UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

ESCUELA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

"SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE DATOS DE LA INDUSTRIA FLORALP S.A EN LA CIUDAD DE IBARRA, BASADO EN LA PLATAFORMA DE SOFTWARE LIBRE"

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTORA: GABRIELA JANETH LÓPEZ PAREDES

DIRECTORA: ING. SANDRA CASTRO

Ibarra – 2015

DECLARACIÓN

Yo, Gabriela Janeth López Paredes con cédula de identidad nro. 1003543681, estudiante de la carrera de Ingeniería en Electrónica y Redes de Comunicación, libre y voluntariamente declaro que el presente trabajo de investigación, es de mi autoría y no ha sido realizado, ni calificado por otro profesional, para efectos académicos y legales será de mi responsabilidad.

.....

LÓPEZ PAREDES GABRIELA JANETH

CI: 1003543681

CERTIFICACIÓN

Certifico que la Tesis "SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE DATOS DE LA INDUSTRIA FLORALP S.A EN LA CIUDAD DE IBARRA, BASADO EN LA PLATAFORMA DE SOFTWARE LIBRE" ha sido realizada en su totalidad por la señorita: LÓPEZ PAREDES GABRIELA JANETH portadora de la cédula de identidad número: 1003543681

.....

Ing. Sandra Castro Directora de la Tesis

UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE INVESTIGACIÓN A FAVOR DE LA UNIVERSIDAD

Cesión de derechos de Autor del Trabajo de Grado a favor de la Universidad Técnica del Norte.

Yo, Gabriela Janeth López Paredes con cedula nro. 1003543681, manifiesto que es mi voluntad de ceder a la Universidad Técnica del Norte, los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador Art.4,5 y 6 en calidad de autor del Trabajo de Grado denominado: Tesis **"SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE DATOS DE LA INDUSTRIA FLORALP S.A EN LA CIUDAD DE IBARRA, BASADO EN LA PLATAFORMA DE SOFTWARE LIBRE"**, que ha sido desarrollado para obtener el título de INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN en la Universidad Técnica del Norte, quedando facultada la Universidad para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autora me reservo los derechos morales de la obra antes citada. En concordancia se suscribe este documento en el momento en que se hace la entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

(Firma):

Nombre: LÓPEZ PAREDES GABRIELA JANETH

Cédula: 1003543681

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA
AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

- **IDENTIFICACIÓN DE LA OBRA.**

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer los textos completos de forma digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad. Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual ponemos a disposición la siguiente investigación:

DATOS DEL CONTACTO	
Cédula de Identidad	1003543681
Apellidos y Nombres	López Paredes Gabriela Janeth
Dirección	El Olivo Alto Av.17 de Julio
Email	gaby_janeth_7@hotmail.com
Teléfono Fijo	2609-101
Teléfono Móvil	993078067

DATOS DE LA OBRA	
Título	"SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE DATOS DE LA INDUSTRIA FLORALP S.A EN LA CIUDAD DE IBARRA, BASADO EN LA PLATAFORMA DE SOFTWARE LIBRE"
Autor	López Paredes Gabriela Janeth
Fecha	11 de junio de 2015
Programa	Pregrado
Titulo por el que se aspira	Ing. Electrónica y Redes de Comunicación
Director	Ing. Sandra Castro

- **AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD**

Yo, Gabriela López Paredes, con cédula de identidad Nro. 1003543681, en calidad de autora y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 144.

.....

Firma Nombre: GABRIELA JANETH LÓPEZ PAREDES

Cédula: 1003543681

Ibarra a los 11 días del mes de junio del 2015

AGRADECIMIENTOS

Quiero hacer extensivos mis más sinceros agradecimientos;

En primer lugar a Dios, que me diste la oportunidad de vivir y de regalarme una familia maravillosa.

A mis padres y hermanas, por con su ejemplo, dedicación y esfuerzo han logrado hacer de mí una persona con valores como la honestidad, el respeto, responsabilidad y tolerancia; a ellos que son mi pilar les dedico este trabajo y los frutos de mi carrera profesional.

A mi directora de tesis, Ing. Sandra Castro, por todo este trabajo en conjunto, enseñanzas y tiempo empleado y paciencia en la realización de mi tesis que me sirvieron para culminar satisfactoriamente mi proyecto.

A los docentes de la prestigiosa Facultad de Ingeniería en Ciencias Aplicas de la carrera de Ingeniería Electrónica y Redes de Comunicación por su guía en mi formación personal y académica.

Al departamento de Sistemas de la industria Lechera FLORALP S.A, en especial al Ing. Xavier Barahona por brindarme su confianza y colaboración para desarrollar este trabajo por su importante aporte y participación activa en el transcurso del mismo.

A todos ustedes muchas gracias.

Gabriela J. López

DEDICATORIA

Mi tesis la dedico con todo mi amor y cariño.

A ti mi Dios y abuelitas que se encuentran en el cielo y sé que cada noche me escuchan gracias por todas las bendiciones que me brindan y por darme la oportunidad de conocer personas de excelente calidad humana con las que he compartido momentos inolvidables.

Con mucho cariño principalmente a mis padres que me dieron la vida y han estado conmigo en todo momento gracias por darme una carrera para mi futuro y por creer en mí, aunque hemos pasado momentos difíciles siempre han estado apoyándome y brindándome todo su amor, por todo eso les agradezco de todo corazón el que estén conmigo a mi lado.

A mis hermanas María, Cristina y Paulina gracias por estar conmigo apoyarme siempre y por hacerme sonreír en los momentos más difíciles, las quiero mucho

A todos mis amigos en especial a Diego, Miriam y Viviana muchas gracias por estar conmigo en todo este tiempo donde hemos compartido momentos alegres, tristes y por su comprensión y generosidad los llevaré siempre en mi corazón.

A todas las personas que me apoyaron de una u otra manera con palabras de aliento durante todo este proceso.

Gabriela J. López

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El proyecto planteado consiste en el diseño e implementación de un sistema de seguridad perimetral que permitirá mayor confiabilidad de la información de la matriz industria FLORALP S.A que se encuentra localizada en la ciudad de Ibarra.

En el primer capítulo se realizará la recolección de información sobre los sistemas de seguridad perimetral que se utilicen en la actualidad tales como los IDS y los Firewall, donde se tomarán en cuenta las principales características para asegurar la privacidad de la información.

Posteriormente en el segundo capítulo se efectuará un estudio de la situación actual de la red, equipamiento con el que cuenta la industria FLORALP S.A e identificar las principales vulnerabilidades que atentan contra la red y de esta forma conocer los requerimientos necesarios para la implementación del sistema de seguridad mediante la norma ISO/IEC 27001.

En el tercer capítulo se realizará el diseño del sistema de seguridad perimetral desarrollando políticas de seguridad basándose en la norma ISO/IEC 27001. Se establecerá además las bases de los lineamientos necesarios para escoger el software libre a utilizarse mediante el estándar IEEE 830.

En cuarto capítulo se describe la implementación del sistema de seguridad de acuerdo al diseño previo del sistema de seguridad perimetral con el propósito de obtener resultados que permitan medir su desempeño y confiabilidad de la red.

En el quinto capítulo se analizará el comportamiento de red mediante ataques para comprobar la efectividad del diseño del sistema de seguridad perimetral permitiendo comprender el comportamiento de la red en el enfoque de seguridad.

Y finalizando en el sexto capítulo se realizará un análisis económico entre los equipos existentes y los que se utilicen en el desarrollo del Sistema de Seguridad Perimetral.

ABSTRACT

The proposed project consists of the design and implementation of a perimeter security system which allows greater reliability of the information matrix FLORALP S.A industry that is located in the city of Ibarra.

In the first chapter the collection of information on perimeter security systems that are used today such as IDS and Firewall, which will take into account the main features to ensure the privacy of information, is performed.

Later in the second chapter a study of the current status of the network equipment with which account industry FLORALP S.A and identify the main vulnerabilities that threaten the network and thereby meet the requirements for implementing the system shall be made security by ISO / IEC 27001.

In the third chapter the design of the perimeter security system is done by developing security policies based on ISO/IEC 27001 standard bases are also establish guidelines necessary to choose free software for use by the IEEE 830 standard.

In the fourth chapter the implementation of the security system according to the previous design of perimeter security system in order to get results to measure performance and reliability of the network is described.

In the fifth chapter the network behavior will be analyzed by attacks to test the effectiveness of the design of perimeter security system allowing understands the behavior of network security approach.

And finishing sixth chapter economic analysis between existing teams and those used in the development of perimeter security system will be made.

PRESENTACIÓN

El presente proyecto se ha propuesto debido a la necesidad de proteger los sistemas de información mediante sistemas de seguridad permitiendo la trasmisión de datos de forma segura y confiable.

La masiva utilización de servicios informáticos y redes como medios para trasferir, procesar y almacenar información en los últimos años ha incrementado, trasformando la información en todas sus formas y estados en un activo de altísimo valor, el cual se debe proteger y asegurar para garantizar su integridad, disponibilidad y confidencialidad.

Los sistemas de seguridad de la información pueden ser algún dispositivo o herramienta física que permita resguardar un bien, un software o sistema que de igual manera ayude de algún modo a proteger un activo y que no precisamente es algo tangible, o una medida de seguridad que se implemente esto se lo puede realizar por medio de las políticas de seguridad que se basan en estándares para su creación.

El uso de estándares abiertos contribuye primordialmente en el aspecto económico de las grandes y pequeñas empresas al permitir el ahorro en licenciamiento y adquisición de hardware, ya que se reutilizan equipos debido a la manejabilidad y bajo consumo de recursos de las aplicaciones instaladas en ellos.

INTRODUCCIÓN

OBJETIVOS DEL PROYECTO

Objetivo General

- Implementar un sistema de seguridad perimetral para la Red de Datos de la FLORALP S.A mediante políticas de seguridad basado en Software Libre evitando así ataques externos e internos.

Objetivos Específicos

- Realizar un estudio de la información referente a la seguridad perimetral identificando y valorando las principales características, para la implementación en la red de datos de la FLORALP S.A.
- Analizar la situación actual de la infraestructura, servicios, protocolos, aplicaciones y accesos de red de la industria la FLORALP S.A, mediante el estándar internacional ISO/IEC 27001 como base fundamental para determinar los requerimientos necesarios para el diseño del sistema de seguridad perimetral.
- Diseñar el sistema de seguridad perimetral, considerando los requerimientos y directrices para el desarrollo de políticas de seguridad.

- Analizar diferentes plataformas de Software en base al estándar IEEE 830 de especificaciones de requerimiento de software para seleccionar la mejor alternativa que se ajuste a los requerimientos del diseño del sistema de seguridad perimetral.
- Implementar el firewall, el IDS y la zona desmilitarizada con las respectivas políticas de seguridad planteadas en el diseño de sistema de seguridad, las cuales protegerán a la red de los posibles ataques externos e internos.
- Realizar pruebas pertinentes que simulen ataques internos y externos hacia la red a través del funcionamiento total del sistema de seguridad perimetral de la red de la FLORALP S.A.

PROBLEMA

La FLORALP S.A es una industria dedicada a la elaboración y comercialización de productos lácteos artesanales, reconocido por su calidad tanto a nivel nacional como internacional. FLORALP S.A cuenta con cinco plantas de producción en Ecuador donde cada sucursal maneja una red independiente es decir que no tienen una conexión entre ellas, una de las dependencias está localizada en Ibarra como plantas propias. La planta de Ibarra cuenta con una red simple que no maneja ninguna política de seguridad siendo vulnerable a cualquier tipo de ataque de Interrupción, modificación e intercepción, estos tipos de amenazas son el resultado de desconocimiento y descuido por la persona encargada de manejar la red por lo que necesitan ser corregidas y documentadas.

La seguridad de la red no ha sido un tema prioritario dentro de la industria por tal motivo su infraestructura es insegura para resguardar cualquier tipo de información que circule por la red de la industria. La información de la Red de Datos de la FLORALP S.A se encuentra expuesta a ataques internos y externos como troyanos, gusanos de red y correos spam que pueden atacar provocando la modificación de direcciones IP esto los hace vulnerables a eventos de amenazas que con llevan a riesgos que puedan provocar pérdidas de información.

Por tal motivo la actual red de la FLORALP S.A necesitará reforzar la seguridad al momento de realizar intercambio de información tomando en cuenta que el nivel de seguridad no solo se debe considerar de forma interna si no fuera de ella, ya que la pérdida de datos puede resultar perjudicial para la empresa, para esto se realizará un sistema de seguridad perimetral permitiendo detectar y eliminar las amenazas que traten de afectar la integridad de la infraestructura de red.

Debido a los constantes ataques y vulnerabilidades en la infraestructura de red de la industria la FLORALP S.A es de vital importancia la implementación de un sistema de seguridad perimetral mediante políticas de seguridad que garanticen un rendimiento de la información. Por lo cual es necesario implementar una infraestructura externa de seguridad que permita tener incorporado un sistema de detección de intrusos para controlar el acceso a los sistemas de la empresa desde el exterior. A través de estos sistemas se podrá examinar las acciones de las aplicaciones que se conectan a la red, y así brindar a futuro servicios de comunicaciones con mayor seguridad en la transmisión.

JUSTIFICACIÓN

La implementación de un Sistema de Seguridad Perimetral en el entorno de la Red Informática, garantizará la confiabilidad y seguridad de la información que se maneja ya que la información que cruza es de carácter privado, las políticas de seguridad son necesarias en la industria ya que la protegerán de las vulnerabilidades, ataques internos y externos que se produzcan.

Es muy importante utilizar una metodología que conduzca a una solución eficaz y eficiente permitiendo establecer políticas y objetivos para mejorar el nivel de seguridad informática para esto se usará la norma ISO/IEC 27001 que permitirá establecer, implementar, monitorear, revisar y mantener un SGSI.

Mediante el diseño del sistema de seguridad perimetral se garantizará la protección de la información que cruza por la red, debido a que este sistema se basa en establecer una coraza que proteja todos los elementos sensibles frente a diferentes amenazas, además nos permite ampliarlo según nuestras necesidades y características de la infraestructura de red, manteniéndonos informados en todo momento de los movimientos que se produzcan dentro de la misma. Este método de defensa basado en el establecimiento de políticas de seguridad dentro del perímetro externo de la red y a diferentes niveles. Esto nos permitirá definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros permitiendo que la industria maneje sus datos de forma segura.

CAPÍTULO I

1 Fundamentos Teóricos De Seguridad En Redes

En este capítulo se sustenta las bases teóricas tomando en cuenta la norma internacional ISO[1]/IEC[2] 27001, se describen los aspectos básicos de la seguridad de la información, los distintos tipos de intrusos y ataques informáticos, además sobre los conceptos, características, amenazas, vulnerabilidades, mecanismos de seguridad en redes y tecnologías de protección como Firewall o IDS[3], como base para el diseño del presente proyecto.

1.1 Seguridad informática

La seguridad informática se orienta a la protección de la infraestructura de red y todo lo relacionado a esta, de tal forma garantiza la confidencialidad, disponibilidad e integridad mediante la protección, clasificación y conocimiento de impactos o daños de las potenciales amenazas o intenciones perjudiciales de forma indirecta o directa para minimizar riesgos.

[1] **ISO:** Organización Internacional de Normalización
[2] **IEC:** Comisión Electrónica Internacional
[3] **IDS:** Sistema de Detección de Intrusos

1.1.1 Confidencialidad

En la seguridad informática la confidencialidad se entiende por la protección de la información buscando prevenir la divulgación de información a personas o sistemas no autorizados, permitiendo únicamente el acceso a personas que cuenten con la debida autorización.

1.1.2 Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema libre de modificaciones.

1.1.3 Disponibilidad

El sistema debe mantenerse funcionando eficientemente, estar disponible para quienes deban acceder a ella y ser capaz de recuperarse rápidamente en caso de fallo.

1.1.4 Autenticidad

Permite asegurar el origen de la información, la identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser.

1.1.5 Debilidades de un sistema de información

En la siguiente Figura 1, se indica las debilidades de un sistema de información.

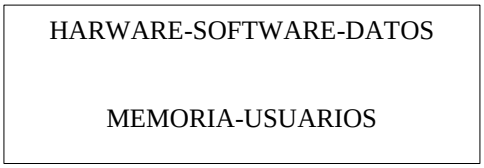


Figura 1. Debilidades de un Sistema Informático

Fuente: Jorge Ramiro Aguirre. Libro Electrónico de Seguridad Información y Criptografía

Los tres primeros puntos conforman el triángulo de debilidades del sistema

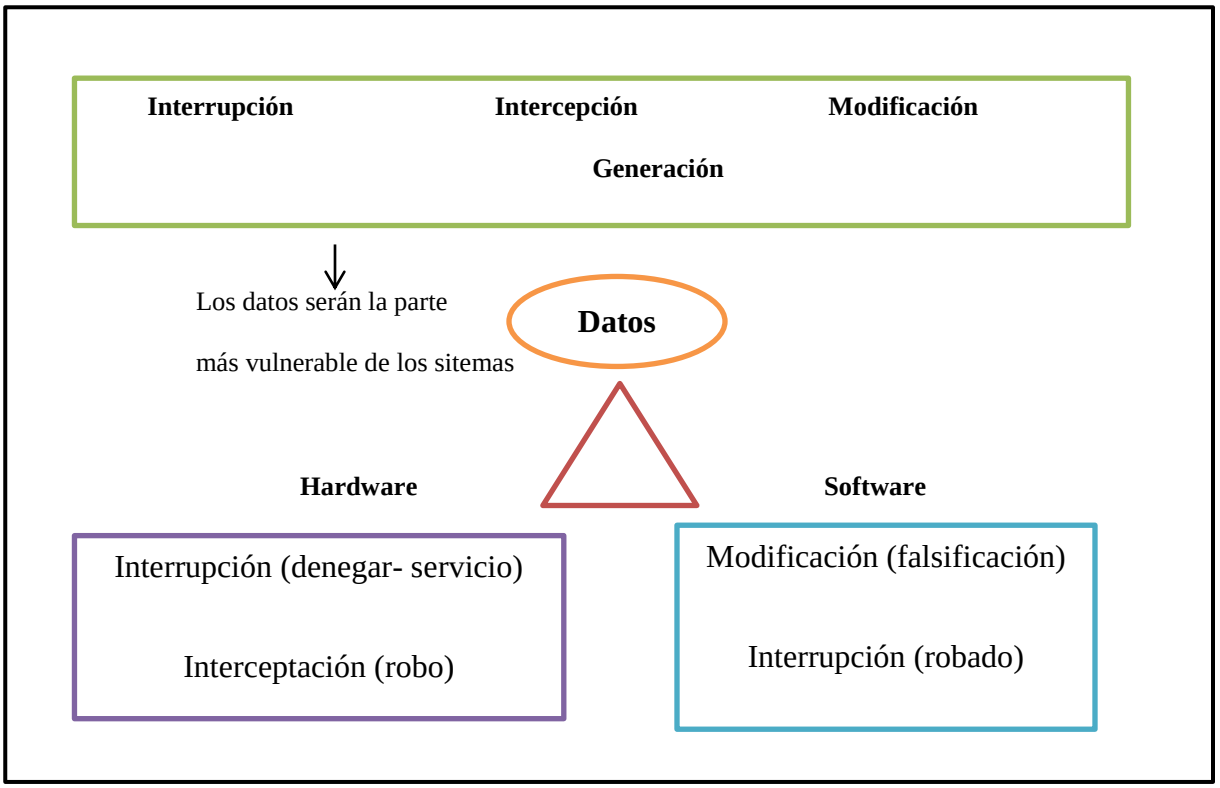


Figura 2. Triángulo de debilidades del sistema

Fuente: Jorge Ramiro Aguirre. Libro Electrónico de Seguridad Información y Criptografía

Según (Aguirre, 2006) especifica que las debilidades de un sistema de información son las siguientes:

- **Hardware**

  Pueden producirse errores intermitentes, conexiones sueltas, desconexión de tarjetas.

- **Software**

  Puede producirse la sustracción de programas, ejecución errónea, modificación, defectos en llamadas a los sistemas.

- **Datos**

  Pueden producirse la alteración de contenidos, introducción de datos falsos, manipulación fraudulenta de datos.

- **Memoria**

  Pueden producirse de un virus, mal uso de la gestión de la memoria, bloqueo del sistema.

- **Usuarios**

  Puede producirse la suplantación de identidad, accesos no autorizados visualización de datos confidenciales.

1.2 Ataques y amenazas

Ataque es un método que intenta desestabilizar el funcionamiento de la red intentando obtener de forma no autorizada la información.

Amenaza es cualquier cosa que pueda interferir con el funcionamiento adecuado de la red aprovechándose de las debilidades del sistema.

1.2.1 Clasificación de las amenazas

1.2.1.1 Amenazas lógicas

Bajo la etiqueta de amenazas lógicas encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros) menciona (Huerta, 2002).

1.2.1.2 Amenazas físicas

Según (Loor, 2013) menciona que las amenazas físicas pueden englobar cualquier error o daño en el hardware que se puede presentar en cualquier momento y afectando a la seguridad y su funcionamiento. Por ejemplo:

- Por acciones naturales: incendio, inundación, condiciones climatológicas, señales de radar, instalaciones eléctricas.
- Por acciones hostiles: robo, fraude, sabotaje.

- Por control de accesos: utilización de detectores de metales, utilización de sistemas biométricos, seguridad con animales, protección electrónica.

1.2.2 Formas de amenazas

Los ataques a los sistemas de seguridad son muy frecuentes por lo que se expone cuatro categorías de ataques como:

1.2.2.1 Interrupción

Es un ataque contra la disponibilidad esto se da cuando el sistema es destruido o se vuelve no disponible. La interrupción puede ser temporal o permanente dependiendo de qué tan grave es la amenaza, estos ataques son más rápidos de identificar pero lo más difíciles de solucionar por ejemplo: la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación.

1.2.2.2 Intercepción

Es un ataque no autorizado que se va contra la confiabilidad del sistema de seguridad, esto se da cuando una entidad puede ser (persona, un programa o un ordenador) desconocido accede a un recurso. La intercepción es la amenaza más difícil de detectar, por lo que no produce ningún cambio en el sistema. Ejemplos de este ataque son acceso a una base datos, a

la lectura de las cabeceras de los paquetes que circulan por la red para poder obtener la identidad de las personas implicados en la comunicación.

1.2.2.3 Modificación

Este tipo de ataques se dedican a conseguir alterar o manipular la información de alguna forma no autorizada este es un ataque contra la integridad, principalmente los intrusos se dedican a cambiar los valores de un archivo o eliminar información que se esté utilizando aprovechándose de las vulnerabilidades de los sistemas de seguridad.

1.2.2.4 Generación

Es un ataque contra la autenticidad, una entidad no autorizada inserta objetos falsificados en el sistema. Ejemplos de este ataque son la inserción de mensajes falsos en una red o añadir registros a un archivo. Estos ataques se pueden clasificar de forma útil en términos de ataques pasivos y ataques activos (Salazar, 2011) .

1.3 Vulnerabilidades

Una vulnerabilidad es todo aquello que provoca que nuestros sistemas informáticos funcionen de manera diferente afectando de forma integral la seguridad del mismo, pudiendo llegar a provocar entre otras cosas la pérdida y robo de información. Estos sistemas pueden ser tratados buscando los puntos más sensibles dentro de un sistema de información evitando que

perturben la confidencialidad, disponibilidad e integridad de los datos ya sea de una empresa o persona.

- **Física:** Se refiere a las debilidades que pueda tener el entorno físico del sistema informático en el que se encuentran los elementos como CPU[4], terminales, cableado, medios de almacenamiento todos estos puntos débiles son afectados continuamente específicamente en su disponibilidad.

- **Natural:** Son todas aquellas vulnerabilidades que tienen que ver con algún desastre natural o ambiental, por lo que no pueden ser evitadas y que el sistema pueda ser dañado se consideran las siguientes manifestaciones de la naturaleza como: terremotos, huracanes inundaciones tales que la infraestructura de red sea incapaz de soportar.

- **De hardware:** Al igual que las amenazas, las vulnerabilidades de hardware tienen que ver con la fabricación o la configuración de los equipos que se van a utilizar. En este caso son consideraciones no tomadas en cuenta para el funcionamiento de los mismos, por ejemplo la falta de mantenimiento constante al equipo o el no tener algún respaldo de las configuraciones, no verificar que el equipo que se compra cuente con los requerimientos necesarios, entre otros.

[4] **CPU:** Unidad Central de Procesamiento

- **De software:** Es el conjunto de programas lógicos que hacen que funcione el hardware o que los protocolos de comunicación carezcan de seguridad.

- **De red:** Son todas aquellas vulnerabilidades existentes en la conexión de equipos, por ejemplo si no existe un control que permita limitar el acceso, se puede penetrar al sistema por medio de la red. También abarca las fallas en la estructura del cableado y el no seguir los estándares recomendados para realizarlo.

- **Humana:** Tienen que ver con las acciones de las personas en el seguimiento de las políticas de seguridad estas ocasionan más daño que todas las anteriores y son las vulnerabilidades más difíciles de defender, por ejemplo ser vulnerable a la ingeniería social donde pueden ser los errores intencionales o no.

1.3.1 Diseño pobre

Un diseño de una red informática es de vital importancia determinar la estructura tanto física como lógica de la red, para evitar que existan huecos de seguridad, problemas de pérdidas de datos y caídas de la red. En todo diseño debe tomarse en cuenta tres elementos importantes a proteger son el software, el hardware y los datos.

1.3.2 Implementación pobre

Se presenta en los sistemas configurados incorrectamente y por lo tanto son vulnerables a un ataque; estos tipos de vulnerabilidades son el resultado de desconocimiento, inexperiencia o descuido en el trabajo.

1.3.3 Administración pobre

Es el resultado de procedimientos inadecuados, controles y verificaciones insuficientes. Las medidas de seguridad no pueden operar en un vacío, necesitan ser documentadas y monitoreadas constantemente por personal capacitado.

1.4 Mecanismos de seguridad

Los mecanismos de seguridad son técnicas que se utiliza para implantar un servicio, es decir, es aquel mecanismo que está diseñado para detectar, prevenir o recobrarse de un ataque de seguridad (Estrella, 2010).

1.4.1 Mecanismos de prevención

En esta etapa se toman las acciones necesarias para prevenir una posible intrusión o la violación de la seguridad, permitiendo aumentar la fiabilidad del sistema. Estas acciones se

pueden realizar tanto a nivel de software o a nivel de hardware. Dentro del grupo de mecanismos de prevención tenemos:

1.4.1.1 Mecanismos de identificación y autenticación

Este sistema es el más utilizado permitiendo identificar de forma única al sistema. El proceso siguiente es la autenticación, es decir, comprobar que la entidad es quien dice ser.

1.4.1.2 Mecanismos de control de acceso

Mediante los mecanismos de control de acceso controlan los tipos de acceso al objeto por parte de cualquier entidad del sistema.

1.4.1.3 Mecanismos de separación

Si el sistema dispone de diferentes niveles de seguridad se deben implantar mecanismos que permitan separar los objetos dentro de cada nivel.

1.4.1.4 Mecanismos de seguridad en las comunicaciones

Se utiliza para garantizar la privacidad e integridad de los datos cuando viajan por la red. Estos mecanismos se basan en criptografía como cifrados de clave pública y privada

clásicamente se utilizan protocolos seguros, tipo SSH[5] o Kerberos, que cifran el tráfico por la red.

1.4.2 Mecanismos de detección

Son aquellos que se utilizan para detectar violaciones a la seguridad o intentos de violaciones ya que si no se da cuenta del ataque el daño va a ser mayor. Como por ejemplo tenemos los programas de auditoría

1.4.3 Mecanismos de respuesta

Son aquellos que se aplican cuando una violación del sistema se ha detectado, ya que busca minimizar los efectos de un ataque o problema y finalmente retomar al sistema a su modo de trabajo normal. Como ejemplo tenemos las copias de seguridad o el hardware adicional.

1.4.4 Mecanismo de análisis forense

Permite determinar las acciones que ha realizado el atacante desde ver que agujeros de seguridad han utilizado para entrar al equipo, hasta ver las acciones que ha realizado en el sistema, de esta forma prevenir y detectar posteriores ataques al sistema.

[5] **SSH**: (Secure Shell, intérprete de órdenes segura): es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

1.5 Modelos de seguridad

Para la correcta implantación de la seguridad informática, se deben establecer y mantener acciones que busquen cumplir con los tres requerimientos para la información, estos son disponibilidad, confidencialidad e integridad.

1.5.1 Seguridad perimetral

El modelo de seguridad perimetral es un uno de los métodos posibles de defensa de un sistema que fortalecen el perímetro externo de la infraestructura de la red basándose en un conjunto de medidas estrategias que permiten y deniegan el acceso a determinados usuarios.

Existen varias tecnologías muy utilizadas como son: Firewalls, IDS, VPNs[6], DMZ[7] que permiten una administración centralizada de la red con niveles de confianza.

Entre sus principales objetivos esta proteger todos los elementos vulnerables que se encuentran amenazados por diferentes agentes externos como virus, troyanos, gusanos de internet, correos basura o spam, phishing, ataques de denegación de servicios y hackeo de páginas web corporativas.

---

[6] **VPN (**Virtual Private Network): Red privada virtual es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet.

[7] **DMZ** (Zona Desmilitarizada): es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.

1.5.2 Seguridad por obscuridad

Un sistema por obscuridad consiste en mantener en secreto la existencia de la red, algoritmos y protocolos utilizados, de tal manera, que cualquier sistema puede ser seguro mientras nadie fuera de su grupo de implementación de seguridad se le permita conocer nada de sus mecanismos internos, un ejemplo de este modelo de seguridad es ocultando contraseñas en archivos binarios suponiendo que “nadie lo va a encontrar nunca”.

Este tipo de modelo de defensa tiene diferentes niveles de implementación para cada zona que se desee resguardar, por ejemplo existen mecanismos donde estos resguardan cada nivel para evitar que la red se encuentre indefensa a cualquier ataque cuando un mecanismo de seguridad falle.

Una gran ventaja de este tipo de estrategia es que cada mecanismo debe ser cuidadosamente configurado para que no existan fallas, es decir, que si una persona no sabe cómo hacer algo para tener un impacto en la seguridad del sistema, entonces esa persona no será peligrosa evitando que los problemas que se tenga sean difundidos al resto de mecanismos.

1.5.3 Defensa de profundidad

(VINUEZA, 2012) Describe que defensa en profundidad es:

El término defensa en profundidad (en ocasiones denominada seguridad en profundidad o seguridad multicapa) procede de un término militar utilizado para describir la aplicación de contramedidas de seguridad con el fin de formar un entorno de seguridad cohesivo sin un solo punto de error. Las capas de seguridad que forman la estrategia de defensa en profundidad incluyen el despliegue de medidas de protección desde los enrutadores externos hasta la ubicación de los recursos, pasando por todos los puntos intermedios.

Este modelo de infraestructura se distingue como una serie de capas dando paso a la seguridad y a garantizar que en caso de que existiera peligro cada capa ofrecerán la seguridad necesaria para proteger sus recursos, es decir, que se basa en la implementación de diferentes zonas de seguridad resguardadas por diferentes mecanismos, donde cada uno de ellos refuerza a los demás, de esta manera, se evita que si uno de los mecanismos falla se deje vulnerable la red.

Este principio se trata de hacer más difícil a un atacante en su camino hacia el objetivo final de acceder los datos confidenciales, esto se logra con la multiplicidad de la protección organizada entorno a múltiples niveles de seguridad cada mecanismo respalda otro que se encuentre en una capa inferior. (Manuel, 2013)

1.6 Tecnologías de seguridad

Las tecnologías de seguridad tienen como objetivo la implementación de diferentes sistemas integrales para la seguridad de la información como son los siguientes:

1.6.1 Firewall

Un Firewall es un sistema o un grupo de sistemas (software o hardware) que permite o deniega diferentes servicios desde el exterior, es decir, que se conecta entre la red y el cable de la conexión a internet solo dejando pasar el tráfico autorizado desde y hacia el exterior como se muestra en la Figura 3.

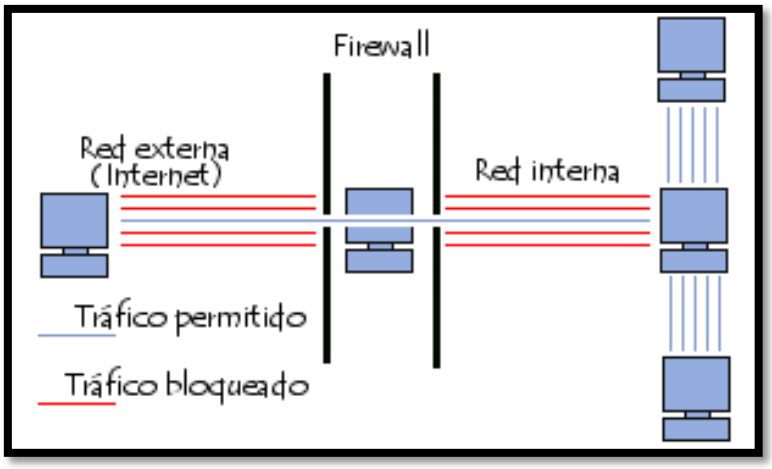


Figura 3. Implementación de un Firewall
Fuente: Seguridad en Linux Recuperado de: Mohan, K., Seagren E .,& Alder R.(2008)

Es fundamental el uso de los firewall para asegurar la red interna mediante la utilización de políticas de seguridad facilitando de esta manera la administración de la red.

Las políticas de seguridad están ligadas al firewall, no es más que una norma que marca el comportamiento de una red con relación a su seguridad. Definir políticas de seguridad a una red significa desarrollar procedimientos y planes que protegerán a los recursos de la red contra perdida y daños por ejemplo por parte de hackers.

Las políticas de seguridad se dividen generalmente en dos tipos:

- Todo aquello que no está expresamente permitido está prohibido.
- Todo lo no es específicamente negado se permite.

1.6.1.1 Tipos de firewall

- **A nivel de Aplicación:** este tipo de firewall se los realiza a nivel de capa 7 del modelo de referencia OSI[8], estos normalmente son servidores Proxy que se utilizan como traductores de direcciones de red tomando en cuenta que tipo de tráfico está cruzando de un lugar a otro, permitiendo un monitoreo de los datos.

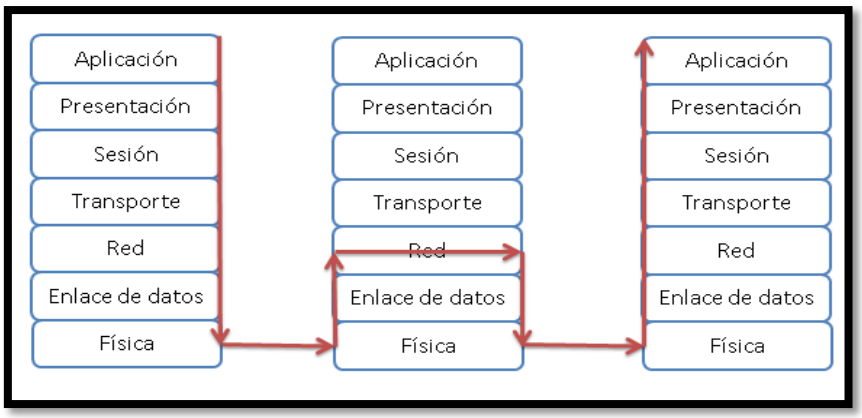


Figura 4. Firewall a nivel Aplicación
Fuente: Firewall Recuperado de: http://es.kioskea.net/contents/590-firewall

[8] **OSI** (Open Systems Interconnect): Interconexión de Sistemas Abierto

- **A nivel de Red:** En este caso analiza el tráfico a nivel de capa 3 del modelo de referencia OSI, las decisiones son tomadas según la dirección de origen y destino de los datos. Este tipo de firewall ofrece una mayor seguridad al momento de permitir o denegar servicios.

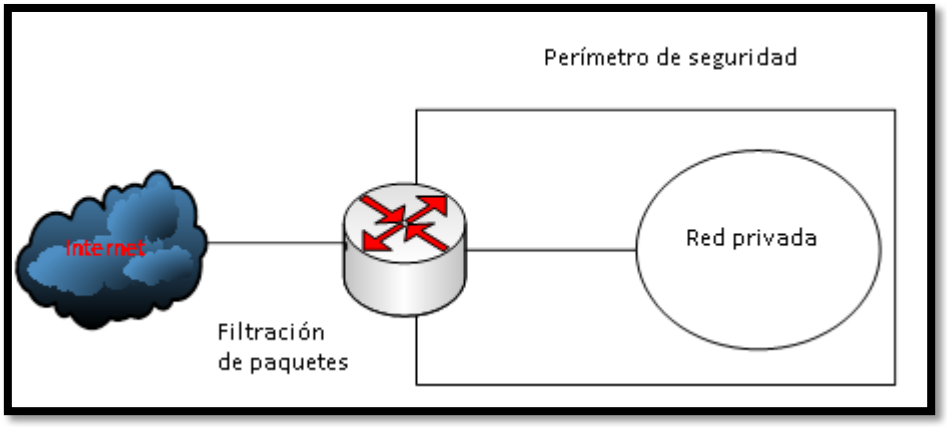


Figura 5. Firewall a nivel Red
Fuente: Firewall Recuperado de: http://es.kioskea.net/contents/590-firewall

1.6.2 VPN

Una red privada virtual (VPN) es una tecnología muy utilizada en empresas de gran tamaño facilitando la extensión de la red pública, de tal forma que permite una conexión segura sin ningún riesgo restringiendo la información a personas ajenas a la empresa u organización.

Cuando se transmiten datos sobre la internet estos son más vulnerables que cuando se encuentran dentro de una red local, por lo que una VPN utiliza túneles para el modo de envío de la información a través de la internet de tal forma que permita a los usuarios que se encuentran en los extremos del túnel disfrutar de la seguridad, privacidad y funciones que antes estaban disponibles solo en redes privadas.

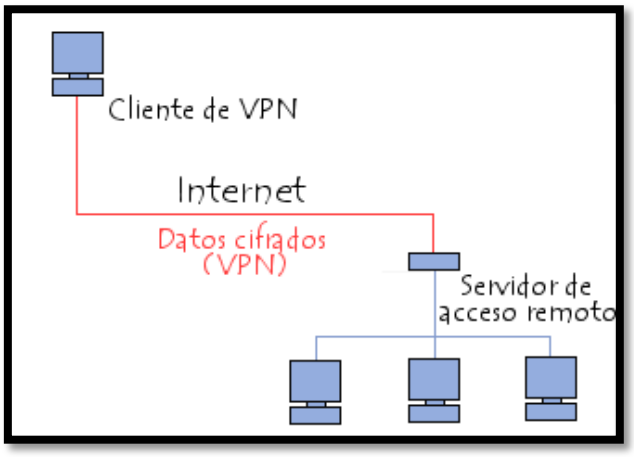


Figura 6. Una red privada virtual
Fuente: Funcionamiento de una VPN Recuperado de: http://goo.gl/ghYxjq

1.6.3 NAT

Un NAT (Network Address Translation –Traducción de direcciones de red), es un esquema implantado por las organizaciones para desafiar la deficiencia de direcciones de las redes IPv4, básicamente traduce direcciones privadas que son normalmente internas a una organización en particular, en direcciones ruteables sobre las redes públicas como internet.

El NAT tiene la tarea de traducir las IPs privadas de la red en una IP pública para que la red pueda enviar paquetes al exterior; y luego realizarla de forma inversa, es decir, traducir luego esa IP pública, de nuevo a la IP privada de una desktop.

Uno de los objetivos de NAT es aumentar las direcciones IP’s mediante la traducción de direcciones de red, de esta manera, proporcionando un nivel de seguridad que complementada con un firewall brindará una mayor seguridad para la red interna de cualquier organización. Como se puede apreciar NAT es un mecanismo muy potente que nos permite crear redes locales con gran flexibilidad.

1.6.4 Modelos de autentificación

Los modelos de autentificación son herramientas que permiten identificar los usuarios o servicios, facilitando el intercambio de la información de manera más segura.

1.6.4.1 Autenticación biométrica

Estos sistemas se basan en características físicas del usuario a identificar como por ejemplo: sus rasgos de su cara o por su voz, de tal forma al usuario le permita autentificarse para que pueda acceder de forma confiable a un determinado recurso.

1.6.4.2 Contraseñas

El método de autentificación se basa en una contraseña donde el usuario la conoce, esta debe llevarse de forma secreta para mantener la autentificación confiable. Pero las contraseñas brindan una seguridad muy frágil debido a que estas pueden ser adivinadas, robadas o si el usuario no la mantiene secreta hace que la confiabilidad se pierda.

1.6.4.3 Tarjetas inteligentes

Una tarjeta inteligente es un dispositivo de seguridad del tamaño de una tarjeta de crédito, proporciona una seguridad pero no completa debido a que puede ser adulterada. Este método de autentificación se basa a tecnología VLSI[9].

1.6.5 Software antivirus

El software antivirus es un programa de computación que detecta, previene y toma medidas para desarmar o eliminar programas de software malintencionados, como virus y gusanos.

Su funcionamiento radica en el reconocimiento de la firma de un virus conocido (Alulema, 2008) afirma que es:

[9] **VLSI**: Very Large Scale Integration, integración en escala muy grande.

Un programa que detecta un virus cuando encuentra una coincidencia entre los resultados escaneados y las firmas de virus almacenados en las bases de datos, estas deben ser actualizadas regularmente caso contrario el programa antivirus se vuelve obsoleto rápidamente.

1.6.6 Sistemas de detección de intrusos

Los sistemas detectores de intrusos son una herramienta de defensa capaz de detectar posibles ataques, aun contando con firewalls que bloquean cierto tipo de flujo de datos, no siempre se puede garantizar que estos estén funcionando como se espera, cuando no es posible bloquear cierto tipo de tráfico y este logra entrar a la red, el sistema detector de intrusos lanza una alarma indicando alguna anomalía alojando esta información en bitácoras o a través de la generación de reportes específicos.

EL IDS cuenta con una base de datos donde aloja los ataques más conocidos que se realizan en la red, por lo tanto, este analiza el tráfico que circula dentro de la red haciendo uso de sensores virtuales para analizarlo y comprobar el tipo de tráfico que es, su contenido y su comportamiento.

Son la parte fundamental de la seguridad de los firewall, estos monitorizan la actividad de los sistemas en busca de violaciones de las políticas de seguridad, tales como ataques de denegación de servicios, sustracción o modificación de la información.

En la Figura 7 se muestra el funcionamiento de un sistema de detección de intrusos

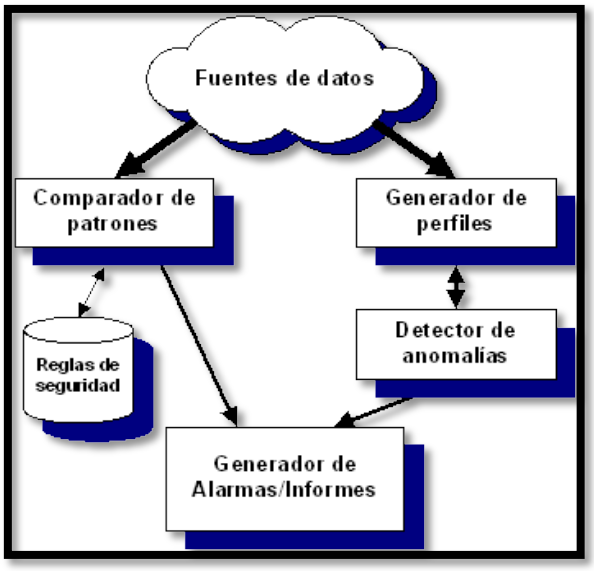


Figura 7. Esquema general de un Sistema Detector de Intrusos
Fuente: Elementos de detección de intrusos Recuperado de: http://www.dgonzalez.net/papers/ids/html/cap02.htm

Existen tres tipos de sistemas de detección de intrusos:

1.6.6.1 HIDS (Host-Bases Intrusion-Detection System)

Es un IDS que vigila un único equipo y por tanto su interfaz corre en modo no promiscuo. La ventaja es que la carga de procesado es mucho menor.

1.6.6.2 NIDS (Network-Based Intrusion Detection System)

Es un sistema de detección de intrusos en una red, detectado intrusiones en todo un segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el

tráfico de la red. Puede estar instalado en uno de los equipos del segmento de la red o en un equipo de la red como un hub o switch.

1.6.6.3 NIPS (Network Intrusion Prevention System)

(VINUEZA, 2012) Encontró lo siguiente:

> Un sistema de prevención de intrusos basado en red es un tipo de mecanismo de seguridad que combina eficientemente las funciones de monitoreo y análisis de los IDS, con la respuesta automática activa que proveen los cortafuegos, de manera que no solo detectan la presencia de intrusos, sino que bloquean y mitigan ataques informáticos.

1.7 Selección de herramientas de monitoreo

El proceso de selección de software es muchas veces ignorado aunque es extremadamente importante al momento de realizar una adopción de un sistema, por lo que es importante identificar 3 etapas que se deben seguir para seleccionar de forma exitosa una herramienta ya sea en código abierto o comercial.

- Identificar sus requerimientos
- Buscar los sistemas que se pacten a los requerimientos funcionales.
- Seleccionar el sistema apropiado que se ajuste a los requerimientos

1.7.1 Características y requerimientos de red

Para la selección del software se debe tomar en cuenta los requerimientos necesarios de la infraestructura de red.

- Implementación sobre cualquier sistema operativo.
- Debe poder monitorear distintas plataformas.
- La aplicación de monitorización debe vigilar sistemas y aplicaciones
- Debe monitorear hardware y software tales como (aplicaciones, Sistemas Operativos, bases de datos, servidores web, procesos, servicios).
- Debe generar informes, estadísticas.
- Debe monitorear todos los equipos que son parte de la infraestructura de red.

1.7.2 Herramientas de monitoreo

Implementar un esquema de seguridad requiere de varias herramientas basadas en software o una combinación de software y hardware, el uso de sensores permite conocer el comportamiento del uso de la red y con ello determinar si se está haciendo un uso adecuado de la misma.

Existen una gran cantidad de herramientas útiles para llevar a cabo este tipo de actividades, a continuación solo se describen algunas de estas herramientas de manera general.

1.7.2.1 Axence NetTools

Axence NetTools es un conjunto completo de control de host, escaneado en red, seguridad y herramientas de administración con una interfaz de usuario muy intuitiva es una combinación fuerte de herramientas todas útiles para un diagnóstico de la supervisión de las conexiones de red del ordenador.

Entre sus características importantes (Software, 2014) menciona las siguientes:

- Escanea la dirección IP.
- Vigila los puertos.
- Escanea los puertos.
- Verifica la dirección.
- Escanea los puertos activos y pasivos.
- Escaneo avanzado de los puertos.
- El más rápido escáner de host (UDP)
- Escáner para HTTP (análisis para el puerto 80 abierto en subred).
- Buscador de paquete TCP.
- Monitoreo del ancho de banda.
- Lista de identificación de puerto (+ escáner de puerto).
- Obtiene información rápida de red.
- Obtiene la dirección remota de MAC.

1.7.2.2 Ntop

Ntop es una herramienta que todo administrador de red la puede utilizar, se basa en código abierto utilizada para controlar en tiempo real los usuarios y aplicaciones que se encuentran consumiendo recursos de la red, permitiéndole al administrador estar siempre informado de cualquier problema de seguridad de tal forma simplificado así la tarea del administrador.

Una gran ventaja que ofrece Ntop es la capacidad de realizar escaneos de diferentes equipos que forman parte de la infraestructura de red con la finalidad de conocer la distribución del tráfico, además se obtiene estadísticas particulares de cada equipo

1.7.2.3 Nmap

Nmap es una herramienta muy utilizada en software libre aunque se encuentra disponible para diferentes sistemas operativos entre sus características tenemos que es útil para el rastreo de puertos abiertos, para evaluar la seguridad de sistemas informáticos y para descubrir servicios o servidores en una red informática.

1.7.2.4 Wireshark

Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones como una herramienta didáctica.

Entre sus características importantes (Samboni, 2006) menciona las siguientes:

- Disponible para Windows y Unix
- Captura paquetes en vivo desde una interfaz de red
- Muestra paquetes con información detallada de los mismo
- Abre y guarda paquetes capturados
- Importa y exporta paquetes en diferentes formatos
- Filtrado de información de paquetes
- Resaltado de paquetes dependiendo del filtro
- Crear estadísticas

En la siguiente tabla 1 se detalla las características necesarias para la selección de la herramienta de monitoreo más eficiente dependiendo de los requerimientos del usuario y de la red mediante un cuadro comparativo.

Tabla 1. Tabla comparativa para las selección de las herramientas de monitoreo

CARACTERÍSTICAS	AXENCE NETTOOLS	NTOP	NMAP	WIRESHARK
Implementación sobre cualquier sistema operativo	✓	✓	✓	✓
Debe poder monitorear distintas plataformas	✓	✓	✓	✓
La aplicación de monitorización debe vigilar sistemas y aplicaciones	✓		✓	
Captura y Filtrado de paquetes				✓
Escaneo de puertos activos y pasivos	✓		✓	
Uso de una interfaz web		✓		
Medición de throughput		✓		✓
Debe monitorear todos los equipos que son parte de la infraestructura de red	✓	✓	✓	
Capacidad y proceso de reacción apropiada ante condiciones que se encuentren fuera del alcance del software		✓		✓
Manejo de alertas	✓		✓	
Bajo licencias libres	✓	✓	✓	✓
Funcionalidad de como satisfacer las necesidades del usuario			✓	✓
Facilidad para la implementación	✓	✓	✓	✓
Estabilidad a nivel de fallos		✓		✓
Visualización de gráficos		✓		✓

Fuente: Realizado por Gabriela López

Las herramientas utilizadas serán las siguientes:

Para el monitoreo de puertos son las siguientes:

- Axence NetTools
- NMAP

Para el monitoreo de tráfico se utilizará las siguientes:

- NTOP
- Wireshark

Las herramientas para el monitoreo de la red se las seleccionó mediante la Tabla 1 donde se muestra las diferentes características que permitan mantener un continuo monitoreo y análisis de tráfico de la red, determinando el tipo de información que circula por el canal de comunicación.

1.8 Estándares de seguridad informática

Los estándares de seguridad son una herramienta que apoyan a la gestión de la seguridad informática, ya que los ambientes cada vez más complejos requieren de modelos que administren las tecnologías de manera integral, sin embargo, existen distintos modelos aplicables en la administración de la seguridad (Seguridad, s.f).

1.8.1 Estándar internacional ISO/IEC 27001

De acuerdo (Estándar Internacional ISO/IEC 27001), menciona que:

> Los estándares internacionales son una muy buena guía que proporciona un modelo para establecer implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). El diseño e implementación del SGSI de una organización está influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados el tamaño y estructura de la organización.

Entre los puntos importantes a considerar con relación a los estándares internacionales, enfocándose en el ISO 27001 se encuentran:

Adoptan algún modelo para aplicarse a los procesos de SGSI, como lo es el modelo PDCA (Planear-Hacer-Checar-Actuar). En la Figura 8 muestra el desarrollo el proceso de implementación de un SGSI:

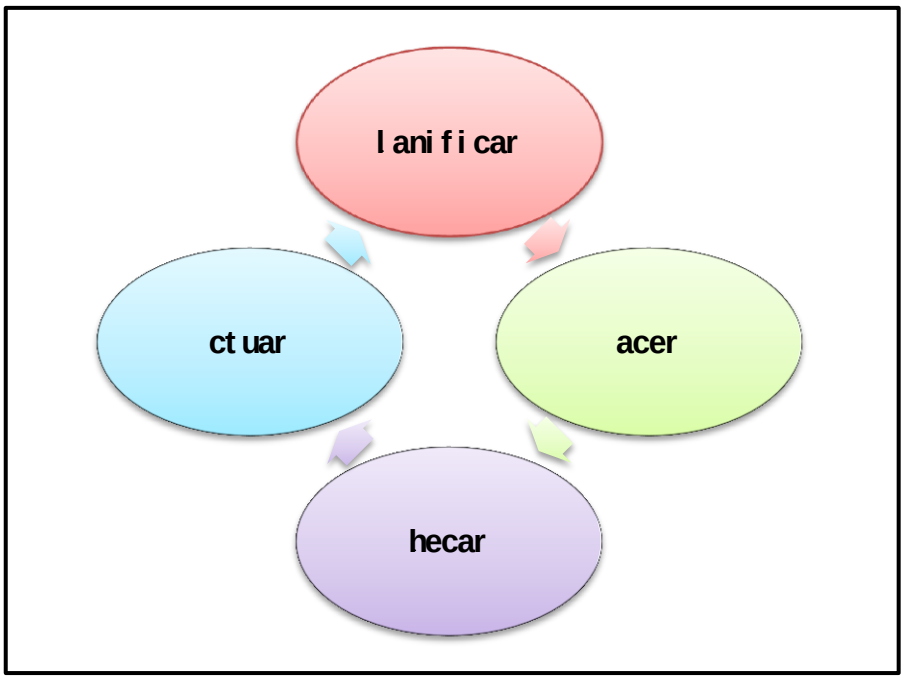


Figura 8. Modelo de desarrollo PDCA
Fuente: Modelo de Gestión (Muro, 2010) Recuperado de: http://goo.gl/poG11L

1.8.1.1 Modelo PDCA

A continuación, vamos a describir las actividades que se realizan en cada una de las cuatro fases del ciclo PDCA.

- **Planificar**

  En esta fase se establecen políticas, objetivos, procesos y procedimientos relevantes para mejorar el riesgo y mejorar la seguridad de la información. Las políticas de seguridad que considere los requerimientos para que luego puedan ser aprobados por la dirección o la gerencia.

- **Hacer**

  Esta fase cubre la implantación de las políticas, controles, procesos y procedimientos que reduzcan el riesgo a niveles considerados como aceptables.

- **Checar**

  Durante esta fase se realizan diferentes tipos de revisiones para comprobar la correcta implantación del sistema, es decir, evaluar y medir el desempeño del proceso en comparación con la política, objetivos y de esta forma reportar los resultados a la gerencia para su revisión.

- **Verificar**

  Tomar acciones correctivas y preventivas basadas a una auditoría interna para el mejoramiento del SGSI, comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar la forma de proceder, además es importante tener la seguridad de que las mejores introducidas alcanzan los objetivos previstos.

1.8.1.2 Áreas y controles

La norma se desarrolla en 11 áreas o dominios que recogen los 133 controles a seguir.

- Política de seguridad.
- Organización de la información de seguridad.
- Administración de recursos.
- Seguridad de los recursos humanos.
- Seguridad física y del entorno.
- Administración de las comunicaciones y operaciones.
- Control de accesos.
- Adquisición de sistemas de información, desarrollo y mantenimiento.
- Administración de los incidentes de seguridad.
- Administración de la continuidad de negocio.
- Marco legal y buenas prácticas.

1.8.1.3 Beneficios

La norma ISO/IEC 27001 puede aportar las siguientes ventajas a la industria.

- Demuestra la independientemente que se respete las leyes y normativas que sean de aplicación. Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Un análisis de riesgos, identificando amenazas, vulnerabilidades e impactos en la actividad empresarial.

- Una mejora continua en la gestión de la seguridad.
- Una garantía de continuidad y disponibilidad del negocio.
- Reducción de los costos vinculados a los incidentes.
- Voluntad de cumplir con la legislación vigente de protección de datos de carácter personal, servicios de la sociedad en la información, comercio electrónico, propiedad intelectual y en general, aquella relacionada con la seguridad de la información.

CAPÍTULO II

2 Estudio De La Situación Actual De La Red

Dentro de este capítulo se estudia la situación actual de la infraestructura de red de la industria lechera FLORALP S.A, se identifica las principales vulnerabilidades que atentan contra la red mediante herramientas de monitoreo y el diagnóstico de la red, de esta forma, conocer los requerimientos necesarios para el diseño del sistema de seguridad perimetral.

2.1 Descripción de la industria lechera la FLORALP

Es una industria dedicada a la elaboración y comercialización de productos lácteos artesanales especializada en quesos maduros, manteniendo características de origen y calidad exigidas por el mercado, asegurando una relación personal, justa y transparente con sus clientes, proveedores, la comunidad y el medio ambiente.

2.1.1 Antecedentes

FLORALP es una industria con visión de futuro, desde su inicio ha innovado y crecido a través de los años empezó elaborando leche pasteurizada y quesos frescos. Hoy se ha convertido en el ejemplo de la industria láctea en la producción de quesos maduros artesanales como son queso holandés, cheddar, brie, camembert, gruyere, parmesano, tilsiter, raclette,

ricotta, mozarella, mantequilla, crema, queso crema, yogurt, etc. Ubicando sus productos en los mejores autoservicios, hoteles, restaurantes, cafeterías, e industrialmente a nivel nacional.

FLORALP crece paulatinamente gracias a la gran familia que se ha formado así es como nace la sociedad de padres e hijos dándole una figura legal más establecida, de tal forma se hace necesario visualizar un camino más claro y empezar a usarse herramientas de planeación estratégica, concluyendo en una visión del futuro que fue el primer motor de establecimiento de sistemas integrados de operaciones, construcción de armonía, sensibilización frente a la comunidad, el medio ambiente y a la nutrición del consumidor final.

Así la era del desarrollo humano, de procesos, de gestión de la calidad, de la mejora continua, del involucramiento donde la decidida intervención apoyo y ejecución de los miembros de la familia gravitaban enormemente en la consecución de las metas y objetivos; fortaleciendo los canales de comunicación internos y mejorando con preocupación permanente la calidad de vida, el conocimiento y el involucramiento de todos los colaboradores de todas las áreas.

FLORALP tiene sus plantas de elaboración de quesos en San Gabriel, Ibarra, Zuleta, y desde hace cinco años en Oxapamba-Perú y sus puntos de distribución y oficinas comerciales están en Ibarra, Quito, Guayaquil, Cuenca, Lima y Perú; hoy está trabajando en la posibilidad de abrir mercado hacia Centro América.

De esta forma se lleva adelante una prospectiva de mercados internacionales naturales para los productos de la industria, siempre definida en hacer quesos maduros de excelente calidad para nichos especializados de dichos quesos y enmarcados en un sistema de gestión integral que garantice la sustentabilidad de la industria y la satisfacción de sus consumidores.

2.1.2 Ubicación geográfica

La FLORALP se encuentra ubicada al Norte de Ecuador, en la provincia de Imbabura, ciudad de Ibarra, en la calle Princesa Pacha 5-163.

2.1.3 Misión

FLORALP es una industria dedicada a la elaboración y comercialización de productos lácteos artesanales especializada en quesos maduros, manteniendo características de origen y calidad exigidas por el mercado, asegurando una relación personal, justa y transparente con nuestros clientes, proveedores, la comunidad y el medio ambiente.

2.1.4 Visión

Alcanzar hasta el año 2020 el crecimiento sustentable de productos lácteos a nivel nacional y americano, aprovechando nuestra experiencia y armonía organizacional, que sirvan de base para la formación de un grupo empresarial y familiar que impulse iniciativas para

mejorar las condiciones nutricionales, culturales, de educación y medio ambiente tanto para sus miembros como para la comunidad, sus clientes y proveedores.

2.1.5 Principios y valores corporativos

Los principios y valores son una parte fundamental dentro de una empresa de tal manera los valores son el reflejo del comportamiento humano basándose en los principios ya que estos son parte importante del que rigen el pensamiento y la conducta de los integrantes que forman parte de una organización.

2.1.5.1 Principios

- Una industria orientada a la satisfacción del cliente y sustentada en resultados.
- Brindar una mayor variedad de servicios que otras industrias competidoras.
- Lealtad y compromiso con la Industria, clientes y proveedores en la maximización de nuestro beneficio.
- Responsabilidad y eficiencia en todos los niveles.
- Innovar continuamente basándonos en las necesidades de nuestros clientes.
- Descentralización y equidad en las actividades internas.
- Potenciar en cada uno de los empleados el compromiso de servicio a la comunidad.
- Demostrar un nivel de disciplina y mejoramiento continuo.
- Liderazgo para todos y en todos los niveles.

2.1.5.2 Valores

FLORALP está basada en una cultura organizacional sencilla, fruto de los criterios de su fundador que hace vivir en la industria la puntualidad, honestidad, transparencia, sencillez y solidaridad con los seres humanos. Ser respetuosos, leales, nobles, justos, constantes y consistentes. Buscar la productividad, la versatilidad, la conciliación y alcanzar el referente de la industria láctea en Ecuador por la capacidad de innovación y armonía organizacional.

- **Honestidad sobre todas las cosas.-** Significa que no hay contradicciones ni discrepancias entre los pensamientos, palabras o acciones. Ser honesto con el verdadero ser y con el propósito de una tarea gana la confianza de los demás e inspira fe en ellos.
- **Compromiso con la organización.-** Es decir, sentir el trabajo como un reto, identidad con la tarea interacción con otros a discreción, retroinformación, actitudes del grupo, percepción de la propia importancia en la organización, así como las inversiones de tiempo, esfuerzo y otras efectuadas en la organización, expectativas de recompensa, confianza en la organización, capacitación, etc.
- **Respeto a las personas.-** Es aceptar y comprender tal y como son los demás, aceptar y comprender su forma de pensar aunque no sea igual que la nuestra.
- **Igualdad de oportunidades.-** Es el principio que reconoce a todos los ciudadanos capacidad para los mismos derechos, se refiere a que tienen las mismas opciones, esto es "Igualdad Social".

- **Iniciativa.-** Se refiere a hacer, lo que se debe de hacer, bien hecho; sin que nadie lo mande. A quien hace una cosa bien hecha sin que nadie se lo ordene, sigue aquel que la hace bien cuando se le ha ordenado una sola vez.
- **Perseverancia con inteligencia.-** Es aquella que se sostiene en una voluntad firme, constante, superior al tiempo.
- **Creatividad.-** Se refiere a la aptitud para crear o inventar. Se la identifica como la habilidad de usar sus pensamientos, valores, emociones y acciones para enriquecer su ambiente de formas nuevas y únicas.
- **Disciplina.-** Es la instrucción que posee una persona en torno a cierta doctrina y la forma precisa en que lo lleva a la práctica. Exige un orden y unos lineamientos para poder lograr más rápidamente los objetivos deseados, soportando las molestias que esto ocasiona.

2.1.6 Infraestructura

Industria lechera FLORALP cuenta con cinco plantas de producción, cuatro se encuentran en Ecuador, Ibarra, San Gabriel como plantas propias, Hacienda Zuleta como socios estratégicos, Nono en conjunto con los ganaderos y una ubicada en Perú, Oxapamba.

Todas las plantas la colocan como una de las industrias más versátiles en su capacidad de producir varios tipos de quesos, especialmente, sin dejar de lado la producción de mantequilla y crema, así como de leche pasteurizada.

Sin embargo, el diseño de las instalaciones de las diferentes plantas tiene mayor capacidad para la producción de quesos de todos los tipos, frescos, semi maduros, maduros, duros y blandos.

En la actualidad la industria posee una capacidad de producir hasta 5000 kilos de queso diarios, y dependiendo del tipo de queso esta puede ampliarse o disminuirse. En el caso de quesos frescos se podría producir hasta 8000 kilos por día y en el caso de maduros hasta 4000 kilos por día.

Figura 9. Ubicación de la Industria lechera la FLORALP

Fuente: Google Maps Recuperado de: http://goo.gl/t5r0cL

2.1.7 Organigrama organizacional

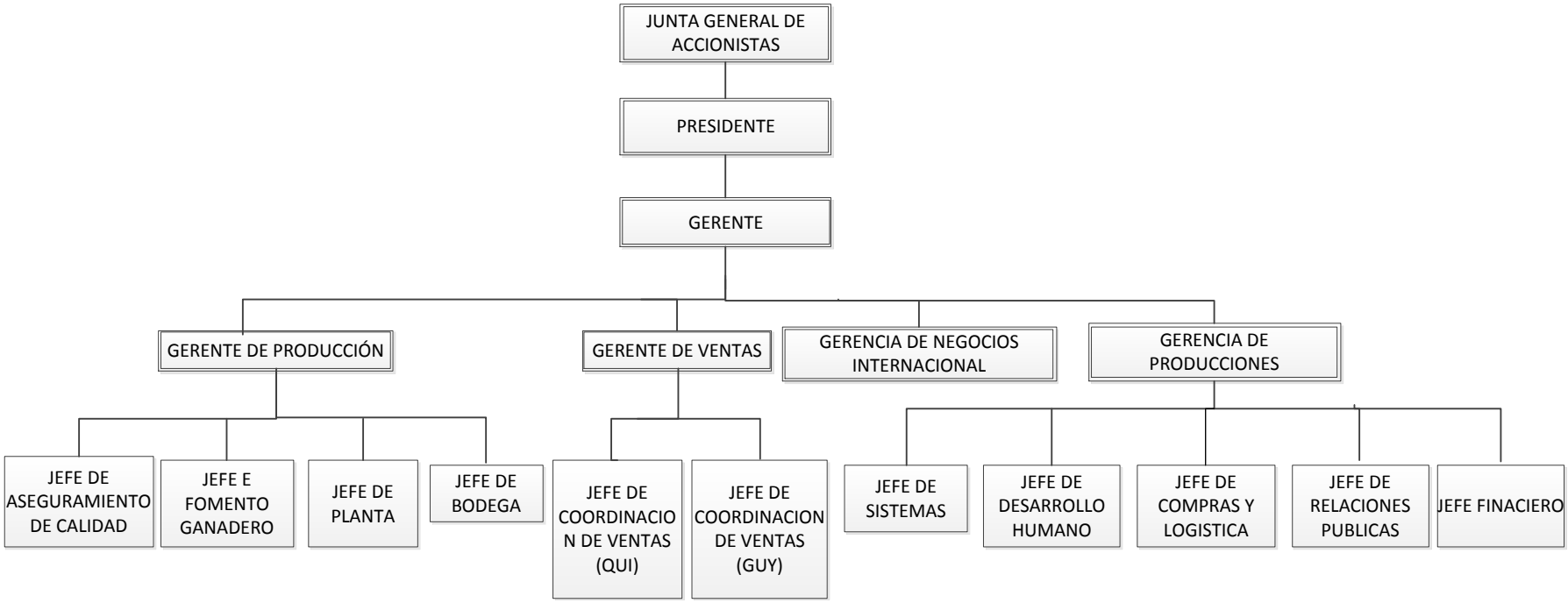


Figura 10. Organigrama organizacional de la FLORALP

Fuente: Proporcionado por el Departamento de Talento Humano

2.1.7.1 Descripción del organigrama organizacional

La industria lechera la FLORALP S.A tiene delimitadas sus funciones y obligaciones mediante una estructura organizacional, en la cual se ocupan diferentes cargos dependiendo de sus laborares dentro o fuera de la industria y se tiene los siguientes departamentos y jefaturas.

2.1.7.1.1 Departamento comercial

Este departamento tiene diversas funciones, una de las más importantes es el representante del cliente dentro de la industria cuya función se centra en la maximización de valor para el consumidor, la satisfacción plena de este con el fin de elevar la rentabilidad de la propia industria por el incremento de su participación en el mercado. Entre las funciones y actividades que realiza dentro de la industria mediante el servidor de aplicaciones son las siguientes:

Figura 11. Funciones realizadas por el Departamento Comercial
Fuente: Servidor de Aplicaciones Recuperado de: http://clikex.floralp-sa.com/clikex/x32_index.htm

2.1.7.1.2 Departamento de sistemas

La principal función del Departamento de Sistemas es crear y ofrecer sistemas de información que permitan dar solución a las necesidades informáticas y de toma de decisiones de la industria. Además, este departamento tiene acceso a todos los recursos de la red para realizar cualquier modificación o configuración tanto en servidores como dispositivos de red, actualmente se encuentran laborado dos personas que son el Jefe de Sistemas y el Asistente.

2.1.7.1.3 Departamento de ventas

Organiza las ventas directas y la relación con intermediarios. A través de la venta, la industria consigue sus ingresos o facturaciones con el objetivo de compensar los gastos de producción y obtener ganancias, las funciones realizadas por el personal que labora en el departamento se pueden apreciar en la Figura12.

2.1.7.1.4 Departamento de compras

Este departamento tiene la función interna de solucionar y satisfacer las necesidades de sus clientes externos, atendiendo las peticiones que le lleguen y una de sus funciones externas es buscar proveedores adecuados y negociar, si procede, las mejores condiciones para la industria. Además, este departamento debe cuidar los costos y los gastos que la industria se produzca ya que se encarga de negociar las mejores condiciones de financiamiento de los

productos o servicios comprados. En la siguiente Figura 12 se puede apreciar las funciones o actividades realizadas dentro del servidor de Aplicaciones de la institución.

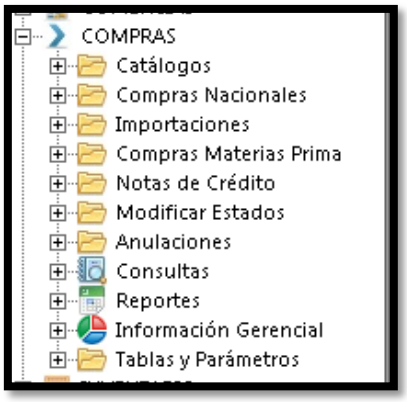


Figura 12. Funciones realizadas por el Departamento de Compras
Fuente: Servidor de Aplicaciones Recuperado de: http://clikex.floralp-sa.com/clikex/x32_index.htm

2.1.7.1.5 Departamento contabilidad y financiero

Este departamento es el más amplio debido a que laboran varias personas con diferentes cargos como gerentes, jefes y auxiliares de contabilidad que son de suma importancia para la industria, ya que aquí abarcan todo lo referente al manejo de las finanzas y contabilidad que se divide de forma jerárquica.

- **Gerente de finanzas**
  - ✓ Jefe de Contabilidad
    - ▪ Auxiliares

Entre sus funciones que realizan por medio del servidor de aplicaciones son las siguientes como se observa en la Figura 13.

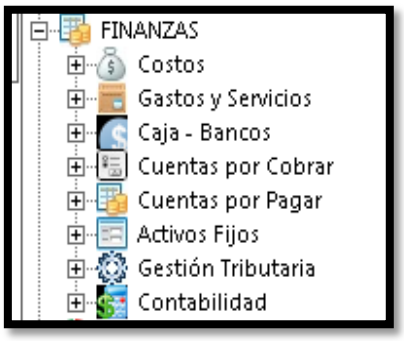


Figura 13. Funciones del Departamento de Finanzas
Fuente: Servidor de Aplicaciones Recuperado de: http://clikex.floralp-sa.com/clikex/x32_index.htm

2.1.7.1.6 Departamento de fomento ganadero

Este departamento se encarga de tratar con los proveedores de leche donde se establecen las condiciones de pago que van a regir todas las operaciones comerciales entre ambas industrias.

2.1.7.1.7 Departamento de talento humano

Este departamento se encarga de todos los procesos para dirigir al personal dentro de la industria, partiendo de la selección de las personas para los diferentes cargos que han sido escogidos y mantener al personal dentro de la industria que trabajen y den lo máximo de sí mismo con actitud positiva y favorable para lograr los objetivos y metas de la industria.

2.1.7.1.8 Jefaturas de seguridad y salud

Se establece los estándares necesarios para respetar especificaciones de producciones requeridas en cuanto a calidad, se regula el producto final con sus debidas características y realizando pruebas de verificación del producto de tal forma satisfaciendo las expectativas del cliente.

2.1.7.1.9 Departamento de mantenimiento

Este departamento se encarga de las tareas técnicas relacionadas con la fabricación, construcción, montaje, funcionamiento, mantenimiento y reparación de máquinas, equipos e instalaciones mecánicos.

2.1.7.1.10 Departamento de bodega

Este departamento se encarga del control y orden de los productos que se encuentran en bodega, tomando los pedidos de acuerdo con lo solicitado por el departamento de ventas.

2.2 Situación actual de la red de datos de la industria lechera FLORALP

Para un correcto diseño de un sistema de seguridad perimetral es importe conocer la situación actual de la infraestructura de red de datos. La topología de red de la industria FLORALP S.A brinda múltiples servicios como son: la trasmisión de datos donde esta permite

compartir servicios internos como los accesos a sistemas de contabilidad, consulta a bases de datos, a redes inalámbricas y publicaciones web, permitiendo de esta forma el desarrollo integral de la industria.

2.2.1 Topología de la red

La topología física de la red de datos de la industria lechera FLORALP S.A permite conocer la estructura de conexiones que tienen los equipos de red y la función que se encuentran desempeñando dentro de la misma. A través de la Figura 14 se podrá apreciar si se encuentra implementado algún modelo jerárquico o es una red plana.

Con esta base se realiza el análisis y la descripción de cada elemento de networking, lo cual permita determinar que equipos se encuentran actualmente en funcionamiento.

2.2.2 Descripción de la topología de la red

Como se observa en la Figura 14 se trata de una red plana que hace uso de varias direcciones IP’s, además, no cuenta con un modelo jerárquico por lo que a continuación se detalla cada equipo de networking.

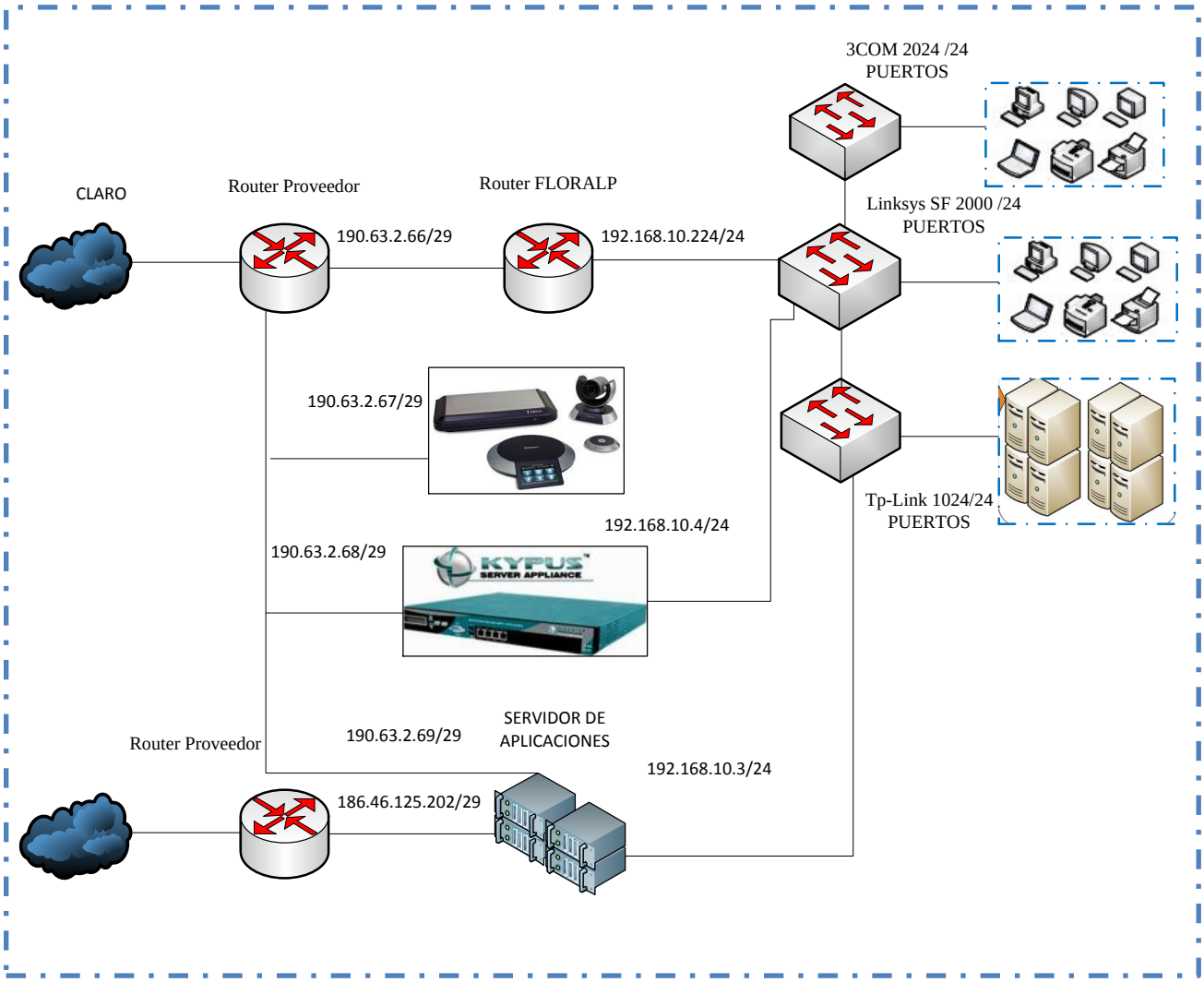


Figura 14. Diagrama de topología de red

Fuente: Graficación en Microsoft Visio 2010 realizado por Gabriela López

Se cuenta con dos routers un Cisco 1700 del proveedor de CLARO y un Cisco1800 del proveedor de CNT[10] que son de propiedad de cada proveedor.

En la parte de distribución existe el router Cisco-Linksys WRT110 donde este hace uso de una de las cuatro IP's públicas, por lo tanto, este canal al no ser filtrado por ningún

[10] **CNT:** Corporación Nacional de Telecomunicaciones

equipo de seguridad como firewall IDS/IPS (Sistema de Detección de Intrusos y Sistema de Prevención de Intrusos), representa una gran vulnerabilidad en cuanto al tráfico que puede ingresar o salir a través de este enlace.

Dos IP’s públicas del proveedor de Claro se usan, una para el servicio de LIFESIZE y la otra IP para el servidor KYPUS donde este brinda el servicio de Firewall diseñado para prevenir el acceso no autorizado, además, este equipo se conecta hacia el switch Linksys SF 2000 donde también provee el servicio de conexión de los usuarios hacia la red externa.

En lo referente al acceso se distingue dos capas: la primera conformada por el switch 3Com 2024 que se encuentra ubicada para la planta de producción que se conecta a través de Fibra Óptica hacia el switch Linksys SF 2000 para la planta administrativa y la segunda por el switch Tp-Link 1024 para la conexión de los servidores, donde estos dan el servicio a los usuarios.

Para el acceso al wireless se lo realiza mediante tres antenas ROCKET M2 de 2.4GHz con SSID X, Y, Z que estas se encuentran conectadas al switch 3COM 2024 ubicado en la planta de producción.

Como se mencionó con anterioridad existen dos proveedores del servicio de Internet Claro y CNT donde cada uno brinda un ancho de banda de 3 Mbps con una compartición 1 a 1, donde cada uno asigna cinco direcciones IP. La conexión principal es mediante fibra óptica, la misma que llega al ODF's Optical-Fiber Distribution Frame (Distribuidor de Fibra Óptica).

CNT se encuentra en una conexión independiente por lo que este se dedica solamente para el servidor de Aplicaciones principal, este servidor además hace uso de una dirección pública del proveedor de CLARO como backup

La topología de red no cuenta con ningún modelo de calidad de servicio es decir no tiene priorización en el tráfico, además, no cuenta con una distribución de VLAN's[11] por lo que dificulta la administración y la gestión de la red.

Los usuarios que acceden a través de la red wireless, usualmente son usuarios temporales que hacen uso del servicio cuando tiene reuniones con los directores y además ciertos usuarios internos que poseen equipos personales.

El cableado estructurado de la mayoría de la planta es de categoría 5e, existen diferentes dependencias donde existe cableado categoría 6, el mismo que tiene un tiempo de uso de aproximadamente 10 años siendo el límite máximo según la norma ASI/EIA/TIA-568B[12] de cableado estructurado. El cableado soporta diversas aplicaciones como de voz y datos, donde la mayoría se encuentran etiquetados para facilitar la administración e identificar posibles errores dentro de la red, pero no existe una documentación completa y precisa del cableado de la red, la tecnología que se maneja actualmente a nivel de interfaces FastEthernet con velocidades de 100 Mbps y 1Gbps.

[11] **VLAN (Virtual Local Area Network):** Es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

[12] **ASI/EIA/TIA-568B:** Estándar para cableado estructurado para servicios de telecomunicaciones.

En toda la planta existen aproximadamente 25 puntos de datos y 23 de voz en el cableado estructurado que se encuentran sin certificar.

Por lo tanto, en la red de datos no existe sistema de protección completo que controle el tráfico que ingresa o sale de ella, convirtiéndose en otra vulnerabilidad, teniendo en cuenta que la mayoría de ataques que se pueden producir, suele suceder por usuarios de la red de datos interna.

2.2.3 Direccionamiento IP

La red de datos de la industria FLORALP utiliza 10 direcciones IP’s públicas que se describen los rangos en la siguiente Tabla 2.

Tabla 2. Direcciones IP's Publicas

IP PÚBLICA	MÁSCARA	DESCRIPCIÓN
190.63.x.x	255.255.255.0	ROUTER FLORALP
190.63.x.x	255.255.255.0	LIFESIZE
190.63.x.x	255.255.255.0	RED EXTERNA
190.63.x.x	255.255.255.0	APPEON
190.63.x.x	255.255.255.0	SIN USO
186.46.x.x	255.255.255.0	SERVIDOR DE APLICACIONES
186.46.x.x	255.255.255.0	SIN USO
186.46.x.x	255.255.255.0	SIN USO
186.46.x.x	255.255.255.0	SIN USO
186.46.x.x	255.255.255.0	SIN USO

Fuente: Proporcionado por el Departamento de Sistemas

La Tabla 3 incluye los rangos de direccionamiento lógicos principales de la red donde se lo detalla a continuación:

Tabla 3. Direcciones IP's de usuarios

ASIGNACIÓN DE SUBRED	MASCARA DE SUBRED	NOMBRE DEL EQUIPO	UBICACIÓN
192.168.10.3	255.255.255.0	IBASVRFLOCLIKEX	Data Center
192.168.10.5	255.255.255.0	IBASVRFLODOM	Data Center
192.168.10.6	255.255.255.0	SERVIDOR	Data Center
192.168.10.7		IBASVRFLODATA	
192.168.10.8		FW_FLORALP	
192.168.10.10	255.255.255.0	----------	Antenas Inalámbricas
192.168.10.11	255.255.255.0	----------	Antenas Inalámbricas
192.168.10.12	255.255.255.0	----------	Antenas Inalámbricas
192.168.10.14	255.255.255.0	VIRTUAL	
192.168.10.15	255.255.255.0	IBAFLOTIJEFE	
192.168.10.18	255.255.255.0	IBAFLOBODSUM	
192.168.10.19	255.255.255.0	IBAFLOFINGER	Planta Administrativa
192.168.10.20	255.255.255.0	IBAFLOFINGER	Planta Administrativa
192.168.10.22	255.255.255.0	IBAFLOFINCARTE	Planta Administrativa
192.168.10.23	255.255.255.0	IBAFLOFINAUX03	Planta Administrativa
192.168.10.24	255.255.255.0	IBAFLOPROPOR	
192.168.10.27	255.255.255.0	IBAFLODOC	
192.168.10.28	255.255.255.0	IBAFLOCALJEFE	Planta Administrativa
192.168.10.29	255.255.255.0	IBAFLOCOSTOS	Planta Administrativa
192.168.10.30	255.255.255.0	IBAFLOMANTENIMIENTO	Planta de Mantenimiento
192.168.10.31	255.255.255.0	IBAFLOMANALMA	Planta de

			Mantenimiento
192.168.10.32	255.255.255.0	IBAFLOTINAS	
192.168.10.39	255.255.255.0	IBAFLOFINPEREZ	Planta Administrativa
192.168.10.40	255.255.255.0	IBAFLOMANTALMAC	
192.168.10.41	255.255.255.0	IBAFLOFOMENTO	Planta Administrativa
192.168.10.42	255.255.255.0	IBAFLOAMBIENTEM	Planta Administrativa
192.168.10.47	255.255.255.0	IBAFLOCOMJEFE	Planta Administrativa
192.168.10.48	255.255.255.0	IBAFLODTHASIS	Planta Administrativa
192.168.10.49	255.255.255.0	IBAFLOGERASIS	Planta Administrativa
192.168.10.50	255.255.255.0	IBAFLOGERGEN	Planta Administrativa
192.168.10.56	255.255.255.0	MASTERMIX-PC	Planta Producción
192.168.10.57	255.255.255.0	IBAFLOCALLAB	Planta Producción
192.168.10.58	255.255.255.0	IBAFLOBODEGA	Planta Producción
192.168.10.60	255.255.255.0	MACBOOKPRO-6B45	Planta Producción
192.168.10.63	255.255.255.0	IBAFLOBODCEN	
192.168.10.67	255.255.255.0	UIOFLOPROCBO	Planta Administrativa
192.168.10.91	255.255.255.0	IBAFLOTIJEFE	Planta Administrativa
192.168.10.93	255.255.255.0	IBAFLOPAQUITA	Planta Administrativa
192.168.10.94	255.255.255.0	IBAFLOFINALEX	Planta Administrativa
192.168.10.98	255.255.255.0	IBAFLOPROEMPA	Planta Producción
192.168.10.120	255.255.255.0	IBAFLOCALMICRO	
192.168.10.133	255.255.255.0	SERVERELASTIX	
192.168.10.146	255.255.255.0	IBAFLOACTIVOS	Planta Administrativa
192.168.10.149	255.255.255.0	GABY	Planta Administrativa
192.168.10.150	255.255.255.0	NPIA39567	Planta Administrativa
192.168.10.152	255.255.255.0	----------	
192.168.10.153	255.255.255.0	----------	
192.168.10.155	255.255.255.0	IBAFLOPROPOC	
192.168.10.156	255.255.255.0	----------	DHCP

192.168.10.157	255.255.255.0	IBAFLOFINGER	Planta Administrativa
192.168.10.159	255.255.255.0	LIDERSOFT	Planta Administrativa
192.168.10.160	255.255.255.0	IBAFLOSISASIS	
192.168.10.164	255.255.255.0	----------	DHCP
192.168.10.165	255.255.255.0	----------	DHCP
192.168.10.166	255.255.255.0	PORTATIL	Planta Administrativa
192.168.10.167	255.255.255.0	IBAFLOPROJEFE	Planta Producción
192.168.10.168	255.255.255.0	FLORALP	
192.168.10.170	255.255.255.0	ARACELI	
192.168.10.171	255.255.255.0	----------	
192.168.10.172	255.255.255.0	RNPE0DB13	
192.168.10.173	255.255.255.0	----------	
192.168.10.177	255.255.255.0	IBAFLOSISASIS	Planta Administrativa
192.168.10.178	255.255.255.0	----------	
192.168.10.180	255.255.255.0	----------	
192.168.10.181	255.255.255.0	----------	DHCP
192.168.10.182	255.255.255.0	----------	DHCP
192.168.10.183	255.255.255.0	----------	DHCP
192.168.10.184	255.255.255.0	----------	DHCP
192.168.10.185	255.255.255.0	----------	DHCP
192.168.10.186	255.255.255.0	IBAFLOFINGER	
192.168.10.189	255.255.255.0	UIOFLOPROSUMI	DHCP
192.168.10.187	255.255.255.0	----------	DHCP
192.168.10.188	255.255.255.0	----------	DHCP
192.168.10.189	255.255.255.0	BAFLOPROCALJEFE	DHCP
192.168.10.190	255.255.255.0	----------	Planta Administrativa
192.168.10.191	255.255.255.0	----------	DHCP
192.168.10.192	255.255.255.0	----------	DHCP
192.168.10.193	255.255.255.0	IBAFLOPROCESOS	Planta Producción

192.168.10.194	255.255.255.0	IBAFLOFGASIS	Planta Administrativa
192.168.10.195	255.255.255.0	UIOFLOVENBAR	Planta Administrativa
192.168.10.197	255.255.255.0	MAX	
192.168.10.198	255.255.255.0	IBAFLOTATJEFE	Planta Administrativa
192.168.10.199	255.255.255.0	----------	
192.168.10.210	255.255.255.0	----------	
192.168.10.223	255.255.255.0	----------	
192.168.10.224	255.255.255.0	----------	Router-Planta Administración
192.168.10.226	255.255.255.0	----------	Router Inalámbrico
192.168.10.227	255.255.255.0	----------	DHCP
192.168.10.230	255.255.255.0	EXECCOPIER	Planta Administrativa
192.168.10.250	255.255.255.0	----------	DHCP

Fuente: Resultados obtenidos mediante el escaneo de IP's Axence netTools

2.2.4 Accesos de los usuarios

Todo el personal que se encuentra laborando en la FLORALP tiene acceso al internet ya sea de forma cableada o inalámbrica, es decir, que pueden acceder a toda la información que circula en la red. Además, tienen conocimiento de las claves por lo tanto pueden acceder a todos los servidores sin ningún problema.

El personal de la institución debe tener acceso solo a la información necesaria para el desarrollo de sus actividades.

Los usuarios al momento que manejan la información no son responsables ya que no cuentan con lineamientos de alguna política de seguridad para la protección de la misma. Además, la información que manejan se encuentra vulnerable ya que personas no autorizadas ajenas a la industria tienen acceso sin ningún problema, por lo que ellos no tienen ningún privilegio durante el tiempo de uso de la red de la FLORALP.

Otro de los accesos en la industria es el correo electrónico institucional, pero la industria no cuenta con un servidor de correo debido a que ellos hacen uso de un hosting externo llamado EICON por este motivo tienen saturado los buzones con correos spam.

2.2.5 Elementos de red

Los principales elementos de red que son parte de la infraestructura de la misma se detallan a continuación:

2.2.5.1 Rack

El departamento de sistemas de FLORALP no cuenta con un datacenter por lo que se encuentran distribuidos por racks localizados, planta administrativa, en la planta de bodega y en la planta de producción estos son muy útiles para el procesamiento de datos estos permiten albergar un gran número de dispositivos de networking, además centralizan el cableado de la industria. La instalación de estos bastidores o rack’s no cuentan con ninguna especificación de algún estándar o normalización.

Figura 15. Rack 1 Planta Administrativa
Fuente: Fotografía capturada por Gabriela López

Figura 16. Rack 2 Planta Administrativa-Bodega
Fuente: Fotografía capturada por Gabriela López

En el interior de cada uno de los rack’s se encuentran los siguientes equipos de red:

Tabla 4. Descripción de los Rack’s

Cantidad	Elemento de red	Ubicación
5	Servidores Físicos	Rack 2
2	Router	Rack 1
1	Switch Administrables	Rack 1
1	Switch no Administrable	Rack 2
2	Switch no Administrable	Rack 3
1	Central PBX	Rack 1
	Equipos de Proveedor CLARO	
2	Router	Rack 1
1	ODF	
2	UPS	Rack 2
1	Monitores	Rack 2
	Equipos de Proveedor CNT	
1	Router	
1	ODF	Rack 2

Fuente: Realizado por Gabriela López

A continuación se detalla cada uno de los elementos de red.

2.2.5.2 Equipos de red

- **Router**

La industria la FLORALP cuenta con router Cisco-Linksys WRT110 como se muestra en la Figura 17 donde este permite la conexión hacia el backbone principal de la red interna. Por medio de este permite establecer una ruta para la compartición de información entre distintas redes, sus características son las siguientes:

Figura 17. Router Cisco-Linksys WRT110

Fuente: LINKSYS Recuperado de: http://support.linksys.com/es-eu/support/routers/WRT110

Características:

- El WRT110 es ideal para la transmisión de vídeo, juegos de Internet y compartir archivos. Estándares de la red.
- WRT110 soporta 802.11n, 802.11g, 802.11b, 802.3 y 802.3u conexiones.
- WRT110 tiene una antena integrada.
- WRT110 tiene seguridad inalámbrica tales como WPA2, WEP, y el filtrado de MAC inalámbrica. Esto permite al propietario para configurar contraseñas de red necesaria para acceder a la red.
- El WRT110 viene con cuatro puertos LAN adicionales para la conexión de cables Ethernet.
- Banda de frecuencia 2.4 GHz.
- Protocolo de direccionamiento: RIP, direccionamiento IP estático.
- Protocolo de gestión remota: HTTP, HTTPS.
- Indicadores de estado: Estado puerto, actividad de enlace, alimentación.

- **Switch Administrable**

El switch administrable de marca Linksys SFE 2000 se puede observar en la Figura 18 este brinda servicio hacia los usuarios de la planta de administración entre sus características están las siguientes:

Figura 18. Linksys SFE 2000

Fuente: P&C COMPANY LTD. ONE STOP SOLUTION Recuperado de: http://www.ipworld.vn/en/san-pham/detail/linksys-sfe2000-24-port-288/

Características:

- Fabricante: LINKSYS
- Modelo/Parte: SFE2000
- Tipo de Dispositivo: Switch de Gestión de Red
- Puertos RJ-45: 24
- GBIC Slots: 2
- Tabla de direcciones MAC: 8K
- Método de conmutación: Store-and-Forward
- Puertos 10/100/1000 Mbps: 4

- **Switch no Administrables**

En toda la infraestructura de red se encuentran algunos switch no administrables entre ellos un switch 3COM de 24 puertos está en la Rack 3, este brinda el servicio a los usuarios de la planta de producción como se observa en la Figura 19 y un Tp-Link 1024 de 24 puertos como se muestra en la Figura 20 este se encarga de manejar los servidores físicos, además existen switch distribuidos alrededor de la industria debido al crecimiento de estaciones de trabajo.

Figura 19. 3Com Baseline Switch 2024
Fuente: SWITCH 3COM BASELINE Recuperado de: http://goo.gl/zzyMGA

Características:

- El 3Com® Baseline Switch 2024 es un switch 10/100 de 24 puertos, sin bloqueo y sin administración.
- Este switch de clase empresarial, que se puede instalar en rack, puede colocarse en el armario de cableado o como unidad autónoma.

- Cualquiera de los 24 puertos del switch pueden ofrecer Ethernet 10BASE-T para usuarios con requerimientos promedio de ancho de banda, o Fast Ethernet 100BASE-TX para usuarios de potencia con conexiones de red más nuevas.
- Tecnología (MDI/MDIX).
- Ofrece una practicidad poderosa y rica en funcionalidad en un robusto paquete diseñado para brindar fiabilidad, larga vida y un bajo coste total de propiedad.

Figura 20. Switch TP-LINK 24 ports10/100Mbps (TL-SF1024)

Fuente: Tp-Link Recuperado de: http://www.micro-kernel.com/tp-link-24-puertos-enrackable-19-1u-p-1487.html

Características:

- Es compatible con IEEE 802.3x control de flujo para modo Full Dúplex y contrapresión para modo Medio-Dúplex
- Conmutación sin bloqueo hacia delante arquitectura y filtra paquetes a velocidad de cable para un máximo rendimiento
- Capacidad de conmutación 4.8Gbps

- Puertos 24 Puertos RJ45 con auto-negociación a 10/100Mbps (Auto MDI/MDIX) Es compatible con dirección MAC auto-aprendizaje y auto-envejecimiento
- Diseño de tamaño compacto para computadoras de escritorio, montaje en Rack
- Diseño Plug and Play facilita la instalación
- Método de transmisión es Store-and-Forward (almacenamiento y retransmisión)

- **Equipos de proveedor**

Se tiene un router Cisco 1700 que brinda el servicio de internet de alta velocidad para la red de la FLORALP, además contiene un convertidor de fibra óptica que permiten convertir la fibra óptica a cable en distintas velocidades.

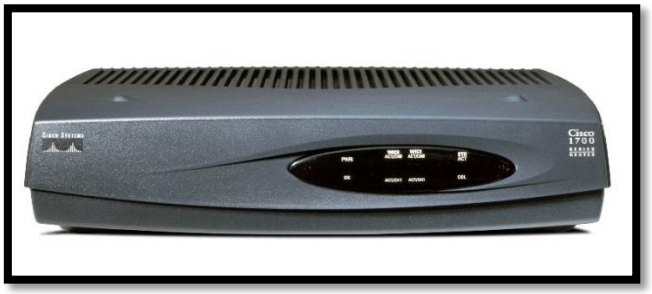


Figura 21. Router Cisco serie 1700
Fuente: Router CISCO 1712 Recuperado de: http://www.inode64.com/router-cisco-1712

Características:

- Los routers Cisco de la serie 1700 proporcionan rapidez y fiabilidad al acceso a Internet y a remotas a través de diferentes tecnologías de acceso WAN de alta velocidad.

- La serie 1700 ofrece una extensa familia de características de seguridad integradas como protección por "firewall", túneles VPN y detección de intrusos o "IDS".
- También proporcionan una vía de acceso a servicios como la Voz sobre IP a través de la convergencia de las redes de voz y datos que ofrecen servicios de procesamiento de llamada y calidad de servicio o "QoS[13]".

El router de servicios integrados Cisco 1800 Series entrega de manera inteligente servicios concurrentes altamente seguros, ofreciendo a los clientes de oficinas pequeñas un sistema único y resistente.

Figura 22. Router Cisco 1800
Fuente: Router CISCO 1800 Recuperado de: http://goo.gl/nDQ4tC

[13] **QoS:** Calidad de Servicio

- **Central Telefónica PBX**

Figura 23. Central Telefónica Analógica kx-ta616

Fuente: Central Telefónica Panasonic Recuperado de: http://www.abadtel.com/centrales+panasonic/digital-kx-ta616.php

Características:

- 6 líneas de entrada.
- 16 internos con conexión de teléfonos híbridos y/o comunes.
- Expansión Simple y Flexible
- Sistema Híbrido. Conexión de TEA y TR sin programación
- Gestión Inteligente de Llamadas Entrantes (DISA, UCD, Identificación de Llamadas y Desvío de Llamadas)
- Gestión Inteligente de Llamadas Salientes y Control de Costes (Enrutamiento Automático, Registro Detallado de Llamadas en el Sistema, Códigos de Cuenta, Limitación de Duración de Llamadas).

2.2.6 Estaciones de trabajo de los usuarios

Una red de datos consta siempre con elementos de acceso a los usuarios que se mencionan a continuación.

Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos. De tal manera, las computadoras se convierten en estaciones de trabajo en red, con acceso a la información y recursos contenidos en el servidor de archivos de la misma.

Existen varias computadoras de escritorio en la industria la FLORALP donde la mayoría de ellas presentan las siguientes características:

- Marca: Intel
- Sistema Operativo Instalado: Windows 8 Enterprise, Windows 7ultime y Windows XP
- Antivirus: Kaspersky
- Programas básicos: Microsoft Office, Adobe Reader, Mozilla, Cleaner y entre otros.
- Memoria: 1GB a 2 GB 116
- Procesador 2.4 a 3 GHz
- Tecnología del procesador: Intel core

- **Portátiles**

Un total de once portátiles las cuales presentan las siguientes características generales:

- Marca: HP, TOSHIBA o Dell
- Sistema Operativo: Windows 7 Ultimate, Windows 8 Enterprise
- Antivirus: ESET NOD 32 o Avast
- Programas básicos: Microsoft Office, Adobe Reader, Mozilla, Cleaner y entre otros.
- Memoria: 2 GB a 4 GB
- Tecnología del procesador: Intel

2.2.7 Servidores

Un servidor es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente, especializada con muy altas capacidades de proceso, encargada de proveer diferentes servicios a las redes de datos, tanto inalámbricas como las basadas en cable; estos servidores tienen sistemas que les permiten resolver ciertas averías de manera automática así como sistemas de alerta para evitar fallas en operaciones de datos críticos, ya que deben estar encendidos los 365 días del año las 24 horas del día.

2.2.7.1 Servidor de dominio

Proporciona resolución de nombre para la red TCP/IP, asocia nombres de los equipos a cambio de direcciones IP automáticas. El servidor de dominio proporciona un método para signar un nombre descriptivo a un Desktop.

2.2.7.2 Servidor de aplicaciones

Con este servidor se puede mantener los datos centralizados de forma íntegra y segura las actualizaciones están garantizadas para todos sus usuarios, limitando el tráfico de la red solamente al tráfico de la capa de presentación, es percibido como un modelo cliente/servidor que mejora el performance de grandes aplicaciones.

Las principales ventajas de la tecnología de los servidores de aplicación son la centralización y la disminución de la complejidad del desarrollo de aplicaciones, dado que las aplicaciones no necesitan ser programadas; en su lugar, estas son ensambladas desde bloques provistos por el servidor de aplicación (Nicolas, 2014).

2.2.7.3 Servidor de respaldos

Toda información es importante y crítica si es más de una empresa, por lo que es muy importante las copias de seguridad para evitar pérdidas de información, puede suponer un gran

coste de reconstrucción de la misma si es posible llegando incluso a detener parcialmente el funcionamiento de la empresa (Morales, 2012).

Se instala un sistema que permite guardar respaldo de cada uno de los equipos de la red: se instala un agente en cada máquina, el cual interactúa con el servidor y se pueden realizar respaldos diarios, semanales, mensuales, lo que nos permite guardar nuestra valiosa información.

Las copias de seguridad son una parte muy importante en el funcionamiento de una compañía, debido a que la pérdida de información o datos críticos podría ser perjudicial e interrumpir en el funcionamiento de la empresa.

2.2.7.4 Servidor DHCP

Un servidor DHCP es un servidor que recibe peticiones de clientes solicitando una configuración de red IP. El servidor responderá a dichas peticiones proporcionando los parámetros que permitan a los clientes auto configurarse (Gómez G. , 2015).

Además, el servidor DHCP proporciona una configuración de red TCP/IP segura y evita conflictos de direcciones repetidas. Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP utilizadas en la red. Los clientes pueden solicitar al servidor una dirección IP y así poder integrarse en la red.

2.2.7.5 Características de los servidores

En la Tabla 5 se indica las características de hardware y software que tiene cada servidor.

Tabla 5. Características de los Servidores

Servidor	Nombre del equipo	Modelo	RAM	Disco	Procesador	Sistema operativo	Ubicación
Dominio	ibasvrflodom	Proliant ML110 e Gen7	10	500GB	Intel xenón 3.10	Server 2012	Rack2
Aplicaciones	ibasvrflodata	Proliant ML370 e Gen5	16	800GB	Intel xenón 3.30	Server 2012	Rack2
Respaldo	ibasvrflobk	Proliant ML350 e Gen8	8	2TB	Intel xenón 3.20	Server 2012	Rack2
Aplicaciones	servidor	Proliant ML380 e Gen8	8	300GB	R2SP2	Server 2003	Rack2

Fuente: Información obtenida de las característica de cada servidor

2.2.8 Administración de red

La red de la industria lechera la FLORALP no posee sistemas que le permitan la administración y el monitoreo de la red, por lo tanto, no cuentan con herramientas que le faciliten el sondeo o el análisis con el fin de conocer alguna anomalía o cambios existentes tanto en hardware y software.

El mantenimiento de los ordenadores es realizado de forma manual por el personal de sistemas, por lo que no es tan eficiente este método debido a que no existe una atención inmediata por el gran número de ordenadores que existen en la industria; es así que los responsables aparte de realizar esta actividad deben ocuparse de los elementos de networking como servidores, cableado estructurado y demás dispositivos que engloban la red de datos.

2.2.8.1 Gestión del software

La instalación del software de las computadoras se lo realiza de forma manual por el personal de sistemas, además la única herramienta que cuentan para observar los ordenadores es mediante el LogMeil que permite un acceso rápido y sencillo a los ordenadores que se encuentran de la industria de forma remota y en alta definición., mediante una cuenta de usuario creada en la web. Este permite trasferir archivos, imprimir de forma remota o mantener a sus ordenadores actualizados desde cualquier parte. En la siguiente Figura 24 nos indica el acceso remoto hacia los ordenadores.

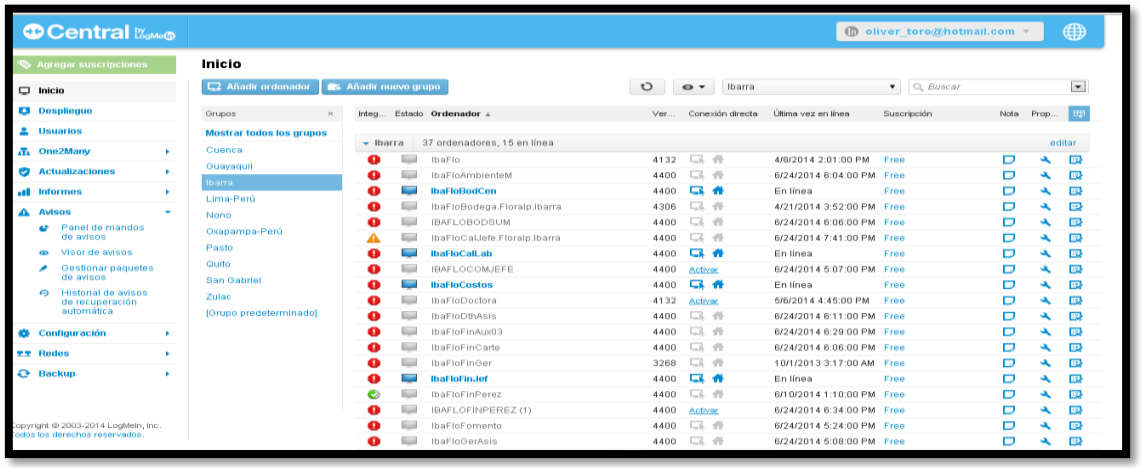


Figura 24. Herramienta del LogMeil

Fuente: LogMeil Recuperado de: https://secure.logmein.com/

2.2.8.2 Gestión del hardware

Todos los dispositivos de red no cuentan con un registro adecuado, lo tienen en un archivo de Excel que no se encuentra actualizado por lo que dificulta la identificación de lo que posee la industria referente a los activos fijos. Cuando existe problemas con algún dispositivo donde el personal de sistemas no pueda solucionarlo es enviado a repararse a alguna empresa dedicada al mantenimiento y correctivo de errores como lo es la Empresa (Electronics Electric y afines).

2.2.8.3 Gestión de usuarios

Para la creación de usuarios el administrador de sistemas se encarga de crear cuentas de usuarios para esto hace uso de los siguientes requerimientos.

Cuenta

- Basado en el cargo del usuario
- Basado en el usuario

Perfil

- Usuario Administrador
- Usuario limitado

El perfil administrador se encarga de crear, modificar y eliminar cuentas con sus respectivas contraseñas teniendo acceso a todos los archivos del sistema.

El perfil limitado tiene las acciones reducidas como al editar insertar y guardar documentos de su propio usuario.

2.2.9 Medición de tráfico de red

Para tener un conocimiento real de cuál es la situación actual de la red se ha realizado un monitoreo de cada IP para determinar la información sobre qué tipo de puertos y protocolos son utilizados dentro de la red interna. Para el monitoreo se ha tomado en cuenta diferentes herramientas de monitoreo que se pueden utilizar, además se deberá considerar que tipo de aspectos van a ser monitoreados, de tal forma entre los más considerados para la realización del presente proyecto son:

- Ancho de banda
- Tipos de Puertos y Protocolos.
- Servicios utilizados

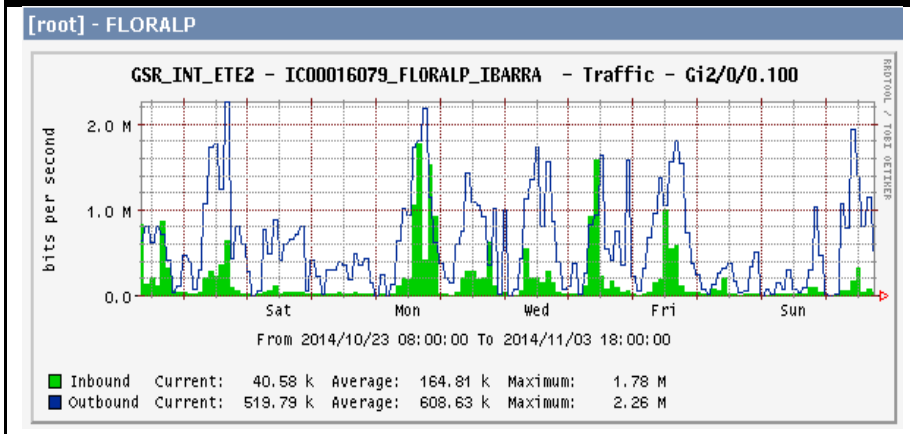
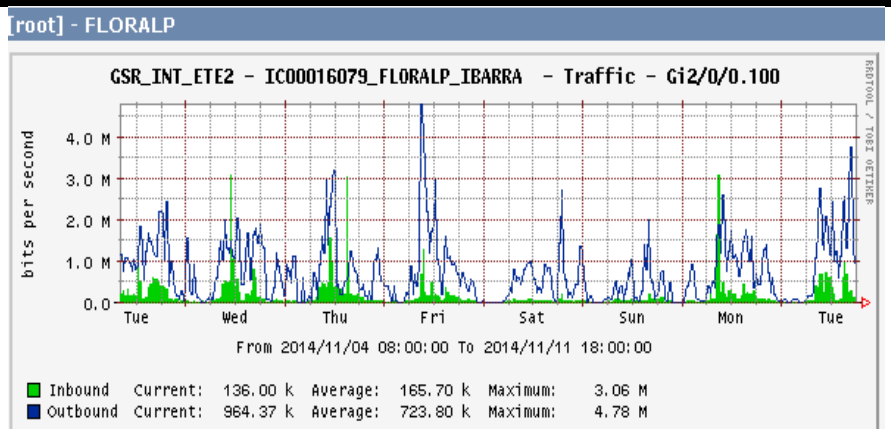
2.2.9.1 Ancho de banda utilizado en la red

Para medir este parámetro se ha utilizado la herramienta dada por el proveedor de servicio de internet como lo es CLARO se lo realiza mediante una IP pública dada por el

proveedor, donde se podrá evidenciar el consumo del ancho de banda dentro de la red. El monitoreo de este parámetro se lo ha realizado durante un mes, tiempo necesario para poder observar el volumen de información que cursa en la red. El monitoreo diario se encuentra en el Anexo A.

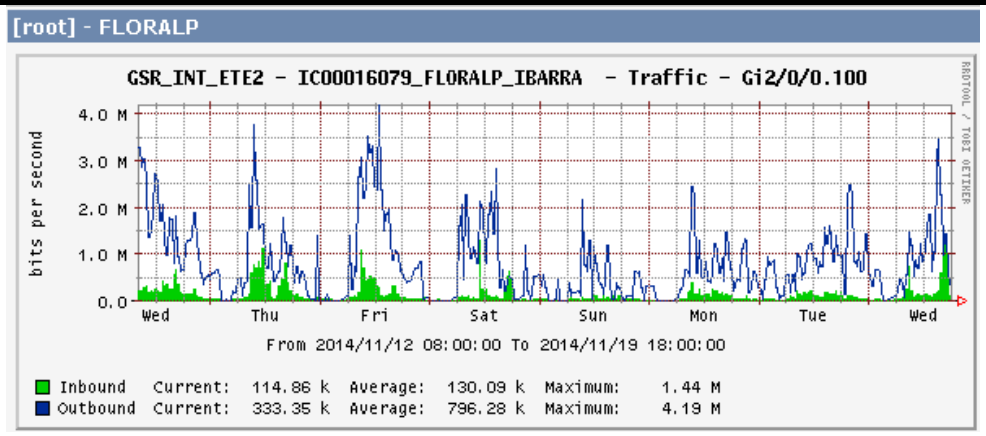
A continuación se muestra gráficas del consumo del ancho de banda por semanas donde se indica el comportamiento durante el día, a continuación se realiza un cuadro resumen donde se marcan los lapsos de tiempo donde se produjeron los picos más altos y a su vez el promedio del volumen de información para luego realizar un análisis de su comportamiento.

Tabla 6. Consumo del ancho de banda que cursa en la Red de Datos de FLORALP de los días 23/10/2014 al 03/11/2014 al 04/11/2014 al 11/11/2014

ANCHO DE BANDA CONSUMO 23/10/2014 al 03/11/2014	ANCHO DE BANDA CONSUMO 04/11/2014 al 11/11/2014
	
En la gráfica se observa el consumo del ancho de banda donde se puede apreciar cuatro picos en el horario de 09:30am a 10:30am, 11:30am a 12:30pm, 16:00pm a 16:30 y de 16:30pm a 17:30pm donde se realiza más congestión de información de la red.	En la gráfica se observa el consumo del ancho de banda donde se puede apreciar tres picos en el horario de 08:00pm a 09:00pm, 10:30am a 11:00pm y de 14:30 a 15:00 donde se realiza más congestión de información de la red.

Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

Tabla 7. Consumo del ancho de banda que cursa en la Red de Datos de FLORALP de los días 12/10/2014 al 19/11/2014

ANCHO DE BANDA CONSUMO 12/11/2014 al 19/11/2014

En la gráfica se observa el consumo del ancho de banda donde se puede apreciar dos picos donde se realiza más congestión de información de la red en los horarios de 15:30am a 16:00am, 11:00am a 11:30pm.

Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

2.2.9.1.1 Análisis del consumo de ancho de banda en la red de datos de la FLORALP

El monitoreo fue realizado en las siguientes fechas del 23/10/2014 hasta el 03/11/2014 en el horario de 8:00 am hasta las 18:00 pm de Lunes a Viernes donde se pudo observar el ancho de banda que se está utilizando. En la tabla 6 se puede observar que a partir de ciertas horas existen una gran mayoría de picos importantes en los días Lunes, Jueves y Viernes de 2.55 Mbps, 2.77 Mbps, 3.19 Mbps y 2.83 Mbps del uso del ancho de banda, por lo que da como resultado una navegación muy lenta y problemas del acceso al servidor además

se establece un ancho de banda promedio, de tal forma determinar el comportamiento del tráfico que circula dentro de la red de datos de FLORALP como se muestra en la Tabla 8.

Tabla 8. Análisis del Ancho de Banda de la Red de FLORALP de la fecha del 23/10/2014 al 03/11/2014

FECHAS [D/M/A]	**ANCHO DE BANDA** [PICO/PROMEDIO]	**ANCHOS DE BANDA** [Mbps]
23/10/2014	Pico[bps]	2.55
	Promedio[bps]	0.3207
24/10/2014	Pico[bps]	0.7161
	Promedio[bps]	0.3321
27/10/2014	Pico[bps]	2.77
	Promedio[bps]	0.6617
28/10/2014	Pico[bps]	0.5046
	Promedio[bps]	0.2361
29/10/2014	Pico[bps]	0.8050
	Promedio[bps]	0.2388
30/10/2014	Pico[bps]	3.19
	Promedio	0.4715
31/10/2014	Pico[bps]	2.83
	Promedio[bps]	0.4830
03/11/2014	Pico[bps]	1.56
	Promedio[bps]	0.1248

Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

El monitoreo fue realizado en las siguientes fechas del 04/11/2014 hasta el 11/11/2014 en el horario de 8:00 am hasta las 18:00 pm de Lunes a Viernes donde se pudo

observar el ancho de banda que se está utilizando. En la tabla 6 se puede observar que a partir de ciertas horas existen una gran mayoría de picos importantes en los días Lunes, Jueves y Viernes de 3.06 Mbps, 3.19 Mbps y 3.40 Mbps del uso del ancho de banda, por lo que da como resultado una navegación muy lenta y problemas del acceso al servidor además se establece un ancho de banda promedio, de tal forma determinar el comportamiento del tráfico que circula dentro de la red de datos de FLORALP como se muestra en la Tabla 9.

Tabla 9. Análisis del Ancho de Banda de la Red de FLORALP de la fecha del 04/10/2014 al 11/11/2014

FECHAS [D/M/A]	ANCHO DE BANDA [PICO/PROMEDIO]	ANCHOS DE BANDA [Mbps]
04/11/2014	Pico[bps]	1.01
	Promedio[bps]	0.3322
05/11/2014	Pico[bps]	3.06
	Promedio[bps]	0.4003
06/11/2014	Pico[bps]	3.19
	Promedio[bps]	0.5507
07/11/2014	Pico[bps]	1.27
	Promedio[bps]	0.2504
10/11/2014	Pico[bps]	3.40
	Promedio[bps]	0.4230
11/11/2014	Pico[bps]	1.52
	Promedio	0.3960

Fuente: Resultados obtenidos mediante el uso de la IP pública de CLARO.

El monitoreo fue realizado en las siguientes fechas del 12/11/2014 hasta el 18/11/2014 en el horario de 8:00 am hasta las 18:00 pm de Lunes a Viernes donde se pudo

observar el ancho de banda que se está utilizando. En la tabla 7 se puede observar que a partir de ciertas horas existen una gran mayoría de picos importantes en los días Miércoles y Jueves de 1.57 Mbps y 1.56 Mbps del uso del ancho de banda, por lo que da como resultado una navegación muy lenta y problemas del acceso al servidor además se establece un ancho de banda promedio, de tal forma determinar el comportamiento del tráfico que circula dentro de la red de datos de FLORALP como se muestra en la Tabla 10.

Tabla 10. Análisis del Ancho de Banda de la Red de FLORALP de la fecha del 12/11/2014 al 18/11/2014

FECHAS [D/M/A]	ANCHO DE BANDA [PICO/PROMEDIO]	ANCHOS DE BANDA [Mbps]
12/11/2014	Pico[bps]	1.57
	Promedio[bps]	0.2038
13/11/2014	Pico[bps]	1.56
	Promedio[bps]	0.3948
14/11/2014	Pico[bps]	1.09
	Promedio[bps]	0.3106
17/11/2014	Pico[bps]	0.3864
	Promedio[bps]	0.1612
18/11/2014	Pico[bps]	0.2183
	Promedio[bps]	0.1408
18/11/2014	Pico[bps]	1.44
	Promedio[bps]	0.3178

Fuente: Resultados obtenidos mediante el uso de la IP pública de CLARO.

2.2.9.2 Monitoreo de protocolos

La presente red carece de un sistema que permita el monitoreo y análisis de red, por lo que este trabajo se lo realiza de forma precaria a través de la interfaz de red, por lo tanto el departamento de sistemas no cuenta con información sobre que puertos y servicios habilitados o servicios utilizados por los usuarios que forma parte de la infraestructura de red.

2.2.9.2.1 Servidores

En la siguiente Tabla 11 se muestra los puertos usados por los servidores dentro de la infraestructura de red de la industria FLORALP que son:

Tabla 11. Puertos y protocolos utilizados por los Servidores

NOMBRE DEL SERVIDOR	PUERTOS
SERVIDOR	smtp [25], pop3 [110], nntp [119], epmap [135], netbios-ssn [139], imap [143], microsoft-ds [445], urd [465], nntps [563], submission [587], imaps [993], pop3s [995], blackjack [1025], ms-sql-s [1433], globe [2002], vnc [5800], vnc [5900]
IbaSvrFloClikex	smtp [25], http [80], pop3 [110], nntp [119], epmap [135], netbios-ssn [139], imap [143], microsoft-ds [445], urd [465], nntps [563], submission [587], imaps [993], pop3s [995], vnc [5800], vnc [5900]

IbaSvrFloDom	smtp [25], name [42], domain [53], http [80], kerberos [88], pop3 [110], nntp [119], epmap [135], netbios-ssn [139], imap [143], ldap [389], microsoft-ds [445], kpasswd [464], urd [465], nntps [563], submission [587], http-rpc-epmap [593], ldaps [636], imaps [993], pop3s [995], globe [2002], msft-gc [3268], msft-gc-ssl [3269], vnc [5800], vnc [5900]
IbaSvrFloBk	smtp [25], domain [53], kerberos [88], pop3 [110], nntp [119], epmap [135], netbios-ssn [139], imap [143], ldap [389], microsoft-ds [445], kpasswd [464], urd [465], nntps [563], submission [587], http-rpc-epmap [593], ldaps [636], imaps [993], pop3s [995], globe [2002], cpq-wbem [2301], compaq-https [2381], msft-gc [3268], msft-gc-ssl [3269], ms-wbt-server [3389], vnc [5800], vnc [5900]

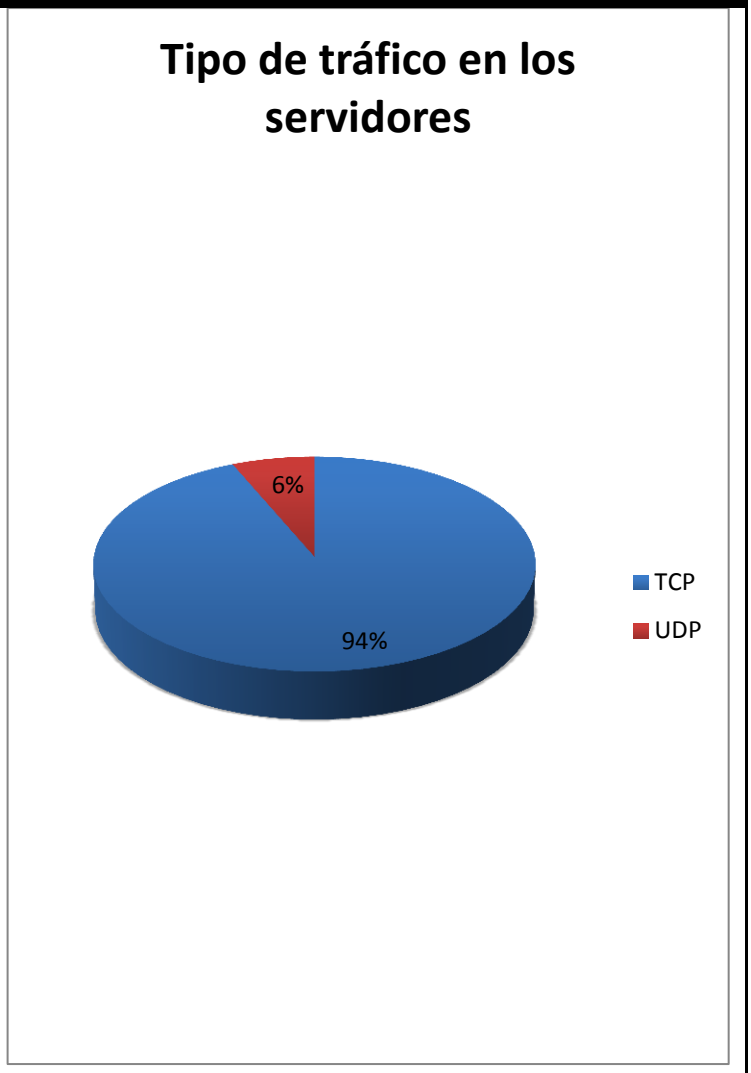
Fuente: Datos obtenidos mediante la herramienta Axence NetTools

En la Tabla 11 se puede apreciar todos los protocolos y puerto habilitados en cada servidor, por lo tanto, se ha realizado un gráfico de todos los puertos conocidos y no conocidos para determinar el porcentaje de qué tipo de tráfico circula dentro de la red.

Como no se cuenta con un switch administrable y no se puede monitorear cada puerto, se ha realizado mediante cada IP tomando en cuenta el número de puertos que se repiten en cada servidor por lo que el resultado es el siguiente.

Tabla 12. Protocolos utilizados en los servidores

PROTOCOLO	PUERTO
smtp	25
pop3	110
nntp	119
epmap	135
netbios-ssn	139
imap	143
microsoft-ds	445
urd	465
nntps	563
submission	587
imaps	993
pop3s	995
vnc	5800
vnc-server	5900



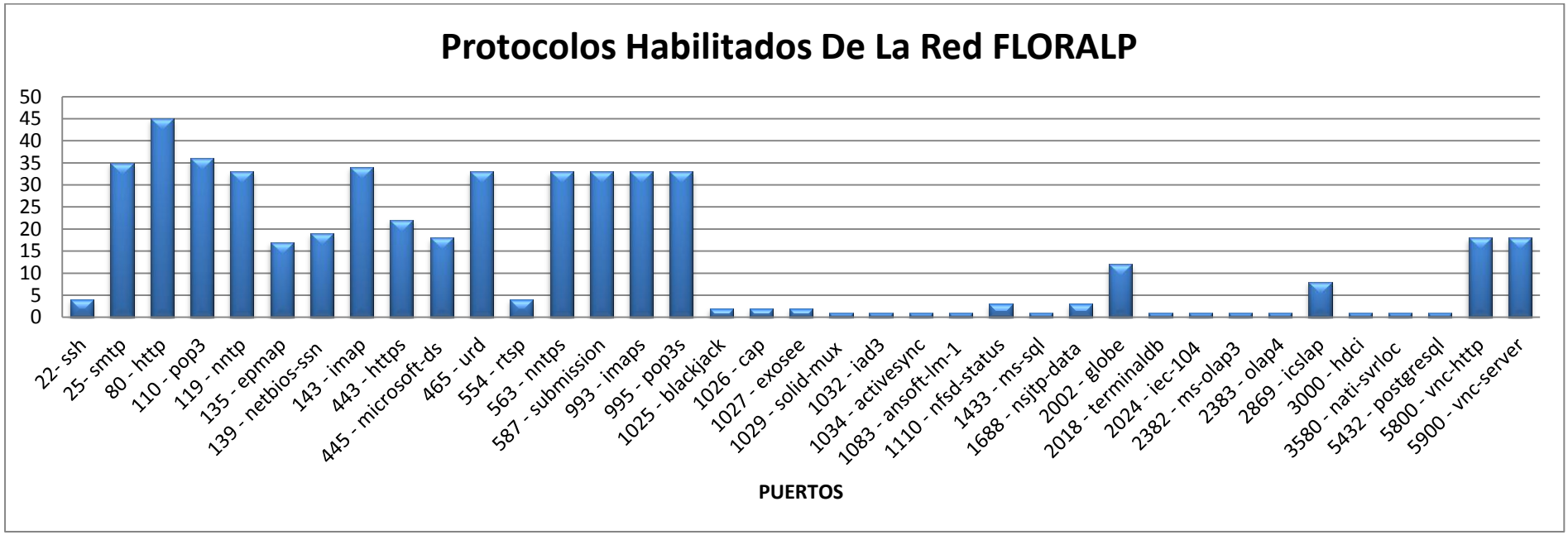
Fuente: Graficación en Microsoft Excel 2010 realizado por Gabriela López

Como se puede observar en la Tabla 12 anterior los datos que se generan muestran que el 94% corresponde al protocolo TCP y el 6% a UDP, es decir que existe una mayoría de puertos conocidos orientados a conexión.

2.2.9.2.2 Desktop

En la siguiente Figura 25 se realiza un cuadro estadístico que nos indica que tipos de protocolos son más utilizados por todos los usuarios y que pertenecen en el rango 192.168.10.0/24. El monitoreo de cada IP de usuario se encuentra en el Anexo B.

Figura 25. Gráfico estadístico de puertos y protocolos utilizados por los usuarios



Fuente: Graficación en Microsoft Excel 2010 realizado por Gabriela López

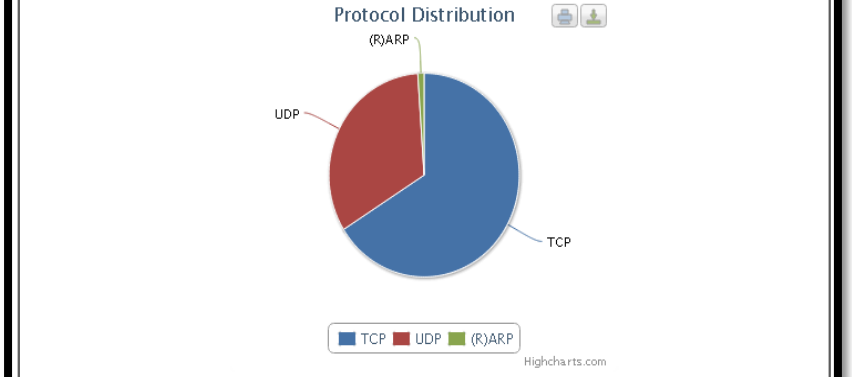
En la siguiente Tabla 13 se indica el tipo de tráfico UDP/TCP que se encuentran utilizando cada IP de usuario dentro de la de red de la industria FLORALP, los datos que se generan muestran que el 66.8 % corresponde al protocolo TCP y el 33.2% a UDP se lo realizó mediante dos herramientas como lo son NTOP y WIRESHARK.

Tabla 13. Estadísticas del tipo de tráfico utilizado por los usuarios

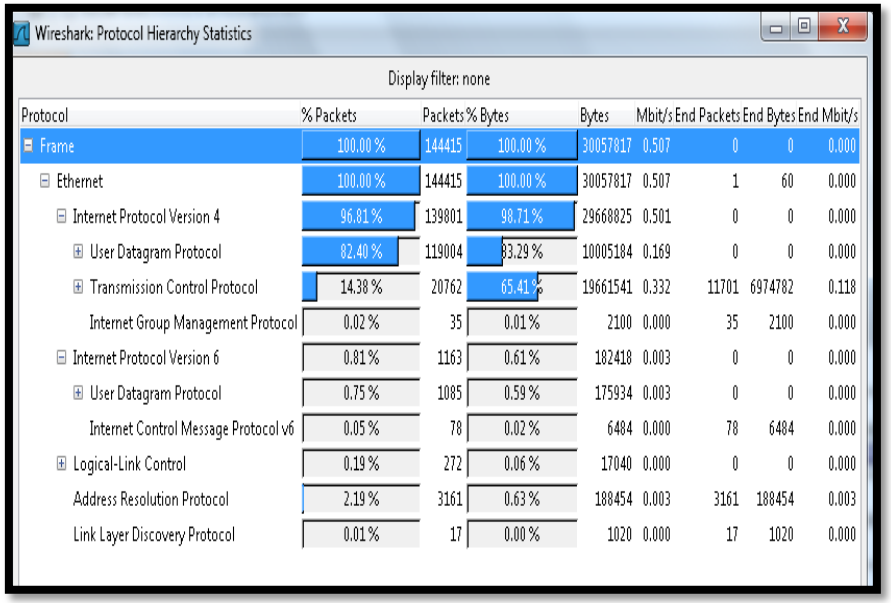
PORCENTAJE DE PROTOCOLOS UDP/TCP

NTOP

L2/L3 Protocol	Data	Percentage			
IP	366.0 KBytes	98.6%	TCP	244.4 KBytes	66.8%
			UDP	121.6 KBytes	33.2%
(R)ARP	4.0 KBytes	1.1%			



WIRESHARK



Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	144415	100.00 %	30057817	0.507	0	0	0.000
Ethernet	100.00 %	144415	100.00 %	30057817	0.507	1	60	0.000
Internet Protocol Version 4	96.81 %	139801	98.71 %	29668825	0.501	0	0	0.000
User Datagram Protocol	82.40 %	119004	83.29 %	10005184	0.169	0	0	0.000
Transmission Control Protocol	14.38 %	20762	65.41 %	19661541	0.332	11701	6974782	0.118
Internet Group Management Protocol	0.02 %	35	0.01 %	2100	0.000	35	2100	0.000
Internet Protocol Version 6	0.81 %	1163	0.61 %	182418	0.003	0	0	0.000
User Datagram Protocol	0.75 %	1085	0.59 %	175934	0.003	0	0	0.000
Internet Control Message Protocol v6	0.05 %	78	0.02 %	6484	0.000	78	6484	0.000
Logical-Link Control	0.19 %	272	0.06 %	17040	0.000	0	0	0.000
Address Resolution Protocol	2.19 %	3161	0.63 %	188454	0.003	3161	188454	0.003
Link Layer Discovery Protocol	0.01 %	17	0.00 %	1020	0.000	17	1020	0.000

Fuente: Datos obtenidos mediante las herramientas NTOP y Wireshark

En el gráfico estadístico de puertos y protocolos utilizados por los usuarios de la Figura 25 se puede evidenciar los diferentes tipos de protocolos que utilizan cada dirección IP, concluyendo que la mayoría de protocolos son TCP tomados en diferentes periodos de tiempo donde existen mayor actividad de los usuarios observar el Anexo B Tabla 21 de tal forma los protocolos más utilizados son:

Tabla 14. Protocolos más utilizados en la Red.

PROTOCOLOS	PUERTO	PORCENTAJE
Otros Protocolos		10%
http	80	9%
imap	143	7%
pop3	110	7%
smtp	25	7%
pop3s	995	6%
imaps	993	6%
submission	587	6%
nntps	563	6%
urd	465	6%
nntp	119	6%
vnc-server	5900	4%
vnc-http	5800	4%
microsoft-ds	445	4%
https	443	4%
netbios-ssn	139	4%
epmap	135	3%
Total		90%

Fuente: Datos obtenidos del Grafico estadístico de puertos y protocolos

Como indica la anterior Tabla 14 se puede evidenciar que el 10% se refiere a otros protocolos que no son tan irrelevantes como lo son: blackjack, cap, exosee, solid-mux entre otros que no son muy frecuentes, por lo contrario el 90% son de protocolos más repetitivos y usados por los usuarios.

2.2.9.3 Monitoreo de servicios

El análisis de este parámetro se lo realiza, mediante los datos obtenidos del monitoreo de puertos y protocolos donde contienen las gráficas de las estadísticas que indican el tipo de servicios más utilizados dentro de la red con lo que se determina que el protocolo HTTP, SMTP y POP3 tienen un porcentaje alto por motivo que los usuarios hacen uso de servicios que prestan cada uno como el correo electrónico, llamadas o trasferencia de archivos mediante Skype y el acceso al servidor de aplicaciones que se lo realiza mediante una página web.

2.2.10 Análisis de la infraestructura de red actual de la industria FLORALP

La infraestructura de red de la industria FLORALP permite comunicarse con múltiples usuarios y compartir información, es decir, es un sistema de comunicaciones que interconecta varios dispositivos electrónicos para facilitar el trabajo y la navegación del internet.

A continuación se puede conocer cuál es el análisis de todos los elementos que forman parte de la infraestructura de la red.

2.2.10.1 Topología de red

En el diseño actual de la arquitectura de red presenta las siguientes características e inconvenientes.

- La topología de red es plana e inadecuada, es decir, no cuenta con un nivel jerárquico dando como resultado una topología desordenada donde la principal ventaja de esta es su sencillez y sus desventajas incluyen la falta de escalabilidad, limitaciones de recursos, control de tráfico, enlaces redundantes y la falta de QoS[14]. Uno de los principales problemas de esta arquitectura es el esquema de direccionamiento, enrutamiento y servicios. En una red plana, el direccionamiento es uno de los problemas que llega a impedir la estabilidad.

- Toda topología de red se caracteriza por contar con un punto central donde se conectan todos los equipos, con este esquema la máxima vulnerabilidad se encuentra en el nodo central como lo es el (switch) ya que si falla, toda la red fallaría sin embargo presenta una ventaja muy importante, el servidor de aplicaciones se encuentra conectado directamente al router del proveedor de CNT de tal forma está aislado del nodo central permitiendo el funcionamiento correcto del servicio sin perjudicar al resto de usuarios externos de las diferentes sucursales que hacen uso de esta aplicación.

[14] **QoS**: Calidad de servicio

2.2.10.2 Direccionamiento IP

En la actual distribución del direccionamiento IP se observó que presenta ciertos inconvenientes como son los siguientes:

- No se toma en cuenta el crecimiento de usuarios y de dispositivos de red, por lo que no se encuentran asignados rangos disponibles para nuevos usuarios y dispositivos de red.
- Desperdicio de direcciones IP's debido a que no se asigna un número exacto de usuarios por cada dependencia para la distribución, evitando que existan direcciones sin uso.
- La mayoría de usuarios se encuentran conectados por DHCP donde el inconveniente es la duplicación de direcciones IP.
- Los rangos de las direcciones IP de los diversos dispositivos de red no se encuentran agrupados por lo que se encuentran mezclados con las IP's que están asignadas a las estaciones de trabajo.
- El orden del direccionamiento no se encuentra bien establecido en su totalidad es decir que todo el rango disponible no tiene un rango definido sin ninguna prioridad para ciertos equipos.

2.2.10.3 Dispositivos de red

Los dispositivos de red son una parte esencial en la infraestructura de red, a continuación se detalla cuál es su estado actual luego de haber conocido sus características.

- Los dispositivos de red muestran información propia de la industria ya sea en su configuración o de forma física, además no se sigue ninguna política de administración de contraseñas para su configuración.
- La ubicación de algunos dispositivos dentro de la infraestructura es inadecuada de tal manera no existe una documentación sobre la configuración.
- La utilización de múltiples equipos de conmutación para extender la red provoca una gran pérdida de rendimiento y eficiencia de la LAN, debido a la cantidad excesiva de broadcasts, en consecuencia el fallo o caída de las comunicaciones.
- Entre las características de los dispositivos de red entre ellos los switch y los router no permiten la creación de VLAN's y la configuración de ACL's para facilitar la administración y fortalecer la seguridad de la red.
- La ubicación de los racks que protegen todos los dispositivos de red no se encuentran en una ubicación apropiada.
- Existen dispositivos sin protecciones y que están en lugares de difícil acceso lo cual impide la disponibilidad para su control o mantenimiento.
- El servicio de conexión redundante proporcionado a través de la red inalámbrica no es óptimo debido a que presenta interrupciones y cortes.
- No existe ningún mecanismo que permita el remplazo de la central telefónica en el caso de que esta colapse.
- No todo el cableado de la red de la organización posee certificación, por lo tanto, algunos cables se encuentran en mal estado.
- Los access point no están ubicados de una forma que facilite su mantenimiento.

- Los cables utilizados para unir los dispositivos de red están desorganizados dentro de los racks, además se puede observar cables sueltos que no dan ninguna utilidad y aun así se encuentran conectados a los dispositivos de red.
- No se cuenta con equipos mucho menos con enlaces redundantes para las conexiones más importantes y para la trasmisión de datos a través del internet.
- No existen políticas que restrinjan el uso del internet debido a la falta de información que especifique su uso dentro de la industria.
- Los usuarios desconocen las amenazas existentes en la Internet debido a la falta de información dentro de la industria.
- Bajas velocidades en la navegación del internet por intervalo de tiempos por lo que dificulta el trabajo del personal y el acceso a los servidores.

2.2.10.4 Equipos de cómputo

Todos los equipos que se utilizan dentro de la industria y que conforman la red si prestan con todos los requerimientos de los usuarios y son capaces de resolver múltiples funciones dependiendo de los usuarios que los hagan uso. Todas las características se encuentran detallados en el ítem **2.2.6** de forma general en los elementos de acceso a la red los usuarios.

2.2.10.5 Análisis de los accesos de los usuarios

En la red LAN de la industria FLORALP se tiene una subred de servicios y aplicaciones las mismas que son usadas por usuarios de la red interna para el desarrollo de sus actividades de acuerdo con función que cumplen dentro de la institución.

A medida que crece el número de usuarios la navegación de internet tiene problemas de lentitud a otros que lo necesitan para desarrollar sus actividades laborales por lo que no se cuenta con un control de navegación.

De tal forma la industria debe tener políticas o alguna norma específica para el control de acceso a la red para poder proteger la seguridad de la información. En este sentido, rigiéndose a las normas, políticas y procedimientos especificados en el SGSI (Sistema de Gestión de Seguridad de la Información) se debe aplicar políticas sobre la utilización de las aplicaciones y recursos internos en la institución.

Los usuarios actualmente que se encuentran conectados dentro de la infraestructura de forma cableada necesitan acceder a los servicios y aplicaciones de la institución de manera segura, controlando el acceso de personas no autorizadas utilizando mecanismos de autenticación que garanticen el acceso solo a usuarios que pertenecen a la institución.

Los usuarios que poseen laptops o teléfonos inteligentes acceden a la red wireless sin la utilización de mecanismos de autenticación, por lo cual, cualquier persona que se encuentre

dentro de esta zona puede acceder a los servicios internos, provocando un punto de inseguridad. A través de esta conexión es sencillo obtener información de la red, tal como: direcciones IP de servidores de aplicaciones, equipos de red, de usuarios, entre otros.

Para la utilización de la red inalámbrica de forma segura, se necesita la implementación de controles de acceso que garanticen la confidencialidad, integridad y disponibilidad de la información. No se toma en cuenta que el internet es una nube a la que puede acceder cualquier persona desde cualquier parte del mundo a cualquier información que esté publicada.

Un inconveniente que se observa es que los encargados de la parte de sistemas no se preocupan por la optimización de los recursos para un buen desempeño laboral, por lo que esto conlleva a tener problemas en la navegación del internet de tal forma se vuelven frágiles a ciertos ataques que puedan producirse desde el exterior de la red.

CAPÍTULO III

3 Diseño Del Sistema De Seguridad Perimetral Para La Red De Datos.

En este capítulo se presenta el diseño del sistema de seguridad perimetral que va hacer utilizado, es importante conocer la capacidad, las limitaciones del software y hardware del sistema a integrarse, con el planteamiento de las políticas de seguridad.

3.1 Planteamiento de las políticas de seguridad

Antes de realizar un diseño de un sistema de seguridad perimetral es importante conocer cuáles son los recursos y servicios que brinda la red. De tal manera se debe realizar un documento donde consten todas las políticas de seguridad de red. En este documento constará de controles y objetivos utilizando el modelo PDCA para establecer las políticas, el manejo y responsabilidad de la red, el diseño de un modelo de seguridad y los planes de contingencia o planes de acción en caso de que la seguridad haya sido violada.

3.2 Controles y objetivos

Para el diseño de las políticas de seguridad de la industria, se debe tomar en cuenta la metodología que presenta el estándar ISO /IEC 27001 con sus controles y objetivos con ayuda del modelo PDCA que se muestra en la siguiente Tabla 15.

Tabla 15. Controles y Objetivos ISO/IEC 27001

CONTROLES Y OBJETIVOS	
A.5	Política de seguridad de información
A.6	Estructura organizativa de la SI
A.7	Clasificación y control de activos
A.8	Seguridad ligada al personal
A.9	Seguridad física y del entorno
A.10	Gestión de comunicaciones y operaciones
A.11	Control de accesos
A.12	Desarrollo y mantenimiento de sistemas
A.13	Gestión de incidente de seguridad
A.14	Gestión continuidad de negocio
A.15	Conformidad y cumplimiento legislativo

Fuente: Guía de controles y objetivos Recuperado de: http://www.iso27000.es/

3.2.1 Políticas de seguridad

Las políticas de seguridad son normas que permiten conocer el comportamiento de la red con relación a la seguridad de la información, cada definición permitirá realizar procedimientos y planes que protejan a los recursos de la red tanto en pérdidas y daños que puedan suscitarse.

Una parte muy importante del desarrollo de políticas es que estas deben ser bien concisas y efectivas ya que de ellas depende mucho que la industria pueda proteger toda su información. Para que el administrador de la red pueda elaborar el documento de las políticas de seguridad debe tener conocimiento de que tipo de servicios y recursos son utilizados por la mayoría de usuarios y de esta forma le permitirá priorizar que tipo de usuarios pueden tener acceso y cuales tendrán restricciones.

Los usuarios que hacen uso de la red de la industria tiene acceso total por lo que resulta un poco complicado la realización de las políticas de seguridad en cuanto a los accesos, al momento de la implementación se debe considerar que esto no impida el funcionamiento correcto de la industria ya que tanto los usuarios y administrador deben existir una aceptación, colaboración para la mantención y ejecución de cada política.

3.2.2 Desarrollo de los controles y políticas del SGSI afines a la seguridad de la información

Cada una de las políticas realizadas en este documento se encuentra elaborada con el apoyo del Jefe del departamento de sistemas. Los diferentes objetivos, controles y políticas utilizadas en el presente proyecto son los siguientes:

3.2.2.1 Objetivos

- Crear políticas que garanticen el buen uso, manejo, integridad, exactitud y preservación de la información de la industria, y protegerla contra la modificación, divulgación, manipulación o destrucción no autorizada o accidental.

- Garantizar la privacidad de la información personal, sensitiva o vital de la industria, sus empleados y sus beneficiarios, de esta forma, proveer de sanciones en caso de que ocurra mal uso o pérdida de información reservada de la industria.

3.2.2.2 Alcance

Estas políticas aplican a todos los departamentos de la industria que tengan acceso a equipos de Computación y/o Sistemas de Información, que ingresan, crean, procesan o tienen custodia de información.

3.2.2.3 Responsabilidad

Son responsables todos los gerentes y jefes de cada departamento, personal administrativo y empleados de observar y cumplir la política de seguridad de la información dentro del área a su responsabilidad y por ende hacer cumplir al personal bajo su cargo.

3.2.2.4 Políticas diseñadas

Cada política del SGSI se encuentra relacionada con los controles antes mencionados en la Tabla 15 a la información para mejorar la confidencialidad, cada política se encuentra definida dentro de diferentes grupos que a continuación son las siguientes:

INDUSTRIA LECHERA FLORALP S.A	
DOMINIO	1. Política de seguridad
CONTROL	1.1 Política de seguridad de la información.
ALCANCE	Estas políticas aplican a todos los departamentos de la industria que tengan acceso a equipos de computación o sistemas de información, que ingresan, crean, procesan o tienen custodia de información.
RESPONSABLE	Son responsables todos los gerentes y jefes de cada departamento, personal administrativo y empleados de observar y cumplir la política de seguridad de la información dentro del área a su responsabilidad y por ende hacer cumplir al personal bajo su cargo.

- Crear políticas que garanticen el buen uso, manejo, integridad, exactitud y preservación de la información de la industria, y protegerla contra la modificación, divulgación, manipulación o destrucción no autorizada o accidental.

- Garantizar la privacidad de la información personal, sensitiva o vital de la industria, sus empleados y sus beneficiarios, de esta forma, proveer de sanciones en caso de que ocurra mal uso o pérdida de información reservada de la industria.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	1. Política de seguridad.
CONTROL	1.2 Política de seguridad de información.
ALCANCE	Esta política se aplica a todos los que pertenecen al departamento de sistemas donde son responsables de la elaboración y ejecución de las políticas de seguridad con el compromiso de las autoridades.
RESPONSABLE	Departamento de sistemas

- El departamento de sistemas debe identificar, supervisar regularmente la implantación de las políticas de seguridad de información.
- Proporcionar apoyo técnico y administrativo a una fuente especializada en

seguridad de la información si fuese necesario.

- El departamento de sistemas debe capacitar a gerentes, jefes, auxiliares y empleados que puedan recibir información complementaria sobre la implantación de las políticas de seguridad de la información.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	2. Organización de la información de seguridad.
CONTROL	2.1 Clasificación y control de activos.
ALCANCE	Esta política se aplica a todos los usuarios que forman parte de la infraestructura de red que hacen uso de los recursos informáticos.
RESPONSABLE	Todos los usuarios

- Identificar los activos sobre todo los de mayor importancia para las aplicaciones o sistemas críticos de la institución.
- Se debe mantener identificados mediante un inventario de activos que debe mantenerse actualizado cada vez que exista alguna modificación en alguno de los activos, identificando los de mayor sensibilidad y criticidad para la industria
- Los activos de información de la industria FLORALP incluyendo software, aplicaciones y archivos solo pueden utilizarse para fines laborales y legales.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	3. Seguridad de los recursos humanos.
CONTROL	3.1 Seguridad ligada al personal.
ALCANCE	Esta política se definirá a todos los usuarios que no pertenezcan a la industria, de tal manera, será responsabilidad de informar sobre cuáles son las políticas de seguridad que rigen antes, durante y finalización de su trabajo.
RESPONSABLE	Departamento de sistemas y todos los usuarios

- A todos los usuarios empleados, contratistas y terceras personas se les deberá proporcionar un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad.
- El personal, contratista y terceras personas deberán aceptar y firmar una solicitud de acceso de la información donde se establecerán sus obligaciones para la seguridad de la información que será llenada y autorizada por el administrador de red, dependiendo del departamento y función que cumplen dentro de la industria.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	4. Seguridad física y del entorno.
CONTROL	4.1 Seguridad de los equipos.
ALCANCE	Esta política debe abarcar a todos los equipos informáticos que son parte de la infraestructura de red que son sensibles a cualquier manipulación por parte de un acceso no autorizado ocasionando la pérdida o el robo de información.
RESPONSABLE	Todos los usuarios

- El personal que no cuente con una estación de trabajo o es ajeno a la industria no está autorizado a utilizar los recursos informáticos o tener acceso a la información de la industria, cabe mencionar que solo tengan autorización dada por el administrador de la red.
- Siempre que un trabajador se percate de algún visitante desconocido dentro de áreas restringidas de la entidad, el visitante debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en áreas restringidas e informar a los responsables de la seguridad de la industria.
- Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.
- Los equipos (PC's, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa por el departamento de sistemas.

- Todos los computadores portátiles, módems y equipos de comunicación deben registrar su ingreso y salida, además, no deben abandonar la entidad a menos que este se encuentre acompañado por una previa autorización respectiva y la validación de supervisión por parte del departamento de sistemas.
- Inspeccionar a los visitantes o usuarios ajenos a la industria a algún recurso informático deben firmar un acuerdo de confidencialidad con dichos usuarios, con el fin de ser informados sobre las medidas de seguridad que deben acatar mientras permanezca dentro de la industria.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	4. Seguridad física y del entorno.
CONTROL	4.2 Seguridad física.
ALCANCE	Evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la industria.
RESPONSABLE	Todos los usuarios

- Toda información almacenada en medios electrónicos que se utilice como parte de la operación normal de la industria debe ser respaldada cada mes mediante servicios de backup. Los procesos de respaldo de información deben aplicarse a todos los equipos de la industria.

- Los usuarios de la industria son responsables de respaldar y proteger la información generada y almacenada en elementos tecnológicos de uso personal que les hayan sido asignados.
- La información que genera y soporta la infraestructura de red de la FLORALP debe ser almacenada y respaldada, de tal forma que se garantice su disponibilidad.
- El departamento de sistemas debe realizar las copias de respaldo, tanto para computadoras de escritorio y de servidores así como los tiempos de retención y rotación de dichas copias.
- El departamento de sistemas es el responsable de realizar cada respaldo de todos los equipos de red (portátiles, desktop, servidores) esto se lo debe realizar los días viernes a una hora adecuada para no interrumpir la continuidad del trabajo del personal de la industria.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	5. Administración de las comunicaciones y operaciones.
CONTROL	5.1 Gestión de comunicaciones y operaciones.
ALCANCE	Se garantiza el correcto tratamiento de la información que asegure la confidencialidad de la información.
RESPONSABLE	Departamento de sistema

- La utilización de la información que se encuentra en las bases de datos o archivos electrónicos con el solo propósito de realizar las operaciones propias de la industria es responsabilidad de los empleados guardar y proteger debidamente la información que han estado utilizando para cumplir con sus tareas y bajo ningún concepto facilitar la misma a terceras personas sin previa autorización.
- Asegurar que todo el personal que se encuentra laborando cuente con capacitación sobre seguridad de la información mediante la publicación de boletines o conferencias, con el fin de de crear una cultura sobre el personal garantizando confidencialidad y disponibilidad de la información.
- Las jefaturas o gerentes de cada departamento son responsables de asegurar el cumplimiento de la política de seguridad por parte del personal bajo su mando.
- Las comunicaciones con equipos externos se realiza utilizando conexiones seguras.
- La infraestructura de la red referente al direccionamiento IP y configuraciones relacionadas con equipos de un nivel de sensibilidad o confidencial deben mantenerse como información reservada.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	5. Administración de las comunicaciones y operaciones.
CONTROL	5.2 Desarrollo y mantenimiento de sistemas

ALCANCE	Todo equipo que realice alguna modificación debe ser documentada por el personal encargado de haber realizado dicha acción donde debe ser solicitada por el responsable de la administración de la red.
RESPONSABLE	Departamento de sistemas

- Realizar los cambios necesarios ya sea en programas o aplicaciones que afecten de forma directa o indirecta a los recursos informáticos debe ser aprobado formalmente por la persona cargada de la administración de la red donde es responsable de aceptar o rechazar las solicitudes de los accesos.
- Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud que se encuentra en el Anexo C5 hasta su implantación.
- Cualquier cambio que se requiera realizar en los equipos ya sea (cambio de procesador, adición de memoria, tarjetas o a la modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	6. Control de Accesos.
CONTROL	6.1 Gestión de comunicaciones y operaciones.

ALCANCE	Debe desarrollarse un procedimiento que permita registrar de manera única a los usuarios que requerirán acceso a la información.
RESPONSABLE	Todos los usuarios

- Verificar que el nivel de acceso otorgado sea el estrictamente necesario para que el usuario pueda realizar únicamente las tareas relacionadas con su trabajo.
- Al momento de registrar un usuario debe firmar un formulario de acceso a la información que se encuentra en el Anexo C1 con el nombre de usuario y al sistema que se le ha concedido acceso con sus privilegios asignados.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	6. Control de Accesos.
CONTROL	6.2 Gestión de comunicaciones y operaciones.
ALCANCE	La política mencionada debe permitir autorizar e impedir los accesos no autorizados a los sistemas de información.
RESPONSABLE	Departamento de sistemas

- Las claves de acceso serán creadas de acuerdo con los estándares de la institución como tener mayúsculas, minúsculas, números, símbolos especiales y una longitud de más de ocho caracteres, además debe ser

encriptada.

- Cada contraseña de cada usuario creada debe ser revisada y renovada periódicamente cada 60 días. El periodo de renovación podría variar dependiendo de las necesidades de la industria.
- El uso correcto de las contraseñas es de carácter personal, el indebido uso de las claves obtenidas de forma ilegal o no autorizada será sancionada de acuerdo con gravedad del efecto que dicha utilización cause a la industria, esta será investigada y sometida a una sanción que se da por parte del departamento de sistemas.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	6. Control de Accesos.
CONTROL	6.3 Gestión de continuidad del negocio
ALCANCE	La política mencionada debe permitir autorizar e impedir los accesos no autorizados a los sistemas de información.
RESPONSABLE	Todos los usuarios

- La industria se reserva el conceder los diferentes niveles de acceso a sus archivos de información, se establece un formulario en el Anexo C1 que es llenado por el jefe inmediato del empleado, bajo su responsabilidad se establece los controles de

solicitud de acceso y el nivel de acceso a sus sistemas electrónicos, de acuerdo con sus necesidades.

- Los proveedores o terceras personas deben ser supervisadas durante el período del tiempo requerido para llevar a cabo las actividades aprobadas.
- El administrador debe tener acceso especial a la red, además los usuarios tendrán ciertos permisos por lo que es necesario que existan un control.
- La autorización para el acceso de la información para los usuarios o personas externas deben ser previamente autorizadas por el administrador de red donde este otorgará dependiendo del departamento y función que cumplen dentro de la industria.
- Si el jefe del departamento de sistemas delegan las tareas operativas de concesión de derechos de acceso estas deben ser documentadas y controladas.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	6. Control de Accesos
CONTROL	6.4 Control de acceso a la red
ALCANCE	La política mencionada debe permitir autorizar e impedir los accesos a los sistemas de información
RESPONSABLE	Todos los usuarios

- El departamento de sistemas deberá filtrar el tráfico evitando el acceso o flujo de información, desde de la red interna hacia la externa o viceversa.
- Los usuarios sospechan que existen alguna brecha de seguridad o infección de virus deben comunicar de forma inmediata al personal del departamento de sistemas.
- El acceso a la red a través de conexiones no seguras podrían afectar el óptimo redimiendo de la infraestructura tecnológica de todo la industria. Para esto es necesario garantizar que cada uno de los usuarios que mantengan acceso a la red y sus servicios brindados no lleguen a comprometer la seguridad de la industria.
- El departamento de sistemas es el único que autorizará los nombres para los usuarios y contraseñas.

PRIVILEGIOS DE ACCESOS A LA RED

Los privilegios de acceso se mantendrán al mínimo necesario para el cumplimiento de las funciones individuales de cada funcionario, estos privilegios serán regulados a través de los siguientes lineamientos de seguridad:

- Deben establecerse por escrito y de forma detallada los privilegios de acceso que se encuentran en el listado de usuarios donde se especifica el nombre, apellido y cargo que ocupa, de ninguna manera se asignarán privilegios generales para todos los servicios.
- Los privilegios se asignan en función de la premisa “solo lo que el usuario necesita

saber", no se retribuye funciones ni accesos a ningún módulo o servicio que no sea los que estrictamente se necesitan para el cumplimiento de su función.

- Los privilegios se asignan a usuarios específicos y nunca a usuarios generales designados a utilizarse para tareas básicas de operación del sistema con datos o información pública.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	6. Control de Accesos
CONTROL	6.5 Control de accesos al Internet
ALCANCE	La política mencionada debe permitir el acceso al servicio de internet, de tal forma, debe establecer las restricciones de conexión con relación a horarios, especialmente a aplicaciones críticas, esta reducción minimizará las posibilidades de accesos no autorizados, protegiendo proactivamente la red de datos e información.
RESPONSABLE	Todos los usuarios

- Se debe disponer de un listado de usuarios autorizados, especificando nombre, apellidos y cargo que ocupa en la industria, así como los servicios para los que están autorizados.
- Es política de la industria restringir a los usuarios de todos los departamentos de

acuerdo a su puesto de trabajo el acceso a la conexión a internet de forma wireless o cableada.

- El servicio de páginas interactivas y de mensajería instantánea como Skype, Facebook y YouTube solo tendrán uso los gerentes o jefes de cada departamento.
- Está prohibido la descarga, uso e instalación de software malicioso no autorizado e intercambio de documentos que brinden cualquier información sobre como atentar contra la seguridad de la información corporativa.
- Se debe realizar el monitoreo permanente de páginas que son visitadas por parte del personal que laboran en la industria o usuarios terceros.
- Los usuarios no deben instalar software en sus estaciones de trabajo, en los servidores de la red, o en otras máquinas, incluso si este software es libre o no licenciado; toda instalación de software debe hacerla un técnico designado luego de la debida verificación y la autorización previa del departamento de sistemas.
- Los servidores disponibles para almacenar información que se encuentran en el internet no deben ser utilizados para las actividades que se realiza dentro de la industria, siempre y cuando sean necesarios la utilización de estos deben ser notificados al administrador para la aprobación y el uso de dichos servidores.
- Todas las conexiones que se realicen hacia a la parte interior y exterior de la red deben ser monitoreadas por parte del departamento de sistemas para protegerse mediante la detección de intrusos.

LIMITACIONES DE TIEMPO DE CONEXIÓN

- El departamento de sistemas deberá establecer periodos de tiempo de conexión hacia la red en caso de procesos o aplicaciones críticas que no sean permitida, a menos que exista un requerimiento por escrito y aprobado que indique lo contrario.
- Los equipos o usuarios sobre los cuales no se establece restricción por horarios, deben estar inventariados y debidamente documentados, las razones por las cuales se realizó esta excepción, incluso si esta es ocasional o temporal.

CORREO ELECTRÓNICO

- Todas las cuentas de correo electrónico deben ser creadas y asignadas solamente por el personal del departamento de sistemas.
- Las cuentas de correo electrónico institucional deben ser utilizadas únicamente para el desempeño de las funciones asignadas dentro de FLORALP.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	7. Administración de incidentes en la seguridad.
CONTROL	7.1 Gestión de incidentes y mejoras
ALCANCE	Dar a conocer a todos los usuarios la manera de solicitar accesos a lugares y a equipos de alta confidencialidad para la industria.
RESPONSABLE	Todos los usuarios

- El jefe de sistemas presentará al jefe de talento humano un cronograma anual de los cursos de capacitación requeridos para los usuarios que tienen accesos a información confidencial de la industria y a usuarios que forman parte de la infraestructura de red, con el objetivo de mejorar la disponibilidad, la confiabilidad de la información.
- Debe realizarse solicitudes y formularios para la obtención de contraseñas, accesos a la información y el registro de alguna modificación de equipos ya sea para mantenimiento o respaldos.

INDUSTRIA LECHERA FLORALP S.A

DOMINIO	8. Marco legal y buenas practicas.
CONTROL	8.1 Conformidad y cumplimiento legislativo.
ALCANCE	Cumplir con todas la políticas diseñadas para cada uno de los usuarios caso contrario se procederá la sanción respectiva.
RESPONSABLE	Departamento de sistemas

- El departamento de sistemas serán encargados de supervisar el cumplimiento de las políticas de seguridad.
- El departamento de sistemas debe determinar la sanción como la cancelación temporal de conexión a cualquier servicio dentro de la red de datos y en algunos casos la suspensión definitiva del mismo para cualquier tipo de abuso cometido dentro de la red de datos.

3.3 Selección de software para firewall en base a la norma IEE 830

3.3.1 Análisis de las posibles soluciones de OPEN SOURCE

A continuación se detalla las principales características de cada posible solución de open source.

3.3.1.1 CENTOS

CentOS, es una distribución de GNU/Linux derivado, o más bien clonado de Red Hat Enterprise Linux, lo que permite una compatibilidad del 100% con los binarios de las aplicaciones desarrolladas para RHEL. Por ello, y al estar "respaldado" por una compañía tan importante como Red Hat, es una de las distribuciones más usadas, de hecho, hoy por hoy es la segunda más usada para aplicaciones Web (Garron, 2013).

La primera versión de CentOS fue lanzada en mayo de 2004 y la última versión estable es CentOS 7.0.1406, lanzada en julio de 2014. CentOS, se utiliza básicamente para la administración de sistemas.

Figura 26. Logo de CentOS
Fuente: Logo de CentOS Recuperado de: http://www.centos.org/

3.3.1.1.1 Características

CentOS funciona bien para servidores, debido a la configuración por defecto de uso fácil y programas incluidos, incluyendo MySQL, de Apache y PHP. Incluye una gama estándar de los navegadores web y utilidades de oficina, excepto programas innecesarios para el uso del servidor. CentOS suministra herramientas para la instalación y gestión de sistemas operativos invitados en el mismo equipo. De hecho, los servidores pueden incluso ejecutar varias copias de CentOS en el mismo hardware. CentOS también incluye características de seguridad y funciones destinadas a ayudar a crear equipos agrupados para una mayor potencia de procesamiento. A continuación se mencionan las características más importantes como lo son:

3.3.1.1.1.1 Estabilidad

CentOS deriva de Red Hat Enterprise Server (servidor empresarial Red Hat) en base a Linux, un sistema operativo comercial. CentOS ofrece mucha más estabilidad operacional a sus usuarios que otros sistemas de Linux distribuidos libremente debido a las similitudes en diseño con el sistema lanzado comercialmente. Comparado con otros sistemas operativos basados en Linux, CentOS solo ejecuta las versiones más básicas y estables de programas, reduciendo el riesgo de bloqueos del sistema (Brachmann, 2013).

3.3.1.1.1.2 Velocidad

CentOS puede operar mucho más rápido que los sistemas operativos basados en Linux similares porque solo ejecuta las versiones básicas de software. De esa manera, el procesador que ejecuta el sistema CentOS no se empantana intentando ejecutar muchas aplicaciones diferentes. Los programas de CentOS tienen menos posibilidades de tener gusanos de seguridad o de bloqueos, que pueden reducir las velocidades informáticas o incluso hacer que el sistema se bloquee.

3.3.1.1.1.3 Confiabilidad

El sistema operativo CentOS puede ejecutar una computadora mucho tiempo sin requerir ninguna actualización del sistema adicional. Las actualizaciones de hardware para CentOS son desarrolladas para ser concurrentes con las actualizaciones del sistema Red Hat Enterprise Linux en el que se basa.

3.3.1.1.1.4 Facilidad de actualización

El ciclo de soporte de actualización para CentOS es de aproximadamente cinco años; otros sistemas basados en Linux tienen ciclos de soporte más cortos, de tres años hasta aproximadamente 18 meses.

3.3.1.1.1.5 Facilidad de uso

En cuanto a facilidad de uso, CentOS, en todos los casos puede optar por programas para el entorno gráfico o para la consola, lo que hace más fácil y más difícil respectivamente, el uso de los programas.

3.3.1.1.1.6 Soporte de arquitecturas

CentOS tiene soporte para múltiples arquitecturas entre ellas se encuentran:

- Intel x86-compatible 32bits.
- Intel itanium 64bits.
- AMD64 e Intel 64.
- PowerPC/32.
- DEC Alpha.
- SPARC.

3.3.1.1.1.7 Requisitos de sistema

Los requisitos de sistema mínimos para hardware recomendado para operar son los siguientes:

Tabla 16. Requerimientos de sistema

Tipo de instalación	RAM (mínimo)	Disco duro (mínimo)	Disco duro (recomendado)	Procesador
Sin entorno gráfico	64 MB	1024 GB	2 GB	Intel Pentium I/II/III/IV/Celeron, AMD K6/II/III.
Con entorno gráfico	2 MB	20 GB	40 GB	Intel Pentium I/II/III/IV/Celeron, AMD K6/II/III.

Fuente: Requisitos mínimos de hardware Recuperado de: http://goo.gl/BJkh0y

3.3.1.1.1.8 Comunidad y soporte

Red Hat y CentOS han decidido unir sus fuerzas; desde ahora CentOS y su comunidad están bajo el apoyo de Red Hat.

3.3.1.2 UBUNTU

Ubuntu es una distribución Linux que ofrece un sistema operativo predominantemente enfocado a ordenadores de escritorio aunque también proporciona soporte para servidores.

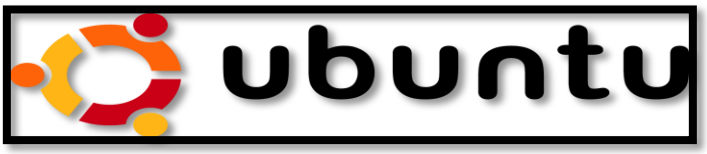


Figura 27. Logo de Ubuntu

Fuente: Logo de Ubuntu Recuperado de http://logo-kid.com/ubuntu-logo-hd.htm

3.3.1.2.1 Características

A partir de la versión 9.04, se empezó a ofrecer soporte extraoficial para procesadores ARM comúnmente usados en dispositivos móviles. Al igual que la mayoría de los sistemas de escritorio basados en Linux, a continuación se describe las principales características de esta distribución de Linux que son las siguientes:

3.3.1.2.1.1 Estabilidad

Ubuntu dado que comparte el código base de Debian, también comparte su estabilidad, aunque las características adicionales pueden hacerlo ligeramente más propenso a cuelgues y fallos.

3.3.1.2.1.2 Velocidad

Ubuntu es más rápido, aunque las características añadidas afectan al rendimiento cuando se compara con Debian con el tiempo Ubuntu se ha convertido en un sistema operativo un tanto pesado y no es precisamente la mejor opción para el que cuenta con un hardware modesto.

3.3.1.2.1.3 Confiabilidad

El sistema incluye funciones avanzadas de seguridad y entre sus políticas se encuentra el no activar de forma predeterminada procesos latentes al momento de instalarse. Por eso no hay un cortafuego predeterminado, ya que supuestamente no existen servicios que puedan atentar contra la seguridad del sistema.

3.3.1.2.1.4 Facilidad de actualización

Las versiones estables se liberan cada 6 meses y se mantienen actualizadas en materia de seguridad hasta 18 meses después de su lanzamiento.

3.3.1.2.1.5 Facilidad de uso

Ubuntu, por otro lado, se dirige a usuarios inexpertos. Esto se refleja en el eslogan de la compañía de Ubuntu también “Linux para seres humanos”.

3.3.1.2.1.6 Soporte de arquitecturas

Ubuntu está destinado principalmente a ser usado en dispositivos de escritorio. Por lo tanto, solo soporta la arquitectura hardware que comúnmente encontramos en los ordenadores de escritorio disponible oficialmente para 2 arquitecturas: Intel x86, AMD64.

3.3.1.2.1.7 Requisitos de sistema

Los requisitos de sistema mínimos para hardware recomendado para operar son los siguientes:

Tabla 17. Requerimientos de sistema

Tipo de instalación	RAM (mínimo)	RAM (recomendado)	Disco duro
Sin entorno gráfico	64 Megabytes	256 Megabytes	1 Gigabyte
Con entorno gráfico	64 Megabytes	512 Megabytes	5 Gigabytes

Fuente: Requisitos mínimos de hardware Recuperado de: http://es.wikipedia.org/wiki/Ubuntu

3.3.1.2.1.8 Comunidad y soporte

La comunidad de Ubuntu, por otro lado, es más acogedora con los recién llegados y principiantes.

3.3.1.3 DEBIAN

Debian es una distribución libre, por completo manejada por la comunidad, no está basada en ninguna otra distribución y por el contrario la mayor parte de las distribuciones actuales están basadas en Debian. Además es famoso por filosofía de estabilidad ante todo, por eso no tiene un cronograma de lanzamiento de nuevas versiones. Estas se liberan cuando están listas esto hace que sea una de las opciones más estables de GNU/Linux que puedas tener.

Figura 28. Logo de Debian
Fuente: Logo de Debian Recuperado de: http://www.debian.org/

3.3.1.3.1 Características

Debian ofrece más flexibilidad y una gran variedad de paquetes fáciles de instalar, además, cuenta con una distribución estable y fiable, con una amplia documentación y una base de usuarios más grande, una mejor facilidad de Java y reproductores multimedia de código abierto, incluso para los formatos propietarios. A continuación se detalla las características más relevantes para Debian que son las siguientes:

3.3.1.3.1.1 Estabilidad

Se puede decir que Debian despide las pantallas azules y los cuelgues aleatorios del sistema; Debian casi nunca caerá que es por lo que es tan popular en aplicaciones de tipo empresarial y de alojamiento web.

3.3.1.3.1.2 Velocidad

Debian es especialmente rápido ya que no viene en un lote con un montón de funciones que degradan el rendimiento y software preinstalado.

3.3.1.3.1.3 Confiabilidad

En lo referente a los problemas de seguridad se solucionan rápidamente con parches de seguridad que se actualizan en internet. Casi no existen los malware o virus para este sistema operativo.

3.3.1.3.1.4 Facilidad de actualización

La actualización de Debian es mucho más sencilla y menos complicada, si solo tienes instalado software estándar y de sus repositorios, aunque Debian no es siempre actualizado tan pronto como otras distribuciones y puede quedarse atrás en algunas de las características.

3.3.1.3.1.5 Facilidad de uso

Debian es una primera distribución Linux para desarrolladores aunque es robusta, segura y potente, no está diseñada exactamente para aquellos nuevos en Linux. La comunidad de desarrolladores han trabajado incansablemente durante los últimos años para hacer el proceso de instalación y de configuración más sencillo.

3.3.1.3.1.6 Soporte de arquitecturas

Debian se ejecuta sin problemas en ordenadores de escritorio (arquitecturas x86 o x64) a dispositivos de mano (arquitectura ARM). A continuación se menciona algunas arquitecturas soportada por Debian.

- Todas las series Pentium (también llamada IA - 32), en el caso de la Corel Duo en modo 32 bits.
- AMD, en todas las series Athlon y las de la Athlon64 en modo 32 bits.
- Cyrix.
- La serie de procesadores Motorola 68X (68020, 68030, 68040 y 68060.)
- Power PC (procesador desarrollado por IBM, Motorola y Apple.)
- ARM.
- Hewlett-Packard PA Risc.
- IBM s/390.
- AMD64 (soporta los procesadores Athlon, Sempron, Pentium D, las series Xeon y Core2)

3.3.1.3.1.7 Requisitos de sistema

Los requisitos de sistema mínimos para hardware recomendado para operar son los siguientes:

Tabla 18. Requerimientos del sistema

Tipo de instalación	RAM (mínimo)	RAM (recomendado)	Disco duro
Sin escritorio	64 Megabytes	256 Megabytes	1 Gigabyte
Con escritorio	64 Megabytes	512 Megabytes	5 Gigabytes

Fuente: Requisitos mínimos de hardware Recuperado de: https://www.debian.org/releases/lenny/arm/ch03s04.html.es

3.3.1.3.1.8 Comunidad y soporte

Lo mejor sobre usar software de código libre es el sentido de comunidad que crean. Debian, dado que básicamente se construyó con desarrolladores voluntarios, tiene una comunidad mucho más grande. La comunidad de Debian suele estar más técnicamente orientada a cambios, modificaciones o actualizaciones.

3.3.2 Especificaciones de requisitos de software en base a la norma IEE 830-1998

3.3.2.1 Introducción

En esta parte se proporciona todas las Especificaciones de Requerimientos de Software (ERS), donde consta de la elección de software para la implantación del servidor de seguridad perimetral, tomando en cuenta la norma IEEE 830.

3.3.2.1.1 Propósito

El siguiente ERS define los requerimientos que debe cumplir el software que se utilizará para la implementación de la seguridad perimetral. Esto permite que el presente documento contenga lineamientos específicos que ayude no solo a la industria en cuestión si no a otras industrias al momento de una implementación de seguridad informática.

3.3.2.1.2 Ámbito

El software que se va a utilizar nos permitirá tener una infraestructura de red más confiable y segura mediante especificaciones y requerimientos de software que nos brinde disponibilidad e integridad de la información, además, una administración centralizada que facilite al administrador realizar cualquier modificación sin ningún problema sin comprometer la continuidad de los servicios de la industria.

3.3.2.1.3 Definiciones, Siglas y Abreviaciones

Infraestructura de red

Infraestructura de red se refiere a todos los dispositivos lógicos y físicos que posee la industria.

Seguridad informática

En la seguridad de la información el objetivo de la protección son los datos y trata de evitar su pérdida y modificación no autorizada. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos.

La seguridad de los datos es esencial, ya que por descuido o divulgación de la información puede ocurrir a través de publicaciones de los empleados en sus cuentas personales o al dejar a la vista de forma accidental datos confidenciales ya sean en sus equipos de trabajo.

Especificaciones y Requerimientos de Software (ERS)

Estas especificaciones tienen como prioridad documentar las necesidades funcionales que debe prestar el software, por lo tanto se identifican los requisitos que serán punto de referencia para validar el sistema final que compruebe que se ajuste a las necesidades del usuario.

Administración centralizada

Una administración centralizada es una parte fundamental donde el software permita reunir varios servicios en un solo donde dependan de un solo punto central.

Interfaz gráfica

La interfaz gráfica es una plataforma que facilita la comunicación entre un programa y el usuario donde el usuario interactúa permitiéndolos realizar acciones como: configurar, ejecutar, administrar, etc. Sin necesidad de escribir comandos y de conocer el funcionamiento interno del programa.

Servicios informáticos

La continuidad de los servicios informáticos permiten que la industria funcione de forma adecuada sin ningún imprevisto, reduciendo la inactividad mediante soluciones rápidas y de alta disponibilidad. De tal forma admite una protección total para la información y todos sus servicios sean físicos o lógicos.

3.3.2.1.4 Referencias

En la siguiente información se detalla las referencias para poder establecer los requisitos necesarios que debe cumplir el software para la seguridad informática.

- IEEE-STD-830-1998: Especificaciones de los Requisitos del Software.
- Proyecto de Titulación: Exponer un documento que contenga una metodología para la implementación de un sistema de seguridad perimetral para la red de

datos de la industria FLORALP S.A en la ciudad de Ibarra, basado en la plataforma de software libre.

3.3.2.1.5 Apreciación Global

En esta guía se define dos partes la primera se hizo referencia a las especificaciones del ERS en la siguiente parte se da a conocer los requerimientos detallados del software que debe cumplir para satisfacer al sistema.

3.3.2.2 Descripción General

3.3.2.2.1 Perspectiva del Software

El software para el servidor de seguridad debe poder ser aplicado en cualquier otra industria dependiendo de los requerimientos de red permitiendo interactuar con los elementos de red que constituyen en la infraestructura de red. Además, se trata de una aplicación que debe ejecutarse o funcionar bajo cualquier arquitectura que se encuentre dentro del equipo.

3.3.2.2.2 Funciones del Software

Optimización

- Alta disponibilidad
- Procesamiento de información

- Libre de licencias
- Flexibilidad en soluciones informáticas.
- Tener una gran comunidad de apoyo y soporte.

Servicios

- Balanceo de carga
- Implementación de más servidores y servicios.
- Actualizaciones periódicas con alta frecuencia de versiones mejoradas.
- Filtrado de paquetes a nivel de capa 2 y 3.

Administración centralizada

- Manejo de backups
- Interfaces gráficas más amigables
- Amplia gama y variedad de herramientas libres en un solo.
- Mayor rendimiento de la información

Compatibilidad

- Mayor compatibilidad de hardware
- Compatibilidad con tarjetas de red
- Con sistemas operativos
- Alto nivel de estabilidad comprobada.
- Independencia tecnológica.

3.3.2.2.3 Restricciones

- El software debe ser estable y de una administración muy amigable para el usuario o responsable, donde este debe contar con conocimientos previos sobre software libre para la implementación del sistema.

- El software debe permitir el intercambio de datos de forma rápida con una estabilidad y flexibilidad en el campo de seguridad informática.

3.3.2.2.4 Atenciones y Dependencias

Para un servidor de seguridad el software debe ser compatible con diferentes arquitecturas.

3.3.2.3 Requisitos específicos

A continuación se realiza los requisitos necesarios para la selección de software.

3.3.2.3.1 Interfaces Externas

3.3.2.3.1.1 Interfaces de Usuario

REQ01: Administración del sistema

El software para la seguridad informática debe tener una interfaz gráfica centralizada donde el administrador o el responsable contará con una visión general de toda las funciones que ofrece dicho software, de tal manera pueda realizar cualquier cambio de forma inmediata sin ningún problema evitándose así el manejo de comandos por medio de la consola y garantizando la disponibilidad y el alto rendimiento de acuerdo con las políticas de seguridad planteadas para la industria.

3.3.2.3.1.2 Interfaces Hardware

REQ02: Compatibilidad de Hardware

El software debe disponer una amplia compatibilidad con los servidores que se implementarán y con todos los dispositivos de entrada y salida.

REQ03: Instalación del Software

El sistema tiene que prestar una facilidad de instalación para cualquier tipo de usuario que desee hacer uso del software.

3.3.2.3.2 Funciones

REQ04: Procesamiento de la Información

El software debe ser capaz de procesar y almacenar información de acuerdo con las necesidades del usuario o comunicarse desde cualquier lugar si se cuenta con una conexión internet.

REQ05: Flexibilidad para soluciones

Debe contar con una plataforma con estabilidad y flexibilidad sin precedentes, de tal forma, permitiendo dar soluciones inmediatas para superar nuevos retos.

REQ06: Capacidad de multitareas

El software debe permitir ejecutar muchos programas al mismo tiempo sin detener la ejecución de aplicaciones. Además, deducir el tiempo muerto (tiempo en el que no puede seguir trabajando en una aplicación porque un proceso aún no ha finalizado), dando una flexibilidad de no tener que cerrar las ventas de las aplicaciones antes de abrir y trabajar con otras.

REQ07: Administración de recursos

El objetivo del software es contener una administración de todos los recursos; el arranque y parada del sistema, la administración de usuarios y grupos, la administración del sistema de archivos, la administración del sistema de impresión, la administración de seguridad e introducción a la configuración de red y los servicios de servidores.

REQ08: Disponibilidad para bakups

Debe soportar la creación de bakups locales, remotos (ftp, ssh, discos externos) permitiendo recuperar los datos desde un punto específico.

REQ09: Capacidad de multiusuario

El software debe asignar el tiempo de microprocesador simultáneamente a varias aplicaciones con la posibilidad de ofrecer servicios a diversos usuarios a la vez, ejecutando cada uno de ellos una o más aplicaciones. La característica que resalta de un grupo de personas es trabajar con la misma aplicación al mismo tiempo, desde el mismo terminal o desde terminales distintos.

REQ10: Multiplataforma

Las plataformas de hardware que se pueden utilizar deben ejecutarse sin problemas en cualquier ordenador de escritorio o servidor.

REQ11: Convivencia con otros sistemas operativos

Pueden estar juntos pero no funcionar al mismo tiempo. Cada vez que se arranque un host, se pueda elegir cuál de ellos se debe cargar, y a partir de este momento solo se puede utilizar aplicaciones destinadas al sistema operativo que estamos ejecutando.

REQ12: Velocidad en la ejecución de servicios

Debido a la multitarea real que incorpora, y que no es necesario cargar su entorno gráfico para ejecutar servicios o aplicaciones, hacen que su velocidad sea muy superior a los actuales sistemas operativos.

REQ13: Código fuente

Debe permitir que el código fuente sea posible modificarlo y adaptarlo a varias necesidades libremente.

REQ14: Crecimiento del sistema

El crecimiento del sistema, el código abierto, y la gran comunidad de miles de programadores, deben ser uno de los más rápidos que existen en la actualidad.

REQ15: Soporte en hardware y software

El sistema operativo debe contar con empresas que lo respalden, para tener un sistema con un soporte sólido.

REQ16: Simplicidad de manejo del sistema

El sistema debe prestar una facilidad del manejo de algunas distribuciones, de tal manera, mejorando el uso gracias al entorno de ventanas, sus escritorios y las aplicaciones diseñadas específicamente para él, cada día resultado ser más sencillo su integración y uso.

3.3.2.4 Selección del software

3.3.2.4.1 Establecimiento de valorización a los requerimientos

Luego de realizar todos los requisitos para la selección del software para la implementación de la seguridad perimetral, se asigna un valor a cada requerimiento y de esta forma determinar la mejor solución.

REQ01: Administración del sistema

0 No cuenta con interfaz gráfica para la administración.

1 Cuenta con una interfaz gráfica para la administración.

REQ02: Compatibilidad de Hardware

0 Soporta pequeña compatibilidad con interfaces de I/O.

1 Soporta mediana compatibilidad con interfaces de I/O.

2 Soporta gran compatibilidad con interfaces de I/O.

REQ03: Instalación del Software

0 Dificultad para la instalación en discos locales y virtuales.

1 Facilidad de instalación en discos locales y virtuales.

REQ04: Procesamiento de la Información

0 Pequeño procesamiento de información.

1 Menor procesamiento de información.

2 Mayor procesamiento de información.

REQ05: Flexibilidad para soluciones

0 No cuenta con herramientas de seguridad.

1 Cuenta con una pequeña lista de herramientas de seguridad.

2 Cuenta con múltiples herramientas de seguridad.

REQ06: Capacidad de multitareas

0 No es posible ejecutar varias aplicaciones y procesos simultáneamente.

1 Cuenta con una pequeña posibilidad de ejecutar varias aplicaciones y procesos simultáneamente.

2 Es posible ejecutar varias aplicaciones y procesos simultáneamente.

REQ07: Administración de recursos

0 No realiza administración de recursos.

1 Realiza administración de recursos

REQ08: Manejo de Backups

0 Admite el respaldo de todo el sistema.

1 Admite el respaldo de todo el sistema incluyendo archivos del disco.

REQ09: Capacidad de multiusuario

0 Solo permite un solo usuario acceder a las aplicaciones y recursos de sistema.

1 Permite dos usuarios acceder a las aplicaciones y recursos del sistema.

2 Varios usuarios pueden accedes a las aplicaciones y recursos del sistema.

REQ10: Multiplataforma

0 Hace uso de una o dos plataformas para la instalación.

1 Hace uso de varias plataformas para la instalación.

REQ11: Convivencia con otros sistemas operativos

0 No reconoce la mayoría de sistemas operativos en una red.

1 Reconoce la mayoría de sistemas operativos en una red.

REQ12: Velocidad en la ejecución de servicios

0 No mantiene la funcionalidad de la red e incluso después de algún problema.

1 Mantiene la funcionalidad de la red e incluso después de algún problema.

REQ13: Código fuente

0 Permite la modificación del código fuente con la existencia de malware o virus.

1 Permite la modificación del código fuente sin la existencia de malware o virus.

REQ14: Crecimiento del sistema

0 Las actualizaciones en los repositorios en tiempo son cortas.

1 Las actualizaciones en los repositorios es tiempo son rápidas.

REQ15: Soporte en hardware y software

0 No cuenta con una comunidad y soporte técnico.

1 Cuenta con una pequeña comunidad y soporte técnico.

2 Cuenta con múltiples comunidades y soporte técnico.

REQ16: Simplicidad del manejo del sistema

0 No es ideal para servidores, no cuenta con seguridad en el sistema.

1 Ideal para servidores, se puede encontrar una mayor seguridad en el sistema.

3.3.2.5 Calificación para cada solución de software para la seguridad perimetral

Luego de realizar la valoración a cada requerimiento basándose en la norma IEE 830, se procede a la comparación respectiva de cada solución de software para la implementación del sistema de seguridad.

Tabla 19.Valoración para cada solución de software

REQUERIMIENTO	CENTOS	UBUNTU	DEBIAN
REQ01	1	1	1
REQ02	2	2	2
REQ03	1	1	0
REQ04	2	1	1
REQ05	2	1	1
REQ06	2	1	1
REQ07	1	0	1
REQ08	1	1	1
REQ09	2	1	1
REQ10	1	0	1
REQ11	1	1	1
REQ12	1	0	1
REQ13	1	0	0
REQ14	1	0	0
REQ15	1	2	1
REQ16	0	0	1
TOTAL	**20**	12	14

Fuente: Realizado por Gabriela López

Una vez realizado la calificación de cada requerimiento se observó que el software con mayor puntaje es CentOS, la confiabilidad y la estabilidad de esta herramienta permite la implementación del sistema de seguridad perimetral.

CentOS entre sus características importantes se destaca por el alto uso como servidores y una gran compatibilidad con sistemas operativos, aplicaciones y servicios; mayor confiabilidad, comunidades, soporte técnico para la solución de problemas, eficiencia de la administración de la red, un alto grado de procesamiento de información y una amplia gama de compatibilidad de plataforma, por lo tanto, CentOS hace la mejor opción para la solución de seguridad informática.

3.4 Selección del software para el sistema de detección de intrusos en base a la norma IEE 830

3.4.1 Análisis de las posibles soluciones de OPEN SOURCE

A continuación se detalla las principales características de cada posible solución de open source.

3.4.1.1 SNORT

Snort es un IDS o sistema de detección de intrusiones es uno de los más utilizados actualmente, es un sistema de código abierto de detección de intrusos de red capaz de llevar acabo análisis de tráfico en tiempo real y registro de paquetes en redes IP. Puede efectuar análisis de protocolos, búsqueda de patrones en el contenido y puede utilizarse para detectar una gran variedad de ataques y sondeos.

Figura 29.Logo de Snort
Fuente: Snort Recuperado de: www.snort.org

3.4.1.1.1 Características

Snort es uno de los IDS (Sistema de Detección de Intrusos) más conocidos y usados en todo el mundo. El equipo de desarrollo ha lanzado una versión Alpha de Snort 3.0 con una gran cantidad de cambios.

3.4.1.1.1.1 Arquitectura

Snort proporciona un conjunto de características que lo hacen una herramienta de seguridad muy potente, entre las que destacan la captura del tráfico ´ de red, el análisis y registro de los paquetes capturados y la detección´ de tráfico malicioso o deshonesto. Antes de nombrar con mayor detalle las características de Snort, es importante conocer y comprender su arquitectura. Snort está formado por un conjunto de componentes, la mayoría de los cuales son plug-ins que permiten la personalización de Snort. Entre estos componentes destacan los preprocesadores, que permiten que Snort manipule de forma más eficiente el contenido de los paquetes antes de pasarlos al elemento de detección, y su sistema de notificaciones y alertas basados en plug-ins, que permiten que la información´ reportada pueda ser enviada y

almacenada en distintos formatos y siguiendo distintos métodos. La arquitectura central de Snort se basa en los siguientes cuatro componentes:

- Decodificador de paquetes o Sniffer
- Preprocesador
- Motor de detección
- Sistema de alertas e informes

Siguiendo esta estructura, Snort permitirá´ la captura y el preprocesador del trafico ´ de la red a través´ de los dos primeros componentes (decodificador de paquetes y preprocesador), realizando posteriormente un chequeo contra ellos mediante el motor de detección´ (según´ el conjunto de reglas activadas) y generando, por parte del último de los componentes, las alertas y los informes necesarios. La siguiente figura 30 muestra la arquitectura básica de Snort.

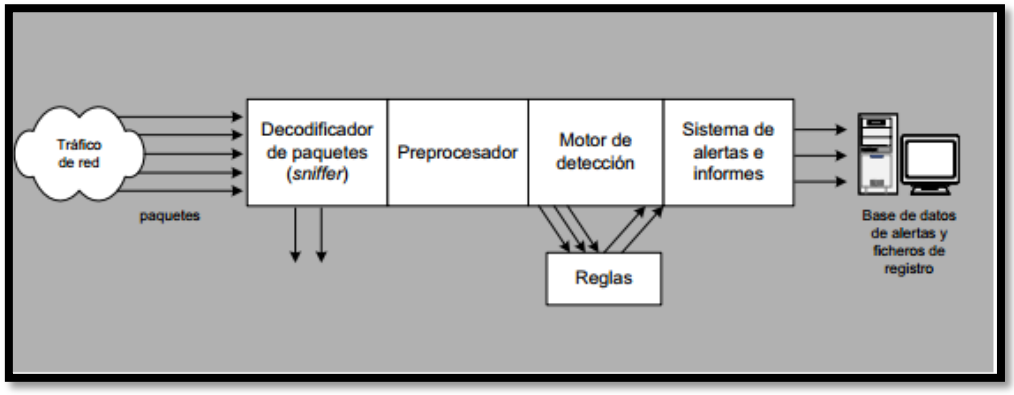


Figura 30.Arquitectura básica de Snort

Fuente: Snort Recuperado de: http://www.deic.uab.es/material/26118-snort.pdf

3.4.1.1.1.2 Facilidad de actualización

Una de las grandes ventajas de Snort es que es opensource, lo que quiere decir que mucha gente colabora en su desarrollo. Uno de los puntos donde mejor se ve es en el desarrollo de nuevas firmas. Es conveniente que realicemos la actualización mínimo una vez al mes de forma habitual y de forma inmediata en el caso de aparición de riesgos muy graves.

3.4.1.1.1.3 Soporte de arquitecturas

Snort está disponible bajo licencia pública, gratuito y funciona bajo plataformas Windows y UNIX/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

3.4.1.1.1.4 Facilidad de uso

Snort entre sus características esta la facilidad de uso debido a que se basa en un análisis de datos en tiempo real son la exactitud o veracidad, la eficiencia , además cuenta con una interfaz gráfica fácil de identificar las alarmas con sus respectivos grupos asignándoles una prioridad a cada uno de ellos dependiendo que anomalía se identifique.

3.4.1.1.1.5 Disponibilidad

La característica más apreciada de Snort, además de su funcionalidad, es su subsistema flexible y disponible de firmas de ataques.

3.4.1.2 SURICATA

Suricata es un motor IPS/IDS de código abierto bajo licencia GPLv2y desarrollado por la comunidad de OISF (Open Infomation Security Foundation), es relativamente nuevo pero con muy buenas características siendo la más importante su arquitectura Multi-hilos, además es totalmente compatible con las reglas Snort y Emerging Threads.

Figura 31.Logo de Suricata
Fuente: Suricata Recuperado de: http://suricata-ids.org/

3.4.1.2.1.1 Arquitetura de Suricata

Suricata funciona a base de multi-hilos, usa múltiples núcleos del CPU para procesar paquetes de manera simultánea. Si está en un CPU con un solo núcleo los paquetes serán procesados uno por uno. Existen 4 módulos por hilo de CPU: Adquisición de paquete, decodificación de paquete, capa de flujo de datos, detecciones y salidas. El módulo de adquisición de paquete lee el paquete desde la red. El módulo de decodificación interpreta el paquete y se encarga de gestionar a qué stream pertenece qué paquete; el módulo de capa de flujo realiza 3 tareas:

- La primera, realiza lo que se conoce como „tracking‟ o rastreo de flujo, que asegura que todos los pasos que se están siguiendo tienen una conexión de red correcta.
- La segunda: el tráfico de red TCP viene en paquetes, por lo tanto el motor de este módulo reconstruye el stream original.
- La tercera: la capa de aplicación será inspeccionada, tanto el flujo HTTP como DCERPC (Distributing Computing Environment Remote Procedure Call) será analizado. Los hilos de detección compararan firmas, pueden existir varios hilos de detección que pueden trabajar simultáneamente.
- Finalmente en el módulo de detecciones y salidas, todas las alertas y eventos serán analizados.

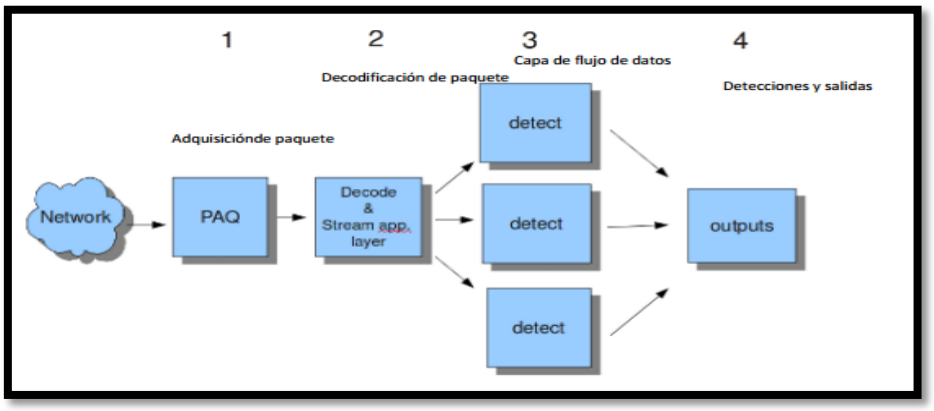


Figura 32.Arquitectura de Suricata
Fuente: Suricata Recuperado de: http://suricata-ids.org/

3.4.1.2.1.2 Facilidad de actualización

Suricata por sí solo no tiene reglas con las cuales comparar los paquetes y discernir cuando hay ataques en la red. Al igual que Snort, Suricata depende de reglas externas para su funcionamiento. Suricata es compatible con todas las reglas desarrolladas para Snort e incluso ha definido nuevos campos en las reglas que Snort no soporta. Entre los desarrolladores que destacan por su continua actividad en el desarrollo y actualización de reglas y firmas de seguridad están: Emerging Threats y SourceFire (desarrolladores de Snort).

3.4.1.2.1.3 Soporte de arquitecturas

Suricata puede ser instalado en varias plataformas. La documentación oficial de suricata ofrece instrucciones de instalación en varias plataformas, entre ellas: Linux (Centos, Ubuntu/Debian), Windows y MAC OS.

3.4.1.2.1.4 Facilidad de uso

Suricata cuenta con una interfaz muy complicada al momento de encontrar alguna anomalía debido al tiempo de respuesta para la detección que es muy lento. ES decir que cuando queremos implementarlos en redes conmutadas ya que no hay segmento de red por donde pase todo el tráfico. Además, tiene problemas en redes con velocidades de tráfico muy altas en las cuales es difícil procesar todos los paquetes.

3.4.1.2.1.5 Disponibilidad

Suricata es una herramienta muy joven en procesos de mejores y optimización debido a que depende mucho de desarrolladores externos.

3.4.2 Especificaciones de requisitos de software en base a la norma IEE 830-1998

3.4.2.1 Introducción

En esta parte se proporciona todas las Especificaciones de Requerimientos de Software (ERS), donde consta de la elección de software para la implantación del sistema de detección de intrusos, tomando en cuenta la norma IEEE 830.

3.4.2.1.1 Propósito

El siguiente ERS define los requerimientos que debe cumplir el software que se utilizará para la implementación del sistema de detección de intrusos. Esto permite que el presente documento contenga lineamientos específicos que ayude no solo a la industria en cuestión si no a otras industrias al momento de una implementación de seguridad informática.

3.4.2.1.2 Ámbito

El software que se va a utilizar nos permitirá vigilar y analizar eventos que ocurren dentro de la infraestructura de red para buscar que indiquen problemas de seguridad (violaciones a políticas) de seguridad, además, una administración centralizada que facilite al administrador realizar cualquier modificación dentro de la reglas del motor de detección sin ningún problema sin comprometer la continuidad de los servicios de la industria.

3.4.2.1.3 Definiciones, Siglas y Abreviaciones

Infraestructura de red

Infraestructura de red se refiere a todos los dispositivos lógicos y físicos que posee la industria.

Seguridad informática

En la seguridad de la información el objetivo de la protección son los datos y trata de evitar su pérdida y modificación no autorizada. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos.

Motor de Detección

Analiza los paquetes en base a las reglas definidas para detectar los ataques.

Violación de seguridad

Cuando se ha detectado alguna anomalía que comprometa la pérdida de información ya sea de modo físico o lógico.

Especificaciones y Requerimientos de Software (ERS)

Estas especificaciones tienen como prioridad documentar las necesidades funcionales que debe prestar el software, por lo tanto se identifican los requisitos que serán punto de referencia para validar el sistema final que compruebe que se ajuste a las necesidades del usuario.

Administración centralizada

Una administración centralizada es una parte fundamental donde el software permita reunir varios detectar varias anomalías en un solo, donde dependan de un punto central.

Interfaz gráfica

La interfaz gráfica es una plataforma que facilita la comunicación entre un programa y el usuario donde el usuario interactúa permitiéndolos realizar acciones como: configurar, ejecutar, administrar, etc. Sin necesidad de escribir comandos y de conocer el funcionamiento interno del programa.

Detección de anomalías

Debe aportan a nuestra seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa, diseñados para detener un ataque, aunque sí pueden generar ciertos tipos de respuesta ante éstos. Po lo tanto aumentan la seguridad de nuestro sistema de seguridad perimetral, vigilando el tráfico de la red, examinando los paquetes analizándolos en busca de datos sospechosos y detectando las primeras fases de cualquier ataque como pueden ser el análisis de nuestra red.

3.4.2.1.4 Referencias

En la siguiente información se detalla las referencias para poder establecer los requisitos necesarios que debe cumplir el software para el sistema de detección de intrusos.

- IEEE-STD-830-1998: Especificaciones de los Requisitos del Software.
- Proyecto de Titulación: Exponer un documento que contenga una metodología para la implementación de herramientas necesarias para complementar un sistema de seguridad perimetral para la red de datos de la industria FLORALP S.A en la ciudad de Ibarra, basado en la plataforma de software libre.

3.4.2.1.5 Apreciación Global

En esta guía se define dos partes la primera se hizo referencia a las especificaciones del ERS en la siguiente parte se da a conocer los requerimientos detallados del software que debe cumplir para satisfacer al sistema.

3.4.2.2 Descripción General

3.4.2.2.1 Perspectiva de la Herramienta

La herramienta que se va ser uso para el sistema de detección de intrusos que servirá como complemento para el servidor de seguridad debe poder ser aplicado en cualquier otra

industria dependiendo de los requerimientos de red permitiendo interactuar con los elementos de red que constituyen en la infraestructura de red. Además, se trata de una aplicación que debe ejecutarse o funcionar bajo cualquier arquitectura que se encuentre dentro del equipo.

3.4.2.2.2 Funciones que debe prestar la herramienta

Optimización

- Alta disponibilidad.
- Tiempo de respuesta inmediata.
- Libre de licencias.
- Tener agentes externos para la actualización del motor de detección.

Servicios

- Cuadros estadísticos de las anomalías encontradas.
- Actualizaciones periódicas con alta frecuencia de versiones mejoradas.

Administración centralizada

- Interfaces gráficas más amigables
- Amplia gama y variedad de herramientas libres en un solo.
- Mayor eficiencia en el almacenamiento de su base de datos.

Compatibilidad

- Mayor compatibilidad con múltiples plataformas
- Alto nivel de estabilidad comprobada.

- Debe detectar de forma exacta y controlar los ataques o patrones defnidos.

3.4.2.2.3 Restricciones

- EL software a implantarse deben ayudar a los administradores a mantener vigilados los sistemas y las redes, estos productos pueden, en tiempo real, percatarse de cuándo está ocurriendo un ataque. Esto ofrece al administrador la oportunidad de reaccionar ante las agresiones o incluso marcarles alarmas donde el sistema fue violado y sus logs están contaminadas, este tipo de sistemas pueden ahorrar a los administradores los días que llevaría averiguar qué pasó exactamente.

3.4.2.2.4 Atenciones y Dependencias

Para un sistema de detección de intrusos debe poder trabajar sobre diferentes arquitecturas y plataformas.

3.4.2.3 Requisitos específicos

A continuación se realiza los requisitos necesarios para la selección de software.

REQ01: Efectividad

El requerimiento importante IDS’s debe ser capaz de detectar de forma exacta y consistente los ataques o patrones definidos.

REQ02: Instalación del Software

El sistema tiene que prestar una facilidad de instalación para cualquier tipo de usuario que desee hacer uso del software.

3.4.2.3.1 Funciones

REQ03: Fácil uso

Debe ser fácil de manejo ya sea por parte de personas no expertas en seguridad.

REQ04: Procesamiento de la Información

El software debe ser capaz de procesar y almacenar información en su motor o base de datos para que el administrador pueda observar de forma inmediata todas las alertas identificadas.

REQ05: Adaptabilidad

El IDS debe adaptarse a diferentes plataformas, ambientes y políticas de seguridad creadas, debido a que no todos los ambientes no son homogéneos, además, debe ser capaz de entender entradas de otros sistemas.

REQ06: Robustez

El software debe permitir ejecutar muchos programas al mismo tiempo sin detener la ejecución de aplicaciones. Además, de ser suficientemente confiables debe contar con mecanismos redundantes y características que permitan operar en caso de fallas.

REQ07: Rapidez

El objetivo del software es ser capaz de ejecutar vigilancia permanente y reportar eventos en momento de ocurrencia.

REQ08: Eficiencia

El uso óptimo de recursos de cómputo, almacenamiento y ancho de banda, por lo tanto, aumentará la afectación mínima al desempeño del sistema vigilado.

REQ09: Escalabilidad

El software debe tener componentes con interfaces estándar bien documentadas estas interfaces deben soportar los mecanismos de autentificación apropiados.

REQ10: Seguridad

Debe contar con las características que eviten utilización por personal no autorizado.

REQ11: Equilibrio

Permitir a usuarios mantener balance entre necesidades de administración y de seguridad.

REQ12: Código fuente

Debe permitir que el código fuente sea posible modificarlo y adaptarlo a varias necesidades libremente.

REQ13: Soporte en hardware y software

El software debe contar con empresas que lo respalden, para tener un sistema con un soporte sólido.

3.4.2.4 Selección del software

3.4.2.4.1 Establecimiento de valorización a los requerimientos

Luego de realizar todos los requisitos para la selección del software para la implementación el sistema de detección de intrusos herramienta complementaria para el sistema de seguridad perimetral, se asigna un valor a cada requerimiento y de esta forma determinar la mejor solución.

REQ01: Efectividad

0 Cuenta con sensores para la detección de patrones sospechosos.

1 Cuenta con muchos sensores para la detección de patrones sospechosos.

REQ02: Instalación del Software

0 Dificultad para la instalación en discos locales y virtuales.

1 Facilidad de instalación en discos locales y virtuales.

REQ03: Fácil uso

0 No cuenta con interfaz gráfica para la administración.

1 Cuenta con una interfaz gráfica para la administración.

REQ04: Procesamiento de la Información

0 Pequeño procesamiento de información.

1 Menor procesamiento de información.

2 Mayor procesamiento de información.

REQ05: Adaptabilidad

0 Hace uso de uno o dos plataformas para la instalación.

1 Hace uso de varias plataformas para la instalación.

REQ06: Robustez

0 Permite un solo usuario ejecutar la herramienta y su configuración.

1 Permite un dos o más usuarios ejecutar la herramienta y su configuración.

REQ07: Rapidez

0 No posee la opción del envió de anomalías mediante una cuenta de correo electrónico.

1 Permite informar al administrador de las anomalías mediante una cuenta de correo electrónico.

REQ08: Eficiencia

0 No es posible ejecutar varias aplicaciones y procesos simultáneamente.

1 Cuenta con una pequeña posibilidad de ejecutar varias aplicaciones y procesos simultáneamente.

2 Es posible ejecutar varias aplicaciones y procesos simultáneamente.

REQ09: Escalabilidad

0 No mantiene una escalabilidad con diferentes interfaces.

1 Mantiene una escalabilidad con diferentes interfaces.

REQ10: Seguridad

0 Permite el uso del software por varias personas.

1 Permite el uso del software por ninguna persona excepto el administrador.

REQ11: Equilibrio

0 No mantiene la funcionalidad de la red e incluso después de algún problema.

1 Mantiene la funcionalidad de la red e incluso después de algún problema.

REQ12: Código fuente

0 Permite la modificación del código fuente con la existencia de malware o virus.

1 Permite la modificación del código fuente sin la existencia de malware o virus.

REQ13: Soporte en hardware y software

0 No cuenta con una comunidad y soporte técnico.

1 Cuenta con una pequeña comunidad y soporte técnico.

2 Cuenta con múltiples comunidades y soporte técnico.

3.4.2.5 Calificación para cada solución de software para la seguridad perimetral

Luego de realizar la valoración a cada requerimiento basándose en la norma IEE 830, se procede a la comparación respectiva de cada solución de software para la implementación del sistema de seguridad.

Tabla 20.Valoración para cada solución de software IDS

REQUERIMIENTO	SNORT	SURICATA
REQ01	1	1
REQ02	1	0
REQ03	1	1
REQ04	2	1
REQ05	1	0
REQ06	0	1
REQ07	1	0
REQ08	2	1
REQ09	1	1
REQ10	1	0
REQ11	1	0
REQ12	1	1
REQ13	2	1
TOTAL	**15**	8

Fuente: Realizado por Gabriela López

Una vez realizado la calificación de cada requerimiento se observó que el software con mayor puntaje es Snort, el grado de integridad al resto del IDS suministra una efectividad al proporcionar confiabilidad y adaptabilidad con diferentes plataformas o ambientes de tal manera es un complemento perfecto para el sistema de seguridad perimetral.

Snort permiten que los administradores y los encargados puedan observar y comprender lo que les dicen esta herramienta revelando problemas antes que ocurra la pérdida., de tal manera Snort hace la mejor opción para la solución de detección y búsqueda de anomalías dentro de la infraestructura de red.

3.4.3 Requisitos de hardware del servidor de seguridad

Los requisitos necesarios que debe tener el hardware donde se desarrollará el sistema de seguridad son los siguientes:

- **Tarjetas de Red**

El firewall requiere un mínimo de dos tarjetas de red utilizadas para la parte interna de la red y la otra para la parte externa de la red que se conecta al internet. Las tarjetas con una velocidad de 100 Mbit/s son aceptables para el uso del servidor de seguridad, es recomendable utilizar tarjetas idénticas para facilitar la instalación.

- **Memoria**

El requisito mínimo para la memoria es de 1GB para la realización de un cortafuego. Los puertos constituyen un " túnel", las comunicaciones y el acceso a ellos están controlados por el firewall. Para que el firewall realice funciones avanzadas, como el filtrado del contenido de los sitios web, se deba agregar más memoria.

- **Disco**

Los discos duros del firewall pueden ser utilizados para almacenar los registros de los intentos de intrusión y uso de la red. Además corre el sistema operativo elegido para el firewall. Un disco duro de 40 GB es suficiente para un firewall básico, sin embargo, el uso de dos discos duros ofrece un mayor nivel de tolerancia a fallos. Ambos discos se deben configurar como un espejo (los mismos datos se registran en ambos discos simultáneamente), es decir, que si uno falla el otro se puede utilizar para restaurar los datos y reducir el tiempo de inactividad

- **Refrigeración**

El entorno donde está ubicado el firewall debe contar con un ambiente de refrigeración debido que el servidor de seguridad trabaja las 24 horas al día, siete días a la semana. Debe proveer una ventilación adecuada de los componentes internos para evitar fallos de hardware.

Las características de hardware del servidor, se detallan a continuación en la Tabla 21.

Tabla 21. Características del Servidor

ProLiant ML350e Gen8 ES-2407 (648376-001)	
	
Hardware	
Familia de procesador	Intel® Xeon® E5-2400 v2
Número de procesadores	2 o 1
Núcleo de procesador disponible	10 u 8 o 6 o 4
Memoria de serie	4GB
Memoria máxima	96GB
Ranuras de memoria por cada socket	6 slots
Disco Duro	2 de 1TB
CD-ROM Drive	Solo se requiere para la instalación
USB	Solo se requiere para la instalación
Video Card	Cualquier tarjeta de video
Floopy Drive	No se requiere
Sound Card	No se requiere
Periféricos	
Monitor	Solo se requiere para la instalación

Mouse	No se requiere
Red	
Banda Ancha	Ethernet, cable DSL
Ranuras de expansión	4 PCI-Express slots estándar

Fuente: Características del servidor Recuperado de: http://goo.gl/mqJs0o

Para la obtención del hardware del servidor de seguridad el departamento de sistemas de la industria lechera FLORALP cuenta con el equipo de cómputo necesario para cubrir perfectamente las necesidades del diseño del sistema de seguridad perimetral, por lo tanto, no implica ningún costo extra para la industria

CAPÍTULO IV

4 Implementación Del Sistema De Seguridad Perimetral Para La Red De Datos

En este capítulo se desarrolla la implementación del Firewall de acuerdo con el planteamiento de las políticas de seguridad, además se realiza un nuevo diseño de topología de red con su respectivo direccionamiento con el propósito de obtener resultados que permitan medir su desempeño y confiabilidad de la red.

Se realiza una zona desmilitarizada DMZ[15] que permita acceder solo personal autorizado a los servidores como: servidores de aplicaciones, DNS[16], Base de Datos, DHCP[17]y de respaldos de manera adecuada obteniendo una administración centralizada de estos equipos.

Además, se desarrolla el IDS como un complemento del Firewall debido a que se vuelve necesaria la utilización de un sistema de detección de intrusos, que se encargue de la vigilancia de la red en busca de comportamientos sospechosos analizando el tráfico en tiempo real y registro los paquetes de la red.

[15] **DMZ:** Zona Desmilitarizada.

[16] **DNS:** Sistema de Nombres de Dominio

[17] **DHCP:** Protocolo de Configuración Dinámica de Máquinas.

4.1 Requerimientos para la implementación del sistema

La industria debe estar sustentada por una infraestructura de red lo bastante robusta para ofrecer un servicio confiable. Además, los servidores y las bases de datos deben tener mecanismos de protección que garanticen su disponibilidad, integridad y confidencialidad.

Las medidas que pueden considerarse deben unir una solución que se implemente a nivel de red y a nivel de host. Ambas deben complementarse con el desarrollo de una cultura informática de buenas prácticas y políticas de seguridad.

En primera instancia, es necesario distinguir la procedencia del tráfico que entra o sale de la red local, conocer que protocolos y puertos son utilizados para poder asignarles prioridades de tal forma garantizar paquetes no confiables hacia los sitios restringidos. A nivel de red, es necesario dividir en varias áreas como WAN, DMZ y LAN que faciliten la administración y optimicen la conectividad.

La red inalámbrica debe ser sustentada con mecanismos de control que permitan separar el tráfico de cada una de ellas, proteger la información y evitar accesos no autorizados.

Cada uno de los miembros de la industria, cumple funciones distintas, por lo que no todos tienen el mismo nivel de acceso a la información o a los servicios asociados. Tampoco la prioridad de acceso es la misma, por lo que es fundamental asignar perfiles de acceso a

nivel de red servicios y datos. Es necesaria la implementación de mecanismos de control que permitan filtrar tráfico, detectar paquetes no deseados y solucionar problemas de seguridad.

La base para la implementación del sistema de seguridad perimetral son los siguientes puntos:

- Topología de red
- Plan de direccionamiento
- Ubicación de servidores y puntos de acceso
- Análisis de los dispositivos de red con el fin de identificar los aspectos de hardware y software que pueden influir con la implementación.

Luego de haber realizado y analizado cada punto se puede dimensionar la red con las aplicaciones y protocolos que están siendo utilizados por los usuarios y servidores así como la necesidad del ancho de banda.

4.1.1 Diseño de la ubicación del servidor de seguridad perimetral

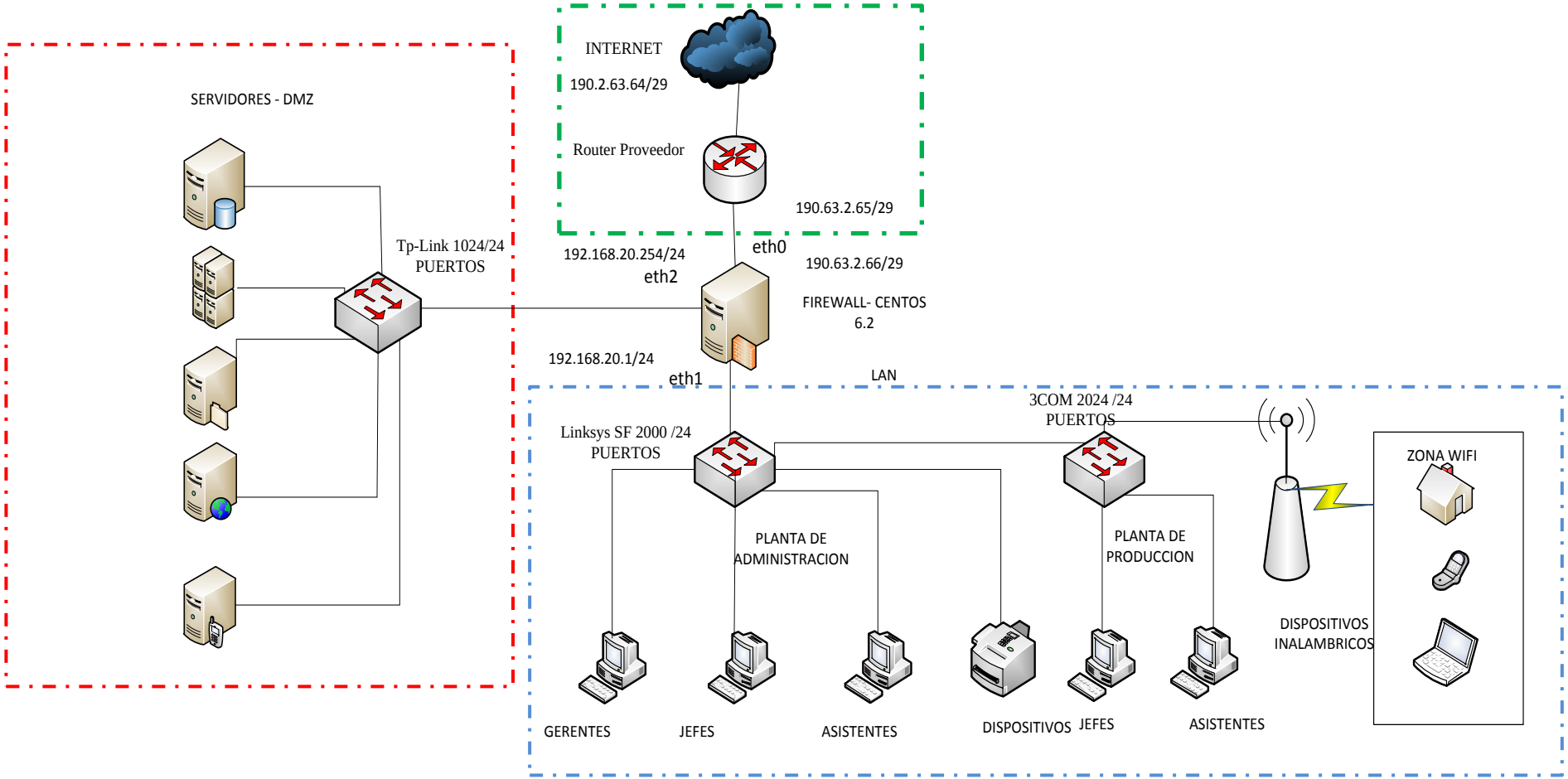


Figura 33. Diseño de la topología de red

Fuente: Graficación en Microsoft Visio 2010 realizado por Gabriela López

4.1.1.1 Direccionamiento IP de las tarjetas de red del servidor de seguridad

Para el nuevo diseño de la red se ha tomado en consideración un nuevo direccionamiento IP que permita la facilidad de identificar cada interfaz del servidor que se encuentra conectado a la infraestructura de red, se mantiene un solo de segmento de red debido a que el número de usuarios no es elevado, de tal manera, evitar el desperdicio de direcciones IP's.

Tabla 22. Direccionamiento del servidor Firewall

CONFIGURACIÓN IP DEL SERVIDOR FIREWALL					
Equipo	**Interfaz**	**IP**	**Máscara**	**Gateway**	**DNS**
SERVIDOR FIREWALL	eth0	190.63.2.66	255.255.255.248	190.63.2.65	200.25.207.114
	eth1	192.168.20.1	255.255.255.0		200.25.207.114
	eth2	192.168.20.254	255.255.255.0		200.25.207.114

Fuente: Direccionamiento IP Realizado por Gabriela López

4.1.1.2 Distribución de direcciones IP's

Con el nuevo direccionamiento se puede organizar los usuarios, equipos y dispositivos de red para ser identificados de manera inmediata, de tal manera, garantizar una administración centralizada. Además se considera ciertas direcciones IP libres para el crecimiento de usuarios y de dispositivos de red.

Tabla 23.Direccionamiento IP para la red de datos FLORALP

ASIGNACIÓN DE SUBRED	MASCARA DE SUBRED	CARGO
192.168.20.3	255.255.255.0	Servidor
192.168.20.4	255.255.255.0	Servidores
192.168.20.5	255.255.255.0	Servidores
192.168.20.6	255.255.255.0	Servidores
192.168.20.7	255.255.255.0	Servidores
192.168.20.8	255.255.255.0	Servidores
192.168.20.9-192.168.20.13		**Direcciones disponibles para servidores**
192.168.20.14	255.255.255.0	Antenas Inalámbricas
192.168.20.15	255.255.255.0	Antenas Inalámbricas
192.168.20.16	255.255.255.0	Antenas Inalámbricas
192.168.20.17	255.255.255.0	Router Inalámbrico
192.168.20.18	255.255.255.0	Router Inalámbrico
192.168.20.19	255.255.255.0	Impresora RICOH
192.168.20.20	255.255.255.0	Biométrico
192.168.20.21-192.168.20.25		**Direcciones disponibles para dispositivos de red**
192.168.20.26	255.255.255.0	Gerente General
192.168.20.27	255.255.255.0	Gerente Financiero
192.168.20.28	255.255.255.0	Gerente Producción
192.168.20.29	255.255.255.0	Jefe de aseguramiento de calidad
192.168.20.30	255.255.255.0	Jefe de planta
192.168.20.31	255.255.255.0	Jefe de compras
192.168.20.32	255.255.255.0	Jefe de canal
192.168.20.33	255.255.255.0	Contador general
192.168.20.34	255.255.255.0	Jefe de fomento ganadero
192.168.20.35	255.255.255.0	Jefe de bodega central

192.168.20.36	255.255.255.0	Jefe de mantenimiento
192.168.20.37	255.255.255.0	Jefe de producto terminado
192.168.20.38	255.255.255.0	Coordinador de administración
192.168.20.39	255.255.255.0	Jefe de seguridad y salud
192.168.20.40	255.255.255.0	Jefe de investigación y desarrollo
192.168.20.41	255.255.255.0	Asistente de contabilidad
192.168.20.42	255.255.255.0	Asistente de contabilidad
192.168.20.43	255.255.255.0	Asistente comercial
192.168.20.44	255.255.255.0	Asistente de mantenimiento
192.168.20.45	255.255.255.0	Asistente de contabilidad
192.168.20.46	255.255.255.0	Asistente de producción
192.168.20.47	255.255.255.0	Asistente de contabilidad
192.168.20.48	255.255.255.0	Asistente de Bodega
192.168.20.49	255.255.255.0	Asistente de producción
192.168.20.50	255.255.255.0	Asistente de producción
192.168.20.51	255.255.255.0	Asistente de DTH
192.168.20.52	255.255.255.0	Asistente de producción
192.168.20.53	255.255.255.0	Asistente de producción
192.168.20.54	255.255.255.0	Jefe de Sistemas
192.168.20.55	255.255.255.0	Asistente de Sistemas
192.168.20.56-192.168.20.76		**Direcciones disponibles para nuevos usuarios**
192.168.20.77	255.255.255.0	DHCP
192.168.20.78	255.255.255.0	DHCP
192.168.20.79	255.255.255.0	DHCP
192.168.20.80	255.255.255.0	DHCP
192.168.20.81	255.255.255.0	DHCP
192.168.20.82	255.255.255.0	DHCP
192.168.20.83	255.255.255.0	DHCP

192.168.20.77-192.168.20.91	**Direcciones asignadas para DHP**
192.168.20.92	255.255.255.0
192.168.20.93	255.255.255.0
192.168.20.94	255.255.255.0
192.168.20.92-192.168.20.253	**Direcciones sin asignación**

Fuente: Nuevo direccionamiento realizado por Gabriela López

4.1.1.3 Diseño y análisis del ambiente del servidor de seguridad perimetral

El servidor de seguridad perimetral asume roles importantes en la industria en este caso es utilizado como firewall para establecer una metodología de seguridad dirigida tanto para el tráfico interno como externo a la red.

Las necesidades de la red son:

- Asegurar el acceso y fiabilidad a la red.
- Mantener la confidencialidad e integridad de la información transmitida.
- Acceso seguro y rápido a los servidores internos.

4.1.1.4 Descripción básica del entorno de trabajo del servidor de seguridad perimetral

El servidor de seguridad perimetral va estar en medio del router del proveedor de CLARO, el switch Linksys SF 2000/24 y del Switch TP-LINK 24 ports10/100Mbps, este servidor va a tener tres interfaces de red, una llamada WAN que va a estar dando la cara al internet, la otra se denomina DMZ donde están ubicados todos los servidores de la industria y la

última interfaz se llama LAN que va a manejar la red interna donde se encuentran ubicados todos los usuarios y dispositivos inalámbricos identificados dentro de la red.

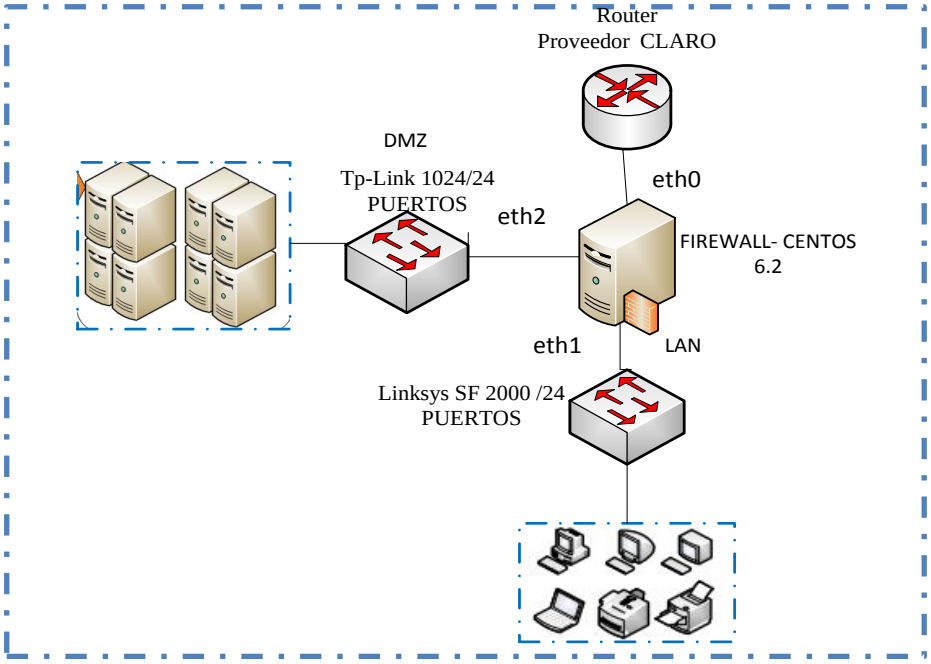


Figura 34.Entorno de trabajo del servidor

Fuente: Graficación en Microsoft Visio 2010 realizado por Gabriela López

4.1.1.5 Servidor firewall

Este servidor va a ser configurado con iptables y con el servicio de squid.

4.1.1.5.1 Diseño y análisis del ambiente de iptables

Este servidor trabaja con tres tarjetas, WAN para la red externa con la IP 190.63.2.66 y las otras para la LAN y DMZ con el rango 192.168.20.0/24. Las interfaces se encuentran configuradas en el Anexo E3, a continuación se muestra la tabla de ruteo de la interfaces

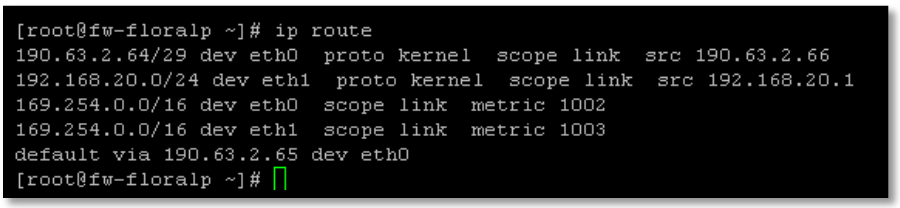


Figura 35.Tabla de ruteo de las interfaces del servidor

Fuente: Captura de pantalla por medio de Putty

Las reglas de las iptables que van a aplicarse para asegurar la red interna como externa son las siguientes:

- Permitir el tráfico a la interfaz interna.
- Permitir el tráfico interno.
- Hacer enmascaramiento de la red externa a la interna y viceversa.
- Permitir acceso desde LAN a WAN por los siguientes puertos.

  Puerto HTTP www
  Puerto FTP control
  Puerto FTP datos
  Puerto SSH
  Puerto HTTPS/SSL para transferencia segura
  Puerto POP3 y SMTP e-mail

4.1.1.6 Proceso de implementación y pruebas de los equipos.

La implementación de este proyecto varía dependiendo del número de usuarios, la localización geográfica, capacidades económicas y necesidades tecnológicas de la industria.

El modelo desarrollo PDCA (Planear-Hacer-Chequear-Actuar) va ser utilizada durante el desarrollo de la tesis; este modelo da un enfoque metodológico permitiendo establecer los requerimientos de seguridad de la información, mediante fases para el mejoramiento el nivel de seguridad informática y reduciendo los riesgos de la seguridad de la industria FLORALP, es decir que cualquier error en una de las etapas conduce necesariamente al riesgo de pérdida de información dando como resultado la afectación de la infraestructura de red. Esto se debe al estricto control que se debe mantener durante la vida del proyecto y a su vez de una amplia documentación escrita.

4.1.1.6.1 Implementación del servidor firewall

Se procede a configurar este servicio a través de iptables, con esto se consigue filtrar paquetes a nivel de red, este mecanismo permite crear un firewall adaptable a los requerimientos de la red de datos de la industria FLORALP.

En el archivo iptables crea reglas dirigiéndose a cada una de ellas diferentes características que deben cumplir todos los paquetes que entren o salgan del área perimetral del servidor. Además para cada regla se específica y se aplica una acción. Las reglas tienen un orden y cuando se recibe o se envía un paquete las reglas se verifican en orden hasta que las condiciones que pide una de ellas se cumple en el paquete y la regla aplicada sobre el paquete la acción que se haya especificado.

Estas acciones se aplican en los denominados targets, que indican la acción que debe aplicarse a cada paquete. Los más usados son bastantes evidentes ACCEPT, DROP y REJECT, pero también hay targets que permiten funcionalidades extras.

El esquema de filtrado de paquetes de Linux se establece en tres tablas bien marcadas cada una con distintas acciones a las que debe pertenecer un paquete su estructura jerárquica se divide así.

FILTER: Se usa para el filtrado general de paquetes y es la tabla predeterminada de Netfilter decide qué es lo que entra y qué no. Está compuesta por las siguientes cadenas:

- **INPUT:** Filtrado de tráfico entrante
- **OUTPUT:** Filtrado de tráfico saliente
- **FORWARD:** Filtrado de tráfico reenvido

NAT: Controla la traducción de direcciones. Permite alterar las direcciones origen y destino del datagrama, analizando algunas propiedades del mismo, está compuesta por las cadenas:

- **PREROUTING:** Permite realizar DNAT.
- **POSTROUTING:** Permite realizar SNAT.
- **OUTPUT:** Traslación de direcciones.

4.1.1.6.1.1 Creación de las reglas con iptables

Se establecen las políticas a aplicar sobre los paquetes y datagramas. En cada regla se encuentran los siguientes objetos.

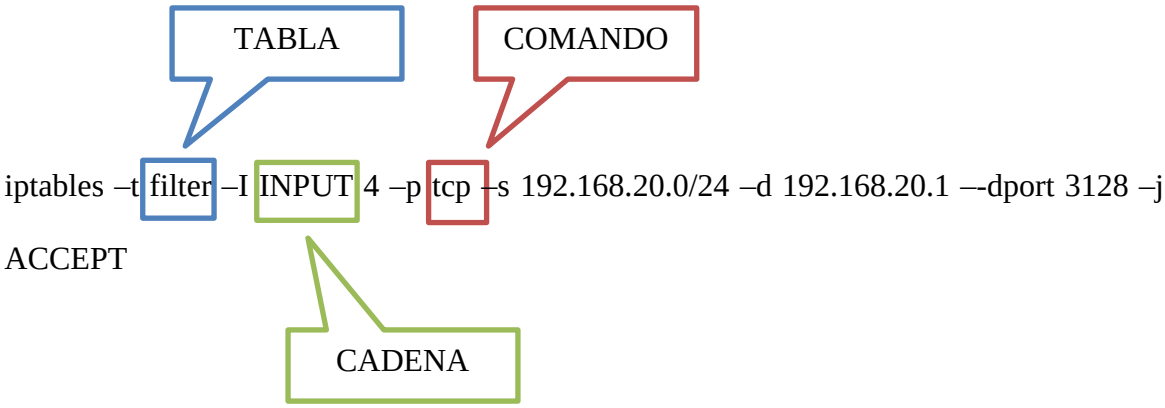
- **Tablas y Cadenas**

Un aspecto importante de las iptables es utilizar múltiples tablas para decidir el destino de un paquete en particular, dependiendo del tipo de paquete que se esté monitorizando y de qué es lo que se va a hacer con el paquete.

- **Comandos y Parámetros**

Los comandos le dicen a las iptables que realicen una tarea específica. Solamente un comando se permite por cada cadena de comandos iptables.

Una vez que se hayan especificado algunos comandos de iptables, incluyendo aquellos para crear, añadir, borrar, insertar, o reemplazar reglas de una cadena en particular, se necesitan parámetros para comenzar la construcción de la regla de filtrado de paquetes. A continuación se muestra un ejemplo de una regla con todos los objetos.



4.1.1.6.1.2 Filtrado de paquetes por iptables.

- Tráfico de la interfaz de loopback

Permitir que cualquier tráfico que provenga de interfaz de loopback se acepte, para ello se insertará la cadena INPUT de la tabla filter con la siguiente regla.

#iptables -A INPUT -i lo -j ACCEPT

```
[root@fw-floralp ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  192.168.20.0/24      192.168.20.1        tcp dpt:squid
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-prohibited
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  192.168.20.0/24      anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-prohibited
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:http state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             192.168.20.0/24
[root@fw-floralp ~]#
```

Figura 36. Tráfico para la interfaz de loopback
Fuente: Configuración de las iptables por medio de Putty

- Tráfico de la interfaz de intranet

Se permite todo el tráfico que provenga de la interfaz de red interna eth1 que controla el tráfico de la intranet de la industria FLORALP, ya que por esta interfaz navegan todos los departamentos y usuarios independientes de la industria.

#iptables -A INPUT -i eth1 -s 192.168.20.1/24 -j ACCEPT

#iptables -A OUTPUT -o eth1 -d 192.168.20.1/24 -j ACCEPT

- Permitir el tráfico interno

Se permite que todos los paquetes ingresen por la eth0 y sean reenviados localmente a través del internet y viceversa.

#iptables -t filter -I FORWARD -i eth0 –o eth1 -j ACCEPT

#iptables -t filter -I FORWARD -i eth1 –o eth0 -j ACCEPT

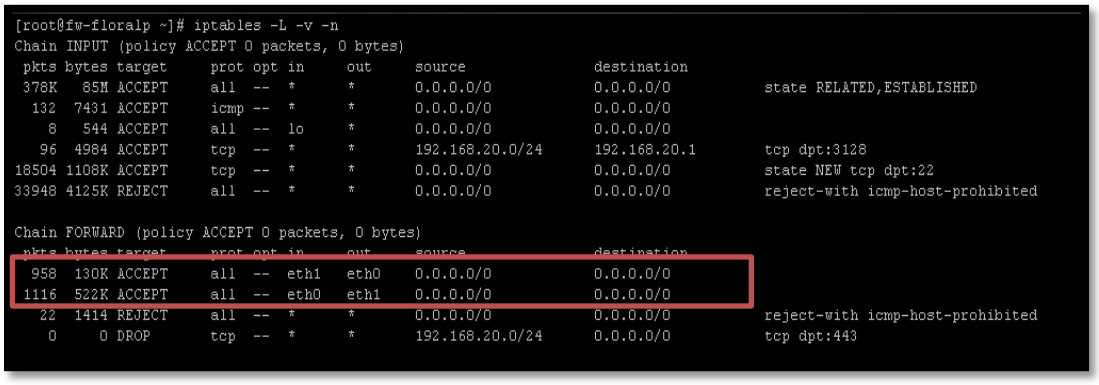


Figura 37. Permitir el tráfico interno

Fuente: Configuración de las iptables por medio de Putty

- Realizar el enmascaramiento de la red externa a la interna y viceversa.

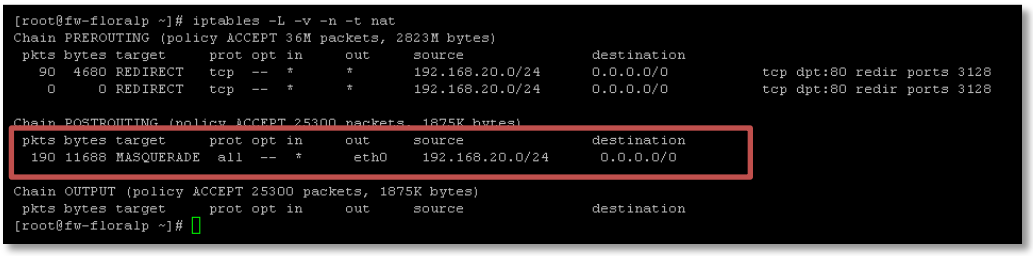


Figura 38.Traducción de dirección de red

Fuente: Configuración de las iptables por medio de Putty

Traducir toda la subred 192.168.20.0/24 y todas las direcciones que pertenezcan al mismo rango puedan conectarse a la WAN, de tal manera, se necesita enmascarar la subred atrás de la interfaz eth0.

- Permitir desde la LAN a la WAN

  - Puerto HTTP www

    #iptables -A FORWARD -i eth1 -p tcp -o eth0 --dport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT

  - Puerto HTTPS/SSL para transferencia segura

    #iptables -A FORWARD -i eth1 -p tcp -o eth0 --dport 443 -j ACCEPT

  - Puerto POP3 e-mail

    #iptables -A FORWARD -i eth1 -p tcp -o eth0 --dport 110 -j ACCEPT

- Puerto POP3 sobre SSL

#iptables -A FORWARD -i eth1 -p tcp -o eth0 --dport 995 -j ACCEPT

- Permitir él envió de paquetes ICMP desde el Departamento de sistemas a los servidores

#iptables -A FORWARD -p icmp -s 192.168.20.54 -i eth1 -d 192.168.20.3 -j ACCEPT

#iptables -A FORWARD -p icmp -s 192.168.20.55 -i eth1 -d 192.168.20.3 -j ACCEPT

#iptables -A FORWARD -p icmp -s 192.168.20.54 -i eth1 -d 192.168.20.4 -j ACCEPT

#iptables -A FORWARD -p icmp -s 192.168.20.55 -i eth1 -d 192.168.20.4 -j ACCEPT

#iptables -A FORWARD -p icmp -s 192.168.20.54 -i eth1 -d 192.168.20.5 -j ACCEPT

#iptables -A FORWARD -p icmp -s 192.168.20.55 -i eth1 -d 192.168.20.5 -j ACCEPT

#iptables -A FORWARD -p icmp -s 192.168.20.54 -i eth1 -d 192.168.20.6 -j ACCEPT

#iptables -A FORWARD -p icmp -s 192.168.20.55 -i eth1 -d 192.168.20.6 -j ACCEPT

#iptables -A FORWARD -p icmp -s 192.168.20.54 -i eth1 -d 192.168.20.7 -j ACCEPT

#iptables -A FORWARD -p icmp -s 192.168.20.55 -i eth1 -d 192.168.20.7 -j ACCEPT

#iptables -A FORWARD -p icmp -s 192.168.20.54 -i eth1 -d 192.168.20.8 -j ACCEPT

#iptables -A FORWARD -p icmp -s 192.168.20.55 -i eth1 -d 192.168.20.8 -j ACCEPT

- Permitir el acceso SSH desde el departamento de sistemas al servidor FIREWALL y denegar el resto de la red

#iptables -A INPUT -i 192.168.20.54 -d 190.63.2.66 -m state –state NEW -p tcp --dport 22 -j ACCEPT

#iptables -A INPUT -i 192.168.20.55 -d 190.63.2.66 -m state –state NEW -p tcp --dport 22 -j ACCEPT

#iptables -A INPUT -s 192.168.20.0/24 -p tcp --dport 22 -j DROP

4.1.1.6.2 Implementación de servicio proxy

4.1.1.6.2.1 Instalación de squid

La opción de instalación siguiente se aplica en el caso de que el paquete no exista o no se encuentre instalado. Todos los pasos de instalación de encuentran en el Anexo E4.

#yum install squid

4.1.1.6.2.2 Revisión de los paquetes necesarios

Revisar si el paquete se encuentra instalado, se puede comprobar en la Figura 39 el paquete se encuentra instalado, así como también la versión actual que se dispone.

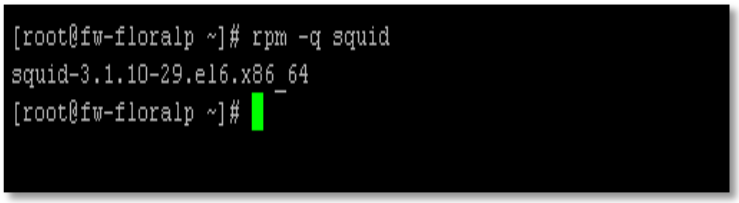


Figura 39. Revisión de la instalación de Squid

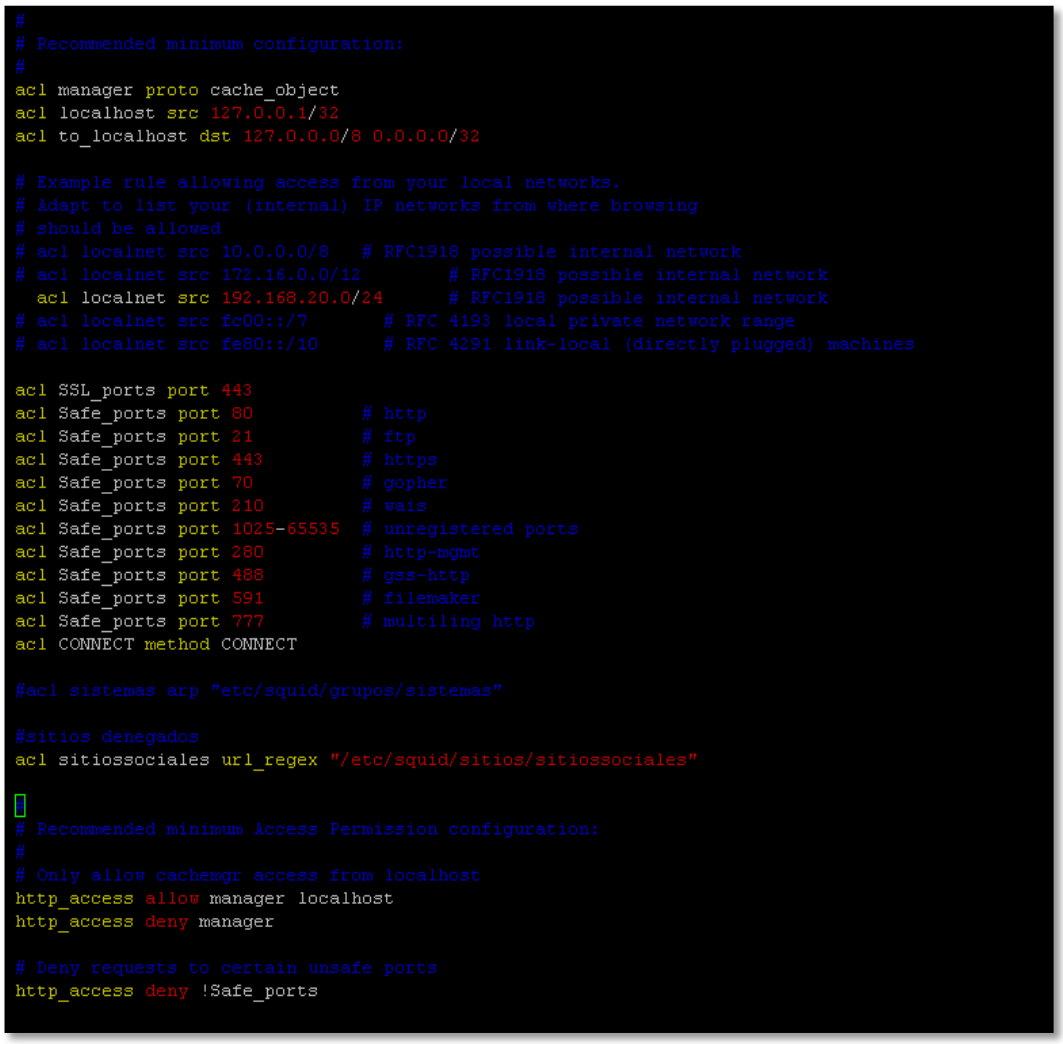
Fuente: Squid, Captura de pantalla por medio de Putty

4.1.1.6.2.3 Configuración de squid

El archivo principal de configuración de squid es bastante extenso, y tiene muchas opciones de configuración como se indica en la Figura 40. Los parámetros a configurar son los siguientes:

- Establecer dirección y puerto por el cual squid va atender peticiones.
- Establecer cuanto usará en cache de memoria.
- Especificar en qué directorio se van a guardar los logs del squid.
- Determinar líneas de control de acceso acl.

Todos estos parámetros de encuentran configurados en el Anexo E4.



```
#
# Recommended minimum configuration:
#
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
# acl localnet src 10.0.0.0/8   # RFC1918 possible internal network
# acl localnet src 172.16.0.0/12        # RFC1918 possible internal network
  acl localnet src 192.168.20.0/24      # RFC1918 possible internal network
# acl localnet src fc00::/7       # RFC 4193 local private network range
# acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#acl sistemas arp "etc/squid/grupos/sistemas"

#sitios denegados
acl sitiossociales url_regex "/etc/squid/sitios/sitiossociales"

#
# Recommended minimum Access Permission configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager

# Deny requests to certain unsafe ports
http_access deny !Safe_ports
```

Figura 40. Archivo de configuración de squid.conf

Fuente: Squid, Captura de pantalla por medio de Putty

Para finalizar la configuración debe redireccionar el tráfico del puerto 80 hacia el puerto 3128 para monitorear todos los usuarios conectados que se encuentran navegando en el internet, mediante la cadena PREOROUTING como se muestra en la Figura 41.

#iptables –t nat -A PREOROUTING -s 192.168.20.0/24 -p top --dport 80 –j REDIRECT –top-port 3128

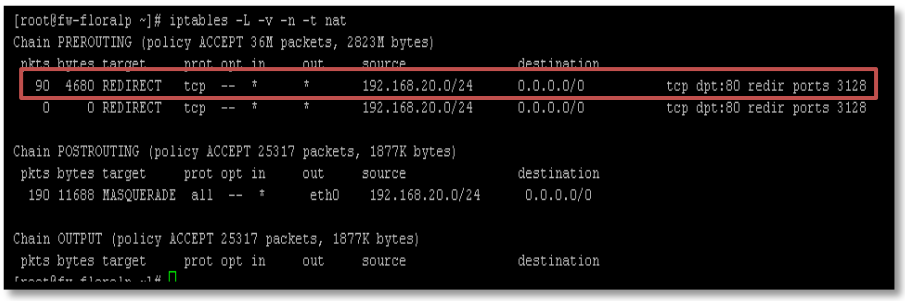


Figura 41.Re direccionar el trafico al puerto del servicio de squid
Fuente: Configuración de las iptables por medio de Putty

4.1.1.6.2.4 Creación de los directorios en el script squid.conf

- **Creación de los directorios sitios y grupos**

El directorio sitios contiene los archivos de los sitios denegados, permitidos y los horarios de navegación dependiendo si es en la mañana o tarde.

En el directorio grupos se encuentran clasificados de acuerdo al cargo que desempeñan cada uno de los empleados dentro de la industria, además, dentro de estos archivos contienen la dirección IP asignada a cada computador para facilitar la administración de los diferentes accesos.

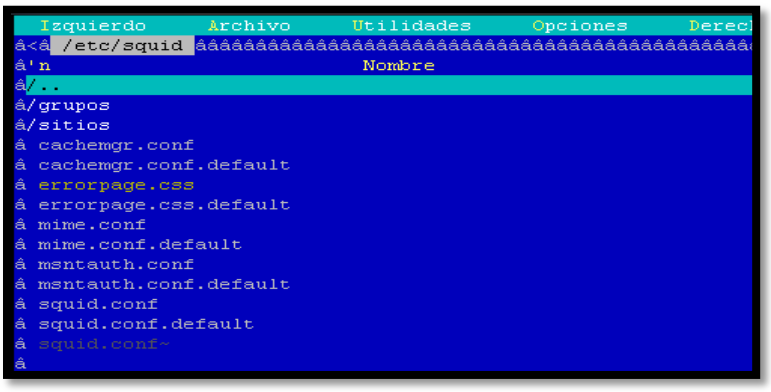


Figura 42. Creación del directorio sitios para squid.conf

Fuente: Squid, Captura de pantalla por medio de la interfaz de comandos

En la siguiente tabla 24 se encuentran los cargos y el número de empleados que se encuentran laborando dentro de la industria. Mirar el Anexo H.

Tabla 24. Cargo y número de Empleados de FLORALP

CARGO	NÚMERO DE EMPLEADOS
Gerentes	3
Jefes	13
Asistentes	21
Ayudantes	71
Total	108

Fuente: Proporcionado por el departamento de talento humano

- **Creación del archivo sitios sociales**

Con este archivo bloquea el contenido del acceso web, por lo tanto se deniega el acceso a todos los sitios sociales más concurridos como por ejemplo www.hi5.com.

vim /etc/squid/sitios/sitiossociales

Figura 43. Archivo para sitios sociales

Fuente: Squid, Captura de pantalla por medio de Putty

- **Creación del archivo sitios denegados**

En este archivo se encuentran las palabras que no pueden ser usadas al momento de realizar alguna consulta en el internet.

#vim /etc/squid/sitios/sitiosdenegados

Figura 44. Archivo para sitios denegados

Fuente: Squid, Captura de pantalla por medio de Putty

- **Creación del archivo sitios permitidos**

En este archivo se encuentran las palabras y páginas web que pueden ser utilizadas al momento de realizar una búsqueda en el internet como por ejemplo bancos y sitios estatales.

vim /etc/squid/sitios/sitiospermitidos

Figura 45. Archivo para sitios permitidos

Fuente: Squid, Captura de pantalla por medio de Putty

- **Creación de los archivos para horarios**

En este archivo se encuentran las direcciones IP de los usuarios a los que se les permite el acceso al internet de acuerdo a un horario establecido, como se puede observar en la Figura 46 la creación de la lista de acceso para el horario permitido para la navegación.

Figura 46. Creación de la lista de acceso para establecer el horario

Fuente: Squid, Captura de pantalla por medio de Putty

- **Creación del archivo para el grupo sistemas**

En este archivo se ubican las direcciones IP de cada usuario que pertenece al departamento de sistemas.

vim /etc/squid/grupos/sistemas

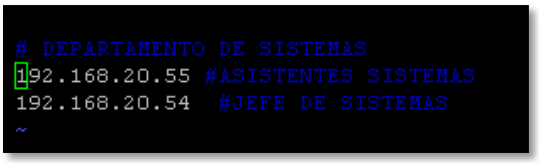


Figura 47. Archivo para el grupo sistemas

Fuente: Squid, Captura de pantalla por medio de Putty

- **Creación del archivo para el grupo gerentes**

En este archivo se encuentran los gerentes de los diferentes departamentos de la industria FLORALP.

vim /etc/squid/grupos/gerentes

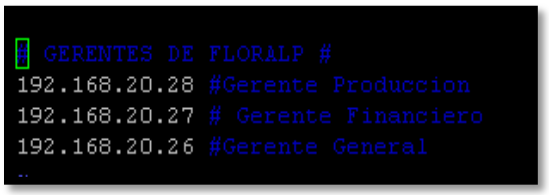


Figura 48. Archivo para el grupo gerentes

Fuente: Squid, Captura de pantalla por medio de Putty

- **Creación del archivo para el grupo jefes**

En este archivo se encuentran los jefes que laboran en los diferentes departamentos de la industria FLORALP.

vim /etc/squid/grupos/jefes

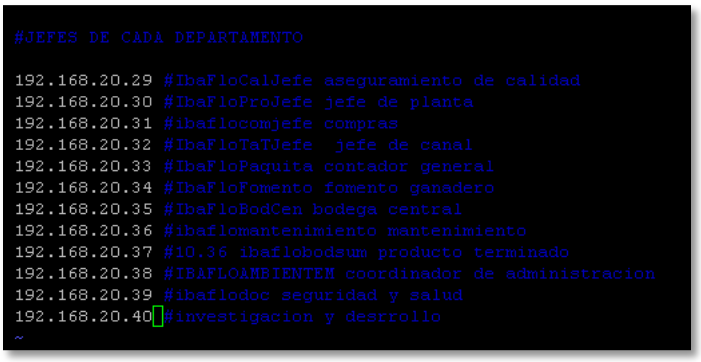


Figura 49. Archivo para el grupo jefes

Fuente: Squid, Captura de pantalla por medio de Putty

- **Creación del archivo para el grupo asistentes**

En este archivo se encuentran los asistentes que laboran en los diferentes departamentos de la industria FLORALP.

vim /etc/squid/grupos/asistentes

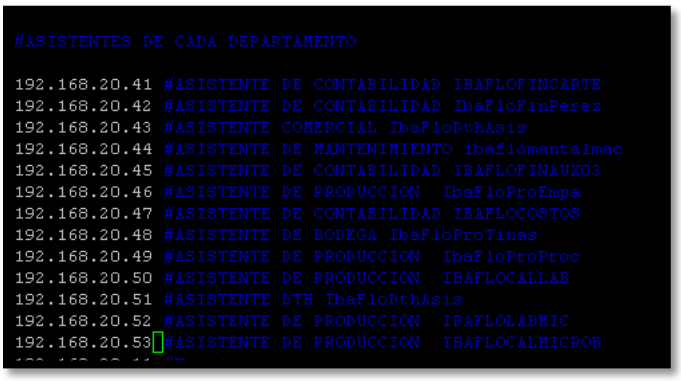


Figura 50. Archivo para el grupo asistentes

Fuente: Squid, Captura de pantalla por medio de Putty

- **Asociación de cada grupo con su sitio de acceso**

En esta parte asociaremos cada grupo con su respectivo sitio donde detalla que tipo de acceso tendrán.

Tabla 25.Asociar cada grupo con su sitio de acceso

Grupos	Sitios Denegados	Sitios Sociales	Sitios Permitidos	Horario en la Mañana	Horario en la Tarde
Sistemas	X	√	√	√	√
Gerentes	X	√	√	√	√
Jefes	X	X	√	√	√
Asistentes	X	X	√	X	X

Fuente: Realizado por Gabriela López

En la siguiente Figura 51 se muestra la configuración dentro del archivo squid.conf creando las listas de acceso asociación con cada grupo.

```
acl sistemas arp "etc/squid/grupos/sistemas"
acl gerentes arp "etc/squid/grupos/gerentes"
acl jefes arp "etc/squid/grupos/jefes"
acl asistentes arp "etc/squid/grupos/asistentes"

#sitios denegados
acl sitiossociales url_regex "/etc/squid/sitios/sitiossociales"
acl sitiosdenegados url_regex "etc/squid/sitios/sitiosdenegados"

#sitios permitidos
acl sitiospermitidos url_regex "/etc/squid/sitios/sitiospermitidos"
```

Figura 51. Creación de las listas de acceso dentro de squid.conf

Fuente: Squid, Captura de pantalla por medio de Putty

A continuación se agrega con un símbolo de ! que significa que se deniega el acceso a ciertas listas de control como se muestra en la Figura 52.

```
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet !sitiossociales
http_access allow localhost
http_access allow sistemas sitiospermitidos sitiossociales !sitiosdenegados
http_access allow gerentes sitiospermitidos !sitiosdenegados
http_access allow jefes sitiospermitidos !sitiossociales !sitiosdenegados
http_access allow asistentes sitiospermitidos!sitiossociales !sitiosdenegados
```

Figura 52. Creación de las listas de acceso dentro de squid.conf

Fuente: Squid, Captura de pantalla por medio de Putty

4.1.2 Ubicación del IDS dentro de la topología de red

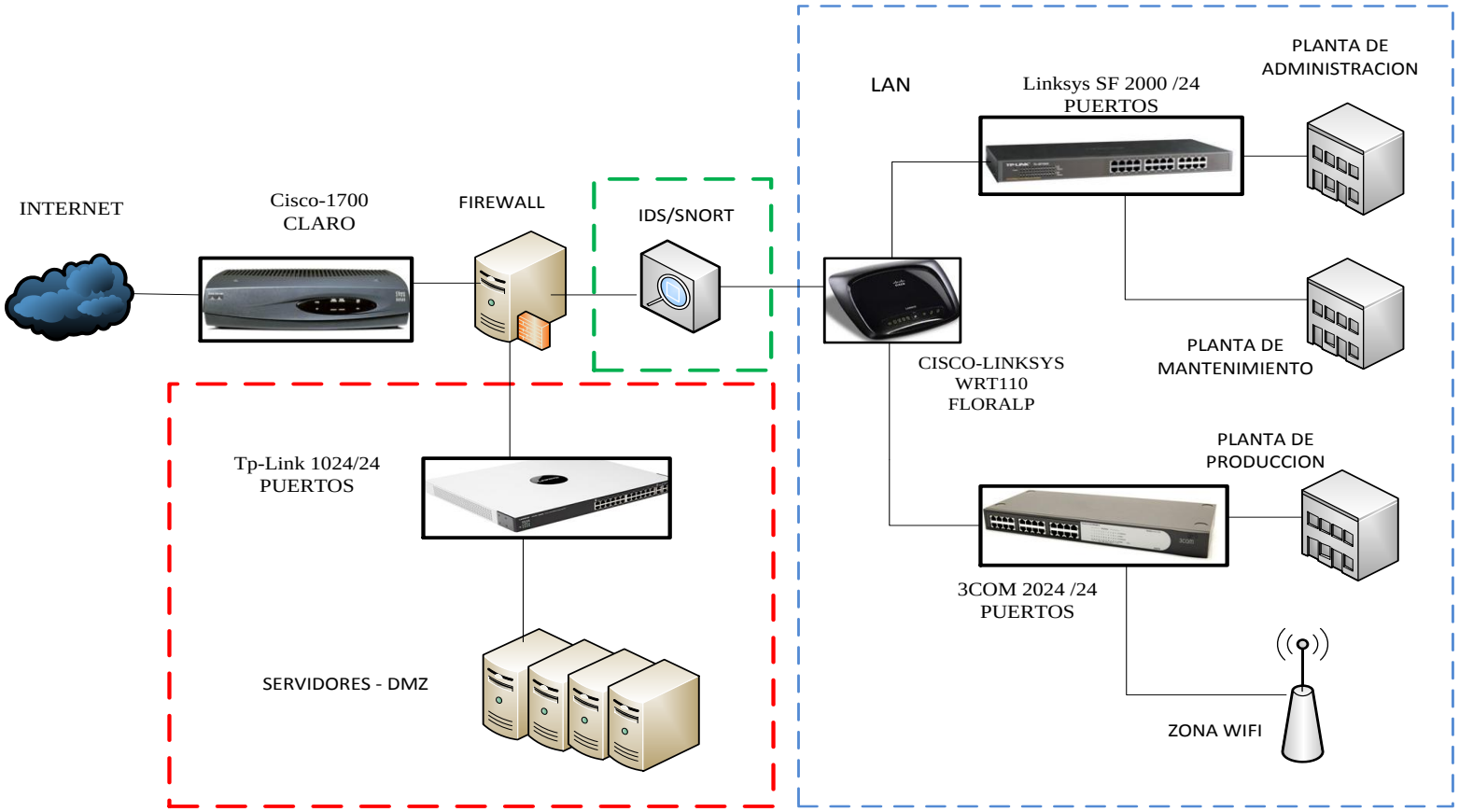


Figura 53. Ubicación del IDS

Fuente: Graficación en Microsoft Visio 2010 realizado por Gabriela López

4.1.2.1 Herramientas para la instalación del IDS

4.1.2.1.1 Snort

Figura 54. Logo de Snort
Fuente: Snort, Recuperado de http://www.snort.org/.

Es uno de los sistemas de detecciones de intrusos de red utilizados actualmente, con un sistema de código abierto capaz de llevar acabo análisis de tráfico en tiempo real y registro de paquetes en redes IP. Puede efectuar análisis de protocolos, búsqueda de patrones en el contenido y puede utilizarse para detectar una gran variedad de ataques y sondeos.

Utiliza un lenguaje flexible para describir el tráfico que debe analizar, entre su base de reglas incluye miles de comprobaciones en busca de múltiples ataques ofreciendo la posibilidad de alertar entiempo real. (Gómez D. G., 2003)

(MICHILENA, 2013) Menciona algunas ventajas para su elección como se muestra a continuación:

- Es basado en Open Source.
- Funciona bajo varias plataformas como Linux y Windows.
- Puede desempeñarse como snnifer, packet logger y NIDS.
- Sus firmas de ataques se actualizan constantemente y son adaptables a cualquier escenario.
- Es ampliamente utilizado por profesionales en seguridad informática, a partir de 1998, año donde fue liberado por primera vez.

Snort como IDS, es una herramienta extremadamente útil para la recopilación de información sobre un ataque o el inicio del mismo, sin embargo, se limita a ser una herramienta pasiva (sin respuesta).

Antes de iniciar la instalación y la configuración de snort es importante conocer su arquitectura de funcionamiento, de tal forma, se pueda ajustar a la red de datos de la industria FLORALP.

Se puede crear varias reglas para detectar cualquier ataque y de esta forma evitar cualquier alerta falsa. A continuación en la Figura 51 se detalla los pasos que sigue snort para detectar alguna alerta.

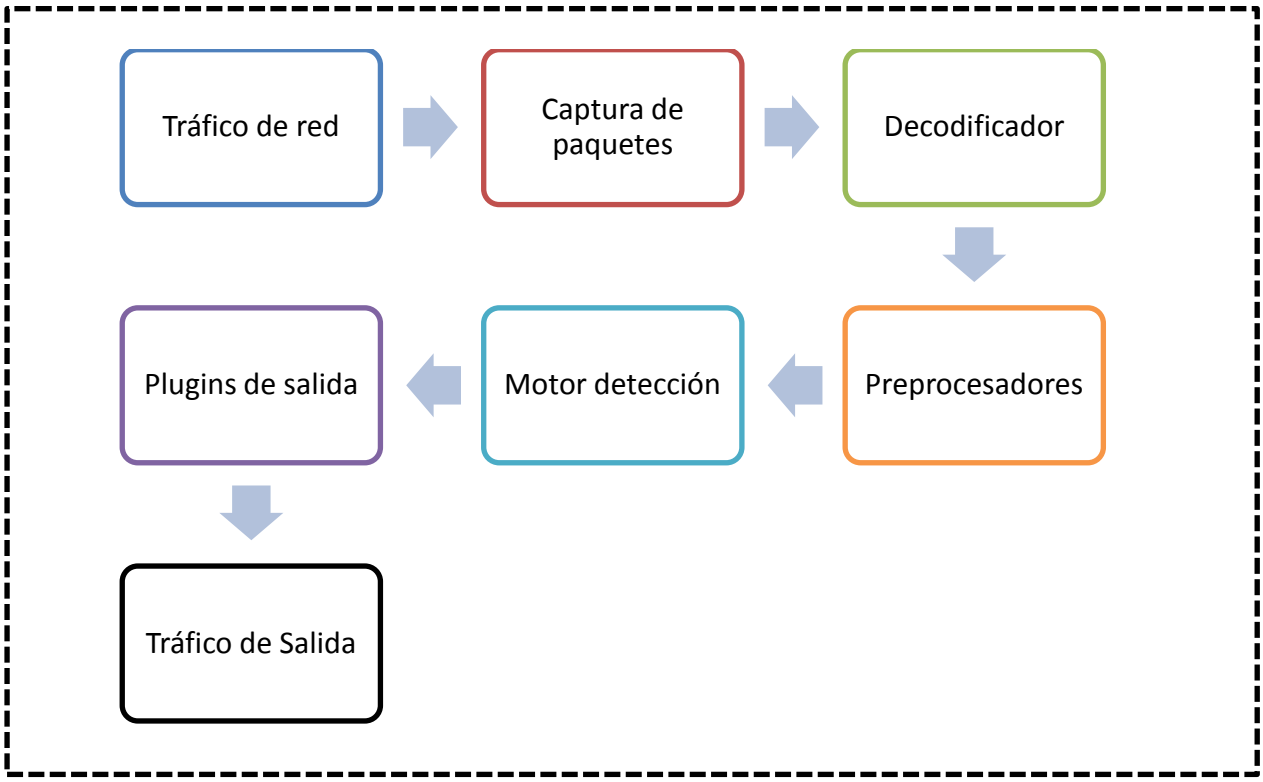


Figura 55. Arquitectura de Snort
Fuente: Snort Recuperado de http://www.adminso.es/images/d/d0/Pfc_Carlos_cap3.pdf

(Galindo, 2009): describe cada uno de los elementos que componen Snort

- **Módulo de captura del tráfico.** Es el encargado de capturar todos los paquetes de la red utilizando la librería libpcap.
- **Decodificador.** Se encarga de formar las estructuras de datos con los paquetes capturados e identificar los protocolos de enlace, de red, etc.
- **Preprocesadores.** Permiten extender las funcionalidades preparando los datos para la detección. Existen diferentes tipos de preprocesadores

dependiendo del tráfico que se analice (por ejemplo, existen los preprocesadores http, telnet)

- **Motor de Detección.** Analiza los paquetes en base a las reglas definidas para detectar los ataques.
- **Archivo de Reglas.** Definen el conjunto de reglas que rigen el análisis de los paquetes detectados.
- **Plugins de detección.** Son partes del software que son compilados con snort y se usan para modificar el motor de detección.
- **Plugins de salida.** Permiten definir qué, cómo y dónde se guardan las alertas y los correspondientes paquetes de red que se generan. Pueden ser archivos de texto o bases de datos.

4.1.2.1.2 Requisitos para la instalación de snort

La instalación y configuración de los requisitos que se mencionan a continuación se encuentran en el Anexo F.

- **Apache**

Figura 56. Logo de Apache
Fuente: Apache Recuperado de http://goo.gl/FvqtjY

Apache es un servidor web HTTP de código abierto para plataformas de sistemas operativos como UNIX y Windows NT. Su propósito es suministrar un servidor seguro y eficiente que brinde servicios HTTP actuales con soporte PHP y configurable para las aplicaciones de bases de datos como MySQL (Camelo, 2010).

- **PHP[18] Y MySQL**

Figura 57. Logo de PHP y MySQL

Fuente: Apache Recuperado de http://goo.gl/Iq2GrK

PHP es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web, entre sus importantes características esta la compatibilidad con las bases de datos como MySQL.

MySQL es un sistema de gestión de base de datos relacional, multihilo y multiusuario, que utiliza como módulo de salida de las alertas proporcionadas por el IDS. Es

[18] **PHP**: Hipertext Preprocesor

necesario tener almacenadas las alertas en una base de datos para mantener un buen funcionamiento del sistema. (Alfaro, 2010).

- **Interfaz BASE (BASIC ANALYSIS AND SECURITY ENGINE)**

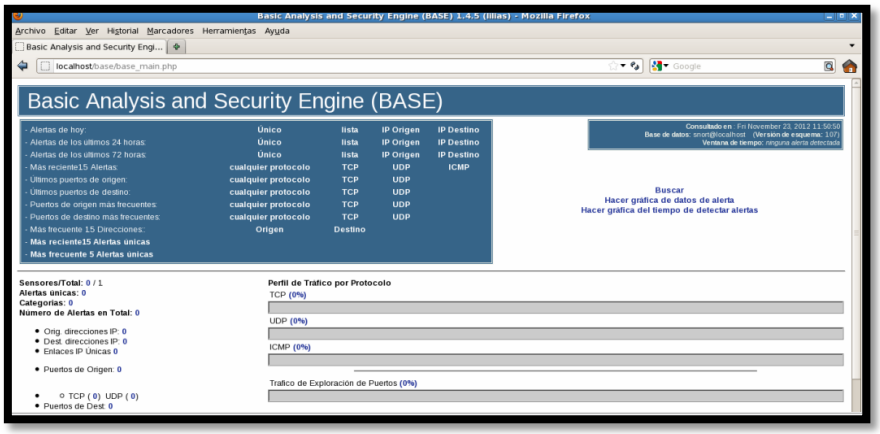


Figura 58. Interfaz gráfica de Base
Fuente: BASE Recuperado de http://www.snort.org

BASE es una interfaz web en PHP que permite gestionar de una forma fácil y cómoda las bases de datos de seguridad generadas por IDS, cortafuegos, y herramientas de monitoreo.

CAPÍTULO V

5 Pruebas y Resultados

En este capítulo se procede a realizar las respectivas pruebas de funcionalidad de cada uno de los servicios implementados en la red de datos, con el fin de observar y comprobar su correcto desempeño. Para lo cual, se propone efectuar la simulación de determinados ataques informáticos y el establecimiento de un conjunto de reglas para filtrado de tráfico específico, acorde a ciertas políticas de seguridad establecidas anteriormente.

5.1 Pruebas del servicio squid

A continuación se realiza pruebas apegándose a las ciertas políticas de seguridad sobre la limitación de la navegación como a ciertas páginas.

- Configuración en los navegadores para que puedan salir por el puerto 3128.
- Acceder a www.google.com por medio del proxy.
- Acceder a la página web de YouTube definida en el archivo sitios sociales desde el grupo asistentes.
- Realizar una búsqueda en google utilizando la palabra “pornografía”, la cual está definida en el archivo sitios denegados.

- Realizar una búsqueda en google utilizando la palabra “sri”, la cual está definida en el archivo sitios permitidos.

5.1.1 Desarrollo de las pruebas del servicio squid

5.1.1.1 Configuración de los navegadores

Para realizar la configuración de los navegadores se debe dirige al menú herramientas y luego a opciones donde se escoge la opción avanzado, en la solapa de Red y luego en Configuración como se muestra en la Figura 59.

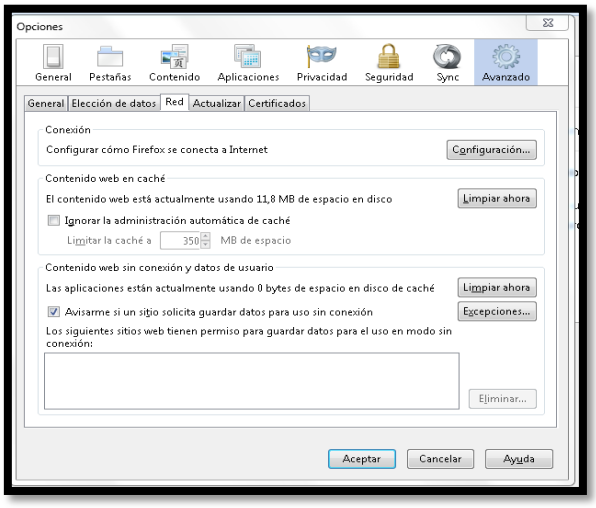


Figura 59. Configuración del proxy en el navegador Mozilla

Fuente: Captura de pantalla de la configuración del proxy

Seleccione la opción "configuración manual del proxy" y complete los datos para el servidor.

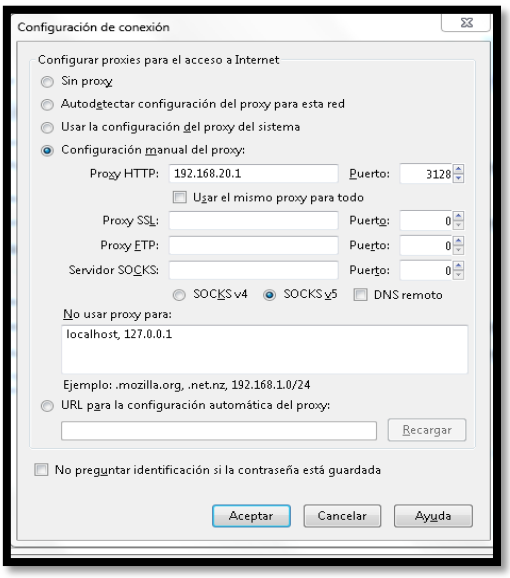


Figura 60. Configuración del proxy en el navegador Mozilla

Fuente: Captura de pantalla de la configuración del proxy

Para configurar en el navegador chrome se debe seguir los siguientes pasos. Dirigirse al menú de Chrome en la barra de herramientas del navegador y seleccione configuración a continuación seleccione mostrar configuración avanzada en la sección "Red".

Figura 61. Configuración del proxy en el navegador Chrome

Fuente: Captura de pantalla de la configuración del proxy

Se procede a cambiar configuración de proxy donde nos lleva al cuadro de diálogo de las propiedades del internet donde se procede a seleccionar la configuración de la red LAN.

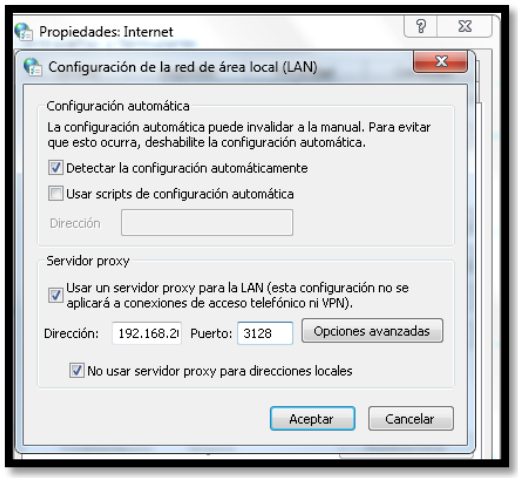


Figura 62. Configuración del proxy en el navegador Chrome

Fuente: Captura de pantalla de la configuración del proxy

5.1.1.2 Acceder a la página Google

Ingresamos a la página www.google.com donde se puede establecer conexión con el servidor Proxy y por ende se tiene conexión a internet desde cualquier máquina.

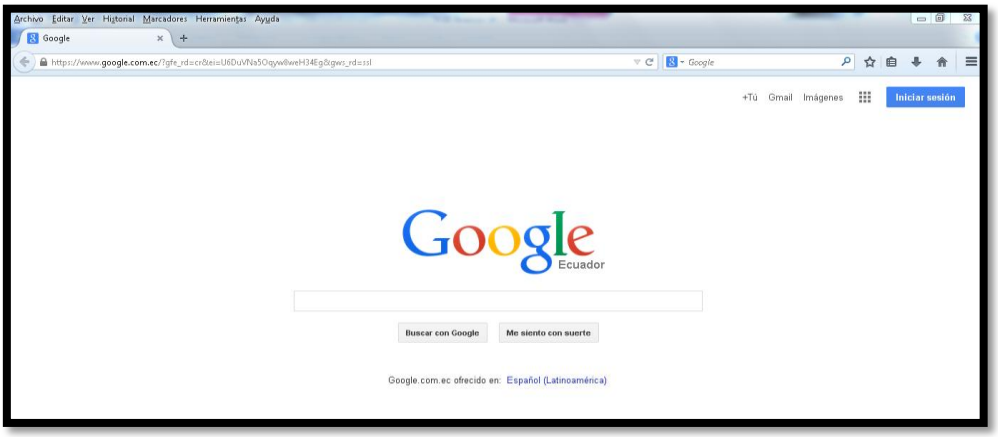


Figura 63. Acceso a la página google.com

Fuente: Captura de pantalla del acceso a google

5.1.1.3 Acceder a la página web de youtube.com definida en el archivo sitios sociales

A continuación se accede al sitio web www.youtube.com definido en el archivo sitios sociales debido a que existe mucha concurrencia, como se muestra en la siguiente Figura 64 la denegación a esta página donde su dirección IP es de un asistente.

Figura 64. Acceso a un sitio social
Fuente: Captura de pantalla del acceso a la palabra youtube

5.1.1.4 Realizar una búsqueda en google utilizando la palabra "pornografía", la cual está definida en el archivo sitios denegados.

En el buscador de google se ingresa la palabra pornografía, la cual está definida en el archivo sitios denegados, se puede evidenciar el mensaje de acceso denegado.

Figura 65. Acceso a un sitio denegado

Fuente: Captura de pantalla del acceso a la palabra pornografía

5.1.1.5 Realizar una búsqueda en google utilizando la palabra "sri", la cual está definida en el archivo sitios permitidos.

Se busca información acerca de páginas gubernamentales como SRI[19], cuya palabra está definida en el archivo sitios permitidos donde permite acceder a la información.

[19] **SRI:** Servicio de Rentas Internas

Figura 66. Acceso a un sitio permitido
Fuente: Captura de pantalla del acceso a la palabra SRI

5.1.1.6 Acceder a internet desde un equipo que tiene una IP definida en el archivo horario, el cual está configurado para no tener acceso a internet de 8:00 am a 13:00 am.

Se prueba el acceso al internet regulado mediante un horario para esto se comprueba que el horario de 08:00 a 13:00 no se tiene acceso a la navegación.

5.2 Test de penetración

A continuación se simulan ciertos ataques informáticos que se cometen usualmente dentro de la seguridad de la información entre ellos: ataques por DoS, avenamiento ARP y por

fuerza bruta. Además se señalan los pasos y herramientas que hacen uso para la ejecución dentro de la red de datos de la industria FLORALP.

Para la realización de estas pruebas se debe considerar el software en este caso se ha escogido Kali Linux la instalación se encuentra en el Anexo G donde no es más que una distribución avanzada gratuita basada en Debian para pruebas de penetración y auditorias de seguridad. Kali Linux es una actualización de BackTrack Linux que cuenta con más de 300 pruebas de penetración.

Otra herramienta indispensable es el analizador de paquetes de red Wireshark, un conocido software de código abierto que permite capturar, visualizar y examinar con detalle el contenido de un paquete de red.

El test de penetración se realiza mediante un conjunto de fases para la simulación de ataques en escenarios controlados permitiendo evaluar la seguridad del sistema de seguridad, de tal forma, encontrar los puntos débiles y vulnerables de la red.

En la siguiente figura 67 indica las fases de un test de penetración.

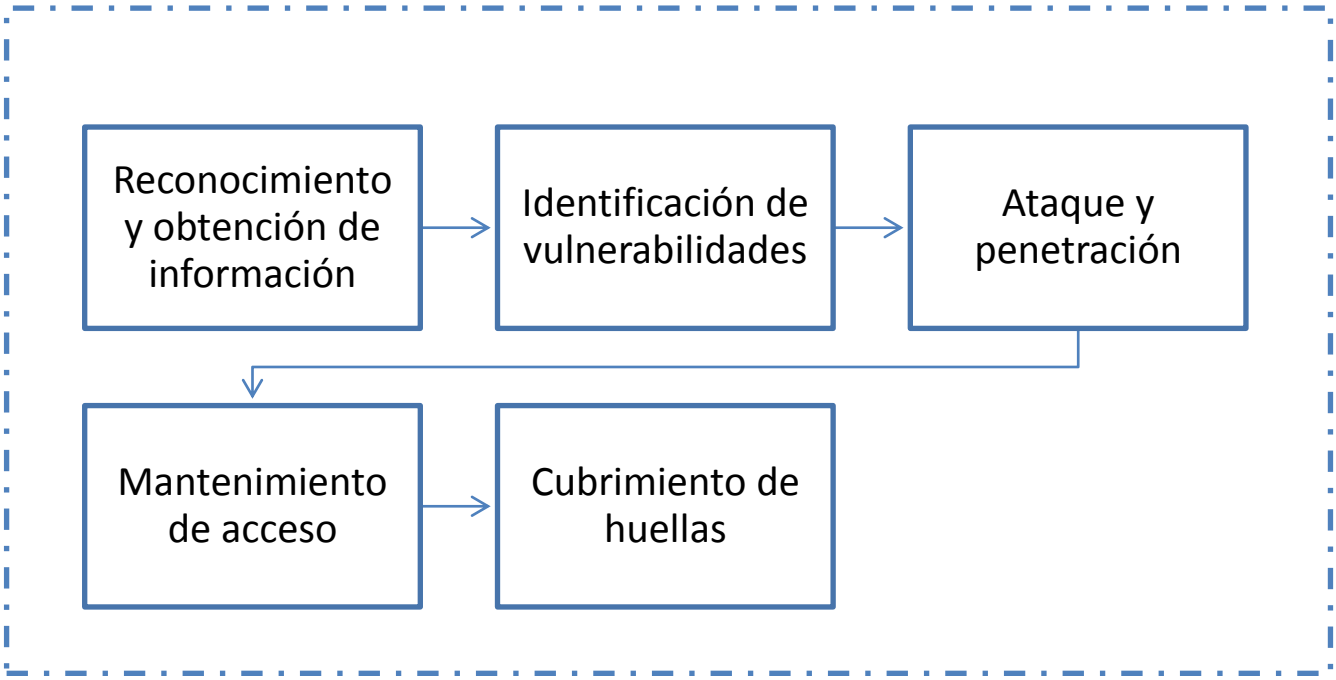


Figura 67. Anatomía de un test de penetración
Fuente: Ataques informáticos, Recuperado de http://goo.gl/VCc6Ef

(Torres, 2012) Menciona que las fases de un test de penetración son las siguientes:

- Fase 1- Reconocimiento y obtención de información

El reconocimiento se refiere a la fase preparatoria donde el atacante obtiene toda la información necesaria de su objetivo o víctima antes de lanzar el ataque. Esta fase también puede incluir el escaneo de la red que el hacker quiere atacar no importa si el ataque va a ser interno o externo permitiendo al intrusos crear una estrategia para su ataque.

Esta fase puede incluir la ingeniería social, buscar que tipos de sistemas operativos y aplicaciones usa el objetivo o víctima, cuales son los puertos que se encuentran abiertos, donde están localizados los routers (enrutadores), cuales son los host (terminales,

computadoras) más accesibles, buscar en las bases de datos la información como direcciones de internet (IP), nombres de dominios, información de contacto, servidores de email y toda la información que se pueda extraer de los DNS (Domain Name Server).

- Fase 2 – Identificación de vulnerabilidades

En esta fase el atacante utiliza toda la información que se obtuvo en la fase del reconocimiento realizando un escaneo de puertos para saber cuáles son los puertos vulnerables para determinar por cual puerto va entrar haciendo uso de herramientas automatizadas permitiendo el acceso al sistema.

- Fase 3 – Ataque y penetración

Esta es una de las fases importantes para el hacker porque es la fase de penetración al sistema, en esta fase el hacker explota las vulnerabilidades que encontró en la fase 2. Dentro de esta categoría incluye los ataques de fuerza bruta, envenenamiento de ARP y denegación de servicios (DoS).

- Fase 4 – Mantener el Acceso

Luego que el hacker gane acceso al sistema objetivo (Fase3) su prioridad es mantener el acceso que ganó en el sistema. En esta fase el hacker usa sus recursos del sistema como

plataforma de lanzamiento de ataques para escanear y explotar otros sistemas que quiere atacar, también hace uso de programas llamados sniffers para capturar todo el tráfico de la red.

En esta fase el hacker quiere permanecer indetectable y para eso remueve evidencia de su penetración al sistema y hace uso de Backdoor (puertas traseras) y troyanos para ganar acceso en otra ocasión y tratar de tener acceso a cuentas de altos privilegios como cuentas de administrador.

- Fase 5 – Cubrir las huellas

En esta fase el Hacker trata de destruir toda la evidencia de sus actividades ilícitas y lo hace por varias razones entre ellas seguir manteniendo el acceso al sistema comprometido ya que si borra sus huellas los administradores de redes no tendrán pistas claras del atacante y el hacker puede seguir penetrando el sistema cuando quiera.

5.2.1 Fase de exploración

5.2.1.1 Escaneo de puertos y host

Para la simulación del ataque se utiliza Nmap una herramienta de código abierto para exploración de red y auditoría de seguridad donde este utiliza paquetes IP en bruto en formas

novedosas para determinar qué hosts están disponibles en la red, qué servicios están ofreciendo y qué sistemas operativos que se están ejecutando.

Este se lo hace mediante la herramienta de Kali Linux donde se puede visualizar que host se encuentran mediante el siguiente comando.

nmap –sn 192.168.20.1/24

Figura 68. Escaneo de host mediante Nmap
Fuente: Exploración de host mediante Kali-Linux

En la figura 69 se muestra el despliegue de la alerta en Snort:

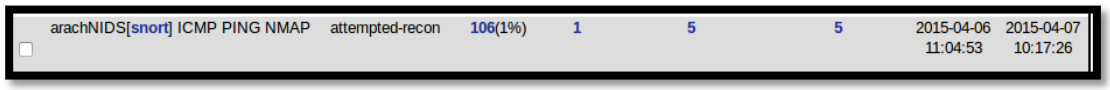


Figura 69. Alertas en Snort
Fuente: Captura de las alertas por Snort

5.2.2 Fase de obtención de acceso

5.2.2.1 Denegación de servicio DOS

La simulación de este ataque busca colapsar determinados equipos o redes informáticas, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios. Cuentan con varias estrategias, entre ellas:

- Denegaciones del servicio por inundación, saturando un equipo con solicitudes para que no pueda responder a las peticiones reales.
- Denegaciones de servicio por explotación de vulnerabilidades, que aprovechan una vulnerabilidad en el sistema para volverlo inestable.

La herramienta se hace uso en esta simulación es LOIC (Low Orbit Ion Cannon) es una aplicación diseñada para realizar ataques de denegación de servicio con el objetivo de envitar una gran cantidad de paquetes TCP, paquetes UDP o peticiones HTTP con objeto de determinar cuál es la cantidad de peticiones por segundo que puede resolver la red antes de dejar de funcionar tanto a sitios web como a direcciones IP específicas de forma relativamente sencilla. Como se indica en la figura siguiente:

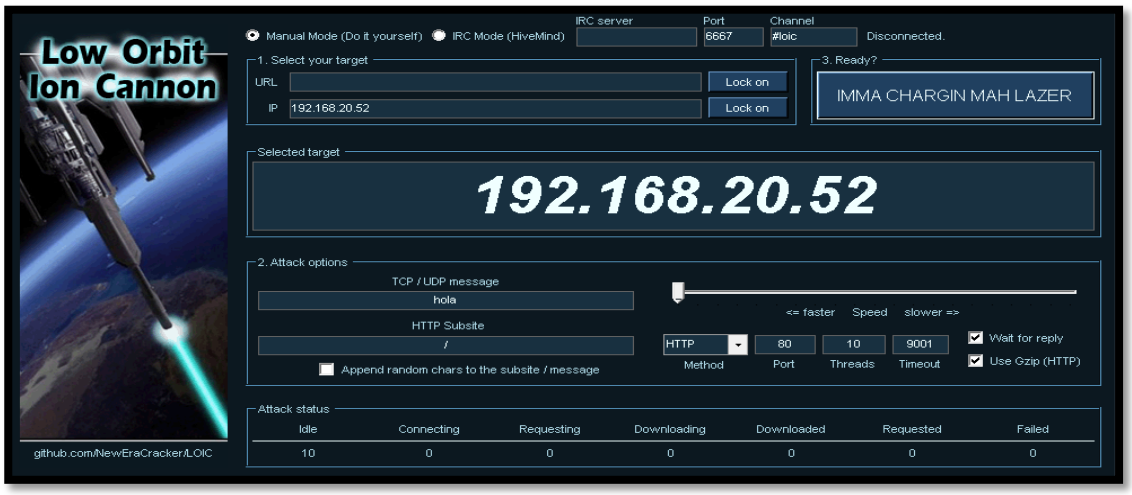


Figura 70. Ataque por inundación DoS mediante LOIC
Fuente: Captura de pantalla de LOIC

A continuación, en la Figura 71 despliega las alertas de snort, donde se señala que el software LOIC ha lanzado paquetes por inundación en contra de una máquina que es parte de la red de datos de la industria.

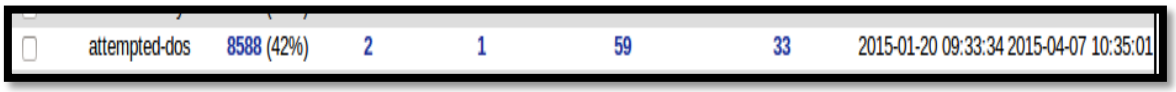


Figura 71. Alertas del ataque DoS por Snort
Fuente: Captura de pantalla de Snort

5.2.2.2 Envenenamiento ARP (ARPSpoofing) Midle an middle

En la simulación de este ataque permite la intercepción de la comunicación en una red conmutada con el fin de capturar o modificar paquetes de ciertas direcciones IP que se

encuentran asociada a su MAC, por lo tanto, ocasiona que se modifique las tabla de resolución de direcciones ARP donde todo el tráfico es redirigido al atacante provocando que la víctima confunda al atacante con el gateway de la red y viceversa.

En esta simulación se emplea la herramienta Ettercap que nos ofrece Kali Linux para simular un ataque de envenenamiento de ARP en contra de una IP perteneciente a la red. Ettercap permite enlistar todas las IP que se encuentran conectadas a la red de datos donde se procede a identificar el gateway y la IP de la víctima como se indica en la Figura 68.

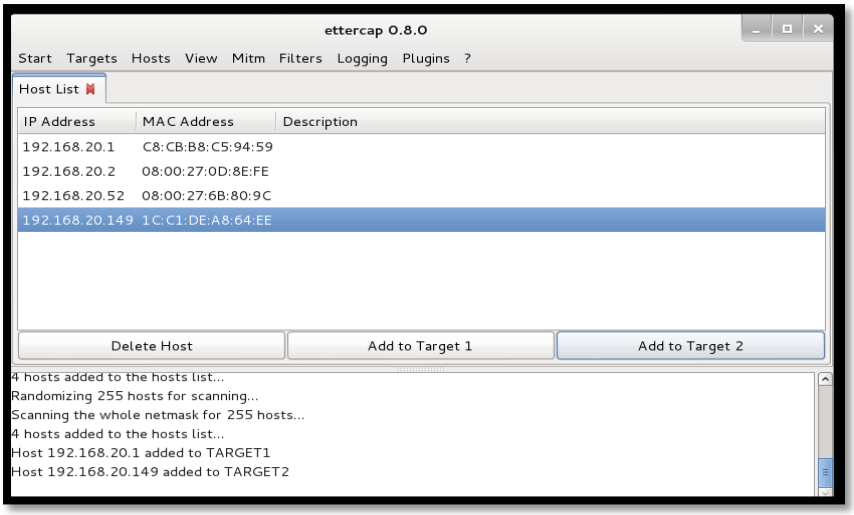


Figura 72. Ettercap en lista las IP's de la red
Fuente: Captura de pantalla de Kali-Linux

Mediante la herramienta de Ettercap y la ayuda de Sniffer (Hombre en el medio) se escoge la IP que va ser atacada duplicando su MAC esta técnica se la realiza de manera bidireccional tanto para la IP atacada como de la IP del atacante.

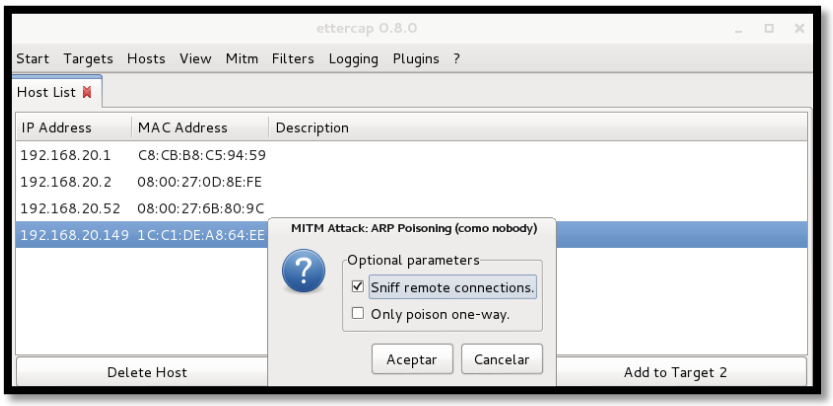


Figura 73. Sniffer de Ettercap

Fuente: Captura de pantalla de Kali-Linux

En la Figura 74 se observa que en la tabla ARP de la víctima se ha modificado la MAC donde la tarjeta de red rechaza estos datos, puesto que, aunque la MAC coincida, la dirección IP del atacante realmente es diferente a la del destino con el que la víctima quiere ponerse en contacto. Es aquí donde entra en juego el modo promiscuo mencionado anteriormente. Si el atacante, además de enviar de forma regular paquetes de respuesta ARP especialmente manipulados (con una asociación falsa a la víctima) pone su tarjeta en modo promiscuo, puede ver la información que le llega y procesarla, es decir que puede obtener la información que la víctima cree estar enviando a otro sistema.

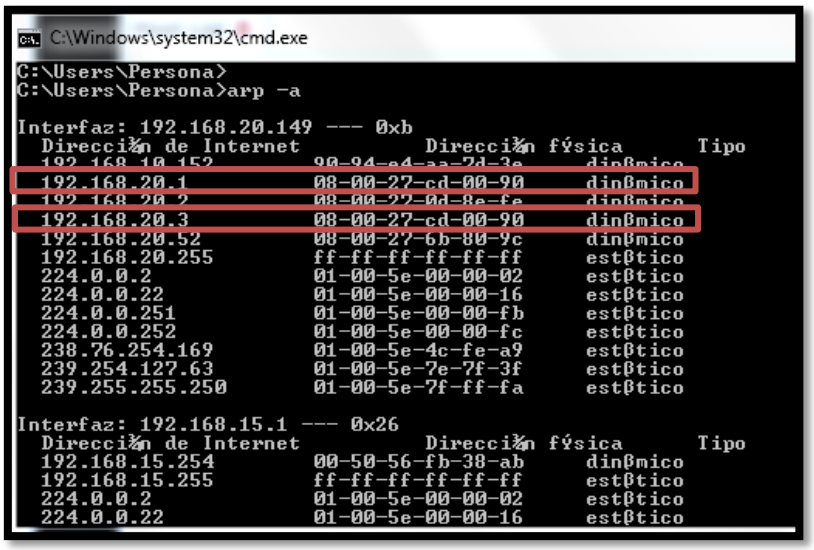


Figura 74. Tabla ARP de la victima
Fuente: Captura de la tabla ARP

Snort no encuentra una coincidencia con alguna regla creada de acuerdo al tipo de tráfico generado, pero se activan las alertas del preprocesador como se muestra la Figura 75.

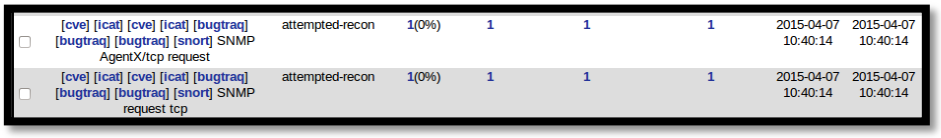


Figura 75. Alertas del Snort
Fuente: Captura de pantalla de Snort

5.2.2.3 Ataque por fuerza bruta

El ataque por fuerza bruta es una técnica muy empleada para el descubrimiento de contraseñas o claves en sistemas o maquinas donde sea posible. Para este posible ataque se hace uso del software antes ya mencionado como es Kali Linux donde este se encargará de

probar algunas contraseñas hasta descubrir la correcta, mediante diccionarios que pueden ser creados.

Para la prueba de esta simulación se utiliza la IP del servidor de seguridad que se encuentra implementado para poder revelar cuál es su contraseña de usuario root utiliza la herramienta Medusa.

Para simular el ataque es necesario crear un diccionario sencillo, es decir, un fichero que contenga una combinación de caracteres, números o contraseñas comunes. La creación del diccionario se lo hace con el siguiente comando.

Figura 76. Creación de diccionario de posibles contraseñas
Fuente: Captura de pantalla de Kali Linux

Antes de realizar el ataque es necesario tener conocimiento de que puertos se encuentran habilitados en este caso utiliza Nmap, donde se puede evidenciar que puertos se encuentran habilitados en este caso se realiza una conexión por medio de la IP del servidor de seguridad donde el puerto 22 (ssh) está abierto y se puede realizar una conexión por medio de este como se indica en la Figura 77.

Figura 77. Escaneo de puertos a la IP del servidor de seguridad
Fuente: Captura de pantalla de Kali Linux

Inicialmente, se intenta acceder al servidor de seguridad autenticándose como usuario root, especificando el lugar donde se localiza el diccionario y por el puerto que se va a realizar la conexión.

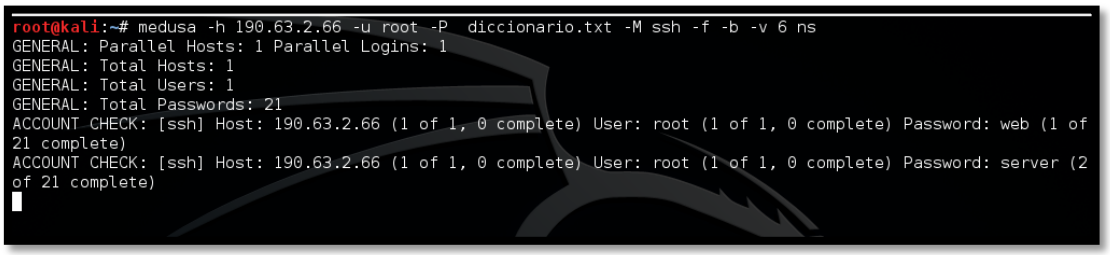


Figura 78.Ataque por fuerza bruta mediante la herramienta Medusa al servidor de seguridad
Fuente: Captura de pantalla de Kali Linux

Tras la introducción del comando se examinan posibles pares de usuario y contraseña que coincidan con las contraseñas o claves configuradas dentro del servidor de seguridad como se muestra en la Figura 79.

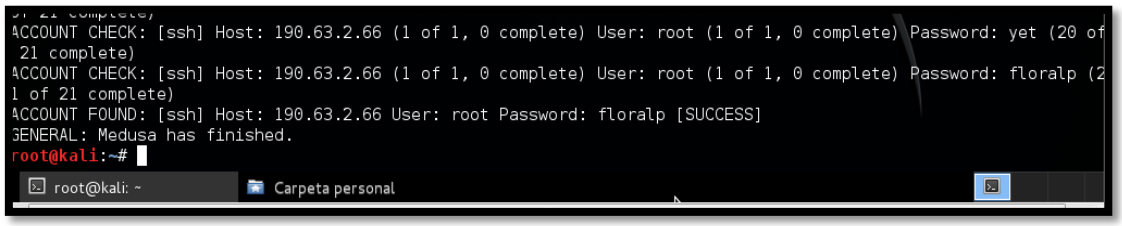


Figura 79. Escaneo de contraseñas mediante fuerza bruta por diccionario
Fuente: Captura de pantalla de Kali Linux

5.3 Análisis de las pruebas realizadas

El servicio que ofrece squid es permitir reducir el tráfico de la red, debido a que el proceso de almacenamiento de la caché del disco duro es más rápido permitiendo que varios usuarios soliciten el mismo servicio sin ninguna interrupción.

Mediante el servicio proxy se puede controlar la navegación a través de listas de acceso a páginas web en concreto limitando y restringiendo ciertos derechos que deben tener los usuarios dependiendo de las funciones que se encuentran realizando en cada departamento.

Squid ofrece la creación de reglas de acceso en las cuales puede especificar qué usuarios se les permita o deniegue el acceso a ciertas páginas inclusive a direcciones web completas o ciertos tipos de archivos y con este método podemos asegurar que los usuarios no descarguen archivos maliciosos desde la web.

Algunas políticas de seguridad se pueden cumplir con el servicio que ofrece squid como lo es el acceso a internet y la limitación de tiempo de conexión permitiendo un alto rendimiento de la navegación y que el ancho de banda sea bien distribuido a ciertos lugares donde merecen la preferencia.

A lo que se refiere el test de penetración permitió que a ciertas técnicas que ofrece Kali Linux simular un ambiente para la ejecución de los ataques internos, donde fueron descubiertos mediante ciertas pruebas comunes como la denegación de servicios, avenamiento ARP y ataques de fuerza bruta donde tuvieron éxito debido a que la red en ese momento no contaba con alguna seguridad.

Además se comprobó la existencia de herramientas de fácil acceso, como son: LOIC (Low Orbit Ion Cannon) y el software Kali-Linux para la ejecución de ataque con la finalidad de que se pueda aprender los métodos y herramientas que se utilizan para tratar de captar información sensible o llevar a cabo cualquier tipo de ataque que se ponga en riesgo cualquier tipo de información.

Para mitigar todos estos ataques se ha procedió a implementar un IDS sistema de detector de intrusos que mediante la activación de ciertas reglas se pudo detectar en tiempo real las pruebas de intrusión que antes se han mencionado identificando su dirección origen, destino y el puerto por donde se encuentra utilizando, donde procede al bloqueo de dichos puertos haciendo que la red de datos se ha más segura y confiable.

Es importante mencionar que ciertas políticas de seguridad cumplen con su propósito debido a la implementación de ciertos servicios, tomando en cuenta controles como seguridad física, copias de seguridad de información, seguridad ligada a los recursos humanos y a la petición de contraseñas se ha podido solventar con ciertas solicitudes y formularios que brindan medidas organizativas donde se busca que los usuario tengan conocimiento y sean responsables de los recursos informáticos que hagan uso.

Mencionar que todas estas medidas aplicadas se consiguió que la industria FLORALP S.A mediante el sistema implementado permita contar con mayor seguridad al momento de cruzar la información a través de la red de datos a su vez mejorando la administración, además se lleva una bitácora donde se registrarán todos los cambios realizados con el objetivo de tener una correcta documentación.

CAPITULO VI

6 Análisis Económico

Se realiza un análisis económico entre los equipos existentes y los que se utilicen en el desarrollo del sistema de seguridad perimetral.

6.1 Presupuesto referencial

Para poder brindar una solución de bajo costo para la industria se realiza un presupuesto referencial de los equipos, instalación, configuración del sistema de seguridad perimetral. Este proyecto al tener un sistema bajo software libre, que es una plataforma segura y libre permite tener una alternativa confiable y económica.

6.1.1 Detalle de las empresas

En base a los requerimientos presentados para la implementación del esquema de seguridad, se solicitó proformas con costos referenciales a empresas especializadas en equipos de venta de equipos de networking.

Para el software, se recurrió a páginas de instituciones y organizaciones que se dedican a la difusión, capacitación y promoción de herramientas “Open Source”.

Las empresas de las cuales se obtuvieron las proformas, costos referenciales y documentación son las siguientes:

- **TECNIT**
- **ALLIANCE TECH**

6.1.2 Detalle del costo promedio referencial

A continuación se detalla el costo referencial para la implementación de la seguridad física, el diseño completo y el diseño básico.

6.1.2.1 Detalle del costo de los equipos de networking

En la siguiente tabla 26 de indica el costo referencial de los equipos de networking para la red de datos de la industria. El detalle completo de las proformas se encuentra en el Anexo I.

Tabla 26. Costo de Equipos de networking

Equipos	Cantidad	Descripción	Costo Unitario	Costo Total
Switch administrable	1	Switch Cisco 24 puertos WS-C2960-24TC-S	$929.00	$929.00
Switch no administrable	2	TL-SF1024D - Switch TP-Link	$67.00	$67.00
Router	3	Router Tp-link Inalámbrico 300 Mbps	$50.00	$150.00
			Total más Iva	$1146.00

Fuente: Realizado por Gabriela López

6.1.2.2 Detalle del costo del servidor

En la siguiente tabla 27 se indica el costo referencial del servidor de seguridad y de adaptadores de red debido a que se requiere más de dos adaptadores. El detalle completo de las proformas se encuentra en el Anexo I.

Tabla 27. Costo del servidor

Equipos	Cantidad	Descripción	Costo Unitario	Costo Total
Servidor	1	ProLiant ML350e Gen8 ES-2407	$1620.00	$1620.00
			Total mas Iva	$1620.00

Fuente: Realizado por Gabriela López

6.1.2.3 Detalle de las herramientas para la instalación

En la tabla 28 se detalla el costo referencial de los implementos necesarios para la instalación del sistema de seguridad.

Tabla 28. Costo de las herramientas para la implementación

Herramientas	Cantidad	Descripción	Costo unitario	Costo Total
Rollo de cable	1	Cable UTP categoría 6a	$175.00	$175.00
Conectores RJ45	1	Funda de 100 unidades cat 6	$22.00	$22.00
Adaptadores de red	1	Tarjeta de red gigabit Ethernet 10/100/1000 Mbps PCI EXPRESS x1 HP	$89.00	$89.00
Kit de Instalación	1	Ponchadora + Crimpeadora + Peladora	$40.00	$40.00
			Total más Iva	$326.00

Fuente: Realizado por Gabriela López mediante Mercado Libre.

6.1.2.4 Detalle del costo ingeniería e instalación

En la tabla 29 se muestra el costo referencial de los honorarios de la persona encargada del diseño e implementación del sistema de seguridad de tal forma deje documentado todo lo realizado, asumiendo en un tiempo determinado. Además se detalla un costo para la socialización sobre el uso de políticas de seguridad para todos los que forman parte de la industria FLORALP S.A.

Tabla 29.Costo de la mano de obra

Parámetros	Tiempo de horas	Costo por hora	Costo referencial
Costo de Implantación	15	$60.00	$1300.00
Documentación	---	---	$200.00
Costo de capacitación al personal de la industria	---	---	$354.00
		Total más Iva	$1854.00

Fuente: Realizado por Gabriela López

6.1.2.5 Detalle del costo del software

En la tabla 30 se detalla el costo referencial del software para el servidor de seguridad en este caso es de Open Source por lo que no tendrá costo alguno.

Tabla 30.Costo de software

Parámetros	Costo referencial
Costo del Software	$0.00
Total más Iva	$0.00

Fuente: Realizado por Gabriela López

6.1.2.6 Detalle del costo total referencial

El costo total referencial para la implementación del sistema de seguridad perimetral se ha tomado todos los equipos y herramientas considerando que fuesen nuevos y en caso de implementación en otra sucursal, como se indica en la Tabla 31.

Tabla 31.Costo referencial total

DETALLES DE COSTOS	COSTO TOTAL
Detalle del costo de equipos networking	$1146.00
Detalle del costo para el servidor	$1620.00
Detalle del costo de las herramientas	$326.00
Detalle del costo de ingeniería	$1854.00
Detalle del costo del software	$0.00
COSTO TOTAL REFERENCIAL	**$4946.00**

Fuente: Realizado por Gabriela López

En la siguiente tabla 32 se muestra el detalle del costo referencial sin tomar en cuenta varios equipos como lo son equipos de networking y el servidor debido ya se cuenta con ellos con el motivo de reutilizar tecnología.

Tabla 32. Costo referencial total para el diseño

DETALLES DE COSTOS	COSTO TOTAL
Detalle del costo de las herramientas	$326.00
Detalle del costo de ingeniería	$1854.00
Detalle del costo del software	$0.00
COSTO TOTAL REFERENCIAL PARA EL DISEÑO	**$2180.00**

Fuente: Realizado por Gabriela López

El total del proyecto es la suma de los componentes para la instalación del sistema de seguridad perimetral es de **$4946.00** en caso de que no se cuente con los equipos.

Pero es importante la reutilización de la tecnología por lo que no se han tomado ciertos equipos debido a que ya existen dentro de la infraestructura de la red y el costo quedaría en un total de **$2180.00** Todos los precios están sujetos a cambios, en vista que fueron cotizados con la fecha de mayo de 2015

6.1.3 Costo beneficio

Para realizar este costo beneficio se cuenta con un costo referencial del presente proyecto para la implementación del sistema de seguridad perimetral, además, se ha considerado la reutilización de equipos debido a que estos ya se encuentran dentro de la infraestructura de red. De tal forma el costo beneficio en términos económicos se realiza de la siguiente manera.

Tabla 33. Beneficio de la reutilización de tecnología

DETALLES DE COSTOS	COSTO TOTAL
COSTO TOTAL REFERENCIAL	$4946.00
COSTO TOTAL REFERENCIAL PARA EL DISEÑO	$2180.00
LA DIFERENCIA ENTRE LOS COSTOS REFERENCIALES	**$2766.00**

Fuente: Realizado por Gabriela López

6.1.4 Cálculo del costo-beneficio

Para el análisis del costo beneficio del proyecto es necesario analizar los costos incurridos en la implementación del sistema de seguridad perimetral y los beneficios que generará el proyecto con la implementación del mismo haciendo uso de tecnología existente, para lo cual utilizaremos la siguiente fórmula:

$$\frac{B}{C} = \frac{Benefcios}{Costos\ y\ Gastos}$$

Luego del análisis de los costos, gastos y beneficios que generan el proyecto aplicamos la fórmula para la determinación del beneficio costo, para lo cual se utilizan los siguientes parámetros de evaluación:

- Si B/C es mayor que 1 se acepta el proyecto
- Si B/C es igual que 1 el proyecto es indiferente
- Si B/C es menor que uno se rechaza el proyecto

Reemplazando los valores en la fórmula tenemos:

$$\frac{B}{C} = \frac{Beneficios}{Costos\ y\ Gastos}$$

$$\frac{B}{C} = \frac{2766.00}{2180.00}$$

$$\frac{B}{C} = 1{,}2$$

Todos los resultados obtenidos indican que es factible y rentable implementar el presente proyecto.

6.1.5 Beneficiarios

Cuando se plantea soluciones de seguridad para la información y las redes de datos, medir con precisión el costo beneficio resulta una tarea un tanto compleja, debido a que esta clase de proyectos representan una inversión que no proporciona beneficios económicos, pero si, beneficios productivos.

El análisis de los beneficio del sistema de seguridad perimetral para la red de datos de la industria lechera FLORALP S.A son los siguientes:

La seguridad generalmente no es una inversión que genere un beneficio económico, se trata de prevenir pérdidas. En otras palabras, cuando se invierte en seguridad, las

instituciones no esperan ganancias, el objetivo es reducir los riesgos que amenazan la información, con el propósito de minimizar la cantidad de pérdidas de información gracias a la inversión que se realiza.

Los beneficiarios de este sistema serian todos los usuarios que pertenecen a los diversos departamentos que hacen uso de los servicios que ofrece la red de datos debido a que toda la información que se encuentran manejando estaría mejor resguardada.

El índice de productividad aumentaría notablemente con la implementación de este sistema en la red de datos mediante la limitación en la navegación a internet.

Otros de sus beneficios son las restricciones de acceso de los usuarios a sitios que eventualmente generen daño y la limitación del uso del ancho de banda en favor de aquellas aplicaciones que son claves para la industria.

Gracias a la utilización de software libre brinda servicios de alto nivel sin pagar ningún precio para la adquisición del mismo permitiendo ser muy competitivo con software pagados.

La reutilización de equipos para este proyecto es de volver a utilizar e incorporar equipos usados que cuenta la industria con el objetivo de generar rentabilidad social y beneficios medioambientales.

Conclusiones y Recomendaciones

Conclusiones

- Se debe tener bases teóricas que nos brinden información suficiente sobre cuáles son las principales características de un sistema de seguridad perimetral como base para la realización del presente proyecto, debido a que esto constituirá como fuente de investigación para próximos interesados sobre seguridad de información.

- El análisis del tipo de tráfico que se encuentra circulando dentro de la infraestructura de la red nos permite conocer los servicios y protocolos que cada uno de los usuarios manejan, de tal forma, se puede determinar los requerimientos necesarios para el diseño del sistema de seguridad perimetral.

- Para el diseño del sistema de seguridad perimetral se ha tomado en cuenta la norma ISO/IEC 27001 para la elaboración de las políticas de seguridad, debido a que se sigue un proceso de mejora continua la que nos permita tener un esquema ágil y flexible que se ajusta a los requerimientos de la industria.

- El análisis de diferentes plataformas de Software en base al estándar IEEE 830 de especificaciones de requerimiento de software permite la selección de la mejor

alternativa que se ajuste a los requerimientos del diseño del sistema de seguridad perimetral.

- Para la implementación de este sistema de seguridad se ha tomado en cuenta integrar dos tecnologías como lo son: el proxy y el sistema de detección de intrusos que garantizan la seguridad, confiabilidad y la disponibilidad de la infraestructura de la red de datos de la industria.

- El uso de software libre en instituciones privadas se ha convertido en un factor fundamental en la gestión, administración y seguridad de las tecnologías de la información debido a que consume muy pocos recursos de memoria, procesador y espacio en disco del computador, permitiendo la reutilización de recursos y disminución de gastos por parte de la industria al no tener que adquirir nuevos equipos.

- Mediante la implementación el servicio del proxy la caché del squid permite el filtrado de contenidos y por su capacidad de hacer caché, se logró aumentar el tiempo de respuesta en la navegación y evitar saturación del canal de internet, manteniendo un monitoreo en tiempo real y estadísticas diarias de navegación.

- Snort es un software IDS de gran aceptación, potente y gratuito lo cual nos permite conocer cuando está siendo atacada mediante sensores que realizan un monitoreo constante.

- La integración IDS identificó satisfactoriamente los ataques simulados con la herramienta Kali-Linux de hacker ético, la cual es ampliamente utilizada para un test de penetración en la red, comprobando su eficiencia frente a una serie de pruebas con diversas técnicas**.**

- Se debe estar conscientes de que no existe algún sistema que brinde una protección completa pero con la mejora continua y la adopción de métodos y estándares de seguridad de la información se mantiene un nivel de seguridad aceptable que reduce los riesgos de la red.

Recomendaciones

- Las políticas de seguridad deben ser informadas a todos los usuarios que se encuentran laborando dentro de la industria donde deben tener conocimiento de cuáles son sus responsabilidades para la protección y el uso responsable de los recursos de la red, en procura de proporcionar una solución eficiente para la seguridad.

- Es recomendable realizar capacitaciones frecuentes sobre seguridad de la información a usuarios de la industria para que tengan los conocimientos básicos necesarios para el manejo adecuado de las herramientas de trabajo.

- Es muy importante tener documentado y actualizado el registro de todas las políticas que son modificadas o creadas para poder mitigar cualquier fallo en caso de que no se haga cumplimiento.

- En la integración del sistema de detección de intrusos debido a que esta se encarga solo de la detección y el monitoreo de comportamientos sospechoso sería ideal la integración de un IPS (Sistema de prevención de intrusos) que puedan trabajar unificados para disminuir anomalías de falsas alarmas.

- Se debe planificar un test de penetración en la red con el fin de permitir conocer la evolución de la seguridad conforme avanza el tiempo y evaluar el resultado de los correctivos aplicados en los problemas con la seguridad de la información.

- Se debe contar con personal con buen nivel de conocimiento en estándares de cableado, herramientas de monitoreo de hacking ético y escaneo de vulnerabilidades con el objetivo de realizar tareas de aseguramiento de la red.

- El monitoreo de servicios tanto de squid y de conectividad a la red es recomendable realizarlo periódicamente para evitar posibles fallas y realizar una oportuna corrección en el sistema.

BIBLIOGRAFÍA

REFERENCIAS BIBLIOGRÁFICAS DE LIBROS, EN LÍNEA Y TESIS

Aguirre, J. R. (2006). *Libro Electrónico de Seguridad Información y Criptografía.* Madrid-España.

Alfaro, E. J. (2010). *Universidad de Valencia*. Recuperado el 19 de Enero de 2015, de http://rediris.es/cert/doc/pdf/ids-uv.pdf

Alulema, D. (Junio de 2008). Estudio y Diseño de un Sistema de Seguridad Permimetral. Quito.

Brachmann, S. (2013). *Las ventajas de Centos.* Obtenido de http://www.ehowenespanol.com/ventajas-centos-info_248710/

Camelo, L. (06 de Julio de 2010). *Seguridad de la Información*. Recuperado el 19 de Enero de 2015, de http://seguridadinformacioncolombia.blogspot.com/2010/06/hablemos-de-apache.html

Estándar Internacional ISO/IEC 27001. (s.f.).

Estrella. (Abril de 2010). *Mecanismos de Seguridad*. Recuperado el Septiembre de 2014, de http://www.buenastareas.com/ensayos/Mecanismos-De-Seguridad/229947.html

Galindo, C. J. (2009). *Diseño y optimización de un sistema de detección de intrusos híbrido.* Recuperado el 16 de Enero de 2015, de http://www.adminso.es/recursos/Proyectos/PFC/PFC_carlos.pdf

Garron, G. (5 de junio de 2013). *CentOS o Debian, para un servidor Web.* Obtenido de http://www.garron.me/es/gnu-linux/centos-vs-debian.html

Gómez, D. G. (Julio de 2003). *Sistema de detección de intrusos.* Recuperado el 16 de Enero de 2015, de http://derecho-internet.org/docs/ids.pdf

Gómez, G. (5 de Enero de 2015). *Servidor DHCP.* Recuperado el 8 de Febrero de 2015, de http://es.slideshare.net/GabOoSkaHapyy/11-servidor-dhcp-43224314

Huerta, A. V. (2002). Obtenido de http://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node12.html

Loor, J. B. (28 de Abril de 2013). *infoberre*. Recuperado el Septiembre de 2014, de http://infoberre.blogspot.com/2013_04_01_archive.html#!

Manuel, I. L. (30 de Mayo de 2013). *SliderShared.com*. Recuperado el 31 de Marzo de 2014, de http://es.slideshare.net/MelvinBrian/seguridad-en-profundidad

MICHILENA, M. A. (2013). *METODOLOGÍA DE SEGURIDAD INFORMÁTICA CON BASE EN LA NORMA ISO 27002 Y EN HERRAMIENTAS DE PREVENCIÓN DE INTRUSOS PARA LA RED ADMINISTRATIVA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA.* Ibarra.

Morales, E. (4 de Septiembre de 2012). *Servidores de Almacenamiento.* Recuperado el 8 de Febrero de 2015, de https://prezi.com/h2r8vlhhzfx0/servidoresalmacenamiento/

Muro, P. (23 de Junio de 2010). *Modelo de Gestión*. Recuperado el Septiembre de 2014, de http://www.arpcalidad.com/pdca-un-modelo-de-gestin/

Nicolas, T. (13 de Agosto de 2014). *Clase de servidores.* Recuperado el 8 de Febrero de 2015, de https://prezi.com/oszezptgvbed/clases-de-servidores/

Salazar, E. (17 de Febrero de 2011). *Clasificacion y tipos de ataques contra sistemas de información*. Recuperado el Septiembre de 2014, de http://cufminformaticos.blogspot.com/2011/02/clasificacion-y-tipos-de-ataques-contra.html

Samboni, D. M. (26 de Febrero de 2006). Recuperado el Febrero de 2014, de http://es.slideshare.net/DIANYSS2012/manual-bsico-de-wireshark

Seguridad, F. d. (s.f). *Fundamentos de Seguridad Informatica*. Recuperado el Octubre de 2014, de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Estandares.php

Software, A. (25 de Septiembre de 2014). *Axence NetTools*. Recuperado el 14 de Noviembre de 2014, de http://www.abcdatos.com/programa/escanear-monitorear-administrar-redes.html

Torres, V. (13 de Marzo de 2012). *Ciber Informatico*. Recuperado el 6 de Abril de 2015, de http://ciberinfosystem.blogspot.com/2012/03/anatomia-de-un-ataque.html

VINUEZA, T. (2012). *HONEYNET VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE DE LA CIUDAD DE IBARRA.* Ibarra.

GLOSARIO DE TÉRMINOS

ACL's: Conjunto de datos que indican al sistema operativo qué permisos tiene un usuario o grupo sobre un determinado objeto de sistema. Cada objeto tiene atributos de seguridad únicos que indican qué usuarios pueden accederlo, y la Lista de Control de Acceso contiene una descripción de los privilegios de acceso de cada objeto y usuario.

AUTENTIFICACIÓN: Proceso de confirmar la identidad de una entidad de sistema (un usuario, un proceso, etc.).

ARP: Son las siglas de Address Resolution Protocol (Protocolo de Resolución de Direcciones). Es el protocolo encargado de traducir una dirección IP a una dirección de capa física (MAC).

CPU: Central Processing Unit. (Unidad central de procesamiento). Es el procesador que contiene los circuitos lógicos que realizan las instrucciones de la computadora.

DHCP: Dynamic Host Configuration Protocol (Protocolo Dinámico de Configuración del Host). Un servidor de red usa este protocolo para asignar de forma dinámica las direcciones IP a las diferentes computadoras de la red.

DMZ: Zona desmilitarizada, red perimétrica, Máquina o pequeña subred situada entre una red interna de confianza (como una red local privada) y una red externa no confiable (como Internet). Normalmente en esta zona se sitúan los dispositivos accesibles desde Internet, como servidores Web, FTP, SMTP o DNS, evitando la necesidad de acceso desde el exterior a la red privada. Este término es de origen militar, y se utiliza para definir un área situada entre dos enemigos.

FTP: File Transfer Protocol (Protocolo de transferencia de archivos). Por medio de programas que usan este protocolo, se permite la conexión entre dos computadoras y se pueden cargar y descargar archivos entre el cliente y el host (servidor).

GESTIÓN DE SEGURIDAD: Es el proceso de establecer y mantener la seguridad en un sistema o red de sistemas informáticos. Las etapas de este proceso incluyen la prevención de problemas de seguridad, detección de intrusiones, investigación de intrusiones, y resolución. En gestión de redes, controlar (permitir, limitar, restringir, o denegar) acceso a la red y recursos, buscar intrusiones, identificar puntos de entrada de intrusiones, y reparar o cerrar estas posibles vías de acceso

GUSANO: Programa que se copia a sí mismo hasta ocupar toda la memoria. Es un virus que suele llegar a través del correo electrónico, en forma de archivo adjunto.

HACKER: Persona que tiene un conocimiento profundo acerca del funcionamiento de redes de forma que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

HACKING ÉTICO: Hacking ético es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.

HTTP: Hypertext Transfer Protocol (Protocolo de transferencia de hipertextos). Es un protocolo que permite transferir información en archivos de texto, gráficos, de video, de audio y otros recursos multimedia.

ICMP: El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol) se utiliza para efectuar el diagnóstico y notificación de errores durante una comunicación.

IPSEC: Es la abreviatura de Internet Protocol Security (Protocolo de Seguridad de Internet). Designa al conjunto de protocolos empleados para autenticar y cifrar los paquetes IP con el objetivo de brindar seguridad a las comunicaciones.

NETWORKING: Término utilizado para referirse a las redes de telecomunicaciones en general.

OSI: Open Systems Interconnection (Interconexión de Sistemas Abiertos). Norma universal para protocolos de comunicación.

OPEN SOURCE: Software libre Código que otorga libertad a los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el mismo. Véase también ("código abierto").

PROXY: Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red.

PROTOCOLO: Lenguaje que utilizan dos computadoras para comunicarse entre sí.

PHISHING: Se refiere a comunicaciones fraudulentas diseñadas para inducir a los consumidores a divulgar información personal, financiera o sobre su cuenta, incluyendo nombre de usuario y contraseña, información sobre tarjetas de crédito, entre otros.

POP3: (Post Office Protocol 3): Protocolo 3 de Correo. Es un protocolo estándar para recibir e-mail.

QoS: Calidad de servicio. En Internet y otras redes, designa la posibilidad de medir, mejorar y, en alguna medida, garantizar por adelantado los índices de transmisión y error. Es importante para la transmisión fluida de información multimedia: por ejemplo, para los usos académicos deInternet2.

SGSI: Un Sistema de Gestión de la seguridad de la Información (SGSI) es un conjunto de políticas de administración de la información.

SMTP: Simple Mail Transfer Protocol. Es un protocolo estándar para enviar e-mail.

SPAM: Recibe este nombre el correo electrónico que se recibe sin ser solicitado. Se considera poco ético, y en ocasiones, puede ser portador de virus. Normalmente su fin es el de la publicidad.

SSL: Son las siglas de Secure Sockets Layer (en español capa de conexión segura). Provee conexiones encriptadas sobre internet para proporcionar autenticidad y privacidad a la información entre extremos.

SSH: Secure Shell es un protocolo de red seguro para la comunicación de data, que permite la conexión de dos computadoras, usualmente una de ellas es un servidor Unix o Linux.

SQUID: Servidor caché / proxy de alta capacidad y rendimiento de código fuente abierto, muy usado en servidores Linux.

SNIFFER: Programa que busca palabras claves que se le hayan impartido en los paquetes que atraviesan un nodo con el objetivo de conseguir información y normalmente se usa para fines ilegales.

SONDEO DE PUERTOS, ESCANEO DE PUERTOS: Barrido de puertos generalmente para determinar qué servicios ofrece un sistema. Es uno de los métodos más comunes entre los atacantes para obtener información de sus objetivos. Véase también ("escaneo sigiloso de puertos").

SPOOFING: Procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo, adoptando otra identidad de remitente con el fin de engañar a un servidor firewall.

SPYWARE: Spyware son unos pequeños programas cuyo objetivo es mandar información, generalmente a empresas de mercadeo, del uso de internet, websites visitados, etc. del usuario, por medio del internet. Usualmente estas acciones son llevadas a cabo sin el conocimiento del usuario, y consumen ancho de banda, la computadora se pone lenta, etc.

TROYANO: (Trojan horse; caballo de Troya) programa que contiene un código dañino dentro de datos aparentemente inofensivos. Puede arruinar parte del disco rígido

VPN: Red Privada Virtual, red generalmente construida sobre infraestructura pública, que utiliza métodos de cifrado y otros mecanismos de seguridad para proteger el acceso y la privacidad de sus comunicaciones.

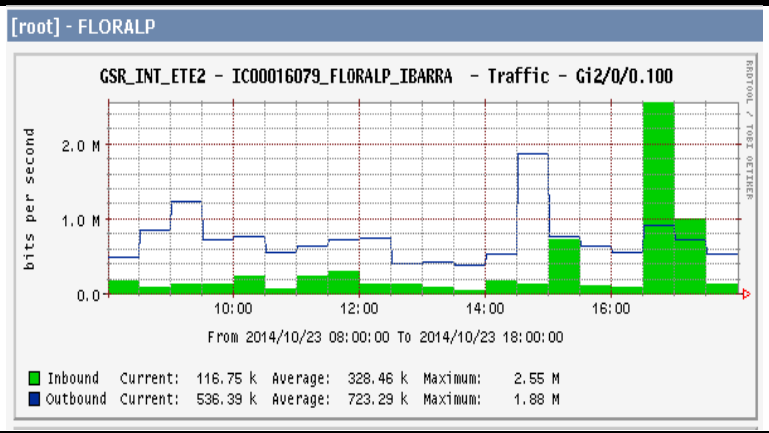
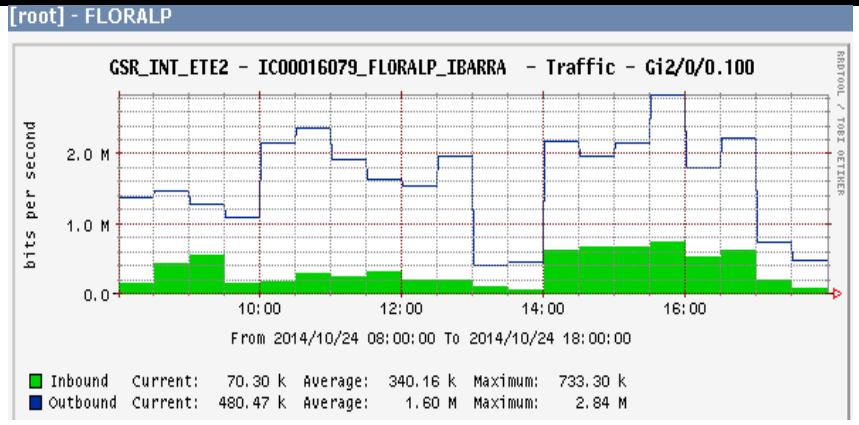
VIRUS: Pequeño programa que "infecta" una computadora; puede causar efectos indeseables y hasta daños irreparables.

ANEXOS

ANEXO A. ANÁLISIS DEL CONSUMO DE ANCHO DE BANDA EN LA RED DE DATOS DE LA FLORALP

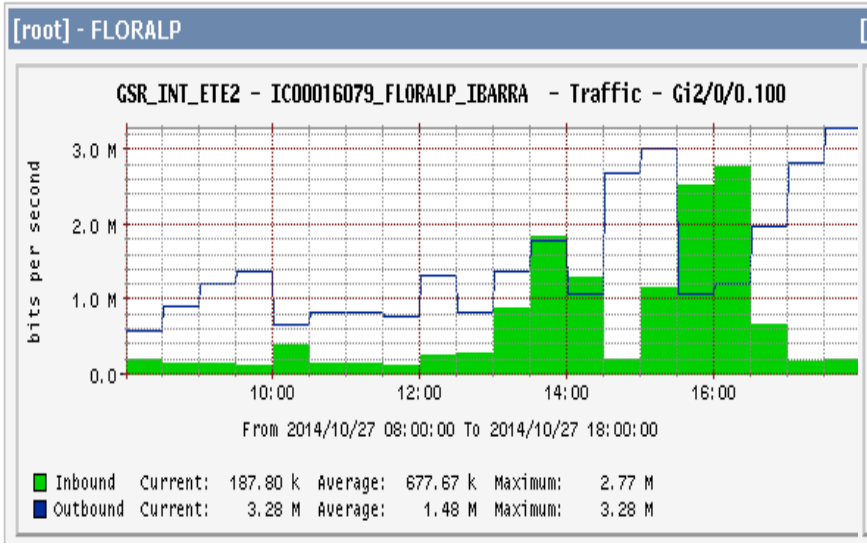
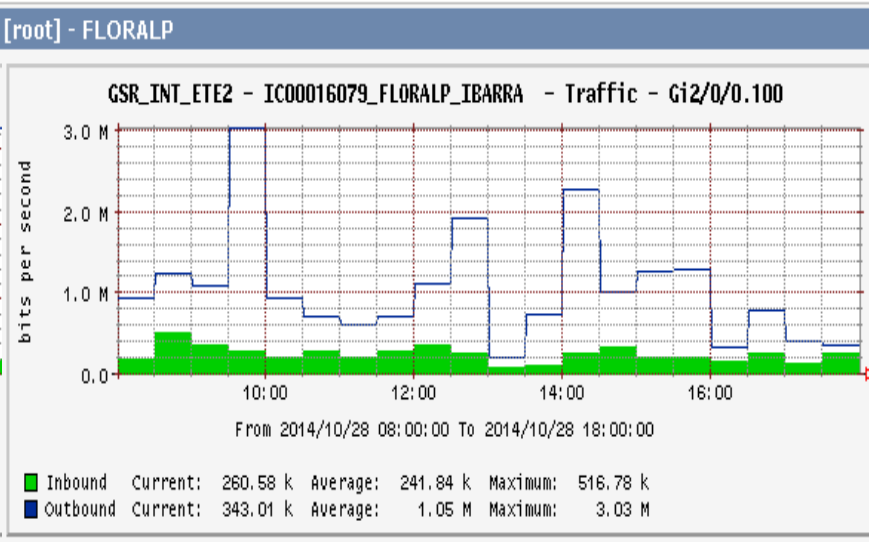
El análisis se lo ha realizado mediante el uso de la herramienta dada por el proveedor de CLARO, que se lo ha realizado a través de una dirección pública. A continuación se muestran figuras del consumo del ancho de banda por días donde se indicara el pico más alto que se ha realizo en todo el día.

Tabla 34. Consumo del ancho de banda de la red de la FLORALP de los días 23/10/2014 al 24/10/2014.

ANCHO DE BANDA CONSUMO 23/10/2014	ANCHO DE BANDA CONSUMO 24/10/2014
	
En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 2.55Mbps en el horario de 16:30 a 17:30 y un promedio de 328.46 Kbps.	En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 733.30 Kbps en el horario de 15:30 a 16:30 y un promedio de 340.16 Kbps.

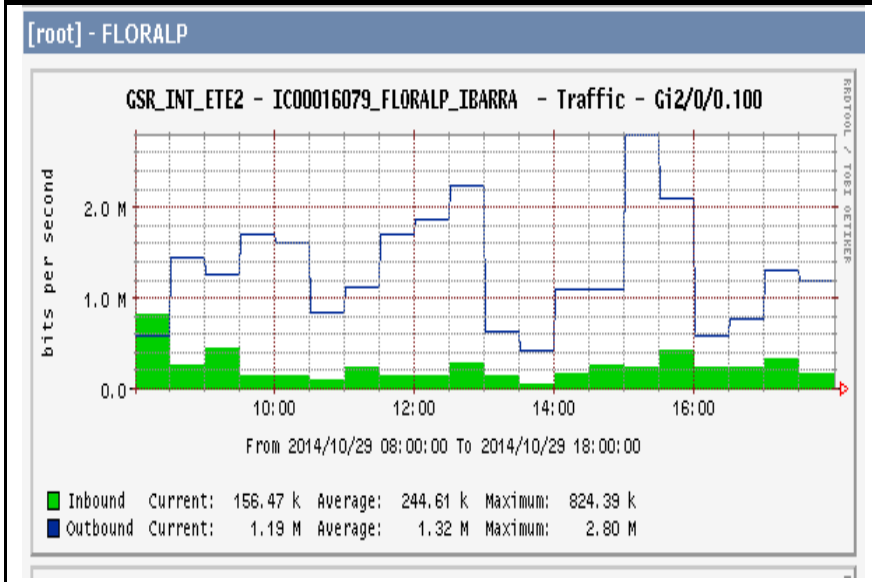
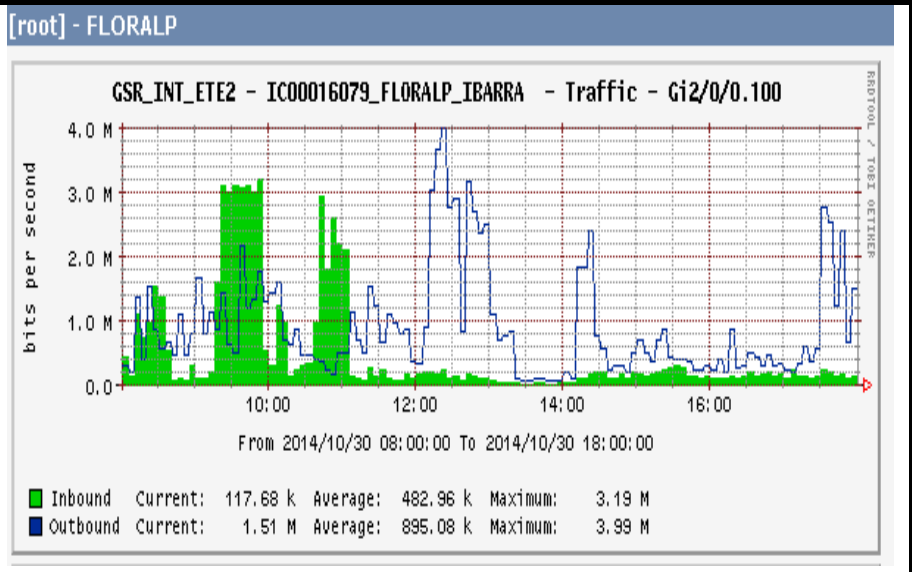
Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

Tabla 35. Consumo del ancho de banda de la red de la FLORALP de los días 27/10/2014 al 28/10/2014.

ANCHO DE BANDA CONSUMO 27/10/2014	ANCHO DE BANDA CONSUMO 28/10/2014
	
En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 2.77 Mbps en el horario de 16:00 a 16:30 y un promedio de 677.67 Kbps.	En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 516.78 Kbps en el horario de 8:30 a 9:00 y un promedio de 241.84 Kbps.

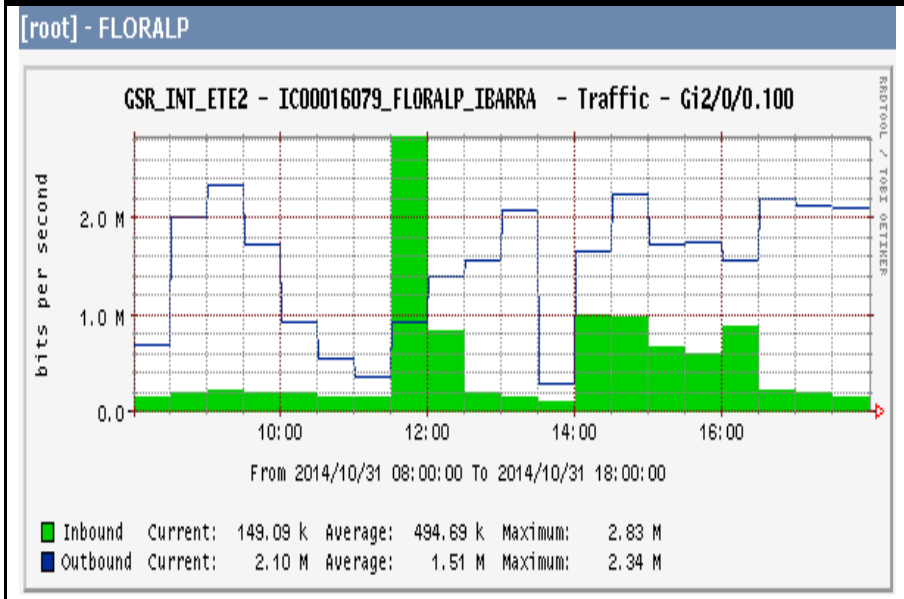
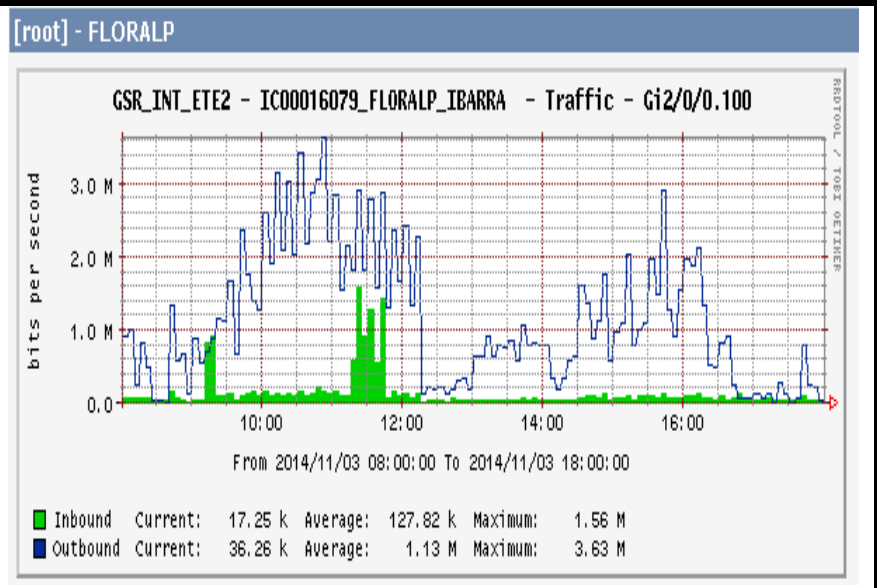
Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

Tabla 36. Consumo del ancho de banda de la red de la FLORALP de los días 29/10/2014 al 30/10/2014.

ANCHO DE BANDA CONSUMO 29/10/2014	ANCHO DE BANDA CONSUMO 30/10/2014
	
En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 824.39 Kbps en el horario de 8:00 a 8:30 y un promedio de 244.61 Kbps.	En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 3.19 Mbps en el horario de 9:30 a 10:30 y un promedio de 482.96 Kbps.

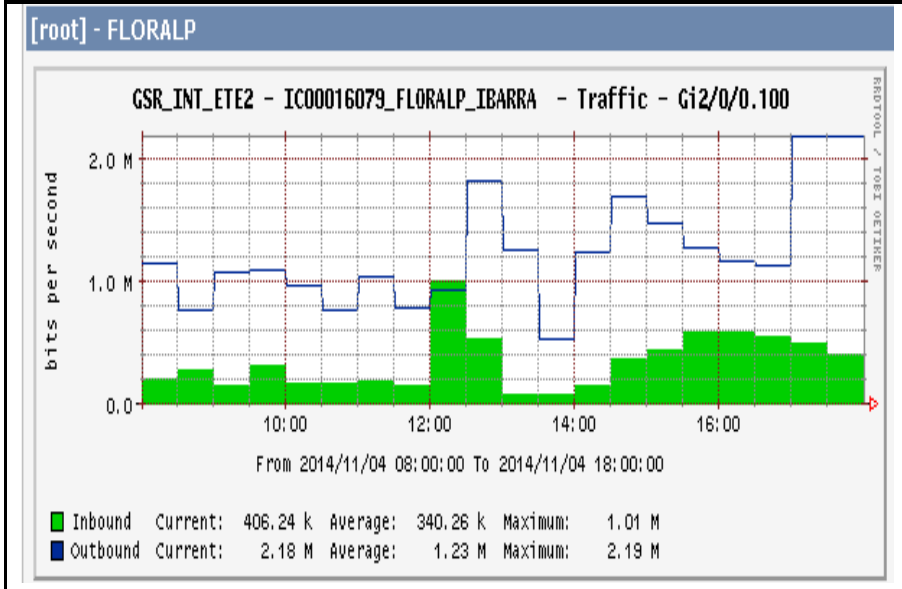
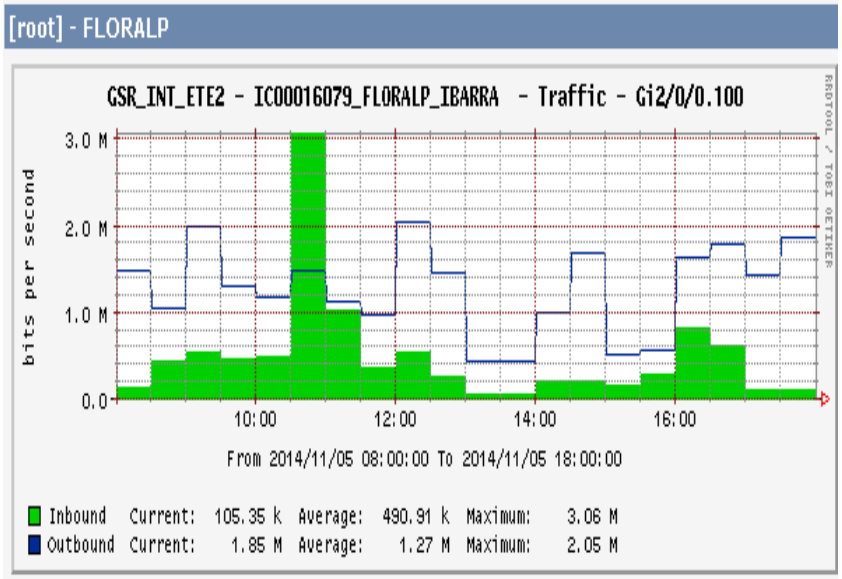
Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

Tabla 37. Consumo del ancho de banda de la red de la FLORALP de los días 31/10/2014 al 03/11/2014.

ANCHO DE BANDA CONSUMO 31/10/2014	ANCHO DE BANDA CONSUMO 03/10/2014
	
En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 2.83 Mbps en el horario de 11:30 a 12:30 y un promedio de 494.69 Kbps.	En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 1.56 Mbps en el horario de 11:30 a 12:00 y un promedio de 127.82 Kbps.

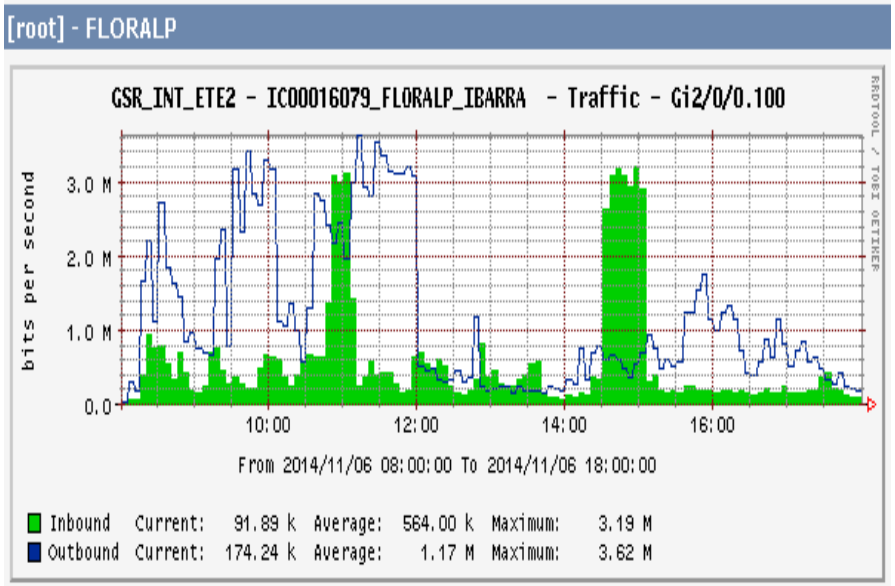
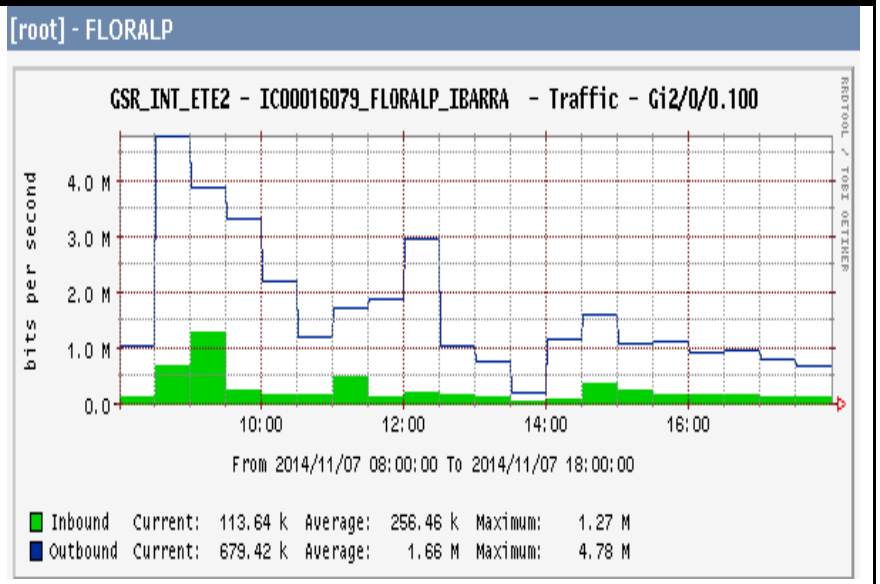
Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

Tabla 38. Consumo del ancho de banda de la red de la FLORALP de los días 04/11/2014 al 05/11/2014.

ANCHO DE BANDA CONSUMO 04/11/2014	ANCHO DE BANDA CONSUMO 05/11/2014
	
En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 1.01 Mbps en el horario de 12:30 a 13:00 y un promedio de 340.26 Kbps.	En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 3.06 Mbps en el horario de 10:30 a 11:00 y un promedio de 490.91 Kbps.

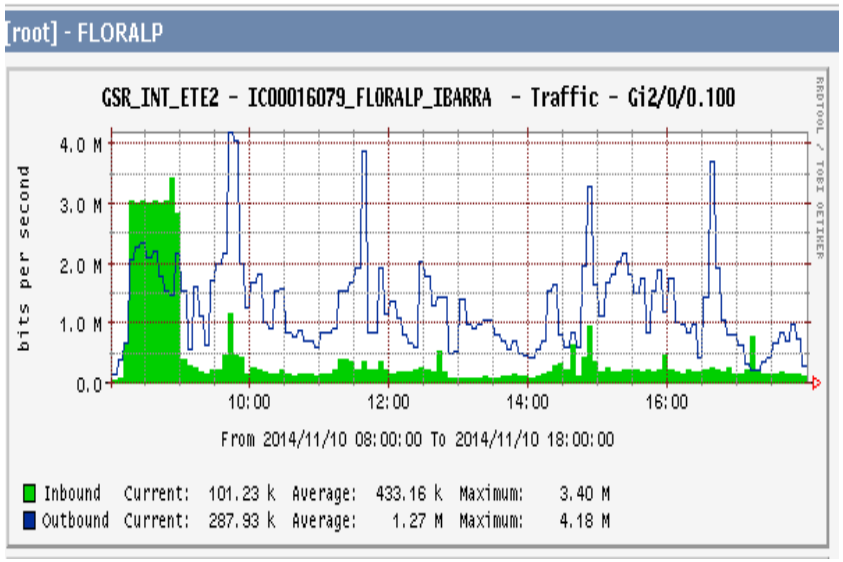
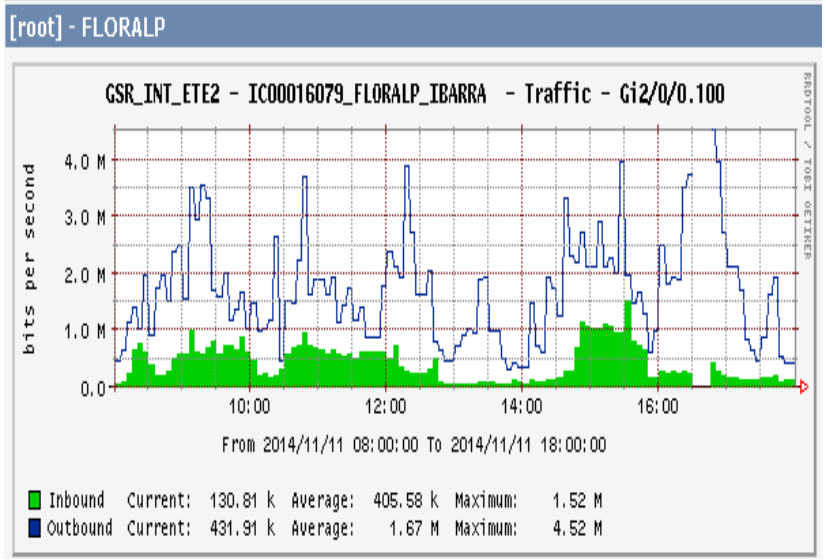
Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

Tabla 39. Consumo del ancho de banda de la red de la FLORALP de los días 06/11/2014 al 07/11/2014.

ANCHO DE BANDA CONSUMO 06/11/2014	ANCHO DE BANDA CONSUMO 07/11/2014
	
En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 3.19 Mbps en el horario de 14:30 a 15:00 y un promedio de 564.00 Kbps.	En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 1.27 Mbps en el horario de 10:30 a 11:00 y un promedio de 256.46 Kbps.

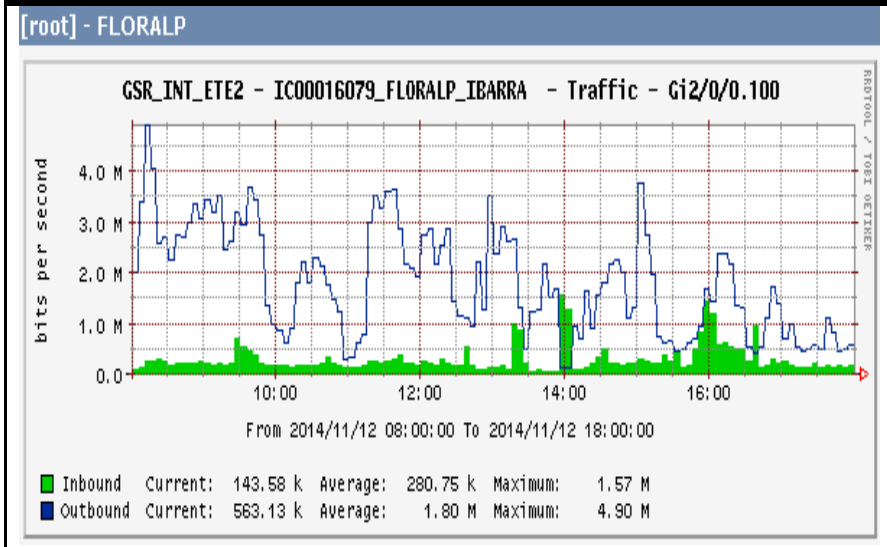
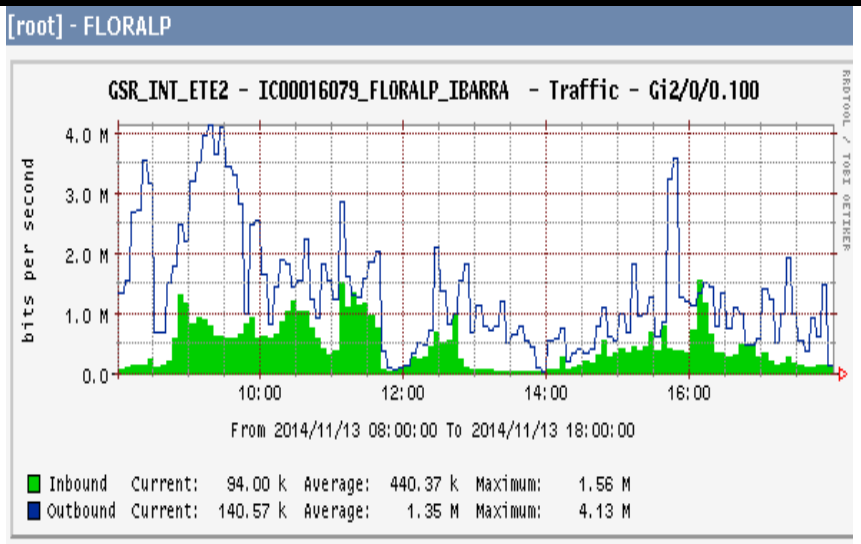
Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

Tabla 40. Consumo del ancho de banda de la red de la FLORALP de los días 10/11/2014 al 11/11/2014.

ANCHO DE BANDA CONSUMO 10/11/2014	ANCHO DE BANDA CONSUMO 11/11/2014
	
En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 3.40 Mbps en el horario de 8:00 a 9:00 y un promedio de 433.16 Kbps.	En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 1.52 Mbps en el horario de 15:00 a 16:00 y un promedio de 405.58 Kbps.

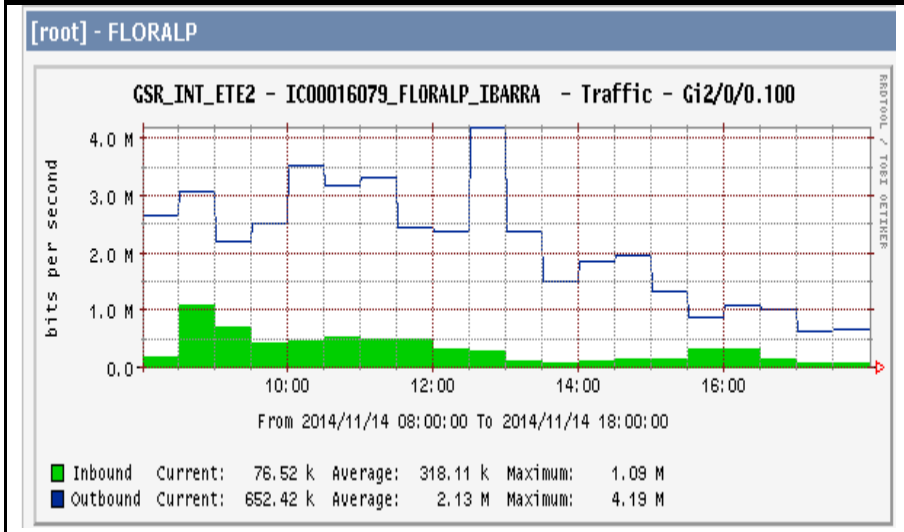
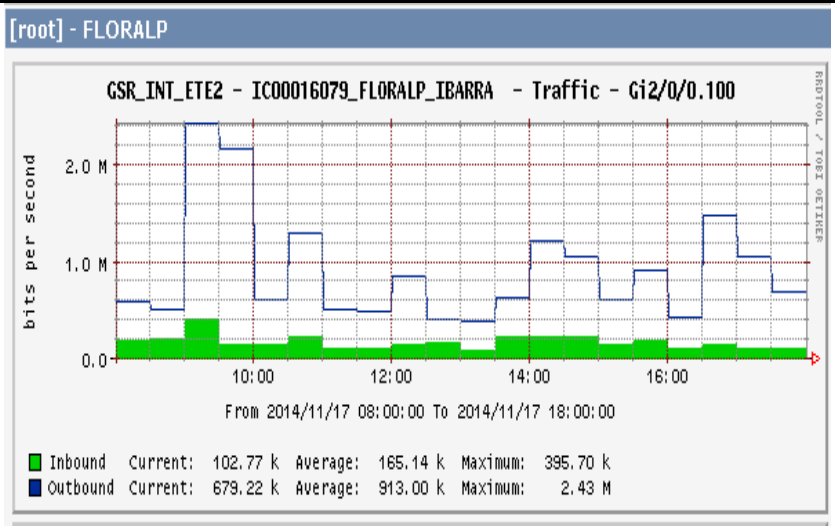
Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

Tabla 41. Consumo del ancho de banda de la red de la FLORALP de los días 12/11/2014 al 13/11/2014.

ANCHO DE BANDA CONSUMO 12/11/2014	ANCHO DE BANDA CONSUMO 13/11/2014
	
En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 1.57 Mbps en el horario de 15:30 a 16:00 y un promedio de 280.75 Kbps.	En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 1.56 Mbps en el horario de 11:00 a 11:30 y un promedio de 404.37 Kbps.

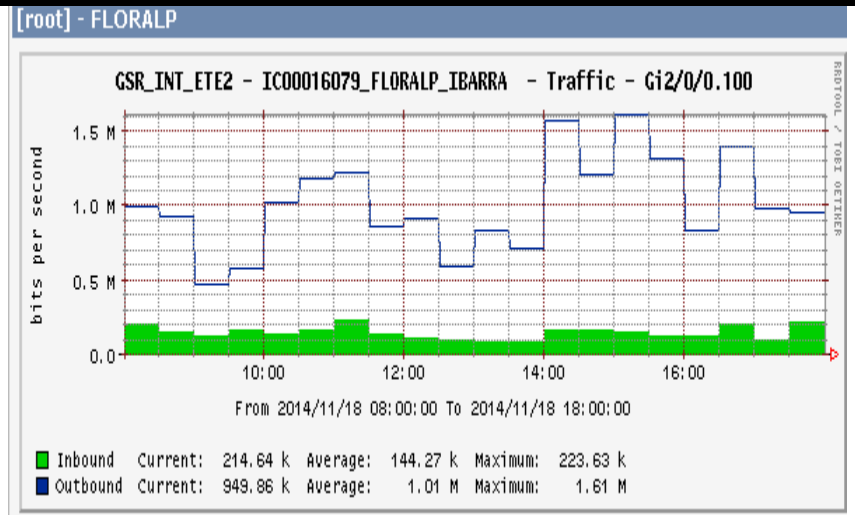
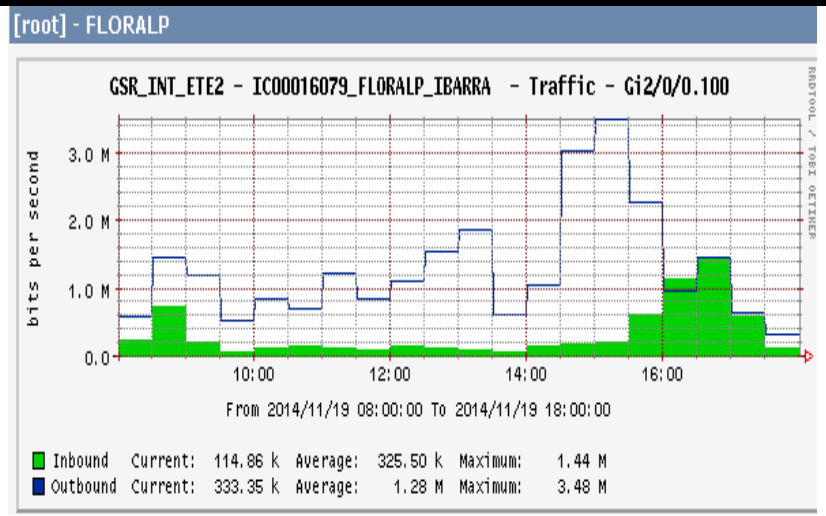
Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

Tabla 42. Consumo del ancho de banda de la red de la FLORALP del día 14/11/2014

ANCHO DE BANDA CONSUMO 14/11/2014	ANCHO DE BANDA CONSUMO 17/11/2014
	
En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 1.09 Mbps en el horario de 08:30 a 09:00 y un promedio de 318.11 Kbps.	En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 395.70 Kbps en el horario de 09:00 a 09:30 y un promedio de 165.14 Kbps.

Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

Tabla 43. Consumo del ancho de banda de la red de la FLORALP del día 14/11/2014

ANCHO DE BANDA CONSUMO 18/11/2014	ANCHO DE BANDA CONSUMO 19/11/2014
	
En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 223.63 Kbps en el horario de 11:00 a 11:30 y un promedio de 144.27 Kbps.	En la gráfica se observa el consumo del ancho de banda donde se puede apreciar un pico de 1.44 Kbps en el horario de 16:30 a 17:00 y un promedio de 325.50 Kbps.

Fuente: Resultados obtenidos del monitoreo mediante el software MRTG proporcionado por una IP pública de CLARO.

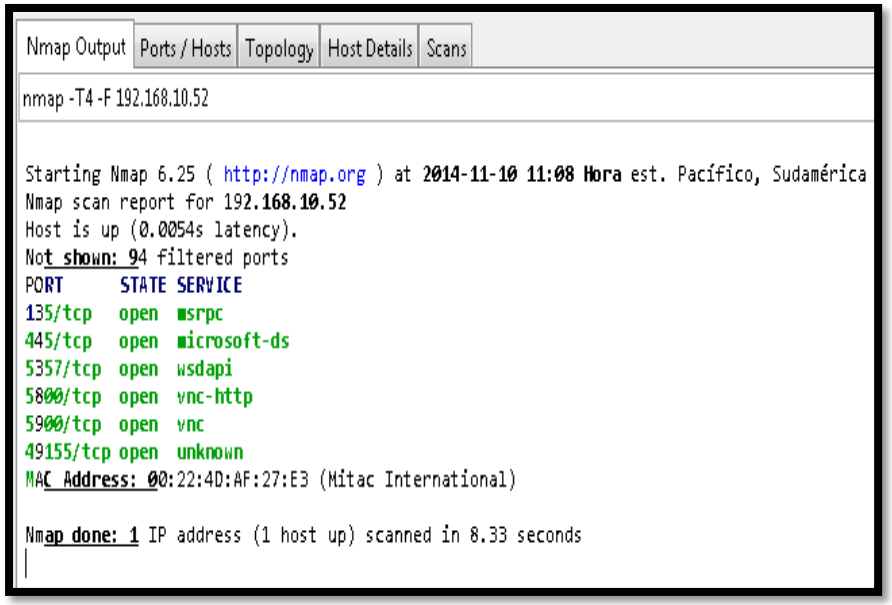
ANEXO B. TIPO DE TRAFICO QUE CIRCULA EN LA RED DE DATOS DE LA FLORALP

El monitoreo se lo ha realizado mediante el uso de la herramienta Nmap/Zenmap y Axence NetTools donde estos nos permitirá escanear que puertos se encuentran habilitados, es decir un informe completo y disponer de toda la información acerca de que servicios son usados por una máquina. En las siguientes Figuras se podrá observar los puertos utilizados por los equipos de los diferentes departamentos dentro de la infraestructura de red de la industria FLORALP.

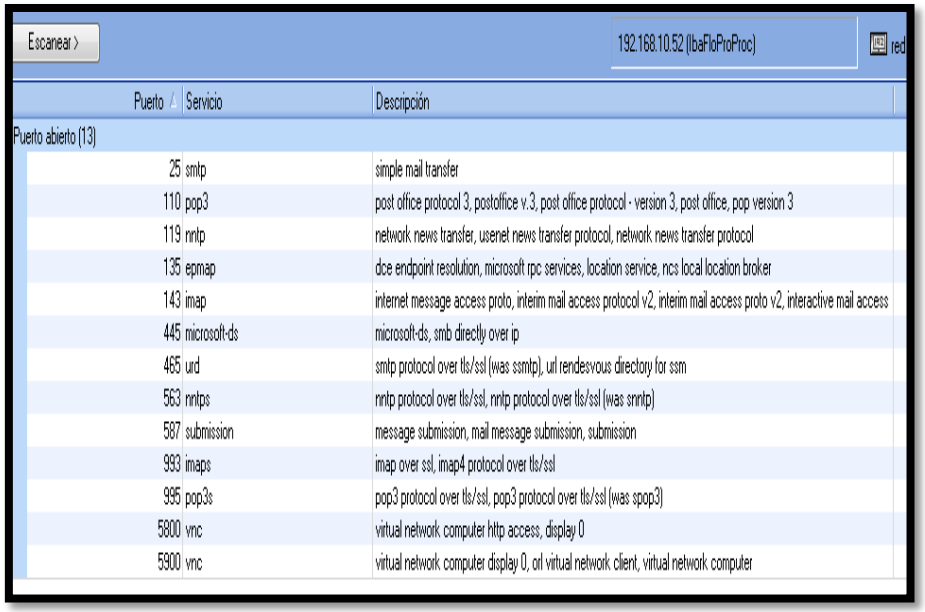
Tabla 44. Puertos habilitados en el Departamento de Sistemas

PUERTOS HABILITADOS DEPARTAMENTO DE SISTEMAS

Nmap/Zenmap



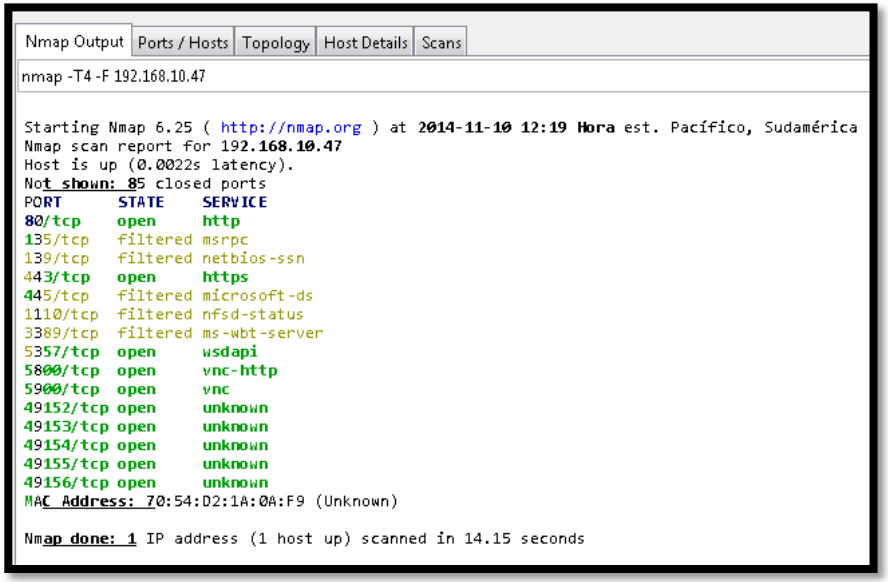
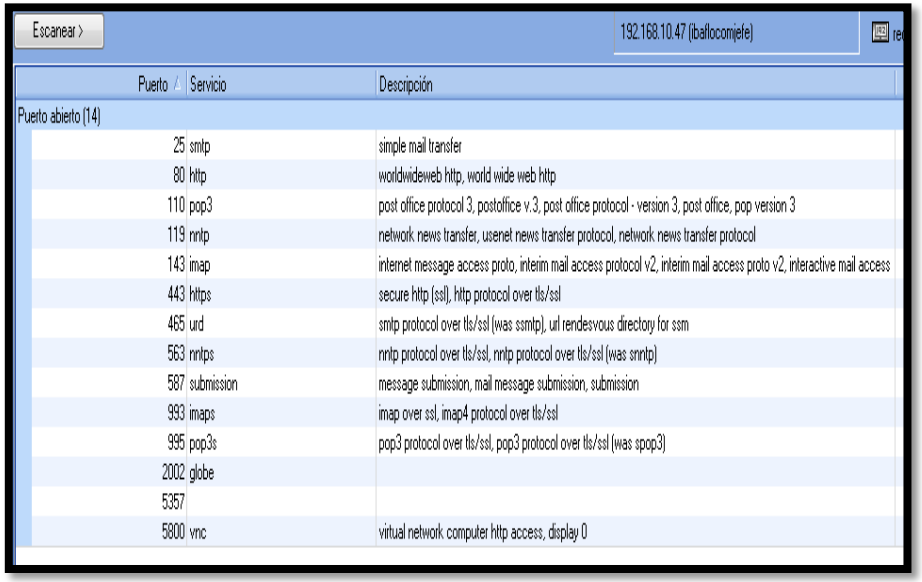
Axence NetTools



En las gráficas anteriores se puede evidenciar los puertos habilitados por una de las máquinas utilizadas en el departamento de sistemas, de esta manera se puede observar que puertos son utilizados, ya que será fundamental para tomar decisiones para las políticas de acceso a los servicios dentro de la red, además para evitar ataques externos e internos.

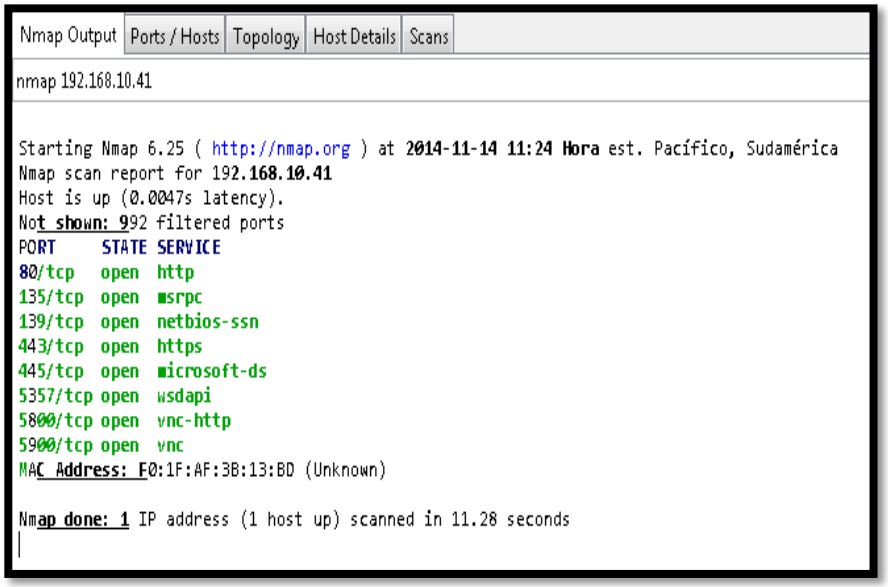
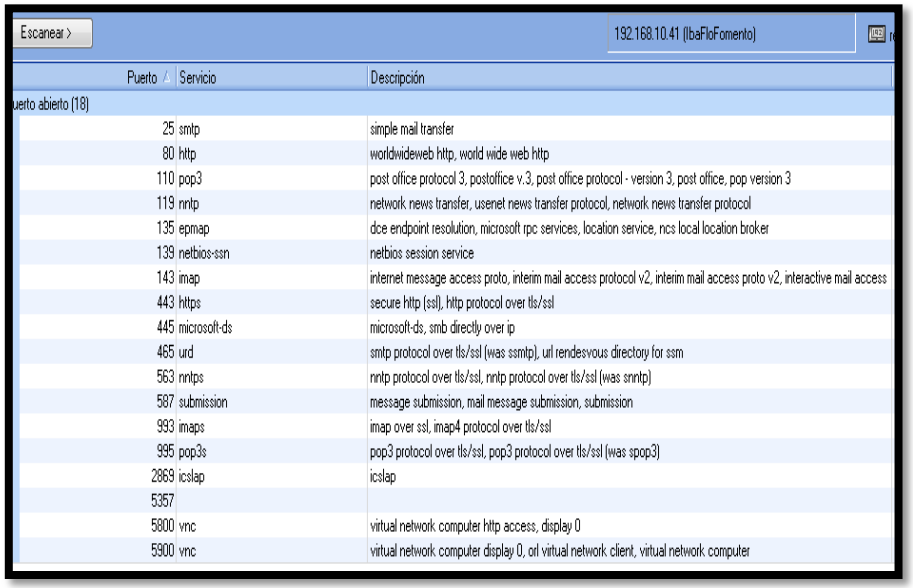
Fuente: Resultados obtenidos a través del programa Nmap y Axence NetTools

Tabla 45. Puertos habilitados en el Departamento de Compras

PUERTOS HABILITADOS DEPARTAMENTO DE COMPRAS	
Nmap/Zenmap	**Axence NetTools**
	
En las gráficas anteriores se puede evidenciar los puertos habilitados por una de las máquinas utilizadas en cada departamento, de esta manera se podrá observar que puertos son más utilizados ya que será fundamental para tomar decisiones para las políticas de acceso a los servicios dentro de la red, además para evitar ataques externos e internos.	

Fuente: Resultados obtenidos a través del programa Nmap y Axence NetTools

Tabla 46. Puertos habilitados en el Departamento de Fomento Ganadero

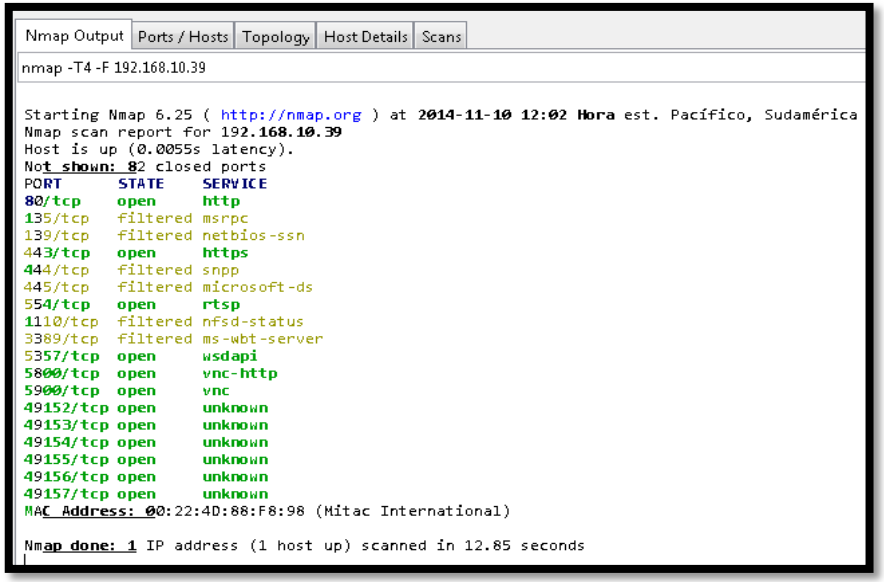
PUERTOS HABILITADOS DEPARTAMENTO DE FOMENTO GANADERO	
Nmap/Zenmap	**Axence NetTools**
	

Puerto	Servicio	Descripción
uerto abierto (18)		
25	smtp	simple mail transfer
80	http	worldwideweb http, world wide web http
110	pop3	post office protocol 3, postoffice v.3, post office protocol - version 3, post office, pop version 3
119	nntp	network news transfer, usenet news transfer protocol, network news transfer protocol
135	epmap	dce endpoint resolution, microsoft rpc services, location service, ncs local location broker
139	netbios-ssn	netbios session service
143	imap	internet message access proto, interim mail access protocol v2, interim mail access proto v2, interactive mail access
443	https	secure http (ssl), http protocol over tls/ssl
445	microsoft-ds	microsoft-ds, smb directly over ip
465	urd	smtp protocol over tls/ssl (was ssmtp), url rendesvous directory for ssm
563	nntps	nntp protocol over tls/ssl, nntp protocol over tls/ssl (was snntp)
587	submission	message submission, mail message submission, submission
993	imaps	imap over ssl, imap4 protocol over tls/ssl
995	pop3s	pop3 protocol over tls/ssl, pop3 protocol over tls/ssl (was spop3)
2869	icslap	icslap
5357		
5800	vnc	virtual network computer http access, display 0
5900	vnc	virtual network computer display 0, orl virtual network client, virtual network computer

En las gráficas anteriores se puede evidenciar los puertos habilitados por una de las máquinas utilizadas en cada departamento, de esta manera se podrá observar que puertos son más utilizados ya que será fundamental para tomar decisiones para las políticas de acceso a los servicios dentro de la red, además para evitar ataques externos e internos.

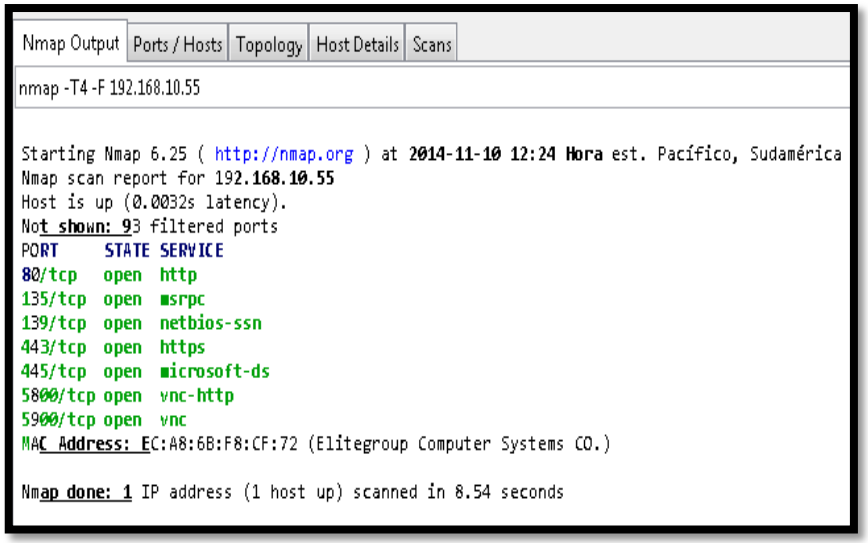
Fuente: Resultados obtenidos a través del programa Nmap y Axence NetTools

Tabla 47. Puertos habilitados en el Departamento de Contabilidad y Finanzas

PUERTOS HABILITADOS DEPARTAMENTO DE CONTABILIDAD Y FINANZAS	
Nmap/Zenmap	**Axence NetTools**
	
En las gráficas anteriores se puede evidenciar los puertos habilitados por una de las máquinas utilizadas por cada departamento, de esta manera se podrá observar que puertos son más utilizados ya que será fundamental para tomar decisiones para las políticas de acceso a los servicios dentro de la red, además para evitar ataques externos e internos.	

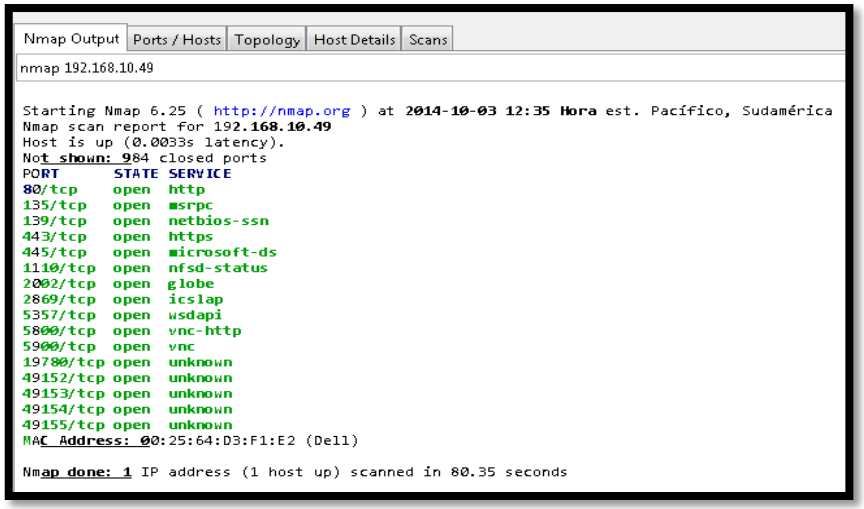
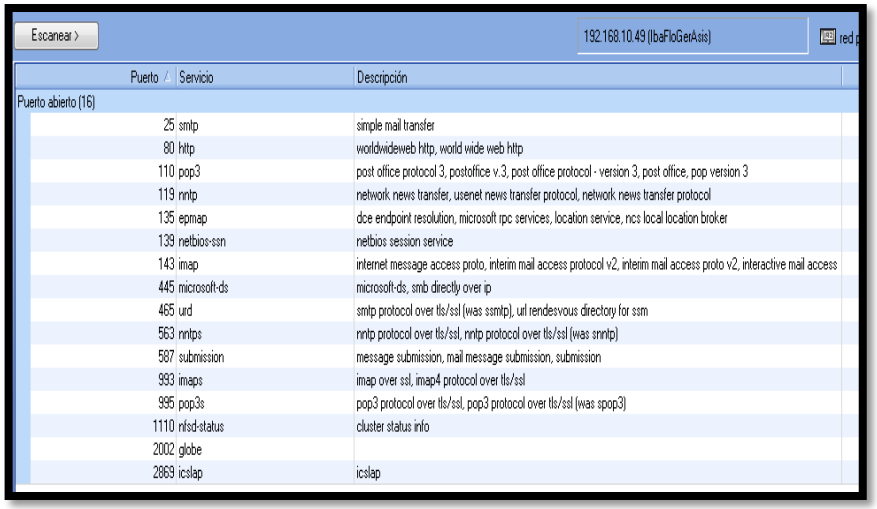
Fuente: Resultados obtenidos a través del programa Nmap y Axence NetTools

Tabla 48. Puertos habilitados en el Departamento de Comercial

PUERTOS HABILITADOS DEPARTAMENTO DE COMERCIAL	
Nmap/Zenmap	**Axence NetTools**
	
En las gráficas anteriores se puede evidenciar los puertos habilitados por una de las máquinas utilizadas por cada departamento, de esta manera se podrá observar que puertos son más utilizados ya que será fundamental para tomar decisiones para las políticas de acceso a los servicios dentro de la red, además para evitar ataques externos e internos.	

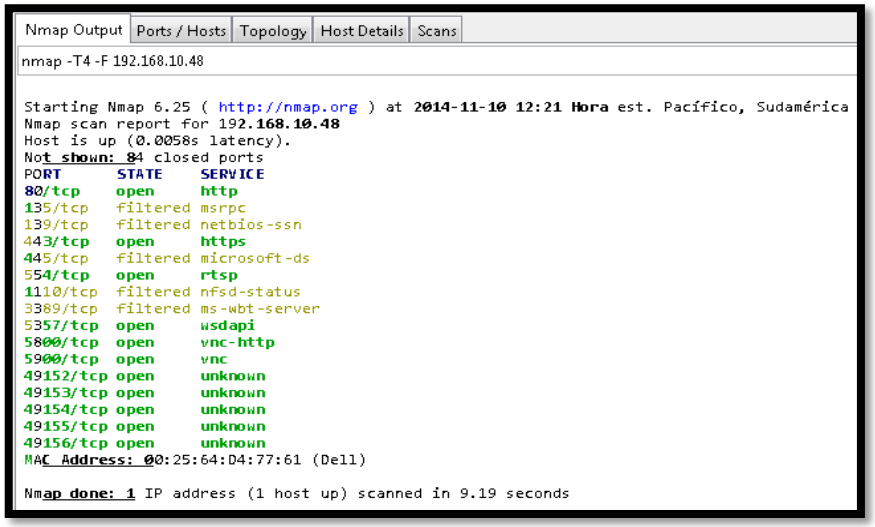
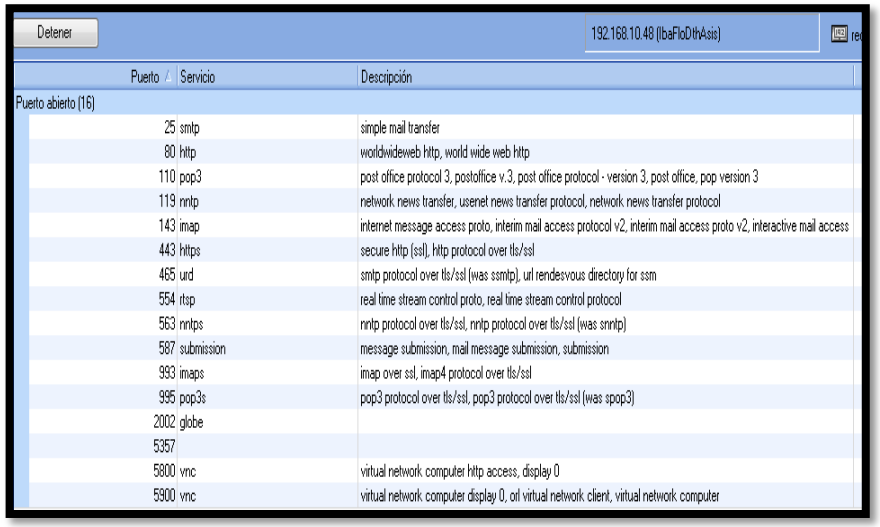
Fuente: Resultados obtenidos a través del programa Nmap y Axence NetTools

Tabla 49. Puertos habilitados en el Departamento de Ventas

PUERTOS HABILITADOS DEPARTAMENTO DE VENTAS	
Nmap/Zenmap	**Axence NetTools**
	
En las gráficas anteriores se puede evidenciar los puertos habilitados por una de las máquinas utilizadas por cada departamento, de esta manera se podrá observar que puertos son más utilizados ya que será fundamental para tomar decisiones para las políticas de acceso a los servicios dentro de la red, además para evitar ataques externos e internos.	

Fuente: Resultados obtenidos a través del programa Nmap y Axence NetTools

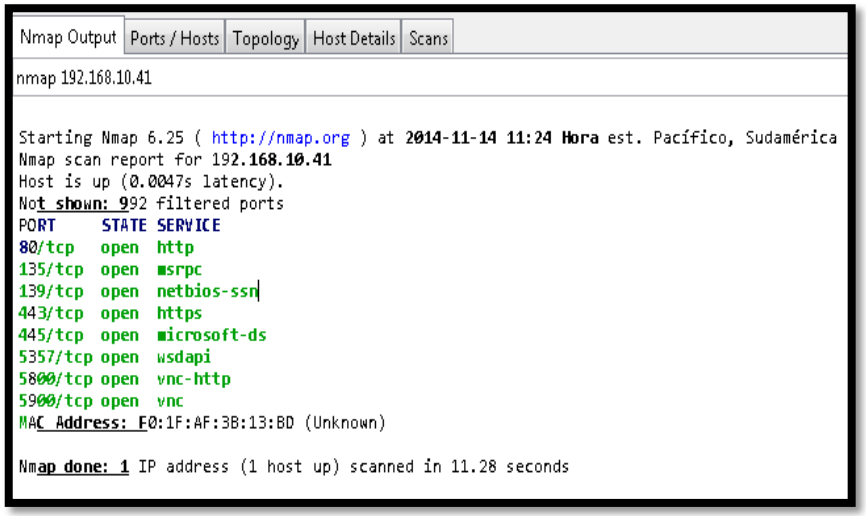
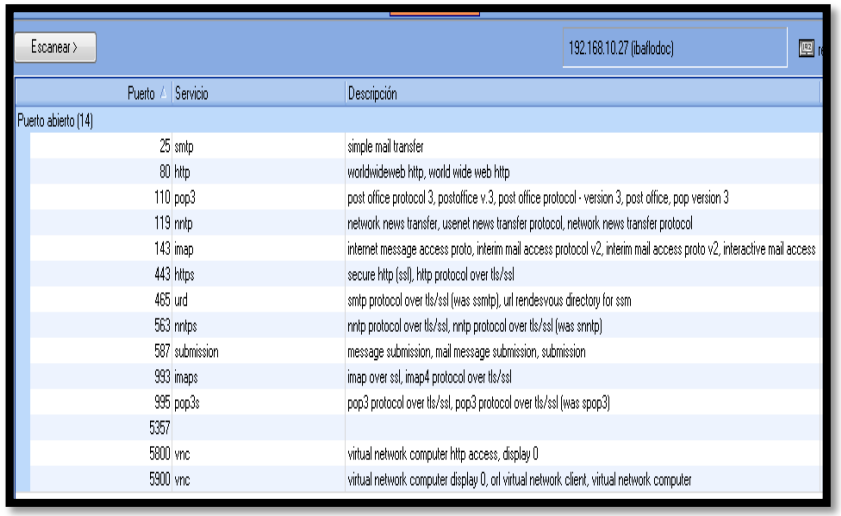
Tabla 50. Puertos habilitados en el Departamento de Talento Humano

PUERTOS HABILITADOS DEPARTAMENTO DE TALENTO HUMANO	
Nmap/Zenmap	**Axence NetTools**
	

En las gráficas anteriores se puede evidenciar los puertos habilitados por una de las máquinas utilizadas por cada departamento, de esta manera se podrá observar que puertos son más utilizados ya que será fundamental para tomar decisiones para las políticas de acceso a los servicios dentro de la red, además para evitar ataques externos e internos.

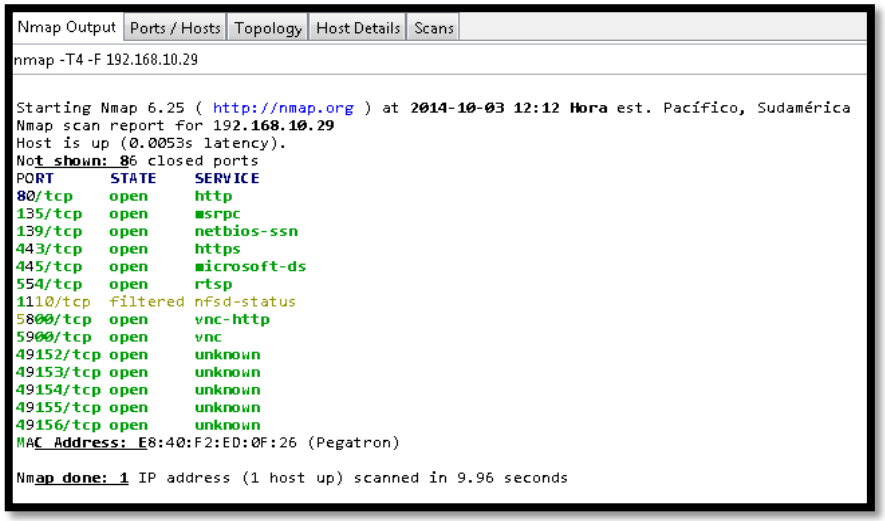
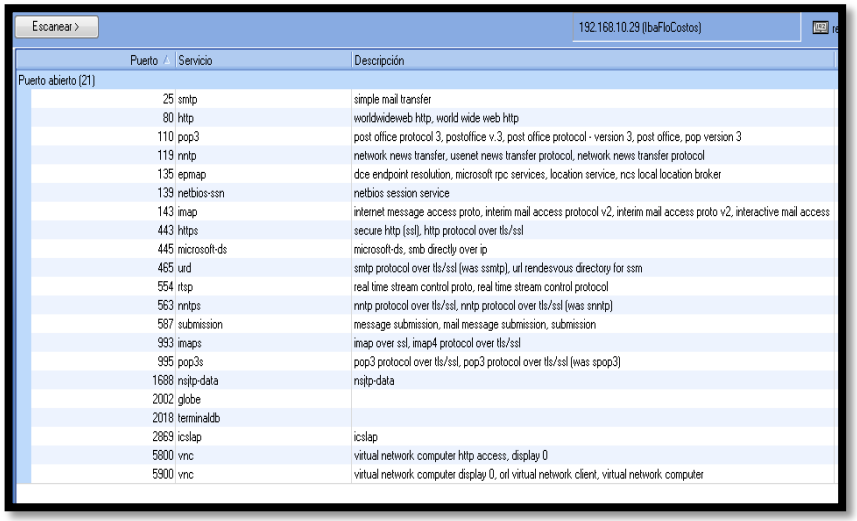
Fuente: Resultados obtenidos a través del programa Nmap y Axence NetTools

Tabla 51. Puertos habilitados en el Departamento de Seguridad y Salud

PUERTOS HABILITADOS DEPARTAMENTO DE SEGURIDAD Y SALUD	
Nmap/Zenmap	**Axence NetTools**
	
En las gráficas anteriores se puede evidenciar los puertos habilitados por una de las máquinas utilizadas por cada departamento, de esta manera se podrá observar que puertos son más utilizados ya que será fundamental para tomar decisiones para las políticas de acceso a los servicios dentro de la red, además para evitar ataques externos e internos.	

Fuente: Resultados obtenidos a través del programa Nmap y Axence NetTools

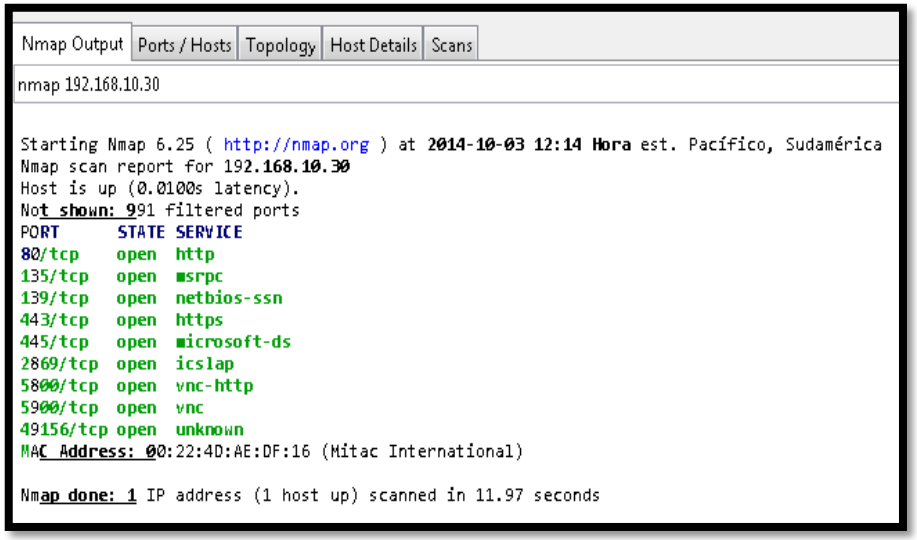
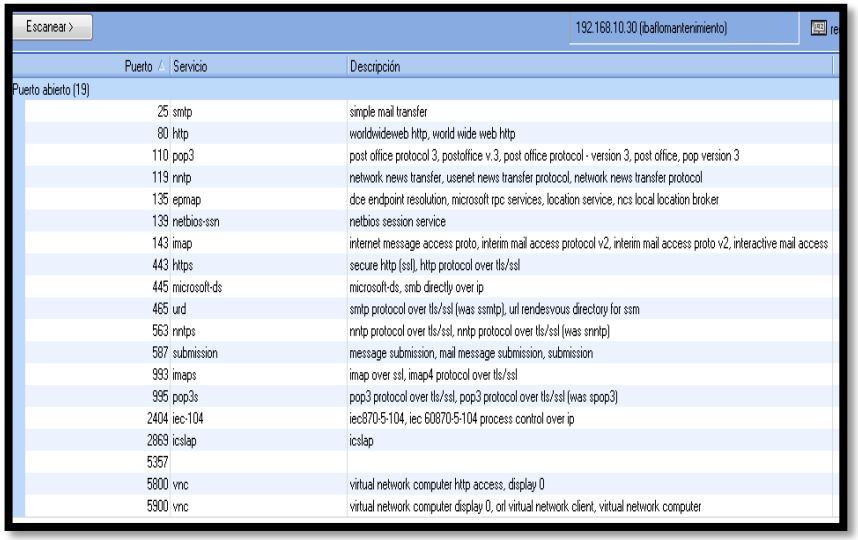
Tabla 52. Puertos habilitados en el Departamento de Bodega

PUERTOS HABILITADOS DEPARTAMENTO DE BODEGA	
Nmap/Zenmap	**Axence NetTools**
	

En las gráficas anteriores se puede evidenciar los puertos habilitados por una de las máquinas utilizadas por cada departamento, de esta manera se podrá observar que puertos son más utilizados ya que será fundamental para tomar decisiones para las políticas de acceso a los servicios dentro de la red, además para evitar ataques externos e internos.

Fuente: Resultados obtenidos a través del programa Nmap y Axence NetTools

Tabla 53. Puertos habilitados en el Departamento de Mantenimiento

PUERTOS HABILITADOS DEPARTAMENTO DE MANTENIMIENTO	
Nmap/Zenmap	**Axence NetTools**
	
En las gráficas anteriores se puede evidenciar los puertos habilitados por una de las máquinas utilizadas por cada departamento, de esta manera se podrá observar que puertos son más utilizados ya que será fundamental para tomar decisiones para las políticas de acceso a los servicios dentro de la red, además para evitar ataques externos e internos.	

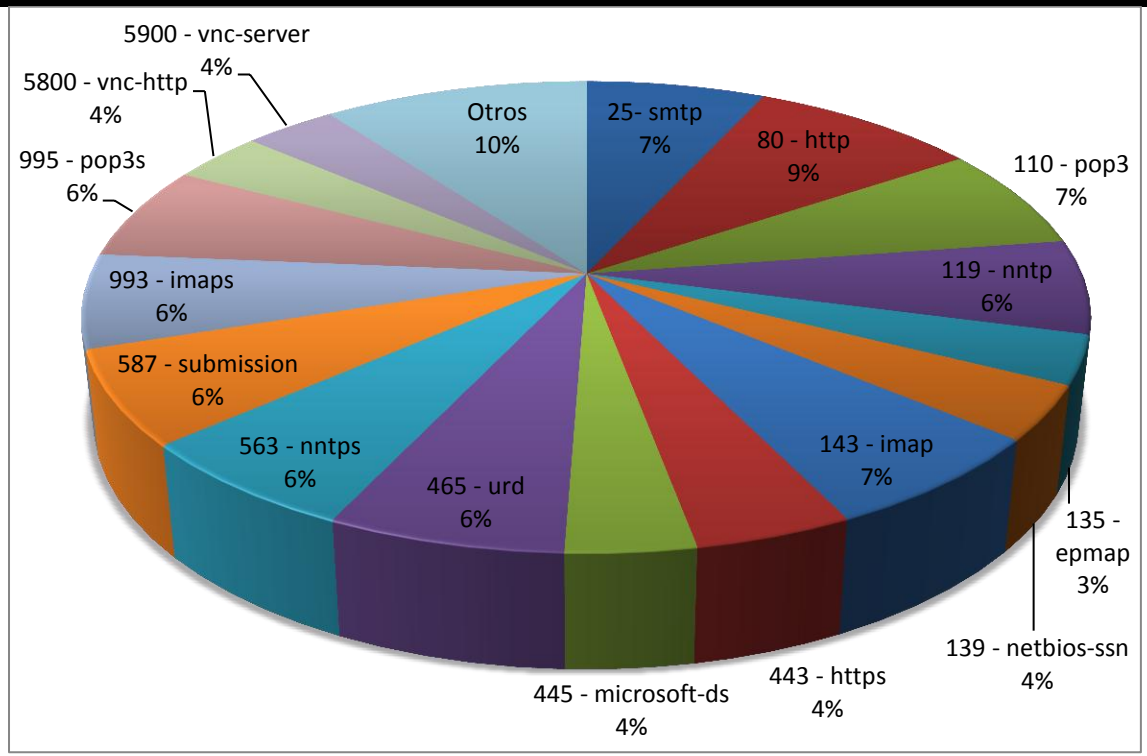
Fuente: Resultados obtenidos a través del programa Nmap y Axence NetTools

En el cuadro estadístico se puede evidenciar los diferentes tipos de protocolos que utilizan cada dirección IP, concluyendo que la mayoría de protocolos son TCP se tomó en periodos donde existe mayor actividad de los usuarios. De tal forma los protocolos más utilizados son:

Tabla 54. Grafico Estadístico de puertos más utilizados por los usuarios.

PROTOCOLO	PUERTO
smtp	25
http	80
pop3	110
nntp	119
epmap	135
netbios-ssn	139
imap	143
https	443
microsoft-ds	445
urd	465
nntps	563
submission	587
imaps	993
pop3s	995
vnc-http	5800
vnc-server	5900

GRÁFICO ESTADÍSTICO



Otros Protocolos

El monitoreo fue realizado con las herramientas Nmap/Zenmap y Axence NetTools donde se puedo observar los protocolos más utilizados por las IP de cada uno de los usuarios, donde el mayor porcentaje lo tiene el protocolo HTTP debido a que los usuarios hacen uso de este la mayoría de servicios que presta el protocolo.

ANEXO C. FORMULARIOS Y SOLICITUDES

ANEXO C1. SOLICITUD DE ACCESO A SISTEMAS DE INFORMACIÓN

FLORALP	**SOLICITUD DE ACCESO A SISTEMAS DE INFORMACIÓN**
1. Datos Generales	
Nombre y Apellido del Solicitante :	
Departamento/Oficina:	
Correo electrónico:	Tel:
2. Datos del administrador	
Nombre y Apellido:	
Cargo:	

3. Datos a los que solicita acceso:
4. Descripción breve, pero específica del trabajo a realizarse relacionado a los datos que solicita acceso:
_____ _____ Firma del Departamento de Sistemas Firma del Solicitante

ANEXO C2. SOLICITUD DE ACCESO A CONTRASEÑAS

FLORALP	**SOLICITUD DE ACCESO A CONTRASEÑAS**

1. Datos Generales
Nombre y Apellido del Solicitante :
Departamento/Oficina:
Correo electrónico: Tel:
2. Datos del administrador
Nombre y Apellido:
Cargo:

3. Datos a los que solicita acceso:

4. Aceptación de obligaciones del usuario

- **a)** El usuario y contraseña por ningún motivo debe ser transferido a otro usuario
- **b)** La suspensión temporaria o definitiva de funcionario deberá ser comunicado de inmediato al jefe de sistemas siguiendo los mecanismos definidos.
- **c)** Los cambios de perfiles de los funcionarios, deberán ser comunicados al administrador de usuarios del sistema siguiendo los mecanismos definidos.
- **d)** Todas las operaciones realizadas en los sistemas, son responsabilidad del funcionario propietario del usuario.
- **e)** Cualquier novedad asociados a las habilitaciones y modificaciones deberán ser comunicados al administrador de usuarios del sistema.

5. Firmantes:

_____ _____

Firma del Departamento de Sistemas Firma del Solicitante

ANEXO C3. REPORTE PARA EL MANTENIMIENTO DE EQUIPOS

FLORALP	**REPORTE DE MANTENIMIENTO DE EQUIPOS**

1. DATOS GENERALES		**2. DATOS DEL CLIENTE**	
NOMBRE DE LA EMPRESA		NOMBRE DEL CLIENTE	
RESPONSABLE DEL TRABAJO		RESPONSABLE	
Área de trabajo		Dirección	
Dirección		Teléfono	
Teléfono		E-mail	
E-mail			

3. FECHA		
DD	MM	AA

4. DESCRIPCIÓN DE EQUIPOS OBSERVACIONES

5. FUNCIONAMIENTO

6. NOMBRE Y FIRMA DE LA EMPRESA	**7. NOMBRE Y FIRMA DEL CLIENTE**
_____	_____

ANEXO C4. BITÁCORA DEL REPORTE PARA EL MANTENIMIENTO DE EQUIPOS

FLORALP

BITÁCORA DEL REPORTE DE MANTENIMIENTO DE EQUIPOS

Fecha del Reporte	Responsable	Modelo	Serie	Falla	Fecha de reparación	Observaciones

ANEXO C5. REPORTE DE SOLUCIONES DE HADWARE Y SOFTWARE POR PARTE DEL DEPARTAMENTO DE SISTEMAS

FLORALP	**FORMULARIO DE SOLICITUD DE SERVICIOS PARA EL DEPARTAMENTO DE SISTEMAS**

1. DATOS GENERALES
Persona solicitante:
Departamento al que pertenece:
Fecha:

2. SELECCIÓN DE SERVICIOS (Señale con una X)				
Reubicación de equipo	Instalación De equipo	Instalación De software	Reporte De errores	Correo electrónico
Mantenimiento de equipo	Reparación De equipo	Actualización de software	Conexión A Internet	Modificación En la base datos

3. ESPECIFIQUE EL PORQUE DEL SERVICIO SELECCIONADO

ANEXO C6. FORMULARIO PARA EL RESPALDO Y RESTAURACIÓN DE DATOS

FLORALP **FORMULARIO PARA EL RESPALDO Y RESTAURACIÓN DE DATOS**		
1. **DATOS GENERALES**		
Fecha:		
Hora de inicio:		
Hora de finalización:		
Responsable:		
2. **TIPO DE OPERACIÓN:** (señale con una X)	Respaldo	Restauración

3. **DESCRIPCION DE RECURSOS RESPALDADOS (señale con una X)**		
APLICACIONES INFORMATICAS	BASE DE DATOS DE FLORALP	INFORMACIÓN DE EQUIPOS DE COMPUTO
Ubicación del archivo		
Nombre del servidor:		
Nombre del equipo de cómputo:		
Dirección IP:		
Directorio:		

4. **DESCRIPCION DE RECURSOS RESTAURADOS (señale con una X)**		
Causa/Motivo de la restauración:		
APLICACIONES INFORMATICAS	BASE DE DATOS DE FLORALP	INFORMACIÓN DE EQUIPOS DE COMPUTO
Resultado/Observaciones		

FIRMA DEL RESPONSABLE
_____

ANEXO D. MAPEO DE PUERTOS

SWITCH LINKYS SFE 2000		
Interfaz	**Pach Panel Etiquetado**	**Descripción**
FastEthernet 0/15	R1-D1	Impresora
FastEthernet 0/11	R1-D2	Sala de espera
FastEthernet 0/1	R1-D3	No identificado
FastEthernet 0/13	R1-D4	Gerente general
FastEthernet 0/1	R1-D5	
FastEthernet 0/2	R1-D6	Recepción
FastEthernet 0/14	R1-D7	Asistente de recursos humanos
FastEthernet 0/3	R1-D8	Jefe de fomento ganadero
FastEthernet 0/4	R1-D9	No identificado
FastEthernet 0/16	R1-D10	Jefe de compras
FastEthernet 0/5	R1-D11	Jefe se seguridad y salud
FastEthernet 0/17	R1-D12	Oficinas para Visitantes
FastEthernet 0/18	R1-D13	Jefe financiero
FastEthernet 0/6	R1-D14	Gerente financiero
FastEthernet 0/7	R1-D15	Jefe de sistemas
FastEthernet 0/19	R1-D16	Asistentes de contabilidad 1
FastEthernet 0/8	R1-D17	
FastEthernet 0/20	R1-D18	Asistentes de contabilidad 2
FastEthernet 0/9	R1-D19	
FastEthernet 0/21	R1-D20	Sala de reuniones
FastEthernet 0/10	R1-D21	No identificado
FastEthernet 0/23	R1-D22	Sin uso

FastEthernet 0/12	R1-D23	No identificado
FastEthernet 0/24	R1-D24	Switch de acceso
GigabitEthernet 0/2	----------	Router Inalámbrico Tp-Link
GigabitEthernet 0/4	----------	FastEthernet 0/1 Router Cisco-Linksys WRT110
GigabitEthernet 0/3	----------	Hacia al Rack 2

SWITCH 3COM 2024		
Interfaz	**Etiquetado**	**Descripción**
FastEthernet 0/1	R2-D13	---------
FastEthernet 0/2	R2-D4	---------
FastEthernet 0/3	R2-D21	Desktop
FastEthernet 0/4	R2-D5	---------
FastEthernet 0/5	R2-D7	---------
FastEthernet 0/6	R2-D12	---------
FastEthernet 0/7	R2-D17	---------
FastEthernet 0/8	R2-D15	---------
FastEthernet 0/9	R2-D19	---------
FastEthernet 0/10	R2-D14	---------
FastEthernet 0/13	R2-D6	Jefe de Calidad
FastEthernet 0/14	R2-D3	---------
FastEthernet 0/15	R2-D8	Laboratorio Materia Prima
FastEthernet 0/16	R2-D9	---------
FastEthernet 0/17	R2-D10	---------
FastEthernet 0/19	R2-D16	Sala de Reuniones
FastEthernet 0/20	R2-D20	---------

FastEthernet 0/21	R2-D18	---------
FastEthernet 0/22	R2-D11	---------
FastEthernet 0/23	R2-D1	Sin uso
FastEthernet 0/24	R2-D2	Sin uso

SWITCH TP-LINK 1024	
Interfaz	**Descripción**
FastEthernet 0/1	Punto de Red
FastEthernet 0/2	Servidor de Aplicaciones
FastEthernet 0/3	Server Data
FastEthernet 0/5	Proliant DL380 Gen8
FastEthernet 0/7	Servidor Dominio
FastEthernet 0/9	Server Flexline
FastEthernet 0/12	---------
FastEthernet 0/13	Proliant ML350

ANEXO E. INSTALACIÓNES Y CONFIGURACIONES

ANEXO E1. INSTALACIÓN DEL SISTEMA OPERATIVO

Al hacer boot muestra 2 opciones para la instalación, la primera el sistema detecta la tarjeta de vídeo y entrara en modo gráfico por lo tanto recomiendo elegir la segunda opción; la cual carga un driver básico de vídeo que diría que todos los equipos reconocen sin problemas.

Figura 80. Instalación de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

La primera pantalla que aparece pregunta si desea verificar la integridad del medio de instalación. Si ya se lo hizo y está seguro, escogemos Skip.

Figura 81. Verificación el medio de Instalación de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

Inicia el entorno gráfico se selecciona next en cuanto aparezca la pantalla de bienvenida de CentOS.

Figura 82. Modo gráfico de la Instalación de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

Se elige el idioma a usar durante la instalación y haga click en el botón Next

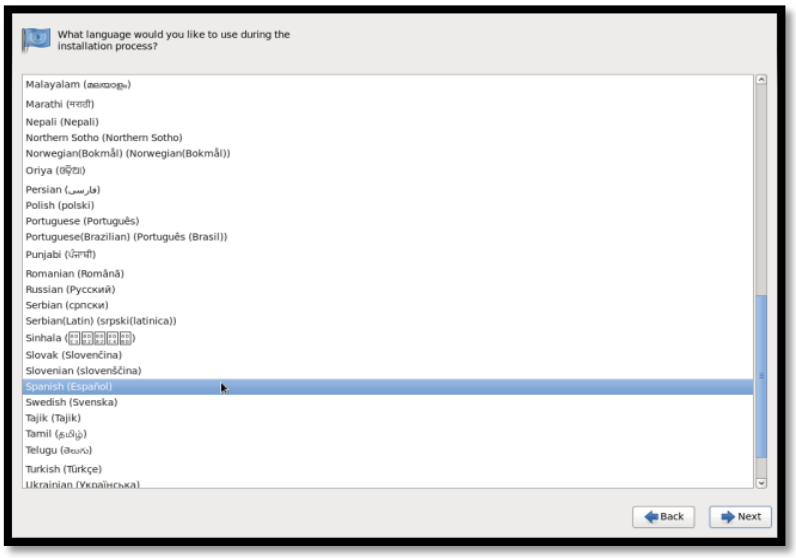


Figura 83. Elección del idioma de la Instalación de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

Elegir la distribución del teclado y dar click al botón siguiente

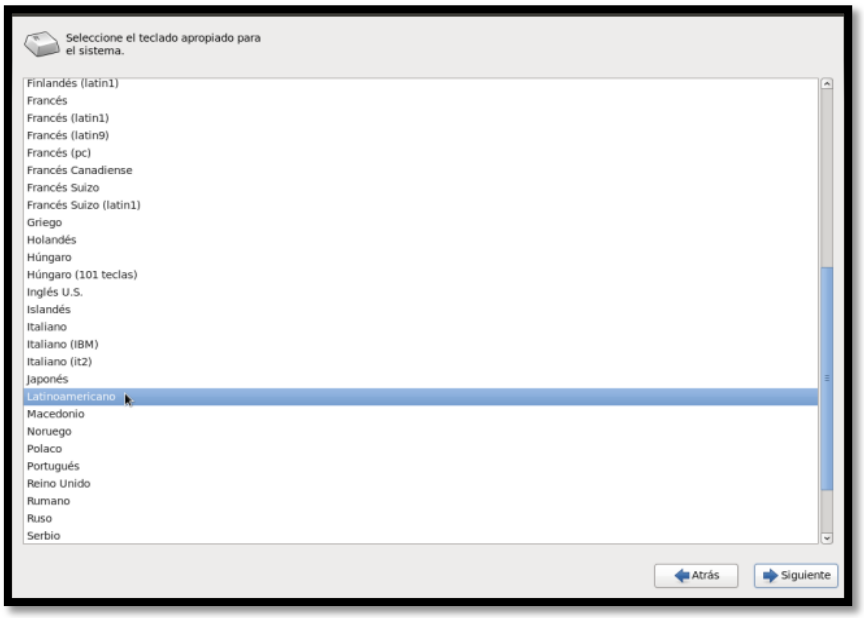


Figura 84. Elección del idioma del teclado para la Instalación de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

En caso de contar con dispositivos de almacenamiento especializados como iSCSI[20], SAN[21], etc, marcar la segunda opción, sino, la primera es la que se elige. Dar click al botón Siguiente.

[20] **iSCSI:** Es un estándar que permite el uso del protocolo SCSI sobre redes TCP/IP

[21]**SAN:** Una red de área de almacenamiento, en inglés SAN (Storage Area Network), es una red de almacenamiento integral

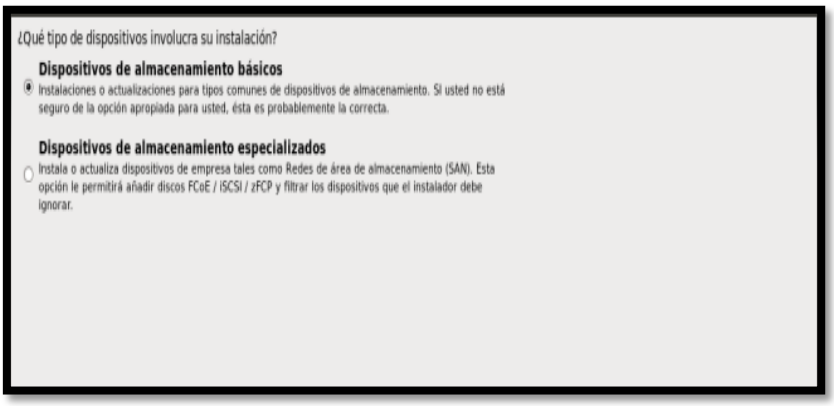


Figura 85. Dispositivos de almacenamiento para la Instalación de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

Se muestra el disco detectado, dar click al botón si descarta todos los datos.

Figura 86. Advertencia del almacenamiento para la Instalación de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

Escoger un nombre para Centos y dar click al botón configure la red. En la tarjeta de red se configura los siguientes parámetros:

Nombre del host: fw-floralp.local

Dirección IP: 192.168.10.8

Mascara: 255.255.255.0

Puerta de enlace: 192.168.10.4

Ya configurada la conexión, dar click al botón cerrar y siguiente. Elegir la zona donde está ubicado el equipo en este caso elegiremos América/Guayaquil luego la zona horaria se activará. Dar click al botón Siguiente.

Escribir una contraseña para el usuario root (administrador del sistema) y dar click al botón Siguiente.

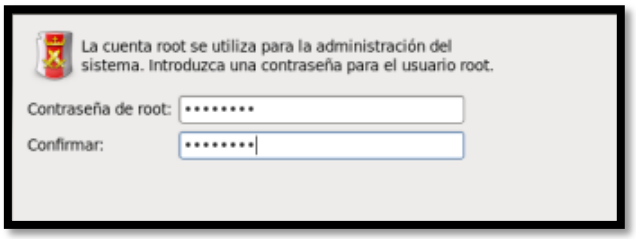


Figura 87. Ingreso de la contraseña de administrador para la Instalación de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

El en siguiente paso se particiona el disco para la instalar. En este caso se usa en su totalidad. Dar click al botón Siguiente.

Figura 88. Particionamiento del disco para la Instalación de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

Ultima oportunidad para no eliminar lo que hay en el disco. Dar click al botón y escribir cambios al disco.

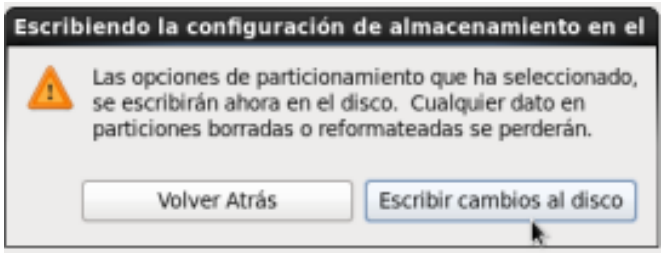


Figura 89. Escribiendo la configuración del disco para la Instalación de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

Siguiente paso, elegir como instalar Centos, con la opción Basic Server es suficiente para instalar y tener las herramientas para después personalizarlo. Dar click al botón Siguiente.

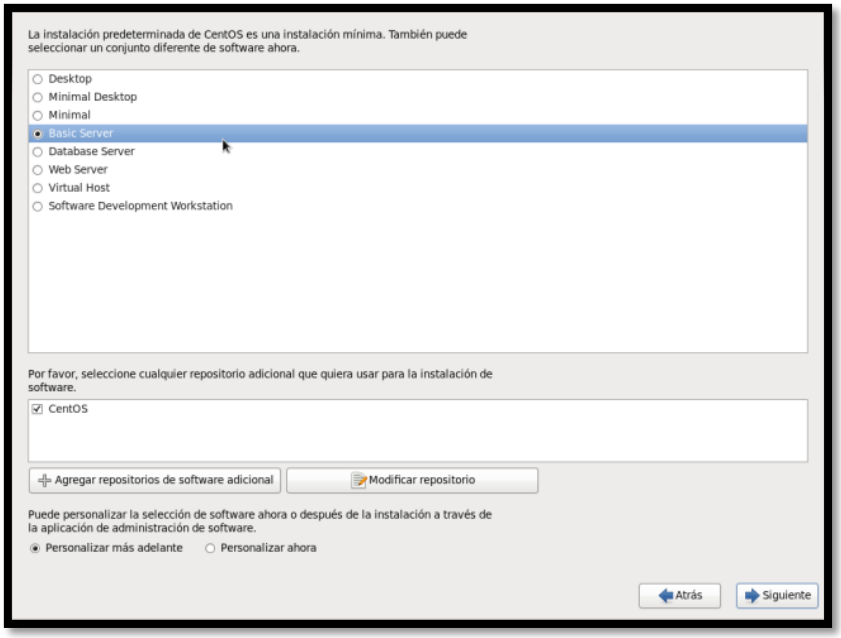


Figura 90. Modo de la Instalación de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

Inicialización de la instalación, luego dar click al botón de reiniciar y ha finalizado la instalación.

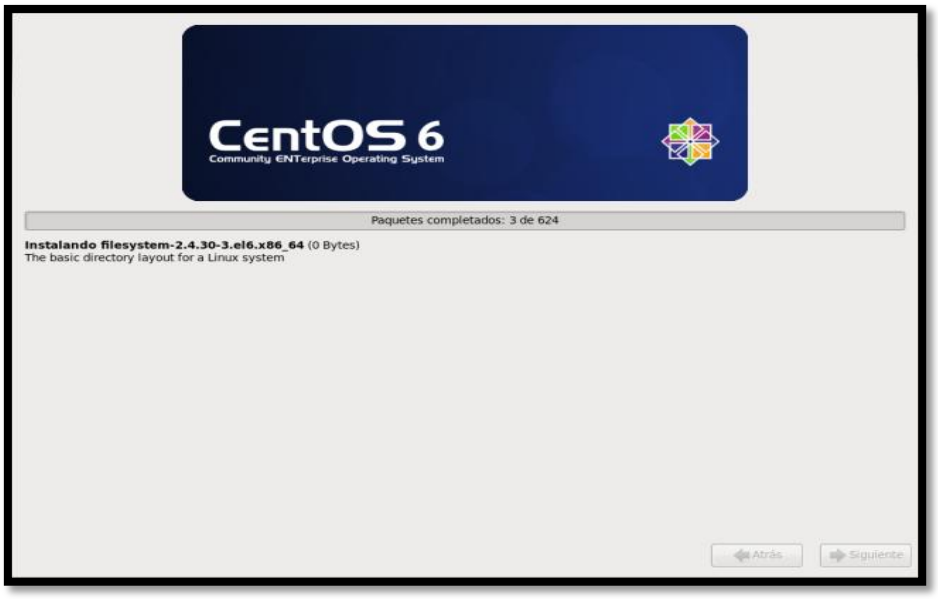


Figura 91. Inicialización de la Instalación de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

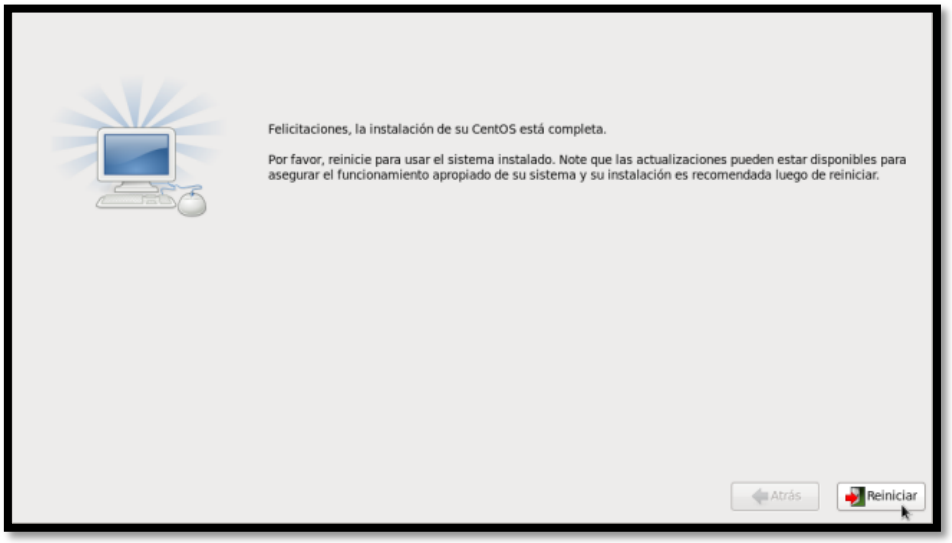


Figura 92. Instalación finalizada de CentOS 6.5
Fuente: CentOS, Captura de la pantalla de la Instalación

ANEXO E2. INSTALACIÓN DE PAQUETES PARA ACCESO REMOTO AL SERVIDOR

Primero se debe actualizar los paquetes por medio del comando. Luego se instala telnet y ssh para el acceso remoto al servidor

```
# yum install update
```

- **Instalar SSH en CentOS**

```
# yum install openssh-server
```

Para que los cambios se realicen y se apliquen, se debe reiniciar el servicio sshd.

```
# service sshd restart
```

- **Instalar TELNET en CentOS**

```
# yum install telnet telnet-server
```

Para que los cambios realizados se apliquen, se debe reiniciar el servicio telnet.

```
# service telnet restart
```

- **Instalar Teamviewer**

Se puede descargar el paquete para las distribuciones Linux basadas en RPM teamviewer_linux.rpm. Dirigiéndose al directorio donde se ha descargado el paquete y ejecutando el siguiente comando yum para instalarlo. Se instala las dependencias que faltan.

```
# wget http://www.teamviewer.com/download/teamviewer_linux.rpm
# yum install teamviewer_linux.rpm
```

ANEXO E3. CONFIGURACIÓN DEL SERVIDOR FIREWALL

- **Configuración de las tarjetas de red.**

    1. **Mediante el siguiente comando se configura la interfaz eth0 y eth1**

gedit /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0

TYPE=Ethernet

ONBOOT=yes

BOOTPROTO=static

IPADDR=190.63.2.66
```

gedit /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=static
IPADDR=192.168.20.1
PREFIX=255.255.255.0
BROADCAST=192.168.20.255
NETWORK=192.168.20.0
```

2. **Se comprueba con el funcionamiento de las tarjetas**

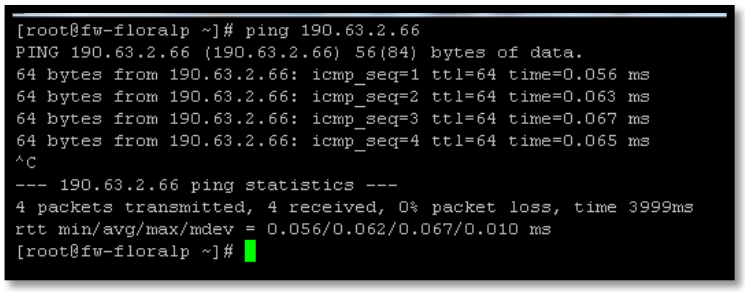


Figura 93. Comprobación de la tarjeta de red
Fuente: Captura de la pantalla del ping a la IP pública

- **Configuración del enrutamiento**

1. **Activar el enrutamiento activando la bandera ip_forward para el tráfico entre interfaces.**

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

2. **Se habilita la comunicación entre las dos tarjetas mediante un puente entre las interfaces**

#Iptables –L –v –n

#iptables -t filter -I FORWARD -i eth0 –o eth1 -j ACCEPT

#iptables -t filter -I FORWARD -i eth1 –o eth0 -j ACCEPT

3. **Se habilita el nateo para la traducción de direcciones IP's mediante las iptables.**

#iptables –L –v –n –t nat

#iptables -t nat -A POSTROUTING -s eth1 –o eth0 –j MASQUERADE

service iptables save

4. **Comprobación del acceso a internet dentro del servidor**

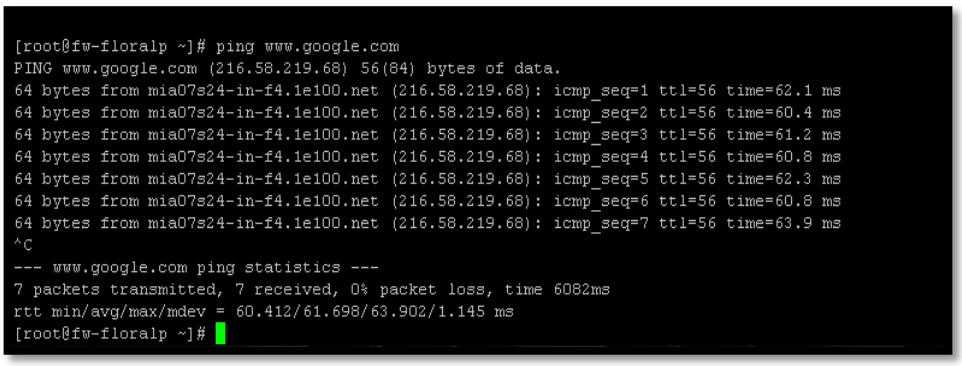


Figura 94. Comprobación de la navegación dentro del servidor

Fuente: Captura de la pantalla del ping a google

- **Configuración del servicio DHCP**

1. **Instalar el paquete dhcp mediante el comando.**

yum -y install dhcp

2. **Se procede a especificar la interfaz que se usa para el servicio dhcp.**

gedit /etc/sysconfig/dhcp

3. **Luego se procede a configurar ciertos parámetros del servicio mediante el comando.**

gedit /etc/dhcp/dhcpd.conf

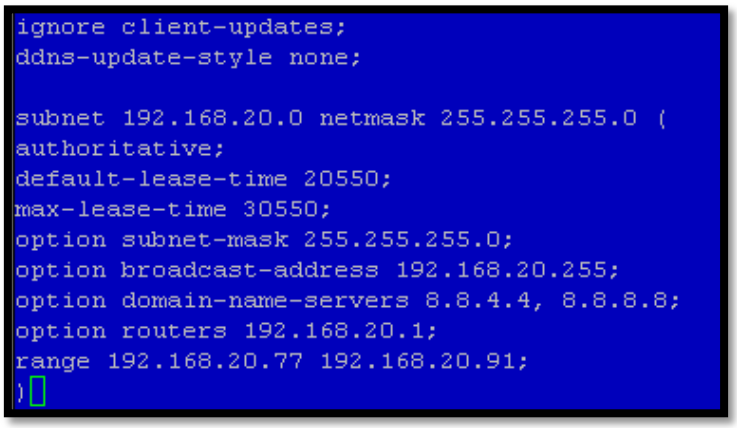


Figura 95.Servicio dhcp
Fuente: Captura de la configuración en CentOS

4. **Iniciar, levantar y revisar el servicio**

#service dhcpd start

chkconfig dhcpd on

#chkconfig dhcpd --list | grep dhcpd

ANEXO E4. CONFIGURACIÓN DEL SERVICIO PROXY

1. **Instalación del servidor proxy mediante el comando**

#yum –y install squid

2. **Editar el archivo de configuración del servidor**

gedit /etc/squid/squid.conf

3. **Activar y desactivar ciertos parámetros**

```
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
# acl localnet src 10.0.0.0/8   # RFC1918 possible internal network
# acl localnet src 172.16.0.0/12        # RFC1918 possible internal network
 acl localnet src 192.168.20.0/24       # RFC1918 possible internal network
# acl localnet src fc00::/7       # RFC 4193 local private network range
# acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines
```

Figura 96. Desactivación Ipv6 y Activación de la red local

Fuente: Captura de la configuración en Squid

```
# Squid normally listens to port 3128
http_port 192.168.20.1:3128 intercept

# We recommend you to use at least the following line.
hierarchy_stoplist cgi-bin ?

# Uncomment and adjust the following to add a disk cache directory.
cache_dir ufs /var/spool/squid 100 16 256
```

Figura 97. Habilitación de la interfaz para Squid

Fuente: Captura de la configuración en Squid

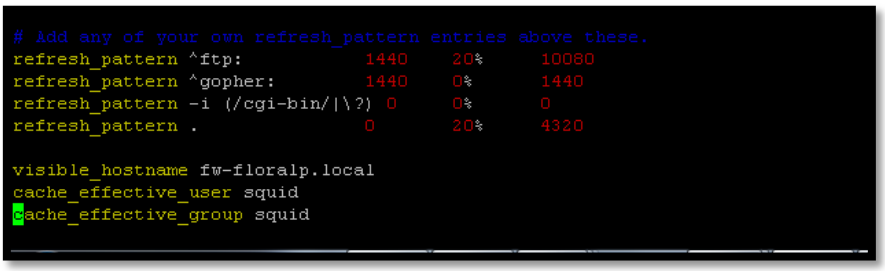


Figura 98.Configuración del nombre, usuario y contraseña para Squid
Fuente: Captura de la configuración en Squid

4. **Verificar el usuario y contraseña de Squid si se encuentra activada con el siguiente comando.**

#cat /etc/passwd | grep squid

#cat /etc/group | grep squid

5. **Luego se le indica al sistema que el servicio se inicie automáticamente cada vez que se reinicie el sistema.**

chkconfig squid on

chkconfig --list | grep squid

6. **A continuación se procede a que todo lo que el puerto 80 escuche se re direccione al puerto del squid al 3128, esto lo realizamos mediante la tabla NAT con iptables. Además permitir que todos los que pertenezcan a la red local se conecten por medio del squid.**

#iptables –t nat –A PREROUTING –s 192.168.20.0/24 –p tcp –-dport 80 –j REDIRECT –-to-port 3128

#iptables –t filter –I INPUT 4 –p tcp –s 192.168.20.0/24 –d 192.168.20.1 –-dport 3128 –j ACCEPT

7. **Guardamos la configuración.**

#service iptables save

ANEXO F. INSTALACIÓN Y CONFIGURACIÓN DE SNORT EN UBUNTU 12.10

1. **Instalación de los siguientes paquetes para los requisitos de SNORT**

```
apt-get install apache2

apt-get install mysql-server
```

2. **Se crea un archivo php llamado info.php utilizando un editor de texto**

```
gedit /var/www/info.php
```

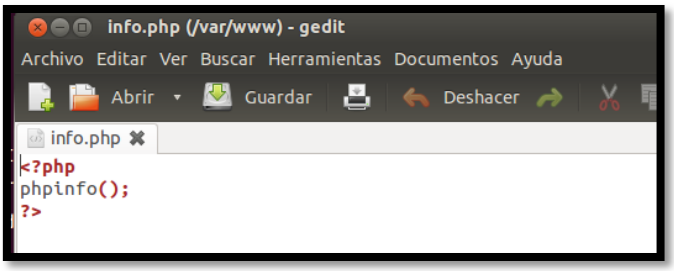


Figura 99.Archivo info.php
Fuente: Ubuntu Recuperado de instalación de Snort

3. **Instalar los paquetes de snort y acidabse**

```
apt-get install snort-mysql snort-doc
```

4. **Luego se define una o múltiples interfaces para la red local**

5. **Se procede a la configuración de acidbase**

- Tipo de base de datos que se va a utilizar en este caso MySQL
- Contraseña de acidbase

6. **Creación de la base de datos snort-mysql**

```
mysql –u root –h localhost –p

create user'snort'@'localhost' identified by

'gaby123';
```

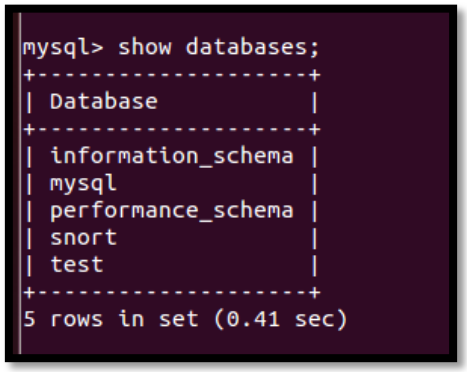


Figura 100. Base de Datos de MySQL
Fuente: Ubuntu Recuperado de instalación de Snort

```
create database snort;

grant all privileges on *.* to

‘snort’@’localhost’;
```

7. Ingresar al directorio

```
cd /usr/share/doc/snort-mysql/
```

8. Se realiza la estructura de la base de datos con el archivo en el directorio.

```
zcat créate_mysql.gz|mysql –u snort –h localhost –pgaby123 snort
```

9. Reconfigurar los paquetes después de su instalación.

```
dpkg-reconfigure –plow snort-mysql
```

10. Se configuran los parámetros de conexión a la base de datos de MySQL

- Método de arranque de Snort
- La interfaz
- El intervalo de direcciones para la red local
- El nombre del servidor de base de datos
- Nombre de la base de datos
- Nombre de usuario para el acceso a las base de datos
- Contraseña para la conexión con la base de datos

11. Reiniciar el paquete snort

```
/etc/init.d/snort restart
```

12. Editar el archivo snort.conf colocando la direcciones de la área local y la configuración de los parámetros de la base de datos MySQL

```
gedit /etc/snort/snort.conf
```

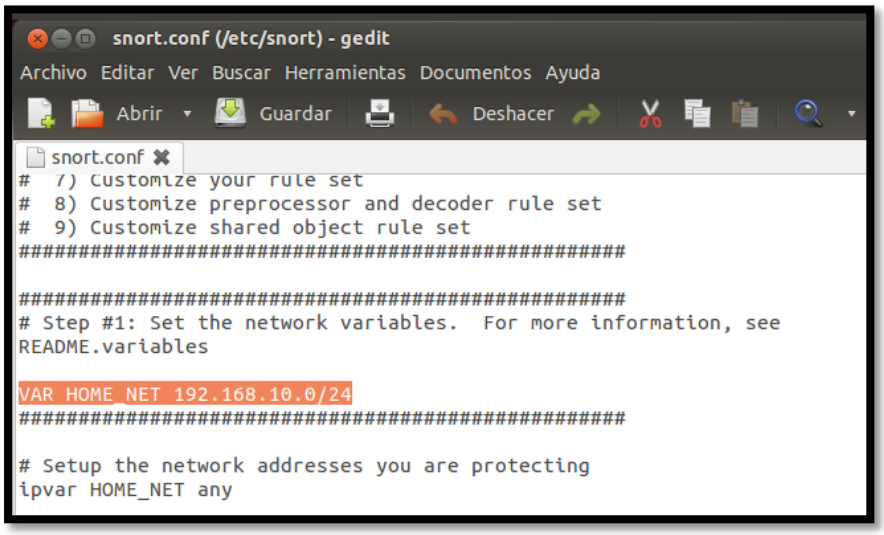


Figura 101. Se modifica el archivo snort.conf

Fuente: Ubuntu Recuperado de instalación de Snort

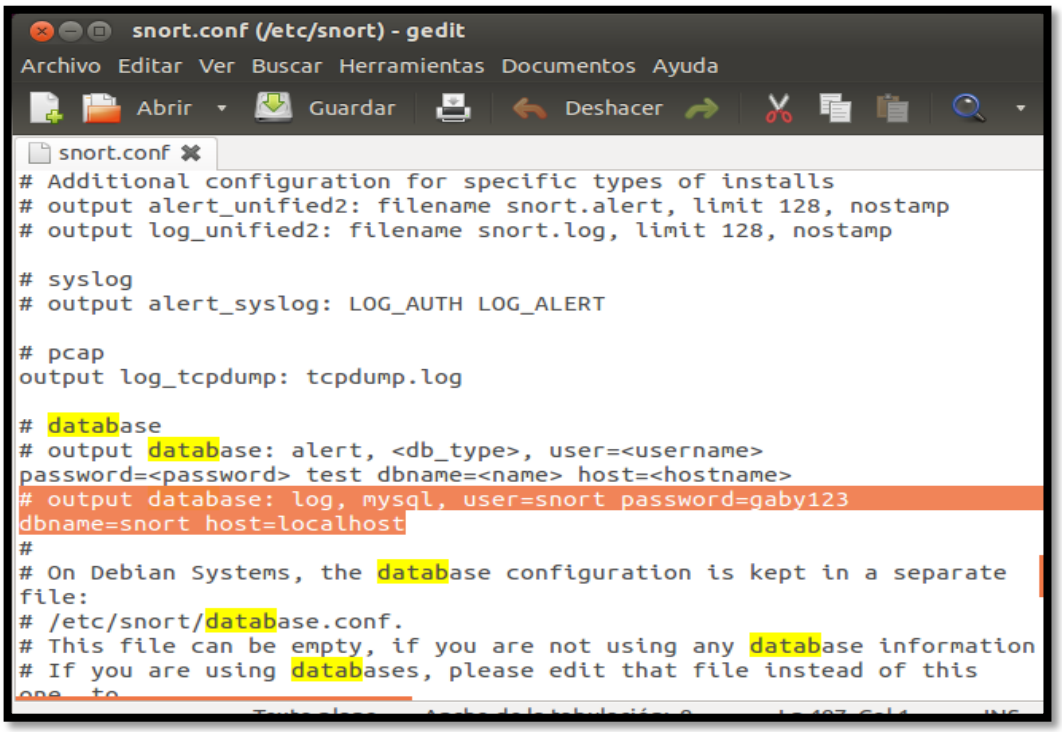


Figura 102. Se modifica el archivo snort.conf con los parámetros de MySQL
Fuente: Ubuntu Recuperado de instalación de Snort

13. Editar el archivo de configuración de database.php donde se ingresa el nombre del servidor y el puerto donde se va a conectar la base de datos.

```
gedit /etc/acidbase/database.php
```

14. Reiniciar los paquetes apache y snort

```
/etc/init.d/apache2 restart

/etc/init.d/snort restart
```

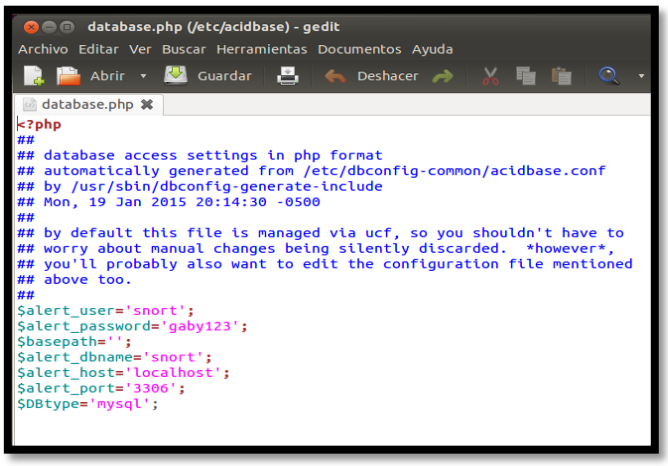


Figura 103. Se edita el archivo database.php
Fuente: Ubuntu Recuperado de instalación de Snort

15. Ingresar a un navegador y cargar la siguiente página

http://localhost//acidbase

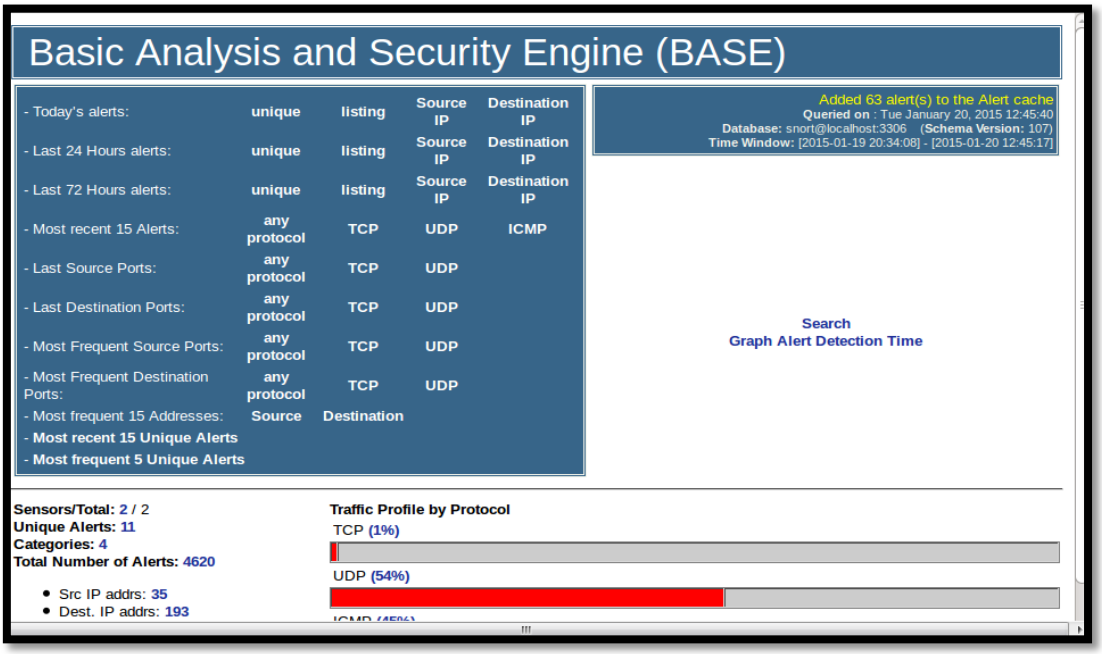


Figura 104.Interfaz gráfica de BASE
Fuente: Ubuntu Recuperado de instalación de Snort

ANEXO G. INSTALACION DEL SOFTWARE DE KALI LINUX

Para iniciar la instalación, arranque elegir una instalación gráfica. A continuación se selecciona el idioma y su país de localización, también permite configurar el teclado.

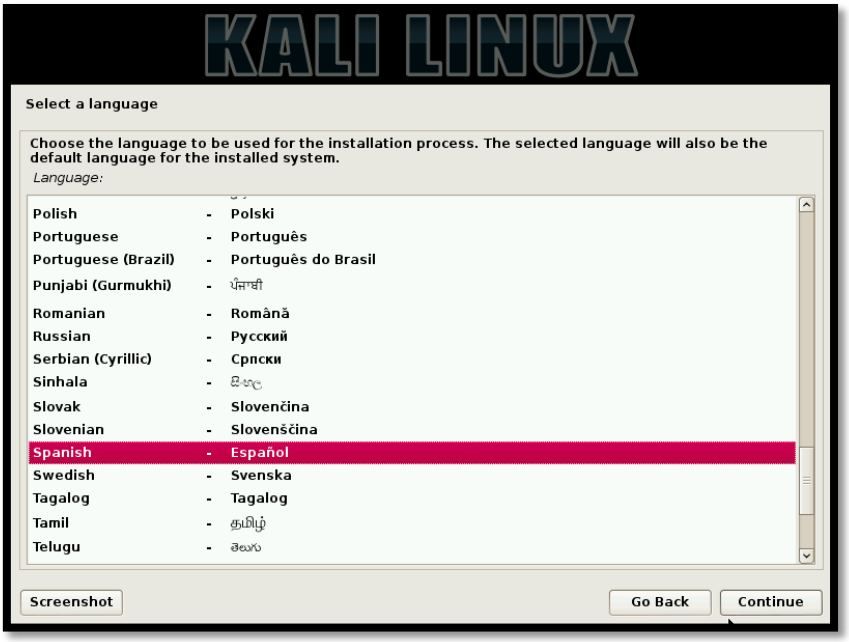


Figura 105. Selección del idioma

Fuente: Captura de pantalla de la Instalación de Kali Linux

El programa de instalación copiará la imagen en su disco duro, probará las interfaces de red, y luego le pedirá que introduzca un nombre y contraseña para el sistema., como se muestra en la siguiente Figura 102.

Figura 106. Ingreso de la contraseña
Fuente: Captura de pantalla de la Instalación de Kali Linux

El instalador prueba sus discos y le ofrece cuatro opciones. En este caso vamos utiliza el disco entero en el ordenador.

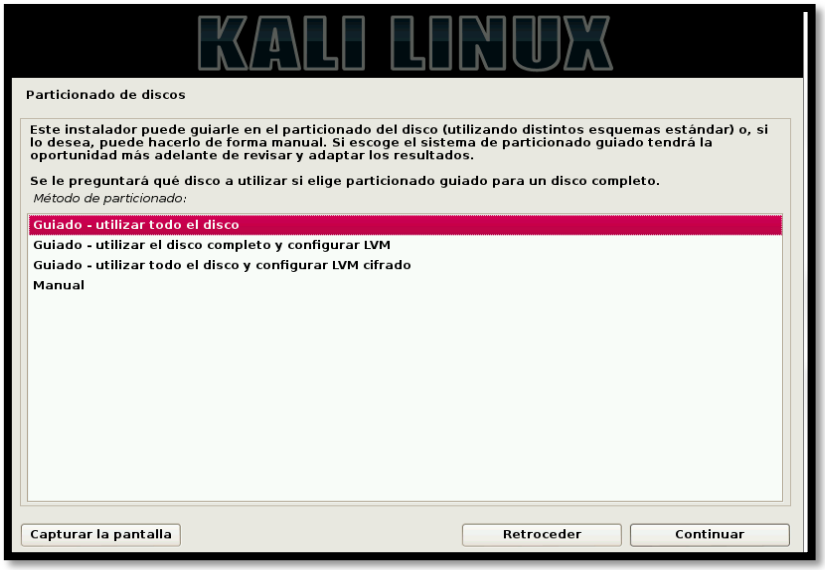


Figura 107. Elección del disco a utilizar
Fuente: Captura de pantalla de la Instalación de Kali Linux

El próximo paso es instalar GRUB, por último, haga clic en Continuar para reiniciar en su nueva instalación de Kali.

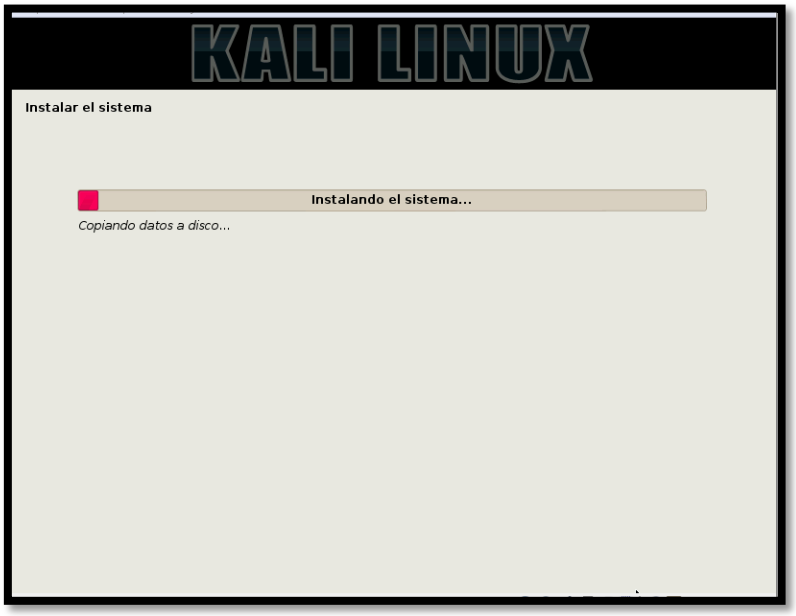


Figura 108. Instalación del sistema Kali Linux
Fuente: Captura de pantalla de la Instalación de Kali Linux

ANEXO H. LISTA DE EMPLEADOS QUE LABORAN DENTRO DE FLORALP

NOMBRE	LOCALIDAD	CARGO
AGUIRRE AGUIRRE LUIS ANTONIO	IBARRA	AYUDANTE DE PRODUCCION
AGUIRRE TOBAR PAOLA ALEXANDRA	IBARRA	ASISTENTE DE CONTABILIDAD
AMAYA MARTINEZ ANA CRISTINA	IBARRA	COORDINADOR ADMINISTRATIVO
ANDRADE MONCAYO DIEGO DARIO	IBARRA	COORDINADOR DE FOMENTO GANADERO
ARAUJO VELASCO JOSE GABRIEL	IBARRA	JEFE DE FOMENTO GANADERO
ARCOS VILLOTA GUIDO MARCELO	IBARRA	AYUDANTE DE PRODUCCION
AUCAY FAJARDO ELIZABETH CRISTINA	IBARRA	ASISTENTE ASEGURAMIENTO DE LA CALIDAD
BARAHONA DAVILA HERNAN XAVIER	IBARRA	JEFE SISTEMAS
BEDON VEGA JULIO CESAR	IBARRA	AYUDANTE DE PRODUCCION
BEJARANO BENITEZ PACA JACKELINE	IBARRA	CONTADOR GENERAL
CABALLERO REINA MESIAS ARTURO	IBARRA	AYUDANTE DE PRODUCCION
CAICEDO LANDAZURI VICTORIA MARIELA	IBARRA	JEFE DE COMPRAS
CARLOSAMA TITUAÑA MIRIAN GRISELA	IBARRA	AYUDANTE DE PRODUCCION
CARTAGENA ONOFRE ANDRES MARCELO	IBARRA	JEFE DE CANAL
CHACHALO AGUILAR JUAN CARLOS	QUITO	AYUDANTE DE BODEGA
CHACHALO AGUILAR SEGUNDO GONZALO	IBARRA	JEFE DE BODEGA DE PRODUCTO TERMINADO

CHACHALO GOMEZ LEONARDO DAVID	IBARRA	AYUDANTE DE PRODUCCION
CHAMORRO PINTO GLADYS MARIELA	IBARRA	AYUDANTE DE PRODUCCION
CHANDI GUERRERO WILMER WILSON	IBARRA	AYUDANTE DE PRODUCCION
CHAVEZ AYALA LIDIA BEATRIZ	IBARRA	AYUDANTE DE PRODUCCION
CLERQUE BENAVIDES DAVID ISRAEL	IBARRA	AYUDANTE DE SUMINISTROS
COLLAGUAZO LLUMIQUINGA EDWIN ANDRES	IBARRA	ASISTENTE DE SISTEMAS
CORRALES QUISTANCHALA LUIS ESTEBAN	IBARRA	ASISTENTE DE CONTABILIDAD
CUASQUI MATANGO ERNESTO MEDARDO	IBARRA	AYUDANTE DE BODEGA
DE LA CRUZ HERRERA HENRY JAVIER	IBARRA	AYUDANTE DE BODEGA
DIAZ LIMAICO EDISON ARMANDO	IBARRA	AYUDANTE DE PRODUCCION
DUARTE CARLOSAMA RICARDO GEOVANNY	IBARRA	AYUDANTE DE BODEGA
ENDARA LOPEZ MARIA ANGELICA	IBARRA	ASISTENTE COMERCIAL
ESCUDERO GALLO ROBERTO CARLOS	IBARRA	ASISTENTE DE MANTENIMIENTO
ESCUDERO GALLO VICTORIA ALEXANDRA	IBARRA	AYUDANTE DE PRODUCCION
ESPINOSA ESPINOSA JUAN MIGUEL	IBARRA	JEFE DE BODEGA CENTRAL
ESPINOZA ESPINOZA MAYRA ALEJANDRA	IBARRA	ASISTENTE DE CONTABILIDAD
FLORES ALBORNOZ RENAN PATRICIO	IBARRA	ASISTENTE DE PRODUCCION
FLORES BUSTAMANTE AIDA MARGOTH	IBARRA	AYUDANTE DE PRODUCCION
FLORES BUSTAMANTE AMALIA JANETH	IBARRA	AYUDANTE DE PRODUCCION

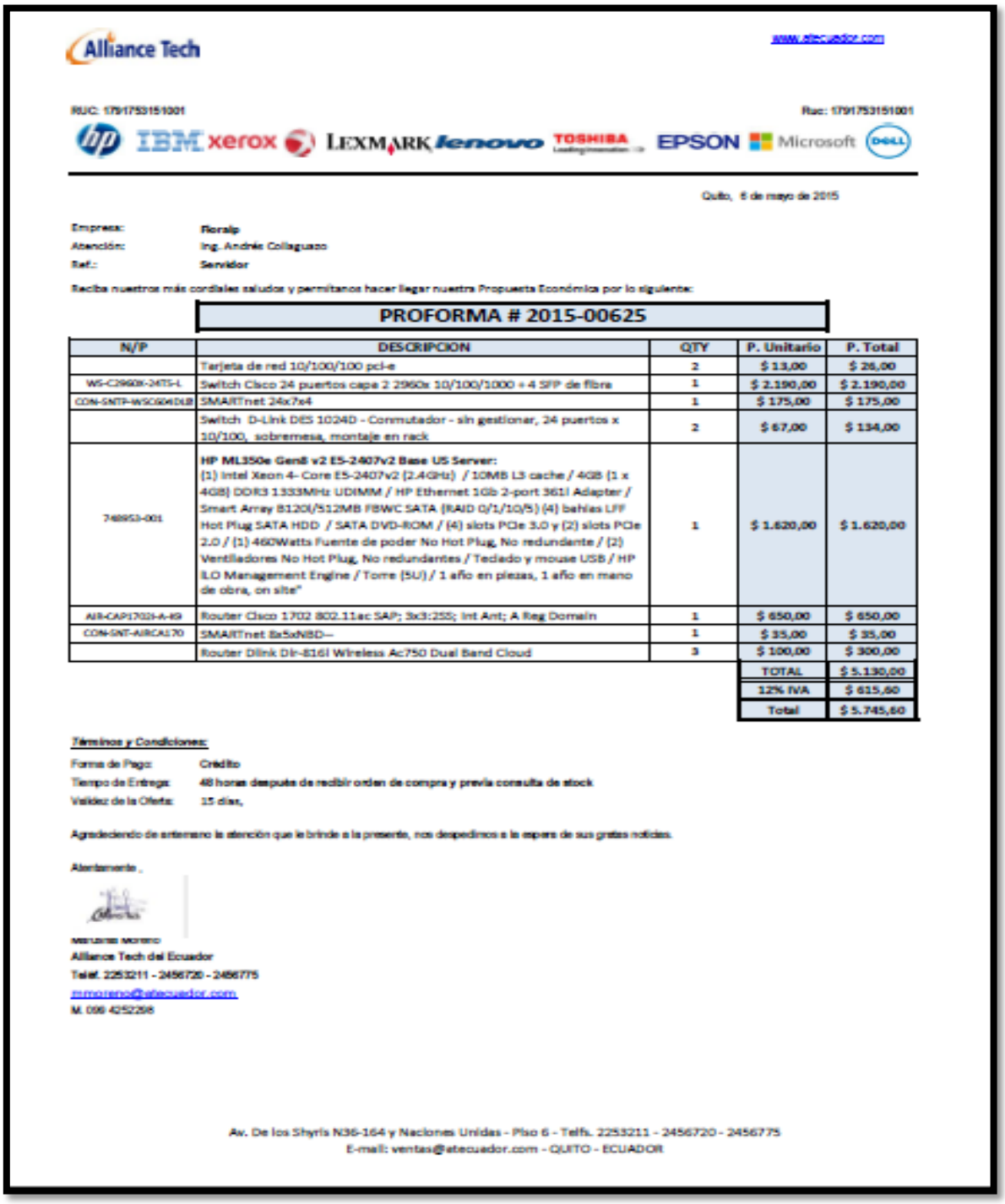
GALARRAGA YEPEZ JENNY ALEXANDRA	IBARRA	AYUDANTE DE PRODUCCION
GALLEGOS SARCO JIMMY FERNANDO	IBARRA	AYUDANTE DE PRODUCCION
GUAMAN CATUCUAMBA JUAN CARLOS	IBARRA	AYUDANTE DE PRODUCCION
GUAMAN MUGMAL JAIME RIGOBERTO	IBARRA	AUXILIAR ADMINISTRATIVO
GUERRA VACA OSCAR GONZALO	IBARRA	AUXILIAR ADMINISTRATIVO
GUERRERO MARTINEZ YURY ANDRES	IBARRA	AUXILIAR ADMINISTRATIVO
HARO HERNANDEZ JIMMY CRISTIAN	IBARRA	AUXILIAR ADMINISTRATIVO
HERNANDEZ ESPINOZA MIGUEL ANGEL	IBARRA	AUXILIAR ADMINISTRATIVO
HERRERIA BASTIDAS FRANCISCO DAVID	IBARRA	ASISTENTE DE MANTENIMIENTO
HURTADO PAGUAY EMILIO JONATHAN	IBARRA	AYUDANTE DE PRODUCCION
IBADANGO RUIZ LORENA SOFIA	IBARRA	AYUDANTE DE PRODUCCION
IBADANGO TABANGO WASHINGTON RUBEN	IBARRA	ASISTENTE DE MANTENIMIENTO
IMBAQUINGO ARTEAGA EVA PILAR	IBARRA	AYUDANTE DE PRODUCCION
INGA PASTAS LUIS FERNANDO	IBARRA	AYUDANTE DE PRODUCCION
LEIVA TUQUERREZ JEFFERSON PATRICIO	IBARRA	AYUDANTE DE PRODUCCION
LEIVA TUQUERREZ JESSICA CRISTINA	IBARRA	AYUDANTE DE PRODUCCION
LOPEZ PORTILLA EDISON NAPOLEON	IBARRA	AYUDANTE DE PRODUCCION
LOZADA MOSCOSO EDGAR PATRICIO	IBARRA	JEFE DE ASEGURAMIENTO DE LA CALIDAD
MARTINEZ ORTIZ MARCELO MIGUEL	IBARRA	AYUDANTE DE PRODUCCION
MELO ASCUNTAR EDUARDO ALONSO	IBARRA	AYUDANTE DE PRODUCCION

MINDA LARA JACOBO FAUSTO	IBARRA	ASISTENTE ASEGURAMIENTO DE LA CALIDAD
MOLINA TAPIA JAIME NEPTALI	IBARRA	AYUDANTE DE SUMINISTROS
MOROCHO MUENALA MAURO PATRICIO	IBARRA	AYUDANTE DE PRODUCCION
OBANDO HINOJOSA MARCO VINICIO	IBARRA	AYUDANTE DE PRODUCCION
OBANDO HINOJOSA MILTON PACO	IBARRA	AYUDANTE DE PRODUCCION
OBANDO REASCOS LUIS MARCELO	IBARRA	AYUDANTE DE PRODUCCION
ORDOÑEZ ALVAREZ RICARDO JAVIER	IBARRA	AYUDANTE DE PRODUCCION
ORELLANA MORILLO LUIS FERNANDO	IBARRA	GERENCIA FINANCIERO
PALACIOS AREVALO ALEJANDRO PAUL	IBARRA	AYUDANTE DE PRODUCCION
PAREDES PEPINOSA JHONATHAN ANDRES	IBARRA	AYUDANTE DE PRODUCCION
PASPUEL SARZOSA GUILLERMO BLADIMIRO	IBARRA	AYUDANTE DE PRODUCCION
PEREZ MUÑOZ EDISON ROLANDO	IBARRA	AYUDANTE DE PRODUCCION
PEREZ PUERRES ELMER IVAN	IBARRA	ASISTENTE DE CONTABILIDAD
PINEDA ARIAS PAMELA IVONNE	IBARRA	AYUDANTE DE PRODUCCION
PINEDA HERRERA MILTON RAUL	IBARRA	AYUDANTE DE PRODUCCION
PINTO AYALA LUIS MIGUEL	IBARRA	AYUDANTE DE PRODUCCION
PIÑAN LIMAICO CRISTIAN GERARDO	IBARRA	AYUDANTE DE PRODUCCION
PIÑAN PONCE JUAN MARCELO	IBARRA	AYUDANTE DE PRODUCCION
PLACENCIA AYALA DIEGO XAVIER	IBARRA	AYUDANTE DE PRODUCCION
PLACENCIA FERNANDEZ ROBERTO CARLOS	IBARRA	ASISTENTE DE BODEGA
PLACENCIA MONTENEGRO CRISTIAN	IBARRA	AYUDANTE DE BODEGA

POZO CHIRAN JOSE ALEJANDRO	IBARRA	AYUDANTE DE BODEGA
PROAÑO PERUGACHI NELSON RAMIRO	IBARRA	AYUDANTE DE BODEGA
PUCHA CUJI CARMEN DOLORES	IBARRA	LABORATORISTA
PUPIALES SERRANO NESTOR WILLAN	IBARRA	AYUDANTE DE PRODUCCION
PURTSCHERT BARAHONA JOAQUIN	IBARRA	JEFE DE INVESTIGACION Y DESARROLLO
PURTSCHERT HEUBI MATHIAS	IBARRA	GERENCIA DE PRODUCCION
PURTSCHERT HOLLENSTEIN NORBERTO XAVIER	IBARRA	GERENCIA GENERAL
PUSDA GUAMAN FREDDY ALEXANDER	IBARRA	AYUDANTE DE PRODUCCION
QUELAL VALENCIA BRANDON FABRICIO	IBARRA	AYUDANTE DE PRODUCCION
QUINTANA DIAZ WILMER FELIPE	IBARRA	AYUDANTE DE PRODUCCION
QUIROZ POZO JHON CRISTIAN	IBARRA	AYUDANTE DE PRODUCCION
REINOSO BENAVIDES MAURICIO RAMIRO	IBARRA	ASISTENTE DE PRODUCCION
RUIZ BENALCAZAR CECILIA ELIZABETH	IBARRA	REBANADORA
RUIZ FLORES CRISTIAN SANTIAGO	IBARRA	ASISNTENTE DE BODEGA
SALCEDO PLAZAS AYRTON ANDRES	IBARRA	ASISTENTE DE PRODUCCION
SANCHEZ SANDOVAL JAIME RAMIRO	IBARRA	QUESERO
SANDOVAL CHECA SILVIA ROSARIO	IBARRA	JEFE DE PLANTA
SIMBAÑA QUINCHE CESAR RODRIGO	IBARRA	AYUDANTE DE PRODUCCION
TAPIA MARROQUIN JONATHAN JAVIER	IBARRA	ASISTENTE DE MANTENIMIENTO
TITO ANDRADE OMAR FERNANDO	IBARRA	JEFE MANTENIMIENTO
TIXICURO TIXICURO MARIA TRANSITO	IBARRA	ASISTENTE DE MANTENIMIENTO

TORRES PORTILLA ROLANDO SANTIAGO	IBARRA	AYUDANTE DE PRODUCCION
TUPE MITES VICTOR ORLANDO	IBARRA	AYUDANTE DE PRODUCCION
VACA AGUIRRE MARIA PAULINA	IBARRA	ASISTENTE DTH
VARELA MANTILLA VIVIANA ROCIO	IBARRA	AYUDANTE DE PRODUCCION
VERA VIVERO DANIEL ELIAS	IBARRA	AYUDANTE DE BODEGA
VILLARREAL HIGUERA GRACIELA	IBARRA	REBANADORA
YACELGA ARAQUE EDISON ANTONIO	IBARRA	ASISTENTE DE PRODUCCION
YAR MORILLO ALEXANDRA CARMITA	IBARRA	ASISTENTE DE PRODUCCION
YAR PEREZ FERLEY EDISON	IBARRA	AYUDANTE DE PRODUCCION
ZAMBRANO ANAGALLO VICTOR ANDRES	IBARRA	AYUDANTE DE PRODUCCION
ZAMBRANO AYALA DARWIN WLADIMIR	IBARRA	AYUDANTE DE PRODUCCION

ANEXO I. PROFORMAS DE EQUIPOS



Alliance Tech

www.atecuador.com

RUC: 1791753151001 Ruc: 1791753151001

Quito, 6 de mayo de 2015

Empresa: Floralp
Atención: Ing. Andrés Collaguazo
Ref.: Servidor

Reciba nuestros más cordiales saludos y permítanos hacer llegar nuestra Propuesta Económica por lo siguiente:

PROFORMA # 2015-00625

N/P	DESCRIPCION	QTY	P. Unitario	P. Total
	Tarjeta de red 10/100/100 pci-e	2	$ 13,00	$ 26,00
WS-C2960X-24TS-L	Switch Cisco 24 puertos capa 2 2960x 10/100/1000 + 4 SFP de fibra	1	$ 2.190,00	$ 2.190,00
CON-SNTP-WSC960LB	SMARTnet 24x7x4	1	$ 175,00	$ 175,00
	Switch D-Link DES 1024D - Conmutador - sin gestionar, 24 puertos x 10/100, sobremesa, montaje en rack	2	$ 67,00	$ 134,00
748953-001	**HP ML350e Gen8 v2 E5-2407v2 Base US Server:** (1) Intel Xeon 4- Core E5-2407v2 (2.4GHz) / 10MB L3 cache / 4GB (1 x 4GB) DDR3 1333MHz UDIMM / HP Ethernet 1Gb 2-port 361i Adapter / Smart Array B120i/512MB FBWC SATA (RAID 0/1/10/5) (4) bahías LFF Hot Plug SATA HDD / SATA DVD-ROM / (4) slots PCIe 3.0 y (2) slots PCIe 2.0 / (1) 460Watts Fuente de poder No Hot Plug, No redundante / (2) Ventiladores No Hot Plug, No redundantes / Teclado y mouse USB / HP ILO Management Engine / Torre (5U) / 1 año en piezas, 1 año en mano de obra, on site"	1	$ 1.620,00	$ 1.620,00
AIR-CAP1702I-A-K9	Router Cisco 1702 802.11ac SAP; 3x3:2SS; Int Ant; A Reg Domain	1	$ 650,00	$ 650,00
CON-SNT-AIRCA170	SMARTnet 8x5xNBD--	1	$ 35,00	$ 35,00
	Router Dlink Dir-816l Wireless Ac750 Dual Band Cloud	3	$ 100,00	$ 300,00
			TOTAL	$ 5.130,00
			12% IVA	$ 615,60
			Total	$ 5.745,60

Términos y Condiciones:

Forma de Pago: Crédito
Tiempo de Entrega: 48 horas después de recibir orden de compra y previa consulta de stock
Validez de la Oferta: 15 días,

Agradeciendo de antemano la atención que le brinde a la presente, nos despedimos a la espera de sus gratas noticias.

Atentamente ,

Alliance Tech del Ecuador
Telef. 2253211 - 2456720 - 2456775
mmoreno@atecuador.com
M. 099 4252258

Av. De los Shyris N36-164 y Naciones Unidas - Piso 6 - Telfs. 2253211 - 2456720 - 2456775
E-mail: ventas@atecuador.com - QUITO - ECUADOR

Re: Proformas de equipos

Eduardo Chuquizán (echuquizan@tecnit.com.ec) Agregar a contactos 28/04/2015

Para: Gabriela López

Abajo los precios solicitados

TARJETA DE RED D-LINK DGE-560T PCI-E GIGABIT 10/100/1000 $ 30,00 + IVA (para PC)
TARJETA DE RED GIGABIT ETHERNET 10/100/1000 Mbps PCI EXPRESS x1 HP $ 89,00 + IVA (para Server)
SWITCH CISCO CATALYST WS-C2960-48TC-S ADMINISTRABLE L2 DE 48 PUERTOS 10/100 + 2 PUERTOS GIGABIT O SFP $1272.00 + IVA
SWITCH D-LINK DES-1024A DE 24 PUERTOS 10/100 DE ESCRITORIO $ 64,00 + IVA
SERVER HP Proliant ML350 GEN9 E5-2620v3 2.4GHZ, MEMORIA 16GB, NO DISCOS, P440 8SFF, FUENTE 500W $3490,00 + IVA
ROUTER WIRELESS N CISCO SMB RV180W VPN FIREWALL GIGABIT $314.00 + IVA
ROUTER WIRELESS N TP-LINK WR841ND DOS ANTENAS 300Mbps $ 50,00 + IVA

Validez de la oferta: 15 días o hasta agotar stock
Forma de pago: 100% contra entrega
Tiempo de entrega: Inmediata previa confirmación de stock
Garantía: Contra defectos de fabricación

Saludos cordiales,

EDUARDO CHUQUIZÁN | ASESOR COMERCIAL |echuquizan@tecnit.com.ec | TECNIT

elf. 02 - 332 0 332 / 332 0 177 / 332 0 178 | Cell: C 099 7338686 M-WhatsApp 0987803802