


*Ilustración 45: generación de par de claves RSA*

*Fuente: Servidor Debian ALLCOMPU*

### 3.5.6 SEGURIDAD A NIVEL DE APLICACIÓN

El objetivo de este nivel tiene como finalidad tratar de establecer algunas protecciones adicionales en el sistema operativo Linux para fortificar determinados aspectos. La idea principal consiste en configurar de forma adecuada funcionalidades necesarias y comunes en el servidor para mejorar la seguridad. Los temas a tratar variarán desde permisos de ficheros, protección de recursos de usuarios entre otros.

## A.- JAULAS CON CHROOT

El servidor como va a tener administración remota, esta esta expuesta por el simple hecho de publicar algún recurso. A pesar de que se ha realizado una buena configuración mediante las capas anteriores, siempre existe una posibilidad de que algún atacante pueda sacar provecho de alguna situación para comprometer el sistema. Un ejemplo claro es cuando una aplicación tenga un *0-day*. Obviamente, al tratarse de un fallo de seguridad en la aplicación el atacante sabrá como actuar en cada caso, utilizando cualquier tipo de *exploit* que aproveche la vulnerabilidad.

Ahora trataremos el uso de la creación de jaulas para el aislamiento de aplicaciones, usuarios, servicios, etc. A este tipo de acciones, en los que aísla algún recurso por prevención se le conoce también como *sandbox* o caja de arena. Dicho concepto aplicable igualmente al uso de virtualización pues realmente se está aislando la ejecución de un proceso o exposición de sus recursos.

El concepto de enjaular un recurso o acceso se llevará a cabo con la aplicación *chroot* cuyo nombre proviene de *Change root.* Como su nombre lo hace pensar, con chroot se modifica la raíz del sistema, para un determinado proceso, haciéndole creer que realmente esa es la raíz de ficheros del sistema. Esto supone que el proceso ejecutado dentro de una jaula chroot "verá" solo lo que se quiere que vea. Inicialmente la jaula es una caja vacía, sin contenido alguno y será necesario poner en ella los componentes justos y necesarios para permitir la ejecución de una aplicación o comando. Veremos unas recomendaciones de uso antes de configurar:

- Nunca utilizar *chroot* para un proceso ejecutado como *root*. No tiene sentido hacerlo así pues el usuario *root* siempre podrá salir de la jaula al sistema de ficheros real.

- Incluir en la jaula los componentes mínimos necesarios para la ejecución de un proceso.

- Mantener los permisos de los ficheros lo más restrictivos posibles.

**Preparando el entorno**

En primer lugar, es necesario crear un directorio de trabajo para chroot. A este directorio se le suele llamar *fakeroot*. Creamos un directorio */var/newroot*. Y seguidamente debemos crear los usuarios en el sistema.

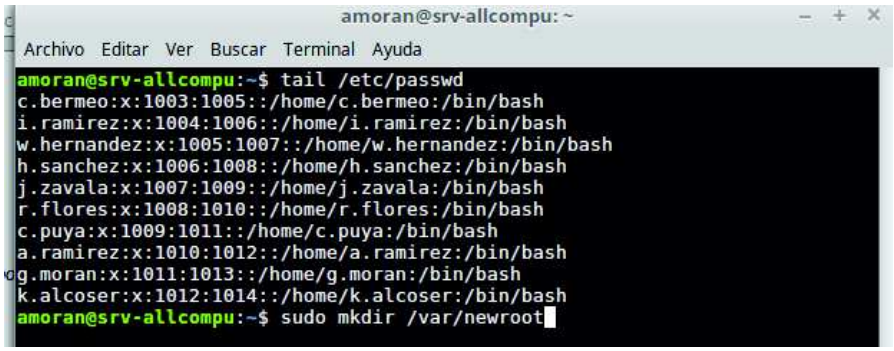


*Ilustración 46: usuarios del sistema*

*Fuente: /etc/passwd*

Hasta este punto la jaula está completamente vacía, por lo que hay que crear una serie de directorios.

Primero se empieza por crear el directorio */bin* para posteriormente copiar el fichero binario *bash* que proporciona la *Shell*. Aunque no es todo, para que *bash* funcione adecuadamente es necesario copiar las bibliotecas compartidas que utilice. Para esto es necesario averiguar dichas bibliotecas con la utilidad *ldd*.

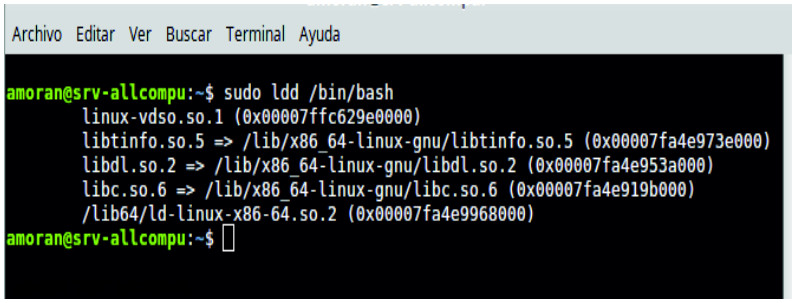


*Ilustración 48: Bibliotecas de bash*

por lo tanto, además de copiar el binario *bash* será necesario incluir la estructura chroot las bibliotecas indicadas por *ldd* par realizar ambas acciones se debe ejecutar las siguientes instrucciones.

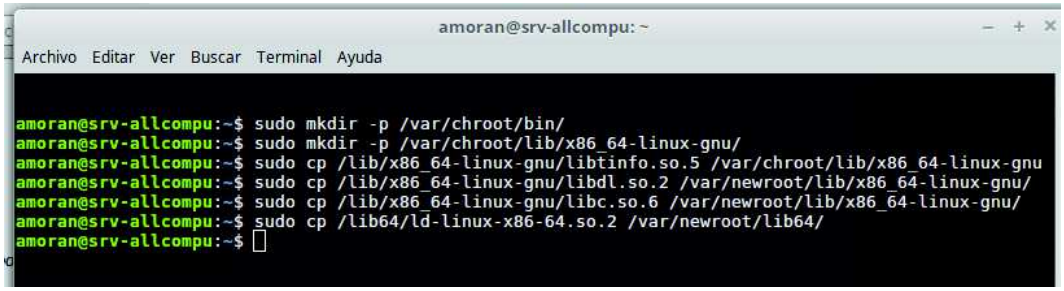


*Ilustración 47: Copiando blibliotecas de binarios*

Ahora que todo está listo, vamos a probar que la jaula nos mostrara un promt. Para ello se utilizará chroot lanzándolo como el usuario c.puya creado anteriormente.

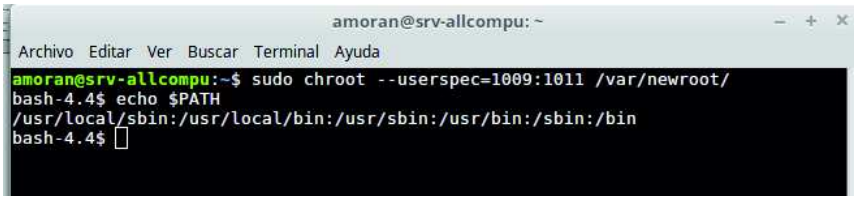


*Ilustración 49: Promt con chroot*

### B.- FAIL2BAN

Esta aplicación desarrollada en el lenguaje *Python* permite la prevención de intrusos en el sistema. Su funcionamiento es penalizar la conexión, ya sea por medio de bloqueo, de un origen que intenta realizar un proceso de fuerza fruta. En otras palabras. Cuando una dirección IP o varias

intentan realizar un ataque de fuerza fruta sobre el servicio SSH. Esta aplicación detectará y penalizará dichos comportamientos.

**Funcionamiento**

*Fail2ban* se encarga de realizar una búsqueda en los *logs* de ciertas aplicaciones, las cuales son especificadas en el archivo de configuración. *Fail2ban* contiene reglas que se han configurado para aplicar la penalización, la cual puede interpretarse como bloqueo de la aplicación en un determinado puerto.

Cuando *Fail2ban* detecta una serie de intentos fallidos, los cuales son predefinidos, la aplicación determina la acción a tomar sobre la dirección IP que provocó dicha situación. Se puede, simplemente, notificar mediante un *email* de lo sucedido, denegar el acceso a la dirección IP, denegarla en determinando puerto y habilitarla en otros, mediante la utilización de *iptables* o el *firewall*.

**Directivas de Fail2ban**

La implantación de *Fail2ban* se realiza a través de los repositorios de las distribuciones de GNU/Linux, por lo que con la ejecución del comando *apt-get install fail2ban* es suficiente para instalar el demonio.

A continuación, directivas más importantes de *Fail2ban* para configurar las reglas necesarias para prohibir el acceso a máquinas que intentan realizar fuerza fruta sobre el servicio SSH.

Las reglas se configuran en el archivo ***/etc/fail2ban/jail.conf.*** La distribución es sencilla, el fichero se divide en áreas. Para las directivas correspondientes con el protocolo SSH se utiliza el identificador [SSH] para señalar en que área se encontrará configurado lo relacionado con dicho protocolo.

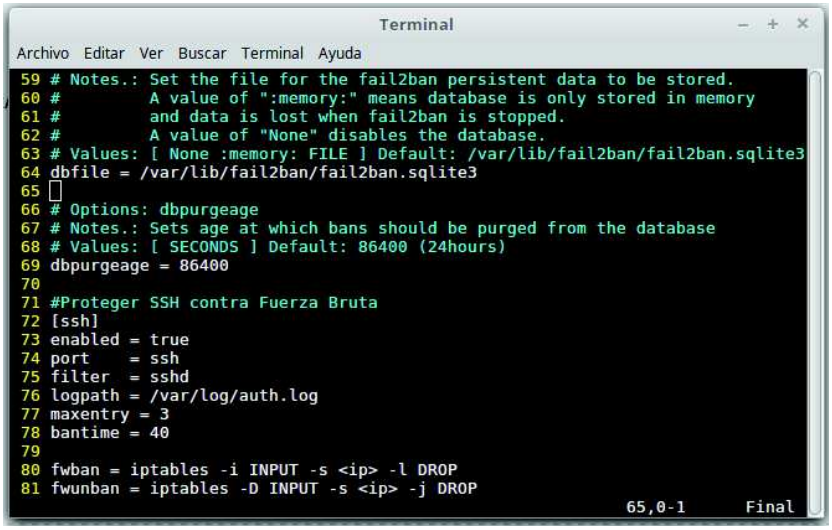


*Ilustración 50: Directivas configuradas de Fail2ban para SSH*

*Fuente: /etc/fail2ban*

La directiva *port* indica el puerto por el cual el servidor SSH está escuchando, la cual por defecto presenta el puerto 22. La directiva *logpath* indica la ruta donde se encuentra el fichero *log* donde *Fail2ban* buscará los intentos de conexión masivos. La directiva *maxretry* indica el número de intentos que puede realizar una dirección IP antes de ser baneada.

La directiva *fwban* indica la acción a realizar cuando se detecte un número, definido por *maxretry,* de intentos. Se podría bloquear el acceso completo al servidor o a determinada aplicación.

La directiva *fwunban* indica la acción a realizar cuando se sobre pase el tiempo de castigo o tiempo de baneo. Generalmente, se eliminan las reglas activadas en el momento de realizar el baneo sobre el cliente.

La directiva *bantime* indica el número de segundos que la dirección IP es baneada de parte del servidor. La directiva *ignoreip* indica una dirección IP o una red que se excluirá del análisis.

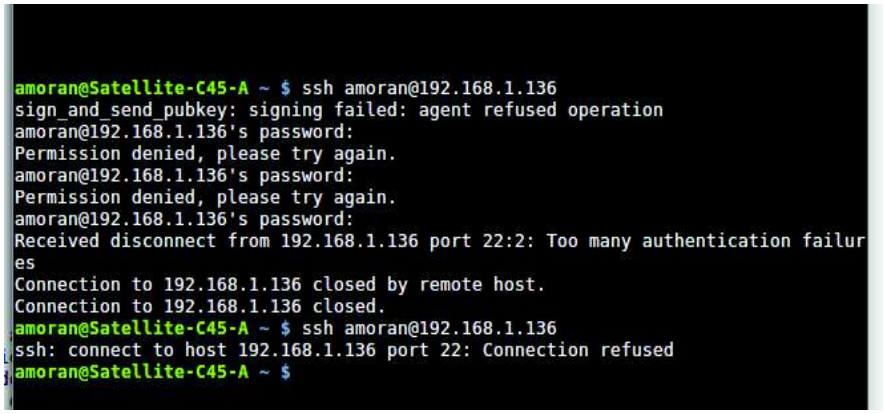


*Ilustración 51: Ip baneada con Fail2ban*

En la siguiente imagen se puede visualizar como queda registrada la IP y la fecha en la que ha sido bloqueada. Este hecho es importante ya que entre más información quede almacenada más sencillo será llevar a cabo un proceso forense sobre lo que ha sucedido.

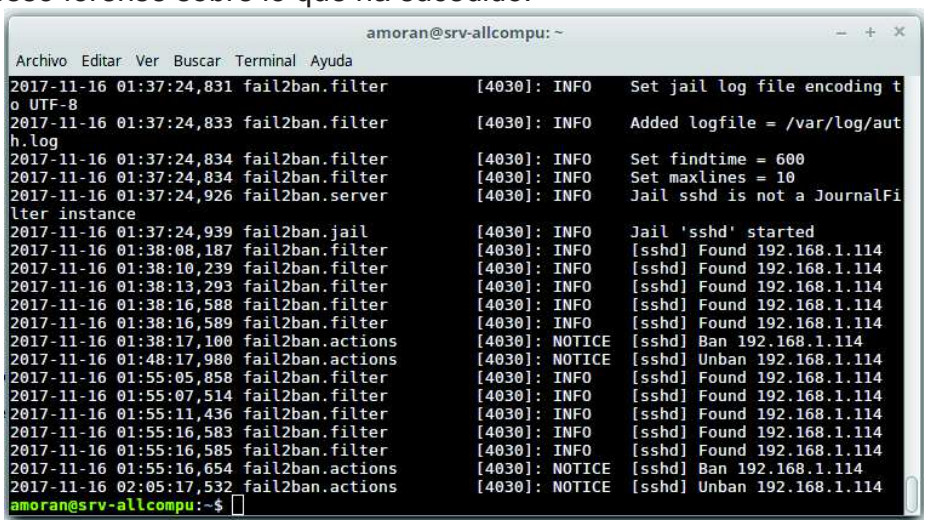


*Ilustración 52: Log de Fail2ban*

### C.- SAMBA

*SAMBA* es un servidor de recursos compartidos que nos brinda la facilidad de compartir dichos recursos con otras plataformas por ejemplo

Windows desde nuestro servidor o entorno GNU/Linux. Esto es de forma casi transparente. De tal manera que no debemos realizar conexiones *sftp* o incluso *ftp* para intercambiar documentos entre los colaboradores de la empresa.

**Instalación**

La implantación de *samba* se realiza a través de los repositorios de las distribuciones de GNU/Linux y otras dependencias.

- ***Samba.*** Servidor de archivos de tipo LanManager para Unix.
- ***Samba-common.*** Archivos comunes de samba utilizados para clientes y servidor.
- ***Smbclient.*** Cliente simple tipo LanManager para Unix.
- ***Samba-doc.*** Documentación de samba.
- ***Smbfs.*** Comandos para montar y desmontar unidades de red samba.
- ***Winbind.*** Servicio para resolver información de usuarios y grupos de servidores Windows

Instalaremos los paquetes necesarios para samba.

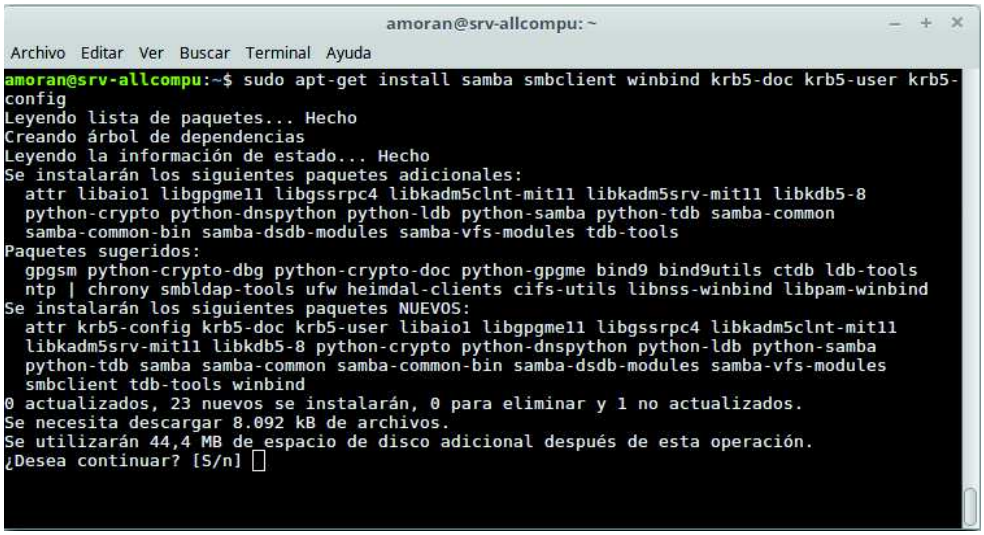


*Ilustración 53: Instalación de Samba*

### Configuración de entorno

A continuación, crearemos todos los usuarios de la empresa que tendrán acceso a los recursos compartidos en la red Windows con sus respectivos permisos.

```
# useradd a.moran
# passwd a.moran
# smbpasswd -a a.moran
# mkdir <ruta/recurso/compartido>
# chown DepTecnico <ruta/recurso/compartido>
```

La orden *useradd* crea un nuevo usuario al sistema, por lo consiguiente la orden *passwd* establece una contraseña para el usuario que se acaba de crear, *smbpasswd* con el parámetro *-a* se asignará una contraseña para acceder a los recursos compartidos con *samba, mkdir* creará un directorio o el recurso que se va a compartir en la red *samba* y por último *chown* cambiará de propietario al directorio creado.

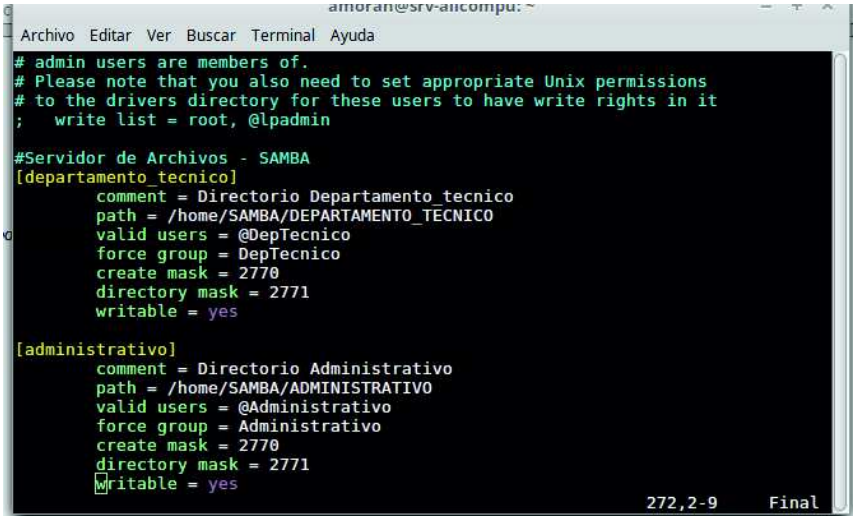


*Ilustración 54: /etc/samba/smb.conf*

**D.- MariaDB**

Cuando se instala el gestor de base de datos en Debian cabe recalcar que por defecto la instalación es bastante segura, sin embargo, a continuación, veremos algunas opciones modificables para aumentar la seguridad.

Existen configuraciones aplicables mediante ficheros y en cambio otras directamente en la base de datos utilizando el cliente *mysql* o bien el comando *mysqladmin*. Las opciones modificables en la propia consola de *MySQL* estarán procedidas por *mysql>,* que es el promt por defecto.

**Dirección escucha**

Se trata de una alternativa que establecida a un valor seguro en la instalación desde Debian. Por defecto MySQL escuchará en local, por lo que no aceptará conexiones que provengan de otras máquinas independientemente de la configuración del firewall. El parámetro es el siguiente:

```
bind-address=127.0.0.1
```

sólo se escuchará en la interfaz con la dirección IP 127.0.0.1, que es *localhost*.

**Carga de ficheros locales**

En las aplicaciones se pueden explotar diversos tipos de ataques, entre ellas SQLi (Inyección SQL), si un atacante descubriese la forma de explotar un SQLi y quisiera acceder a ficheros del sistema, podría obtener información de los archivos accesibles por el usuario que ejecute el servicio MySQL.

Por defecto, desde la consola de MySQL se podría hacer lo siguiente.

```
Mysql> select load_file('/etc/passwd');
------
c.puya:x:1009:1011::/home/c.puya:/bin/bash
a.ramirez:x:1010:1012::/home/a.ramirez:/bin/bash
g.moran:x:1011:1013::/home/g.moran:/bin/bash
------
```

Además de *load_file* exite el método LOAD DATA LOCAL INFILE

Para deshabilitar la carga de ficheros desde MySQL y envitar una posible fuga de información desde el sistema de ficheros mediante SQLi, se debe realizar la siguiente configuración en el fichero */etc/mysql/mysql.conf.d/mysqld.cnf*

```
[mysql]
------
Local-infile      = 0
Secure-file.priv  = /dev/null
```

La configuración anterior fue ejecutada de manera global para todos los usuarios de MySQL. Ahora también se puede restringir el acceso a la carga de archivos por usuario, eso se hace mediante la reducción de permisos de usuario, para eso se revoca el privilegio *file_priv* mediante la siguiente consulta.

```
mysql> select user,host,file_priv from mysql.user
```

**Mysql_secure_installation**

Se trata de un script encargado de asegurar determinados aspectos de MySQL. Buscará usuarios anónimos, establecerá contraseña para el usuario root, eliminará las bases de datos de test, etc. La ejecución de este script es indiferente si es antes o después de ejecutar algún tipo de configuración.

### 3.5.7 SEGURIDAD A NIVEL DE INFORMACIÓN

**CIFRADO DE FICHEROS**

Hasta este momento se ha conseguido cifrar el sistema de ficheros o en otras palabras las particiones que lo contienen. El método resulta efectivo, pero aún puede existir alguna posibilidad más de conseguir acceso a información privilegiada estando físicamente en el servidor.

Esto debido a que en ocasiones se olvida cerrar las sesiones o simplemente no se bloquean. Si se diera este caso, todas las prácticas implementadas hasta el momento serían en vano. Por muy fuerte que sea el cifrado de las particiones y su ***passphrase***, se haya protegido el gestor de arranque, etc. No servirá de nada para esta situación pues el sistema está completamente desbloqueado y funcional.

Existen varios métodos para mitigar estos riesgos, pero en este apartado implementaremos el método para cifrar ficheros o archivos sensibles mediante el uso del GPG, Gnu Privacy Guard.

**Sobre GPG y su modo de funcionamiento**

***GPG, Gnu Privacy Guard,*** es una implementación del estándar ***OpenPGP***, que a su vez nació como versión libre de **PGP, Pretty Good Privacy.** Se encuentra disponible en la mayoría de las distribuciones Linux, al igual está disponible en los repositorios oficiales de cada distribución.

Mediante el uso de la aplicación ***gpg*** se pueden realizar las siguientes acciones:

- Firmado de ficheros mediante el uso de clave privada. Su finalidad consiste en determinar si el fichero firmado pertenece a quien dice ser.
- Cifrado de ficheros mediante el uso de clave pública. Consiste en proteger un fichero cifrándolo por completo haciendo uso de una clave pública.
- Cifrado de ficheros mediante el uso de una ***passphrase***. Es exactamente igual que el caso anterior salvo que se usa cifrado simétrico, Una misma clava para cifrar y descifrar.

La última acción es la más conocida y sencilla de llevar a cabo, pero como contrapartida no resulta tan flexible como su homónima de clave pública.

A continuación, es necesario hacer una introducción al funcionamiento de la criptografía de clave pública.

**Funcionamiento básico de la criptografía de clave pública**

Consiste en un método de por el cual se utilizan un par de claves dependientes una de la otra. En las dos claves están la privada y la pública. Como su nombre lo indica, la pública puede ser accesible por cualquier persona y la privada solo debería estar en poder de la persona a la que pertenezca.

Aunque no es obligatorio, pero si necesario para aumentar el grado de seguridad, la clave privada debe disponer de una ***passphrase*** para desbloquearse su uso. Si cayera en manos no deseadas y no estuviera protegida se podría llevar a cabo una suplantación de identidad y acceso a contenido sensible.

El uso de estas claves, son el de cifrado y firmado de ficheros

**Cifrado y descifrado de ficheros**

La finalidad de cifrar es la de mantener la privacidad de los datos. Puede ser para compartir el mensaje o archivo con una persona o bien para protegerlos en un disco y desbloquearlos cuando sea necesario. El proceso para el cifrado es el siguiente:

A. Se cifra el contenido con la clave pública, porque cualquier persona con acceso a la clave pública puede cifrar el contenido de un mensaje o fichero.

B. El proceso de descifrado se realiza mediante la pareja de la clave pública que ha cifrado el mensaje o archivo. Es decir, es necesario utilizar la clave privada asociada a la clave pública que ha cifrado. Si la clave privada se generó con una ***passphrase*** asociada será necesaria introducirla para acceder al archivo.

**Cifrado simétrico con GPG**

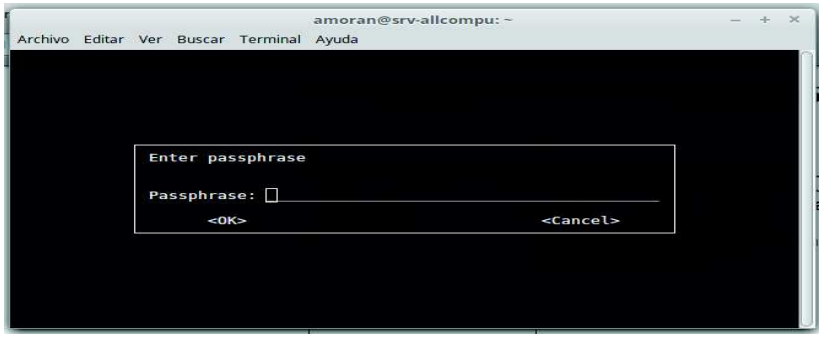


*Ilustración 56: Estableciendo passphrase para el cifrado*

A continuación, haremos el cifrado de un archivo de vital importancia para la empresa (por motivos de confidencialidad con ALLCOMPU, no será mostrado dicho documento original, por lo cual simularemos con un archivo de prueba con datos aleatorios). Para ello se hará uso del cifrado simétrico con ***gpg*** usando el parámetro ***–symmetric.***

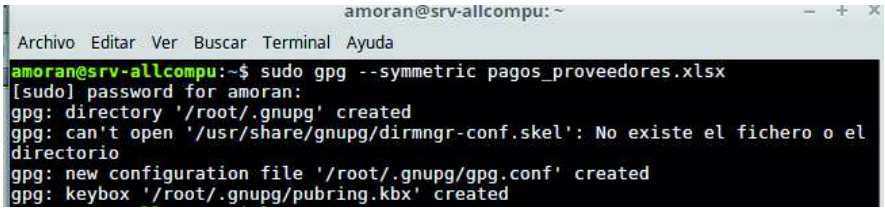


*Ilustración 55: Cifrado de fichero pago_proveedores.xlsx*

El fichero se ha cifrado y se ha generado su versión cifrada con extensión. gpg**.** Obviamente, debe eliminarse el fichero no cifrado para disponer de la copia cifrada únicamente. Si se trata de hacer un volcado al archivo se observa que la salida es “basura” o información aleatoria.

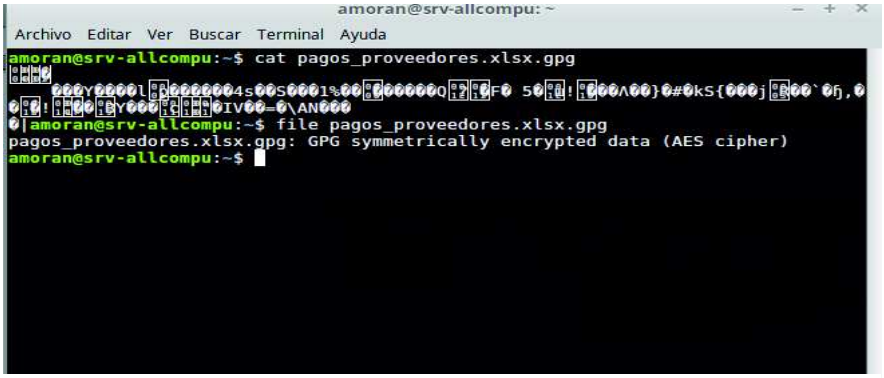


*Ilustración 57: Volcado de fichero pago_proveedores.txt.gpg*

No es posible identificar el tipo de fichero ni visualizar la información que contienen. Para descifrar el archivo se vuelve a usar el comando ***gpg*** pasando los parámetros ***–decrypt y -o.*** Respectivamente para descifrar el archivo y volcarlo en el nombre que se indique.

### Cifrado asimétrico con GPG

A continuación, se realizará el mismo proceso que en el caso anterior salvo que esta vez se usará la implementación de cifrado asimétrico o criptografía de clave pública de ***gpg.***

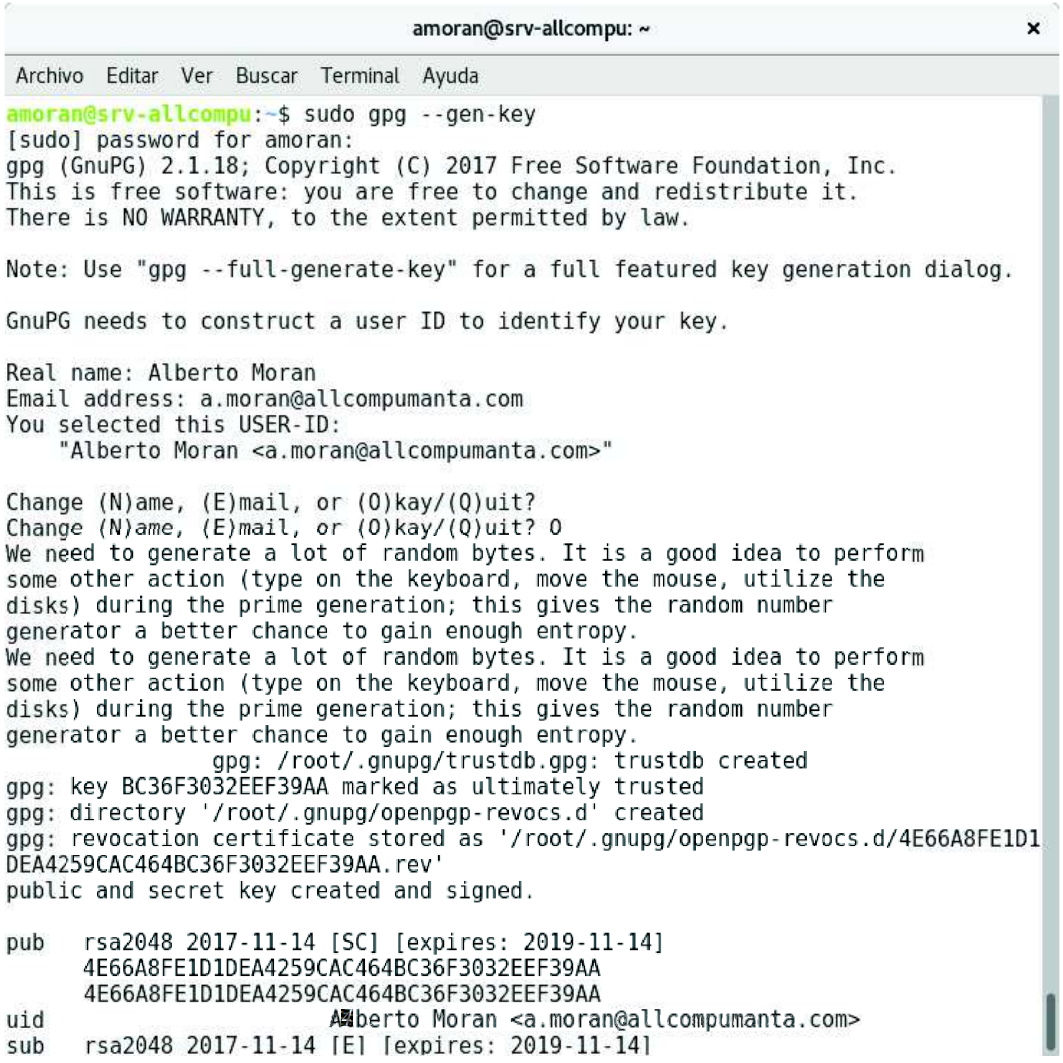


*Ilustración 58: Generación de claves privadas y públicas*

Dependiendo de la actividad del sistema, se necesitará más o menos entropía y el proceso de generación de la clave será más o menos duradero. Es necesario producir actividad en el sistema para que la generación aleatoria de la clave sea lo suficientemente aleatoria.

En esta implementación se utilizó mediante el algoritmo ***RSA*** como algoritmo tanto para el cifrado como para la firma, con una longitud de 2048 bits y una caducidad de dos años. Cuando el proceso finaliza se generan los ***keyrings*** en la carpeta personal del usuario. A partir de este momento se podría importar, exportar, revocar, etc. Las claves públicas y privadas.

En este caso, continuando con el cifrado de archivos, se cifrará el mismo archivo anterior con la orden:

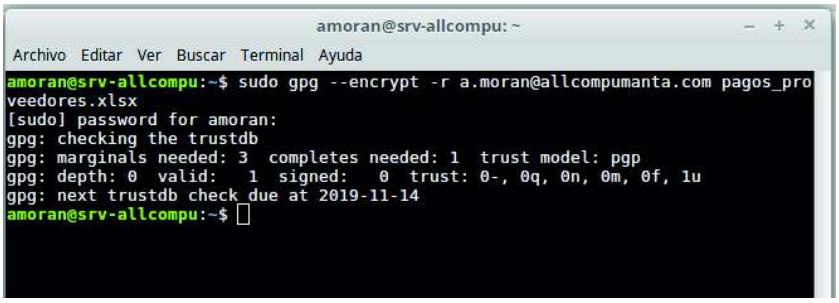


*Ilustración 59: Encriptando archivo RSA:2048 bits asimétrico*

No se ha solicitado ninguna contraseña o frase de paso ya que el cifrado se realiza mediante clave pública. En el proceso de descifrado, al ser realizado con la clave privada, sí será necesario introducir la frase de paso. Como ocurrirá en el caso del cifrado asimétrico, el resultado obtenido ha sido el mismo y no será posible visualizar el contenido del fichero a menos que se descifre. Para el descifrado se usará nuevamente la misma orden que en caso de clave simétrica.

Después de ello, el fichero volverá a estar disponible para su visualización o edición.

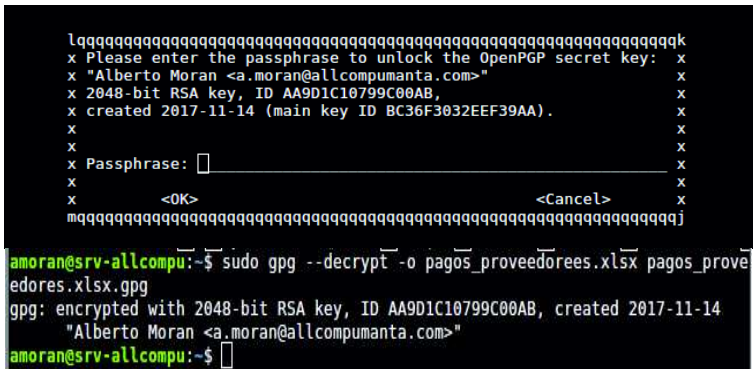


*Ilustración 60: Descifrando archivo con clave privada*

# CAPÍTULO IV

# 4. SEGUIMIENTO Y MONITOREO DE RESULTADOS

El seguimiento y monitoreo debe ser continuo para después hacer una comparación de resultados esperados y la utilidad de la información con el fin de cumplir objetivos previamente establecidos.

En la etapa de la implementación se trabajó a la par con el personal técnico de la empresa, revisando los archivos de registros de las aplicaciones o sistemas que se implantaron en este proyecto, lo cual permitió corroborar que la implementación está trabajando satisfactoriamente.

De esta manera se garantiza que el proyecto está cumpliendo con todos los componentes que se presentaron en esta propuesta implantada.

En la empresa ALLCOMPU, al poner en prácticas el modelo defensa en profundidad; implementado con base de tecnologías libres, teniendo como base el sistema operativo Debian GNU/Linux y las políticas de seguridad de acceso a la información y a las redes de la misma, se ha visto que los departamentos como los colaboradores han ido tomando más conciencia de la importancia de la aplicación de las mismas, se ha visto reflejado en la acción más oportuna y evitando perdidas de información.

El desarrollo de actividades se ha mejorado gracias a la implantación de estas políticas y el modelo. El departamento técnico, ha sido capaz de mantener el acceso y confiabilidad a los datos a nivel de red como el funcionamiento de cada equipo.

## CONCLUSIONES

Una vez que se ha culminado el proyecto de aseguramiento de redes y sistemas informáticos de la empresa privada ALLCOMPU, basado en entornos GNU/Linux, se logró cumplir los objetivos propuestos, llegando a las siguientes conclusiones:

| Objetivo | Conclusión |
|---|---|
| Determinar los mecanismos de seguridad informática que posee la empresa ALLCOMPU en la red y sus sistemas informáticos | Se implementó políticas internas que ayudaron a minimizar los riesgos en los sistemas y redes de voz y datos de la empresa |
| Analizar la técnica de Hardening (aseguramiento) más adecuada que permita, sus estrategias de aplicabilidad, incluyendo técnicas que se deben considerar para realizar su implementación. | Se determinó la mejor decisión que beneficiaba a la empresa que permitió tener un nivel de seguridad de redes y sistemas informáticos más elevado |
| Implementar el modelo defensa en profundidad mediante el uso del sistema operativo Debían GNU/Linux. | Se implementó el modelo defensa en profundidad, el cual permitió minimizar los riesgos y asegurar el entorno, mediante la aplicabilidad de las aplicaciones y estrategias de seguridad. |
| Implementar métodos de seguridad a la red inalámbrica. | Se atribuyó medidas de seguridad inalámbrica para equipos de que permiten el acceso a la red mediante conexiones sin cable, como cambios de contraseñas |

| | |
|---|---|
| | periódicas, autenticación por MAC y utilizando métodos de autenticación con algoritmos de cifrado más robustos. |

*Tabla 5: Conclusiones del proyecto*

Con la implementación del modelo defensa en profundidad, se cumple con los objetivos de tener un entorno corporativo más seguro. Ayudando al buen desempeño de la empresa y a la confiabilidad, disponibilidad e integridad de los sistemas informáticos y redes de la empresa.

## RECOMENDACIONES

- Que el departamento técnico se encargue de la concienciación (charlas, capacitaciones) de la seguridad de la información y mantenga el sistema y servidor actualizado en versiones actuales.

- Las reglas aplicadas en este documento, pueden variar dependiendo de las necesidades o servicios que se incluyan o se excluyan de la empresa, por lo cual toca estar en constante monitorización o supervisión de las reglas del firewall.

- Adquisición de un servidor para respaldo o backup de la información, lo que ayudará a la disponibilidad de la misma..

- Que se revisen o monitoreen los archivos de registro del servidor y tomar decisiones en base a ellos, para asegurar el entorno corporativos y de los sistemas.

# BIBLIOGRAFÍA

Alfon. (22 de febrero de 2011). Seguridad y Redes Obtenido de http://seguridadyredes.wordpress.com/2011/02/22/ids-ips-suricata-entendiendo-y-configurando-suricata-parte-i/

Estrada, A. C. (2011). Seguridad por NIveles. España: DarFE.

Martínez, C. G. (2010). Modelo de Defensa en Profundidad.

García, J. L. (2014). Ataques en redes de datos IPv4 e IPv6

Verdeguer, J. L. (2013). Hacking y Seguridad VoIP

Romero Ternero, M. D., Barbancho Concejero, J., Benjumea Móndejar, J., Rivera Romero, O., Ropero Rodríguez, J., Sánchez Antón, G., & Sivianes Castillo, F. (2010). Redes Locales. Madrid: Paraninfo.

ISO (International Standard Organization). “Estándar de Seguridad ISO 27002”

Información Activo valioso para las empresas; Gabriel Alejandro Granados http://www.visionindustrial.com.mx/industria/desarrollo-industrial/informacion-activo-valioso-para-las-empresas.html

Firewall (5 enero 2017). iptables Debian GNU/Linux. Obtenido de https://wiki.debian.org/iptables

Lubos Rendek (2017). Samba. Obtenido de https://linuxconfig.org/how-to-configure-samba-server-share-on-debian-9-stretch-linux

Margaret Rouse (2014). RSA algorithm (Rivest-Shamir-Adleman). Obtenido de http://searchsecurity.techtarget.com/definition/RSA

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (México). *Metodología de la Investigación.* MCGRAW-HILL.

Martín C A y Perez P G. (2014). Hardening de servidores GNU/Linux

# ANEXOS

## ENTREVISTA SOBRE SEGURIDAD INFORMÁTICA

La siguiente entrevista va dirigida para obtener datos relevantes, sobre el aseguramiento de redes y sistemas informáticos, y el modelo defensa en profundidad. Dirigido al personal administrativo y técnico de la empresa ALLCOMPU.

1. ¿Conoce acerca del modelo "defensa en profundidad" para la gestión de la seguridad de la información?

2. ¿Qué herramientas de seguridad usa usted en su entorno informático?

3. ¿Qué tipo de políticas o normas de seguridad informática usted recomendaría aplicar?

4. ¿Qué herramientas de seguridad usted reconoce para un aseguramiento informático?

5. ¿En la actualidad la red informática de la empresa considera que es vulnerable?

6. ¿Cuál sería el mecanismo eficiente para realizar el seguimiento de los equipos en la red?

7. ¿El tener una red plana afecta la productividad en ciertas ocasiones?

8. Si la empresa tiene conexión sin cables (WIFI), ¿utiliza las medidas de seguridad pertinentes para proteger dicha conexión?

9. Comparten archivos entre colaboradores, ¿Qué medidas de seguridad ayudan a la integridad de los archivos?

10. El trabajar con una red plana todos los sistemas informáticos específicamente VoIP ¿La concurrencia de llamadas de la telefonía sobre IP, afecta el desempeño de la red?

## GLOSARIO

**DMZ:** Demilitarized Zone (Zona Desmilitarizada)

**DNS:** Domain Name System (Sistema de Nombres de Dominio)

**FTP:** File Transfer Protocol (Protocolo de Transferencia de Archivos)

**HTTP:** Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto).

**ICMP:** Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)

**IDS:** Intrusion Detection System (Sistema de detección de intrusiones)

**IEC:** Comisión Electrotécnica Internacional.

**IEEE:** Institute of Electrical and Electronic Engineers (Instituto de Ingeniería Eléctrica y Electrónica)

**IP:** Internet Protocol (Protocolo de Internet)

**IPS:** Intrusion Prevention System (Sistema de Prevención de Intrusiones)

**ISL:** Inter-Switch Link 166

**ISO:** International Standard Organization (Organización Internacional para la Estandarización)

**MAC:** Media Access Control (Control de Acceso al Medio)

**NIC:** Network Interface Card (Tarjeta de Interfaz de Red)

**OISF:** Open Information Security Foundation (Fundación Abierta de Seguridad de Información)

**RAV:** Risk Assessment Values (Valores de la Evaluación de Riesgos)

**SMB:** Server Message Block (Servicio de Bloqueo de Mensajes)

**SMTP:** Simple Mail Transfer Protocol (Protocolo Simple de Transmisión de Correo)

**SSH:** Secure SHell.

**TCP:** Transmission Control Protocol (Protocolo de control de transmisión)

**TIC:** Tecnologías de la información y la comunicación

**TLS:** Transport Layer Security (Seguridad de la Capa de Transporte)

**UDP:** User Datagram Protocol (Protocolo de Datagrama de Usuario)

**UPS:** Uninterrupted Power Supply (Sistema de Alimentación Ininterrumpida)

**URL:** Uniform Resource Identifier (Identificador uniforme de recurso)

**VLAN:** Virtual Local Area Network (Red de Área Local Virtual)

**VTP:** VLAN Trunking Protocol