ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN REDES Y COMUNICACIÓN DE DATOS

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO ELECTRÓNICO EN REDES Y COMUNICACIÓN DE DATOS

AUTOR: EDGAR RUBÉN PILACUÁN ERAZO

TEMA: IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL PARA LA EMPRESA TEAMSOURCING CÍA. LTDA. CON SOFTWARE LIBRE (CLEAROS) Y DESARROLLO DE LAS POLÍTICAS DE SEGURIDAD BASADAS EN EL ESTÁNDAR ISO-27001.

DIRECTOR: ING. CARLOS ROMERO

CODIRECTOR: ING. FABIÁN SÁENZ

SANGOLQUÍ - ECUADOR

2015

CERTIFICACIÓN

UNIVERSIDAD DE LAS FUERZAS ARMADAS

ESPE

INGENIERÍA ELECTRÓNICA EN REDES Y COMUNICACIÓN DE DATOS

Ing. Carlos Romero

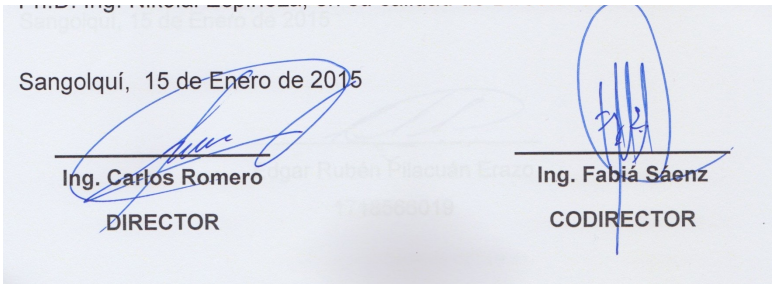
Ing. Fabián Sáenz

CERTIFICAN

Que el trabajo titulado "**Implementación de un sistema de seguridad perimetral para la empresa TeamSourcing cía. ltda. con software libre (ClearOS) y desarrollo de las políticas de seguridad basadas en el estándar iso-27001.**", realizado por Edgar Rubén Erazo Pilacuán, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas.

Debido a que se trata de un trabajo de investigación recomiendan su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a Edgar Rubén Erazo Pilacuán que lo entregue al Ph.D. Ing. Nikolai Espinoza, en su calidad de Director de la Carrera.



UNIVERSIDAD DE LAS FUERZAS ARMADAS

ESPE

INGENIERÍA ELECTRÓNICA EN REDES Y COMUNICACIÓN DE DATOS

DECLARACIÓN DE RESPONSABILIDAD

EDGAR RUBÉN PILACUÁN ERAZO

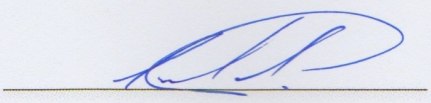
DECLARO QUE:

El proyecto de grado denominado "**Implementación de un sistema de seguridad perimetral para la empresa TeamSourcing Cía. Ltda. con software libre (ClearOS) y desarrollo de las políticas de seguridad basadas en el estándar iso-27001.**", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan al pie, de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 05 de Enero de 2015



Edgar Rubén Pilacuán Erazo

1718566019

UNIVERSIDAD DE LAS FUERZAS ARMADAS
ESPE

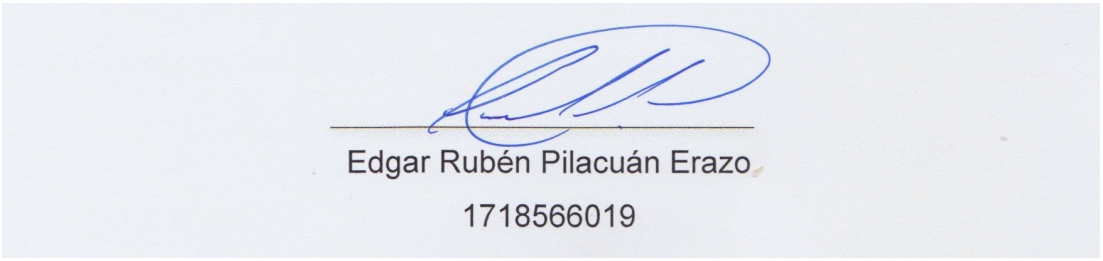
INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

AUTORIZACIÓN

Yo, Edgar Rubén Pilacuán Erazo

Autorizo a la UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE, la publicación, en la biblioteca virtual de la Institución del trabajo "Implementación de un sistema de seguridad perimetral para la empresa TeamSourcing Cía. Ltda. con software libre (ClearOS) y desarrollo de las políticas de seguridad basadas en el estándar iso-27001.**", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría**

Sangolquí, 05 de Enero de 2015



DEDICATORIA

Dedico esta proyecto de una manera especial a mis padres, Sabina y Pedro, quienes con su esfuerzo han sabido ofrecernos todo lo que nos haga falta a mi y a mis hermanas, a Dios por siempre mantenernos juntos como familia, a Johanna y Nicolás las personas más importantes del resto de mi vida y a mis Profesores y amigos de la ESPE, quienes fueron un baluarte fundamental durante todo este proceso.

AGRADECIMIENTO

Agradezco infinitamente a Dios por brindarme la oportunidad de estudiar esta carrera, a mis padres que siempre me dieron ánimos y aliento para nunca darme por vencido bajo ningún obstáculo y a mis hermanas quienes hemos pasados momentos buenos y malos pero siempre nos hemos dado una mano.

Gracias por siempre estar a mi lado Johanna, gracias por darme un hijo tan hermoso, gracias por ser paciente y por comprender cada una de mis actitudes, gracias infinitas por siempre hacerme feliz, y a ti Nicolás por venir a complementar nuestras vidas, se que algún día elegirás ser alguien de bien y q contribuirás a hacer de este lugar un mundo mejor con tu conocimiento, espero que elijas ser Ingeniero, pero si no lo haces, te apoyaré en lo que decidas ser, Te Amo Hijo.

Muchas gracias a mis amigos de toda la vida, Edison, José Luis, Roberto, Karla, Carlos, Alex, Stalin, Juan, Paúl, Mauricio, y especialmente a Julio, quien a más de siempre ser un buen amigo me ha dado una lección de vida, y espero que nunca cesen sus ganas de vivir.

GRACIAS TOTALES

Edgar.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ECUACIONES

RESUMEN

El presente proyecto tiene como fin el desarrollo de las Políticas de la Seguridad de la Información basadas en el estándar ISO 27001, para las áreas donde la seguridad de la información siempre debe mantener los principios de, Disponibilidad, Confidencialidad e Integridad, las cuales han sido aplicadas según la realidad de la empresa TeamSourcing .Cía. Ltda.Para lo cual se ha implementado un software firewall, Open Source, llamado ClearOS , el cual es muy utilizado en pequeñas y medianas empresas, con alrededor de 100 a 150 usuarios o dispositivos, y no están en la capacidad o no tienen como objetivo del negocio destinar muchos recursos a dispositivos de conectividad pero que desean mantener su red de una manera ordenada y completamente administrable, además de tener distintas funcionalidades que serán de mucha ayuda en la administración y mantenimiento de una red local teniendo como premisas las políticas antes descritas y manteniendo la seguridad de la información cada día menos expuesta a vulnerabilidades de usuarios internos y externos. Recordemos que no hay método para mantener la seguridad total, pero si podemos hacer los esfuerzos posibles para mantenerla los más segura posible.

PALABRAS CLAVE:
1. ClearOS
2. ISO 27001
3. Open
4. Source, Políticas de Seguridad Perimetral
5. Software firewall.

ABSTRACT

This project is aimed at develop the Advancement of Information Security based on ISO 27001 standard, for areas where information security must always upholding the principles, Availability, Confidentiality and Integrity, which have been applied according to the reality of the company TeamSourcing .Cía. Ltda. For which we have implemented a firewall software, Open Source, called ClearOS, which is widely used in small and medium enterprises, with around 100-150 users or devices, and are not in the capacity or are not intended business spend significant resources to connectivity devices but want to maintain their network in an orderly and fully managed way, besides having different functionalities that will be very helpful in managing and maintaining a local network having premised policies described above and keeping the information security each day vulnerabilities less exposed to internal and external users. Remember that no method to maintain total security, but if we can make the effort to maintain the safest possible.

KEYWORDS:
1. ClearOS
2. ISO 27001
3. Open
4. Source, Perimeter Security Policy
5. Software firewall.

1. CAPÍTULO I
Aspectos Generales.

1.1. Introducción.

En la actualidad en todas las organizaciones o empresas las redes de datos se han convertido en puntos clave de análisis y de desarrollo para estas, por lo que se invierte gran cantidad de tiempo y dinero en la capacidad que tengan de ser eficientes o robustas, así como en la capacidad de desempeño y funcionalidad que puedan tener, también se debe tomar muy en cuenta la tolerancia latente a fallos y los sistemas de seguridad a implementarse para no ser víctimas de intrusos, ataques, etc.

Las soluciones para proteger una red son diversas, empezando desde: proxies, IDS_1 , sistemas de actualizaciones automáticas de software, sistemas de administración y control para monitorear la seguridad y firewalls, este último con la capacidad de permitir o denegar el paso de paquetes a la red de datos, en otras palabras, es un dispositivo, un equipo o un sistema, que delimita dos redes, que cifra y descifra el trafico de diferentes ámbitos en base a normas y criterios.

El firewall o cortafuegos, como tecnología nace con la internet en cuanto a su uso global y de conectividad a finales de los años 1980, cuyos predecesores fueron los routers utilizados a finales de esta década, que mantenían las redes separadas unas de otras. La valoración de a internet como una comunidad pequeña de usuarios con máquinas compatibles para el intercambio y colaboración de información, terminó con una cantidad de violaciones a la privacidad del internet

Como se denotó antes, los predecesores del Firewall son routers, los cuales separaban únicamente las redes unas de otras, pero también existieron otros tipo de dispositivos, los cuales citaremos a continuación:

- Nivel de Aplicación de Pasarela:

Aplica mecanismos de seguridad para aplicaciones específicas, tales como FTP o Telnet, lo cual puede ser eficaz, pero también degrada su rendimiento.

- Circuito a nivel de Pasarela

Aplica mecanismos de seguridad cuando una conexión TCP o UDP esta ya establecida, es decir, una vez que la conexión se ha establecido los paquetes pueden fluir sin más control entre los anfitriones.

- Cortafuegos de capa de redo de filtrados de paquetes.

Funciona a nivel de la capa de Red del protocolo TCP/IP, como filtro de paquetes IP.

- Cortafuegos de capa de Aplicación.

Trabaja en el nivel de aplicación, de manera que los filtros se pueden adaptar de mejor manera a las características propias de los protocolos de este nivel.

- Cortafuegos personal.

Se lo llama personal, ya que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red. (Rivas, 2010)

Hoy en día todas las empresas sean estas pequeñas empresas están o deberían estar protegidas por un firewall en su red de datos, de manera tal que esta pueda ser más confiable y robusta, de lo contrario, esta se vería con una debilidad durante algún ataque de una persona u organización mal intencionada, en la búsqueda de acceder a información que puede ser sensible y relevante para la empresa.

1.2. Antecedentes

La Empresa TeamSourcing Cía. Ltda., es una organización integradora de servicios móviles, la cual a través de tecnologías como USSD, IVR, SMS, APR, NFC y MMS, oferta servicios no solo dedicados al entretenimiento y descargas móviles, sino también ofrece servicios como: M. Commerce (Transferencias, pagos y consultas de cuentas o tarjetas de crédito a través del celular), M. Camping(Permite acceder a productos, catálogos o promociones desde su celular), M. Loyalty (Obtiene reportes en línea de lo que está sucediendo con los negocios desde el móvil), Mobitrans (Plataformas transaccionales móviles para operadoras móviles, MVNOs o integradores brinda un valor agregado, apoyándoles en sus transacciones de cobro y en las transacciones de entrega de contenido), LBS (Ubica los recursos, clientes o servicios con el uso del celular a través de la localización), M. Social (Permite acceder a Redes Sociales desde cualquier teléfono móvil y sin necesidad de internet).

TeamSourcing Cía. Ltda. ha desarrollado la más completa plataforma móvil de servicios que permiten a las empresas comunicar, investigar y comercializar a través de canales móviles de gran penetración. (TeamSourcing, 2014)

La red interna de TeamSourcing Cía. Ltda., está conformada aproximadamente por 150 hosts, compuesta de computadores personales, de escritorio, teléfonos celulares, tablets e IPs dedicadas exclusivamente para teléfonos IP. Los cuales están actualmente administrados por el software de distribución libre Elastix (asterisk).

Vyatta es un sistema operativo open source para routers y firewals basado en GNU/Linux (Debian).

Se ejecuta en arquitecturas x86 y proporciona funciones avanzadas de networking. Todas las funciones son configuradas y administradas a través de una CLI de estilo Cisco, en el cual se ha configurado algunas

funcionalidades útiles para la empresa, como son las IPs para extensiones telefónicas a las distintas áreas que lo necesitan, así como también a las personas encargadas de Call-Center. Se han creado 4 de subredes diferenciadas según el área en las que están asociadas de la siguiente manera: (Matamala, 2012)

Tabla 1. Distribución de host

Interfaz	IP	Departamento	# de host
ETH0_EQUIPOS	192.168.60.0	EQUIPOS	19
ETH0_ADM	192.168.61.0	ADMINISTRATIVOS	38
ETH0_CC	192.168.62.0	OTROS	6
ETH0_IT	192.168.63.0	IT	92
Total de hosts			155

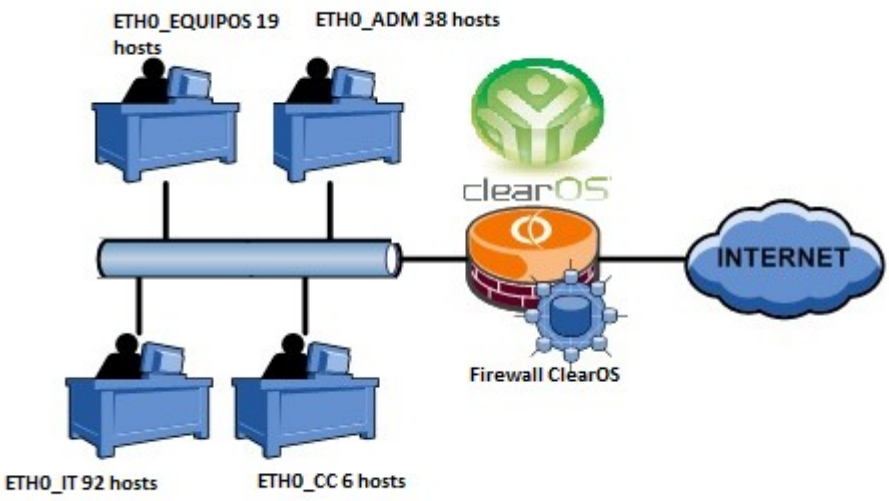


Figura 1. Distribución de usuarios por áreas

Estas distribuciones se han creado siguiendo ciertos parámetros como son: el tipo de usuarios, tipo de tráfico de datos que van a tener los usuarios, el ancho de banda y las restricciones de páginas web que se necesiten.

Actualmente mantenemos problemas en la configuración y distribución del servicio de DHCP, para que la conexión funcione debemos hacer lo siguiente

Primero, se debe realizar un registro de dirección MAC en una dirección ip libre en el software Vyatta.
Segundo, en el host se debe asignar estáticamente la dirección ip, máscara y DNSs principal y secundarios de la subred correspondiente al software Vyatta.
Debido a que no es suficiente que el host se registre con la clave al Acces Point correspondiente.
Se mantienen muchos problemas de virus, los que en su mayoría son adquiridos por los usuarios del área comercial o administrativa, los cuales se los puede contrarrestar, con el escaneo de virus y spam que viene integrado con ClearOS.
Actualmente se mantiene una Estructura de Red, en donde los cambios que se realicen se deben hacer con mucho cuidado, así como, inserción de IPs duplicadas, o de equivocaciones tales como dobles puntos o comas, ya que por ser Vyatta manejado a través de una interfaz por consola, se cometen mayores errores debido a usuarios inexpertos o errores accidentales, que pueden entorpecer el correcto funcionamiento de la distribución del internet.

Las redes de datos son un conjunto de computadoras o dispositivos de comunicaciones que se comunican entre si a través de un medio particular.
También podemos definir a las redes de datos como sistemas que se diseñan y construyen en arquitecturas con el fin de ser más eficientes en sus objetivos de uso, hablando de la parte física de cómo llevar los paquetes de datos de una red a otra, se necesita tener una conectividad entre estos enlaces, los cuales pueden ser los principales puntos de falla o puntos débiles si algún motivo fallo llegase a pasar o se pueda deshabilitar.

El ideal dentro de una red de datos, es que debe de ser lo suficientemente robusta, para soportar cualquier eventualidad, pero yendo a la parte real y suponiendo nuestro diseño como “ideal” se encuentran brechas o puntos de falla que pueden ser creados por nosotros, la solución consiste en por lo menos en estos llamados puntos de falla, mantenerlos lo más protegidos

posible, tanto a nivel físico como también en el resto de niveles de la arquitectura TCP/IP, por lo que se podrá tener una información que recorre a través de nuestra red siempre disponible, sin errores y lo más fluida posible.

ISO 27001.

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total que es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (PriteshGupta.com, 2012)

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

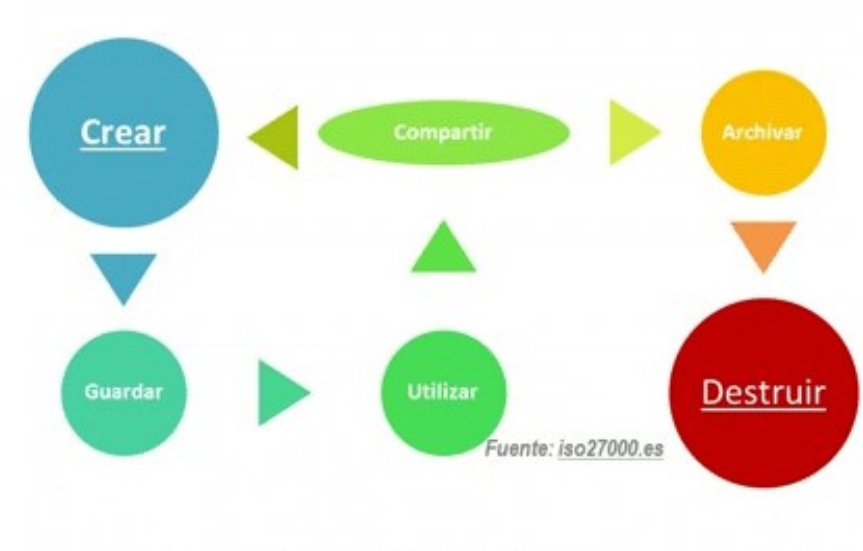


Figura 2 Ciclo de Vida para garantizar el C-I-D

Fuente: (iso27000.es)

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI. (PriteshGupta.com, 2012)

1.3. Justificación.

Se requiere desarrollar un modelo de seguridad perimetral de la red LAN de la empresa, el en cual se desea implementar los siguientes lineamientos establecidos en el Estándar ISO-2700.

- Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas.
- Eventos de seguridad de la información: Ocurrencia de un evento identificado sobre un sistema, servicio o red, cuyo estado indica una posible brecha en la política de seguridad de la información o fallo en el almacenamiento de la misma, también cualquier situación previa desconocida que pueda ser relevante desde el punto de vista de la seguridad.
- Incidente de seguridad: uno o varios eventos de seguridad de la información, no deseada o inesperada que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazan a la seguridad de la información.
- Sistema de administración de la seguridad de la información (ISMS: Information Security Management System). Parte de los sistemas de la empresa, basado en el análisis de riesgo de negocio, cuya finalidad es establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información.

NOTA: el ISMS incluye las políticas, planes, actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

- Integridad: Propiedad de salvaguardar la precisión y completitud de los recursos.
- Riesgo residual: El riesgo remanente luego de una amenaza a la seguridad.
- Aceptación de riesgo: Decisión de aceptar un riesgo.
- Análisis de riesgos: Uso sistemático de la información para identificar fuentes y estimar riesgos.
- Valoración de riesgo: Totalidad de los procesos de análisis y evaluación de riesgo.

- Evaluación de riesgo: Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de significativo del riesgo. (Corletti, 2006)

Dichos lineamientos del estándar ISO-27001 estarán sujetos a las necesidades de nuestra red corporativa, que en la actualidad tiene algunas características que citaremos a continuación:

- No existen reglas de la correcta repartición del Ancho de Banda, por lo que, descargas muy grandes en ocasiones roban el ancho de banda destinado a la conexión vis ssh a los servidores para trabajar sobre ellos o sobre los servidores de base de datos.
- Mala distribución del servicio de DHCP, ya que para que esto en realidad suceda, es necesario hacer un registro previo en el firewall en el que coincidan IP y dirección MAC.
- No se tiene detección de virus o intrusiones a través de firewall, actualmente, se ha instalado un antivirus en cada computador de escritorio o personal de la empresa, pero no se está protegido a nivel de computadores portátiles de visitantes, a través de teléfonos celulares y tablets.
- No existe una configuración estable, que prohíba la utilización de páginas web, que no están relacionadas con el ambiente laboral y que restrinja el acceso a ciertos funcionarios de la empresa.
- La falta de un ambiente gráfico en el manejo del software Vyatta, dificulta la revisión de las configuraciones existentes con las configuraciones futuras.
- La distribución de subredes creadas actualmente, no funcionan correctamente, debido a la mala asignación del pool de direcciones.

La importancia de los servicios que se brindan en una red corporativa y el avance del software, han permitido desarrollar sistemas operativos que se pueden levantar a un bajo costo, mismos que dotarían a la red de

funcionalidades, de redundancia y alta disponibilidad, tal es el caso del software desarrollado por la organización ClearOS, de Clear Fundation, el cual funciona en arquitecturas x86 y proporciona funciones avanzadas de networking, el cual tiene similares características a los equipos Cisco pero a costos inferiores. ClearOS mantiene una plataforma libre así como versión de pago, la cual se diferencia de la comercial tan solo por el soporte que ofrecen los técnicos de esta organización. (Clear Foundation, 2014)

Algunas de las ventajas o funcionalidades que tiene el software ClearOS, son:

- Escaneo de virus y spam a través de la pasarela de paso para tráfico http así como imap, pop y smtp (parecido al plugin copfilter de ipcop).
- Filtrado de contenidos/protocolos a través de proxy de una manera realmente fácil y rápida.
- Firewall sencillo con detección de intrusiones.
- Servidor LDAP con autenticación de SAMBA (muy fácilmente configurable).
- Sistema de impresión (CUPS) y recursos compartidos (sistema de ficheros e impresoras) a través de SAMBA.
- Servidor FTP (ProFTPD), WEB (apache 2 con módulo de php) y MySQL con administración a través del proyecto phpMyAdmin.
- Servidor de correo electrónico (postfix), con soporte de captura de correo de otras cuentas (maildrop), SMTP, POP y WebMail.
- Sistema de Backup de configuración del servidor (tanto local como remota en el servidor del proyecto).
- Informes de logs sobre cada uno de los servicios. (Garcia, 2012)

Todas estas funcionalidades serán muy útiles para TeamSourcing Cía. Ltda., ya que se necesita tener énfasis específico en las características relacionadas con el escaneo de virus, filtrado de contenidos/protocolos a través de proxy, detección de intrusiones y el informe de logs de cada uno de los servicios instalados, al momento no se tiene ninguno de estos servicios o

se podría optimizar características del software Vyatta con mejores resultados.

Se desea definir una normativa de Seguridad de la Información basada en el estándar ISO-27001 la cual define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privados o públicos, pequeños o grandes.

1.4. Fundamento teórico.

1.4.1. Introducción

En toda empresa las redes de datos se han convertido en uno de los puntos más relevantes de su funcionamiento, por tal motivo las mismas deben tener grandes capacidades de desempeño y funcionalidad, a la par de ser tolerante a fallos y mantener sistemas de seguridad que la mantengan protegida de intrusos o ataques.

Las maneras de mantener protegida a una red son diversas, y una de estas es haciendo uso de un Firewall, el cual es un sistema diseñado para permitir o denegar el paso de paquetes a través de la red de datos, es decir, se define como un sistema que delimita la conexión entre dos redes, el cual cifra y descifra el tráfico entre redes de distintos ámbitos, a partir de diferentes criterios y normas.

“Mientras el internet se establecía como servicio global en los años 80 surge la tecnología firewall, inicia con los routers establecidos a finales de esta década, como predecesores de los firewall actualmente para seguridad de redes, ya que mantenían las redes separadas, esto terminó debido a grandes violaciones de seguridad por medio de internet realizadas a finales de los años 80 tales violaciones fueron:

- “Clifford Stoll, que descubrió la forma de manipular el sistema de espionaje alemán.
- Bill Cheswick, cuando en 1992 instaló una cárcel simple electrónica para observar a un atacante.
- En 1988, un empleado del Centro de Investigación Ames de la NASA, en California, envió una nota por correo electrónico a sus colegas que decía: “Estamos bajo el ataque de un virus de Internet! Ha llegado a Berkeley, UC San Diego, Lawrence Livermore, Stanford y la NASA Ames."

El Gusano Morris, que se extendió a través de múltiples vulnerabilidades en las máquinas de la época. Aunque no era malicioso, el gusano Morris fue el primer ataque a gran escala sobre la seguridad en Internet; la red no esperaba ni estaba preparada para hacer frente a su ataque.”

- Primera generación – firewall de red: filtrado de paquetes

El primer firewall desarrollado fue de tipo de filtrado de paquetes en 1988 por el equipo de ingenieros de Digital Equipment Corporation (DEC).

Este firewall actúa mediante una inspección de los paquetes, es decir si un paquete coincide con el conjunto básico de reglas de filtro el paquete será descartado o rechazado.
Se filtra cada paquete basándose únicamente en la información contenida en el paquete en sí. Los protocolos TCP y UDP comprenden la mayor parte de comunicación a través de Internet, utilizando por convención puertos bien conocidos para determinados tipos de tráfico, por lo que un filtro de paquetes puede distinguir entre ambos tipos de tráfico. El filtrado de paquetes llevado a cabo por un firewall y este actúa en las tres primeras capas del modelo de referencia OSI..

- Segunda generación – firewall de estado

Durante 1989 y 1990, tres colegas de los laboratorios AT&T Bell, Dave Presetto, Janardan Sharma, y Nigam Kshitij, desarrollaron la tercera generación de servidores de seguridad. Esta tercera generación cortafuegos tiene en cuenta además la colocación de cada paquete individual dentro de una serie de paquetes. Esta tecnología se conoce generalmente como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por el firewall, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo. Este tipo de cortafuegos pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

- Tercera generación - cortafuegos de aplicación

Son aquellos que actúan sobre la capa de aplicación del modelo OSI. La clave de un firewall de aplicación es que puede entender ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.”

Acontecimientos posteriores

En 1992, Bob Braden y DeSchon Annette, de la Universidad del Sur de California (USC), dan forma al concepto de firewall. Su producto, conocido como "Visas", fue el primer sistema con una interfaz gráfica con colores e iconos, fácil de implementar y compatible con sistemas operativos como Windows de Microsoft o MacOS de Apple. En 1994.

La funcionalidad existente de inspección profunda de paquetes en los actuales cortafuegos puede ser compartida por los sistemas de prevención de intrusiones (IPS).

Otro de los ejes de desarrollo consiste en integrar la identidad de los usuarios dentro del conjunto de reglas del firewall. Algunos firewall proporcionan características tales como unir a las identidades de usuario con

las direcciones IP o MAC. Otros, como el firewall NuFW, proporcionan características de identificación real solicitando la firma del usuario para cada conexión. (Rojas, 2013)

1.4.1. Redes de datos

1.4.1.1. Conceptos

Concepto etimológico: “En concreto, podemos establecer la siguiente información al respecto:

- Red, procede del latín. Más exactamente emana del vocablo “rete”, que es sinónimo de malla.
- Datos. Esta palabra es fruto de la evolución de la palabra latina “datum”, que puede traducirse como “dado”.”

Una red de datos se constituye de una serie de elementos, (ordenadores, routers, switch, Access point, dispositivos móviles, etc.), son autónomos y están interconectados entre sí por medios físicos y lógicos y que están en la capacidad de compartir recursos.

“Una red es una estructura que cuenta con un patrón característico. Puede hacer referencia a la interconexión de computadoras y otros dispositivos que comparten recursos.

Dato es un término que indica una información, un documento o un testimonio que permite alcanzar un conocimiento o deducir las consecuencias legítimas de un hecho.

Se conoce como red de datos a la infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos. Cada una de estas redes ha sido diseñada específicamente para satisfacer sus objetivos, con una arquitectura determinada para facilitar el intercambio de los contenidos.

No obstante, no podemos pasar por alto tampoco que una red de datos se pone también en funcionamiento con otros dos objetivos primordiales:

compartir tanto el software como el hardware y otorgarle soporte y centralización a la administración pertinente.

De la misma manera, al llevarla a cabo se logra mejorar notablemente la rapidez y fiabilidad del intercambio de información y reducir costes en la empresa o entidad que decida crearla.

Cuando hablamos de una red de datos, hay que tener en cuenta que ella debe contar con una serie de elementos fundamentales para que pueda entenderse como tal y también para que ejerza sus funciones sin problemas:

• Servidores, que vienen a ser como los administradores de la información y de todo el proceso en sí.

• Pach Panel´s, que son los sistemas que se encargan de organizar todo el cableado necesario.

• Hubs, que proceden a acometer lo que sería la amplificación de las señales que toman protagonismo en ese intercambio de información.

Los cables conocidos como Pach Cord o el conocido como cableado de tipo horizontal son otras de las propuestas que también cobran protagonismo en una red de datos.

Por lo general, estas redes se basan en la conmutación de paquetes. Pueden clasificarse de distintas maneras de acuerdo a la arquitectura física, el tamaño y la distancia cubierta.

De acuerdo a su alcance, una red de datos puede ser considerada como una red de área personal (Personal Area Network o PAN), red de área local (LAN), red de área metropolitana (MAN) o una red de área amplia (WAN), entre otros tipos.

Una red PAN es aquella red que interconecta computadoras situadas cerca de una persona, mientras que una red LAN favorece el intercambio de datos en una zona pequeña (como una oficina o un edificio).

La red MAN, por su parte, brinda una cobertura en un área geográfica extensa y la red WAN, en un área geográfica aún más extensa. Esto quiere

decir que una red de datos WAN permitirá compartir datos en una superficie de gran extensión.” (Definicion.de , 2014)

1.4.1.2. Seguridad Perimetral

Un sistema de seguridad perimetral tiene por premisa la protección de todo el sistema informático desde el exterior, es decir, colocar una coraza que proteja todos los elementos sensibles de ser vulnerados, sean estos: datos, configuraciones, accesos, etc.
Esto quiere decir que todo el tráfico que vaya a fluir por nuestra red, previamente debe de ser analizados, aceptado o rechazado en función de las reglas que hayamos previsto para determinar el potencial riesgo de seguridad para nuestra red.

Historia

En un inicio la seguridad en redes estaba orientada y concentrada directamente en las host, y es muy lógico suponer esto, ya que estos eran quienes concentraban todos los servicios del sistema de una empresa. Tanto los archivos, como la ejecución de archivos se mantenían concentrados en este sistema, por lo que los usuarios únicamente disponían de un Terminal que les permitía ejecutar, mediante un sistema de transferencia, aplicaciones entre el Terminal y el sistema central y para esto la persona encargada de velar por la seguridad de red, se dedicaba a asegurar que el sistema central estuviera protegido del ataque de intrusos desde afuera y debido a que antes la infraestructura de comunicación se basaba en conexiones punto – punto, esta labor resultaba bastante sencilla, además también de tener en cuenta otro de los puntos críticos, como lo son las líneas de comunicación por MODEM, de los ataques maliciosos, los cuales consistían en averiguar el número de teléfono desde el cual se conectaban, e introducir los datos correctos de autenticación

En los años 80 además de los servidores el administrados de la red también tenía que estar preocupado del recientemente aparecido ordenador personal y las redes LAN, lo que conllevaba que los puntos críticos aumentaban a cada uno de los terminales de la red de datos, aplicaciones y la capacidad de ejecutar código maligno en sus sistemas, el cual, en su mayoría se propagaba través de disquetes o a finales de esta década en CD-ROM, para quienes la solución más óptima era con un antivirus que se actualizaba regularmente con el envío de un e-mail para mantener la integridad del sistema.

En los 90 las actualizaciones de los antivirus se realizaban mediante una conexión a internet, cada 2 días, ya que surgen los sistemas personales, provocando que los puntos críticos de una red se comiencen a multiplicar, cada usuario con un modem y con conexión a internet es un riesgo potencial para el sistema.
A mediados de esta misma década se hacen cada vez más populares los sistemas de conexión mediante proxies o routers que permitían a todos los usuarios de la red el acceso a internet; esto da una gran ventaja a los usuarios finales, pero su administración cada vez se convierte en un gran reto debido a la necesidad de mantener la red libre de ataques, virus y demás vulnerabilidades.

Los nuevos retos de la seguridad en redes.

En la actualidad debido al gran auge de internautas y diversidad de terminales que tienen la posibilidad de una conexión a internet, la vulnerabilidad de un sistema a ser atacado por ese creador de virus o ese hacker que ahora por ende tiene más medios para poder acceder a sistemas remotos. Tomemos en cuenta que la internet ahora no solo se dedica a ser una biblioteca inmensa de conocimientos, sino que además se ha convertido en un gran grupo de personas que mantienen una estrecha colaboración en conocer vulnerabilidades de los sistemas y aplicaciones.

Estas colaboraciones se materializan en páginas web de cómo atacar sistemas, cursos paso a paso de creación de virus que solo detallen texto plano de todo lo tipiado desde que se instaló o de como descifrar claves de Acces Ponit con seguridades bajas. Esto ha llevado a los administradores a pasar de ser simples usuarios avanzados que conoce los posibles ataque a ejercer una labor de análisis de vulnerabilidades y configuración de sistemas antes de que estos ataques se produzcan, y disponer una serie de planes de contingencia en caso de que estos se produzcan y hacer que los puntos críticos de una red sean los menos posibles.

Tipos de ataques

Problemas relacionados con ataques externos

Los ataques externos sobe todo en el sector de las Pymes donde el responsable de informática, cuando es preguntado sobre los problemas relacionados con hackers y otros problemas relacionado con un hacker y otros problemas de seguridad, la respuesta es “no tenemos información que pueda interesar a nadie”. Este es el más grave de los errores a darse, debido a que un hacker no le interesa la información dichamente de la empresa, sino el acceder a la plataforma y utilizarla para el ataque desde ahí a otros sistemas, o a su vez como un sistema de almacenamiento de aplicaciones o servicios ilegales, como un ejemplo puede ser que dicho hacker logró acceder a nuestros servicios de ftp o www, para almacenar pornografía o software ilegal, si no tenemos un control de archivos y/o directorios de nuestro sistema los accesos a través de la red. Con esto, un hacker experimentado, después de haber explotado al nuestros servicios de ftp o www, simplemente con que tenga la capacidad de ejecutar un ataque desde nuestro sistema hacia el de nuestros clientes, los responsables de los otros sistemas afectados podrán exigirnos responsabilidades como consecuencias de estos ataques.

Otros tipos de hackers, llamados “experimentales”, después de ir descubriendo paso a paso a que tiene acceso y cual es su alcance final en su momento deciden experimentar estos conocimientos sin conocer las

consecuencias deciden ejecutar programas o virus que pueden afectar o parar nuestro sistema y esto implique tener que reinstalar aplicaciones y servicios para que el sistema pueda estar operativo de nuevo, además de que dichos virus pueden borrar información del sistema, o borrar todo el disco duro, o bien enviar mails repetitivos con virus hacía nuestra agenda de contactos, lo que puede dar una mala imagen a nuestra empresa y resultar en desconfianza de la misma y pérdidas económicas.

Problemas relacionados con ataques internos.

Uno de los temas menos tratados en seguridad de la información, es la seguridad interna, para lo cuales los administradores de la red se limitan a establecer una serie de criterios para la creación de carpetas o discos de acceso restringido y caves de usuario, las cuales es el principal problema de seguridad la información en cuestiones seguridad interna. Pero en sí el principal problema de seguridad interna es la propagación de claves, las cuales se pueden prostituir debido a un manejo obsoleto de estas, para lo cual existen dos posibilidades, una que la clave sea muy complicada y que la una persona que entre en reemplazo de otra tenga que anotarla, ya sea en un papel o en un documento de texto, o que sea muy fácil, que contenga los nombres o placas de autos sus marcas y sean sencillas de recordar para cualquiera.

Otras de las vulnerabilidades típicas es la posibilidad de instalación de programas bajados de internet, los cuales pueden ser programas limpiadores de archivos que son promocionales por quince días, juegos, wallpapers, los cuales se ofrecen de manera gratuita con el afán de que justo a esto se bajen virus o programas que el funcionamiento de sus equipos personales baje su rendimiento.

El reto de mantener una política de seguridad adecuada.

El reto de las políticas de seguridad dentro de una empresa, es que se mantengan o funcionen de una manera proactiva, es decir, mediante una evaluación de riesgos el administrador tendrá que evaluar los riesgos de seguridad para poder prevenirlos antes de que estos se produzcan, y para esto la única forma de hacerlo es revisar los puntos críticos del sistema y protegerlos.

Los puntos críticos como ya hemos citado se encuentran en el perímetro de nuestra red, por lo que podemos enumerar los siguientes:

- Accesos a internet.

La medida más eficiente para proteger los accesos de a internet consiste en la implementación de un firewall, el cual es muy efectivo si este incorpora la opción de IDP (intrusión, detección and prevención), pero en sí para mantener un control todavía más eficaz, la mejor opción es tener un acceso a Internet único, por lo que para los otros accesos es preferible tener una vpn entre todas ellas e impedir el acceso a internet desde las mismas, de esa forma tendremos un solo acceso a internet que nos permitirá tener un control más exhaustivo de los que pasa por nuestra red.

Como segunda medida es recomendable incorporar un segundo firewall, y con configuración o tecnología diferente al primero, así si alguien logra ingresar al primero y es un hacker que conoce las vulnerabilidades del primer sistema podrá atravesar la primera barrera, pero para la segunda no, con lo cual podremos detectarlo antes de detectar daños, puesto que al ingresar al segundo firewall necesitará puertos, servicios o herramientas que no deberían estar libres en esta zona protegida, y nos dará más tiempo antes de que pueda romperlo, y así poder atajarlo.

- Accesos remotos.

En estos casos es indispensable evitar los accesos remotos vía modem, ya que cualquier usuario con un poco de conocimientos podría ser capaz de averiguar el número de teléfono, y de ser el caso de necesitar accesos remotos, las mejor opción es el uso de VPNs y cambiar sus claves de encriptación habitualmente, estas claves deben ser cambiadas con un

software de encriptación previo, es decir, que si nuestra clave es: “mi clave”, este software, la encriptará y nosotros podremos repetirla varias veces, pero en la encriptación siempre se verán caracteres diferentes. La longitud y robustez de las claves que utilicen los usuarios es también algo muy importante de analizar para este tipo de accesos, para lo cual se deberá tener claves que cumplan con combinación de caracteres alfanuméricos, y distinción de mayúsculas y minúsculas, además de bloquear dichas claves al término de un cierto número de intentos erróneos.

- Usuarios.

En el caso de los usuarios el cambio de claves se conservan los mismos criterios de longitud y complejidad de claves personales, además de no hacerlas públicas hacia otros miembros de la empresa.

Se debe también tomar en cuenta los dispositivos como CD o USBs que en ciertas ocasiones son utilizados para extraer información hacia el equipo que podría conllevar virus o programas que afecten al entorno de la red, por lo que se debe evitar la instalación de aplicaciones de terceros, esta medida se la debe aplicar tanto para aplicaciones de ofimática y de gestión habituales de la empresa, como a las soluciones de seguridad y de acceso a red.

- Medidas protectoras internas.

En las reglas del firewall deben estar definidos los departamentos de nuestra empresa, ya que algunos tienen información más sensible que otros, y contemplar la posibilidad de instalar servidores separados, de tal forma que la comunicación entre departamentos se las realicen a través del firewall con reglas definidas, con el objetivo de que los únicos protocolos que van a pasar a través de la red interna, sean los necesarios para poder usar los servicios de bases de datos, aplicaciones internas, etc.

Fiabilidad y disponibilidad.

La fiabilidad o confiabilidad en las redes de datos pueden traducirse en una serie de parámetros de calidad, tales como errores, pérdidas, retardos y otros. La calidad como continuidad operativa de las redes y por ende de los servicios, es quizás, el enfoque más importante al momento de establecer medidas de dicha calidad frente al cliente y a la vez, el más complicado de definir por su condición variable aleatoria y de las expectativas del cliente.
Típicamente se habla e confiabilidad o fiabilidad, performance, disponibilidad, MTBF, MTTR, etc., el gran dilema es establecer la definición de estos parámetros y llevarlos a mediciones prácticas y hacer un buen uso y comprensión de ellos. No se debe mezclar todo en un mismo nivel, es decir, no se puede reunir en un mismo nivel los conceptos de degradación, mejora continua, mantenimiento de la red y confiablidad-disponibilidad, se debe crear una conciencia de que la confiabilidad viene dada por la calidad de la ingeniería de diseño y construcción de las redes.

Típicamente se ha descrito, para equipos y sistemas, que la confiabilidad esperada, obedece a una tendencia de fallas que sigue un comportamiento en el tiempo, en una función que se le denomina la curva de la bañera, la cual es una gráfica que representa los incidentes de falla durante el período de vida útil. Se llama así porque tiene la forma una bañera. En ella se pueden apreciar tres etapas:

Mortalidad temprana.- Se caracteriza por tener una elevada tasa de fallas que desciende rápidamente con el tiempo. Estas fallas pueden deberse a diferentes razones como equipos defectuosos, instalaciones incorrectas, errores de diseño del equipo, desconocimiento del equipo por parte de los operadores o desconocimiento del procedimiento adecuado.
Vida útil.- Con una tasa de errores menor y constante. Las fallas no se producen debido a causas inherentes al equipo, sino por causas aleatorias externas. Estas causas pueden ser accidentes fortuitos, mala operación, condiciones inadecuadas u otros.

Envejecimiento.- caracterizada por una tasa de desperfectos rápidamente creciente. Las fallas se producen por desgaste natural del equipo debido al transcurso del tiempo: cumple su vida útil como activo.

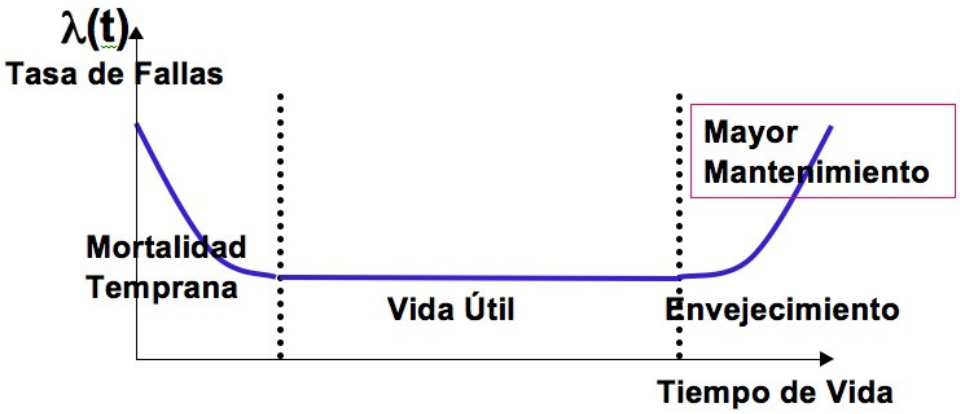


Figura 3. Curva de la bañera, representa los incidentes de falla durante el período de vida útil.

Fuente: (Apablaza, Calidad de redes y servicios de telecomunicaciones., 2011)

Confiabilidad, Disponibilidad y Mantenibilidad

Como ya se ha mencionado, confiabilidad y disponibilidad van de la mano de la mantenibilidad, la cual es el proceso de recuperación desde un estado de falla y extensión o aseguramiento de la vida útil del activo.

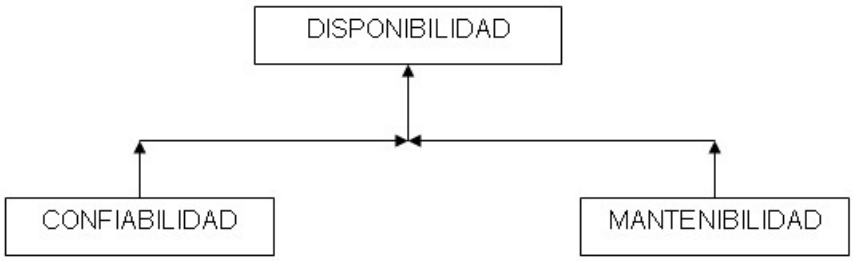


Figura 4. Disponibilidad de la red.

Fuente: (Apablaza, Calidad de redes y servicios de telecomunicaciones., 2011)

El mantenimiento se puede clasificar en distintos tipos, según sus objetivos. Desde el punto de vista de la confiabilidad, ésta tiene por objeto recuperar o asegurar la operatividad del sistema, esto se consigue en forma preventiva o correctiva. Preventivamente, conociendo las perspectivas de probabilidad

de falla, a medida que se acerca el instante de tiempo predicho por las curvas de confiabilidad, debiera aplicarse el mantenimiento para no caer imprevistamente en una indisponibilidad. Obviamente un mantenimiento correctivo, que corrige una imperfección, que ha llevado a un equipo o sistema a no prestar adecuadamente los servicios esperados de él, está recuperando su nueva puesta en servicio, es decir, es un nuevo tiempo inicial para las curvas de confiabilidad, pero con nueva pendiente, debido a que seguramente persistirán algunas condiciones de envejecimiento.

Desde el punto de vista de las estadísticas de disponibilidad, se excluyen los eventos de interrupción programada por mantenimiento, ya que una intervención bien programada y planificada, evitará la interrupción de servicios, o bien, podrá acordar con los usuarios un tiempo de interrupción controlado.

La mantenibilidad se define también como “la probabilidad de que un equipo que ha fallado pueda ser reparado dentro de un período de tiempo dado”. Existen equipos cuya operación es continua a lo largo del tiempo, por lo tanto, si el equipo está fuera de servicio es la falla, pero si el proceso de operación indica que el equipo está sujeto a un intervalo de tiempo prefijado (o eventual, como un grupo electrógeno de respaldo) de funcionamiento y de “descanso”, entonces, en estos intervalos, cuando el sistema está apagado, se le puede efectuar el mantenimiento preventivo o programado y se considera que falla sólo cuando se requiere de su servicio y no funciona.

La mantenibilidad se interpreta etimológicamente como la acción de mantener y conservar los sistemas. Cuando se habla de sistemas continuos, una acción es el trabajo efectuado para corregir o reparar una falla.

Generalizando, mantenimiento es el conjunto de todas las acciones que tienden a reponer las condiciones operativas iniciales del sistema, el mantenimiento aumenta la disponibilidad del sistema, pero requiere

accesibilidad del sistema para permitir el mantenimiento. En el lenguaje común se usa indistintamente el término mantenimiento o mantención.

La Posibilidad de Mantenimiento, es la aptitud de un dispositivo, en condiciones especificadas de uso, a ser conservado o repuesto en un estado, en el cual pueda efectuar las funciones requeridas, cuando el mantenimiento se efectúa en condiciones preestablecidas y usando los procedimientos y medios descritos. Se mide mediante la tasa de reparabilidad.

Tipos de mantenimiento.

Siempre que se formaliza el estudio de alguna área del conocimiento, se intentan clasificaciones, así se encuentra una taxonomía del mantenimiento o mantención, según se puede ver en el diagrama de la próxima figura.

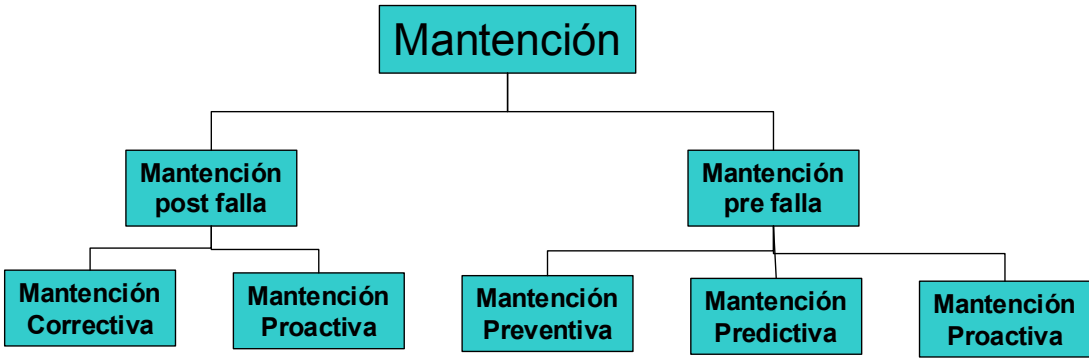


Figura 5. Tipos de mantenimiento que se pueden implementar.

Fuente: (Apablaza, Calidad de redes y servicios de telecomunicaciones., 2011)

Estas formas de mantenimiento, sin duda, son una orientación de clasificación según su oportunidad en el tiempo, la mantención preventiva es sistemática y programada; la predictiva está centrada en la condición de operatividad del elemento, mientras la mantención proactiva está para evitar la aparición o recurrencia de las fallas, y la mantención correctiva viene luego de una falla, y es la mas comúnmente ejercida por razones obvias, y a la vez la que exige un nivel de estrés mayor.

Mantenimiento correctivo: tipo tradicional, es la acción de mantenimiento (reparación) que se efectúa después de la aparición de la falla. El tiempo de reparación puede ser largo porque está ligado a la individualización y diagnóstico de la falla. Afecta a este tiempo también la existencia de repuestos in-situ, como así los tiempos de traslado, sobre todo en telecomunicaciones, en que existe una gran dispersión geográfica de las instalaciones. Con base al conocimiento de la tasa de falla, puede realizarse un dimensionamiento del stock de repuestos de almacén sí esta tasa es elevada se necesitan muchos repuestos

El diagnóstico es un conjunto de técnicas aptas para evaluar el estado de un sistema y también prever que pueda surgir la falla. Es la etapa crítica para la restitución del sistema defectuoso. Requiere de personal con mucha experiencia, con habilidades de deducción, rapidez de interrelacionar experiencias anteriores y toma de decisiones acertadas. Es útil predisponer de técnicas diagnósticas de falla para reduce tiempos y costos de mantenimiento, pero agrega costos de sensores, transductores, sistemas de supervisión y gestión remota de las configuraciones, y software de sistemas expertos, que ayudan al auto diagnosis.

Mantenimiento preventivo: el componente es sustituido antes de que falle, cuando se prevé que está entrando en periodo de fallas por desgaste. La acción de mantenimiento es efectuada en tiempos prefijados (time-based maintenance), se aprovechan los momentos en los que no se requiere la disponibilidad del sistema, su tiempo de activación es de duración inferior, respecto del mantenimiento correctivo. La disponibilidad crece, a condición de que se logre, con un buen control de calidad, utilizar para la sustitución dispositivos con tasa de falla constante o estable (es decir privados de fallas infantiles). En electrónica de telecomunicaciones es complejo ejercer este tipo de mantención pues en envejecimiento o desgaste no es tan manifiesto como en dispositivos mecánicos.

La definición de los objetivos del mantenimiento, debiera definirse en la etapa de proyecto, así como la elección del tipo de mantenimiento (correctivo o preventivo) para establecer la condición óptima para alcanzar los niveles de confiabilidad preestablecida en el diseño. Es necesario poder determinar los tiempos requeridos en horas hombre, para cada una de las fases de mantenimiento, lo mismo que el desarrollo de la documentación técnica que incluya el plan logístico de intervención.

Con el tiempo, la estrategia de mantenimiento ha evolucionado, se propende al mínimo costo de reparación, máxima disponibilidad operativa, mínimo costo de usuario. Se pasa de mantenimiento basado en tiempo, a mantenimiento basado en condición, esto es en prevenir, mas que en reparar.

Los tiempos de reparación de un equipo caracterizan la mantenibilidad y, el tiempo promedio para reparar se define como el total de horas inoperables dividido entre el número de acciones de mantenimiento.

Los tiempos para reparar dependen generalmente de la duración de las actividades de:

- El enfriamiento del equipo (no aplica en algunos casos)
- Administrativas (si las hay, como obtención de permisos de acceso o de viáticos)
- Traslados al sitio siniestrado (si corresponde)
- Ubicación y diagnóstico de la falla
- Espera de los materiales y repuestos
- Reemplazo de componentes dañados
- Calentamiento del equipo (no aplica en algunos casos)
- Reinicio, reconfiguración

Los tiempos requeridos para el enfriamiento, el calentamiento y los trámites administrativos son, generalmente, constantes pero la sumatoria de los

tiempos para la ubicación de la falla, espera de los repuestos y reemplazo de los componentes, tienen un comportamiento aleatorio sujeto a toda la estructura logística, al entrenamiento del personal, al tipo de falla, etc. Sin embargo, el tiempo de duración de la falla es la sumatoria de los tiempos parciales antes mencionados. En algunos sistemas hay un tiempo implícito en el intervalo de falla, el cual incrementa la duración de la misma y se define como “tiempo muerto”, en donde aun cuando se ha presentado la falla no hay conocimiento de ella por falta de reporte; por lo general, ocurre con equipos que se encuentran ubicados en lugares distantes o en zonas aisladas de los grupos de trabajo.

Criterios de Riesgo y Costos

Analizado desde la perspectiva de los costos, los gastos (OPEX) propios de un mantenimiento preventivo, redundan en un beneficio por evitar indisponibilidades que incurran en el no cumplimiento de los SLA o en pérdidas de tráfico.

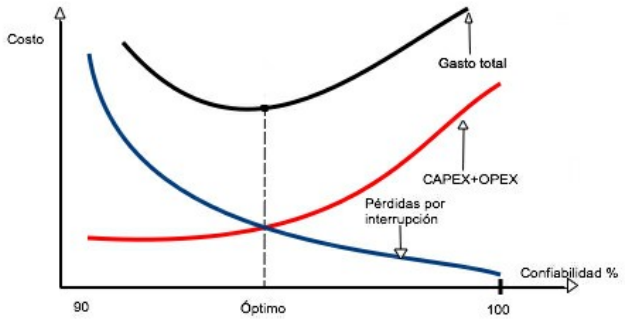


Figura 6. Criterios de Riesgo y Costos.

Fuente: (Apablaza, Calidad de redes y servicios de telecomunicaciones., 2011)

Un análisis probabilidades de disponibilidad (probabilidades de falla y probabilidad del tiempo de recuperación) asociados a costos, permitirá definir estrategias de mantenimiento, como puede ser la oportunidad de realizar un mantenimiento correctivo, preventivo o de diagnóstico. Desde estos datos se podrá priorizar acciones e inversiones. Como primera opción un análisis de Pareto podrá ser útil para dedicar mayores esfuerzos en

aquellos problemas que tienen más relevancia, detectando “los pocos vitales de los muchos triviales”, ya que por lo general, el 80% de los resultados totales se originan en el 20% de los elementos.

De la figura 6, se puede deducir que no es necesario invertir indiscriminadamente, ni de esperar que la confiabilidad de las redes y sistemas sea a toda instancia de “5 nueves”.

La indisponibilidad redunda en un daño económico para el usuario final, lo mismo que para el operador. Si la confiabilidad de los componentes no varia, el daño económico crece al crecer la complejidad del sistema. El daño económico crece al crecer la tasa de falla de cada uno de los componentes simples.

Nuevamente se insiste en que las acciones sobre el proyecto, pueden maximizar la confiabilidad de un producto industrial, de un sistema, o de una red, en esta fase se alcanza la confiabilidad intrínseca. En las fases sucesivas del ciclo de vida, R disminuye, como consecuencia de apartarse del proyecto inicial durante la producción u operación, o por la puesta en servicio, o por el envejecimiento durante el funcionamiento. El proyecto debe prever todos los aspectos de confiabilidad, con referencia a las prestaciones requeridas en servicio. Para dispositivos reparables (disponibilidad más que confiabilidad) es necesario tomar en consideración, sobre el proyecto, también todas las acciones que favorecerán el mantenimiento del producto, sistema o red que se activa para prestar servicios.

Nivel de Criticidad.

Para definir nivel de criticidad, usualmente los efectos de la falla se clasifican en:

I. Insignificante: el efecto sobre la confiabilidad y/o disponibilidad es mínimo.

II. Menor: no afecta la seguridad, pero sí la confiabilidad-disponibilidad.

III. Mayor: no afecta la seguridad, pero sí la confiabilidad-disponibilidad de manera importante.

IV. Crítica: es afectada la seguridad

En una red de telecomunicaciones podrá analizarse todas las situaciones de vulnerabilidades que puedan existir y asociarlas a un nivel de criticidad.

El autor del "Arte de Mantener" recomienda los siguientes criterios para definir el nivel de criticidad:

Tabla 2. Criterios para niveles de criticidad.

Índice de gravedad	Criterio	Índice de frecuencia	Criterio2
1	detención ≤ 0.5 horas	1	≤ 1 vez/año
2	detención ≤ 1.5 horas	2	≤ 1 vez/mes
3	detención ≤ 5 horas	3	≤ 1 vez/semana
4	detención ≤ 24 horas	4	≤ 1 vez/día
5	detención ≥ 24 horas	5	≥ 1 vez/día

Fuente: (Mendoza, 2010)

Una buena ingeniería contemplará desde los inicios de un proyecto, en sus etapa de concepción y diseños, la confiabilidad esperada y todos los medios para alcanzarla. Si como se espera de una red de telecomunicaciones, que presta servicios fundamentales para la sociedad, una disponibilidad de "5 nueves" debe analizarse de acuerdo a los distintos criterios que se han desarrollado aquí.

Un análisis detallado desde los cimientos (componentes, sistemas y subsistemas) hasta el resultado final de la red implementada, conlleva contemplar una revisión de la arquitectura total, definir objetivos de confiabilidad, ejecutar una asignación a las partes. (Apablaza, CALIDAD DE REDES Y SERVICIOS DE TELECOMUNICACIONES)

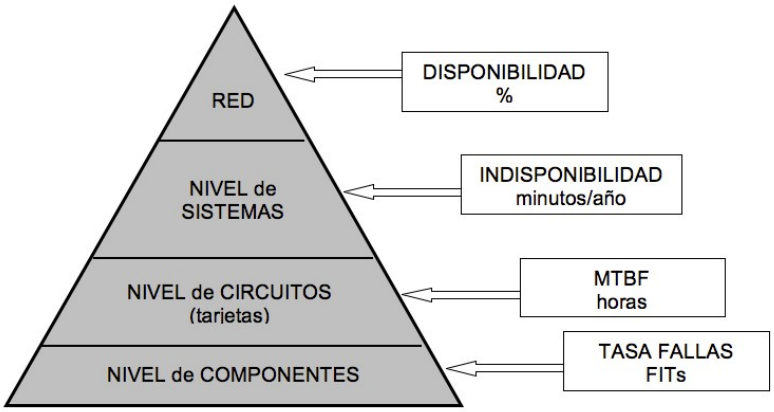


Figura 7. Arquitectura total de confiabilidad de una red.

Fuente: (Apablaza, Calidad de redes y servicios de telecomunicaciones., 2011)

1.4.2. ClearOS

1.4.2.1. Concepto

ClearOS se define como un Sistema Operativo (SO) que proporciona a la empresa seguridad de la red y servicios de aplicación a las pequeñas y medianas empresas (PYMES). Que permite a una organización para proteger contra las amenazas entrantes, salientes establecer políticas de uso y/o funcionamiento y ser más productivos a través de la utilización de los servicios integrados.

Esta guía de inicio rápido describe los pasos necesarios para instalar y empezar a administrar el servidor ClearOS. Se supone que el usuario es un poco familiarizado con la instalación de software y tiene una comprensión básica del hardware del equipo y el trabajo en red.

ClearFundation se dedica a la siguiente Visión y Objetivos:

Visión: La visión de ClearFundation es que cada hogar, pequeña organización y entorno de TI distribuido en el mundo merece adecuada seguridad, la filtración, y la gestión. Acceso a Internet es el gran igualador en economía, pero cada red requiere seguridad y gestión.

Los propósitos: Los fines para los que ha sido ClearFundation organizados son los siguientes:

- Asegurarse de que cada pequeña organización y entorno de TI distribuido en el mundo puedan tener la seguridad adecuada, la filtración y gestión.
- Defender el software de código abierto como la disposición al público y su libre distribución.
- Promover el desarrollo, la mejora y la aplicación del software de código abierto dentro de ClearOS.
- Asegurar que las personas de cualquier lenguaje y capacidad puedan utilizar ClearOS para sus propios fines. (ClearFoundation, 2014)

Utilidades de ClearOS según requerimientos disponibles.

La selección de Hardware ClearOS server es un sistema operativo basado en Linux. Como tal, requiere el software hardware dedicado para instalar y en Windows instalar y ejecutar como una aplicación.

Se tiene muchas opciones para elegir el hardware para el servidor. Afortunadamente, se ha diseñado ClearOS con requisitos mínimos de hardware en comparación con los productos de Microsoft, lo que le permite "reciclar" un equipo de escritorio o comprar hardware nuevo pero no necesariamente vanguardia en términos de especificaciones. La mejor configuración dependerá de ubicación del servidor, el número de usuarios, escalabilidad, uso y muchos otros factores.

En primer lugar debe de considerar si una estación de trabajo (un ordenador de sobremesa) o un servidor montado en rack es el que mejor se adapta a sus necesidades. La siguiente tabla le dará algunos de los puntos a tener en cuenta a la hora de tomar su decisión.

Tabla 3. Tipos de equipos a instalar ClearOS.

CPU-Estación de trabajo	Montado en un Rack
Más barato	Toma menos espacio, pero requiere un Rack
Puede ser ubicado en cualquier lugar	Incrementa los niveles de ruido

Fácil de mover o reubicar	Requiere mínimo uso de periféricos.
Se puede optimizar su expansión	Adecuado para un cuarto de equipos
Puede ser configurado por otros usuarios.	

Fuente: (ClearCenter, 2014)

Tabla 4. Modos de funcionamiento de ClearOS.

Modo	Tarjetas de red requeridas.
Standalone	1
Gateway	2
Multi-WAN/DMZ	3 o más

Fuente: (ClearCenter, 2014)

NOTA: En modo Multi-WAN existe la posibilidad de utilizar dos o más conexiones a través de 1 o más proveedores de servicios de Internet (ISP) para el beneficio de la distribución de la carga y recuperación de errores.

El hardware necesario depende de lo que las demandas de recursos uso normal en el servidor. Por ejemplo, la página web proxy y filtrado de contenido para 50 usuarios requiere una mayor exigencia de procesador y de memoria que la de un sistema que ejecuta un firewall simple. Las siguientes directrices pueden ser utilizados para estimar los requerimientos del sistema:

Tabla 5. Requisitos del sistema de acuerdo al número de usuarios

CPU y Memoria	Menos de 5 usuarios	5 -10 usuarios	10 -50 usuarios	50 - 250 usuarios
Procesador/CPU	500 MHz	1 GHz	2 GHz	3 GHz
Memoria RAM	512 MB	1 GB	1.5 GB	2 GB

Fuente: (ClearCenter, 2014)

1.4.2.2. Utilidades y limitantes de ClearOS en sus versiones libre y de pago.

ClearOS Comunidad es un servidor, sistema operativo de red y puerta de enlace conectado a la nube diseñada para los hogares, aficionados y desarrolladores de Linux. ClearOS viene con un completo mercado de fácil de instalar aplicaciones y la solución es muy fácil de configurar gracias a la intuitiva interfaz basada en web . Edición ClearOS Comunidad está diseñado para el desarrollo de aplicaciones y pruebas de los usuarios de la comunidad y expertos de Linux. Si usted está buscando para funcionar ClearOS en un entorno de producción

La edición Community es de código abierto y la versión gratuita diseñada para el disfrute de los usuarios de Linux. Va a encontrar más diversión y aplicaciones personales como servidores de medios en esta edición, pero no soporte, ya que es patrocinado por supuesto. Pero hay un montón de grandes características sin ningún tipo de coste.

(ClearCenter, 2014)

Para las empresas, sin fines de lucro, escuelas y otras organizaciones profesionales, ClearOS Profesional es la respuesta. Esta edición no sólo viene con soporte comercial de la ClearCARE equipo ClearCenter, pero también un número de aplicaciones empresariales diseñadas exclusivamente para la edición profesional. Además de todas las aplicaciones en la Community Edition, también puede adquirir las siguientes aplicaciones opcionales:

- Conector de Active Directory
- Google Apps Sincronización
- Sincronización de la cuenta (Master / Slave)
- Antimalware prime proporcionado por Kaspersky

Tabla 6. Detallado de diferencias entre ClearOS Community vs ClearOS Professional.

Comparación	clearOS community	clearOS professional

Características	Community	Professional
Servidor, red y puerta de enlace		
75 Aplicaciones Gratis	✓	✓
Calidad Garantizada de software	Actualizaciones solo en ambiente de pruebas	✓
Destinado a ambientes tipo	Desarrolladores y expertos en Linux	Producción/Entornos Comerciales.
Destinado Número de Usuarios	Menos de 10	Hasta 1000
Apoyo técnico		
Foros de la comunidad	✓	✓
Documentación en línea	✓	✓
ClearCARE, Nivel I Apoyo	-	✓
ClearCARE, Soporte Nivel II	-	✓
ClearCARE, Nivel III Consulting	-	Disponible
ClearCARE, Soporte por correo electrónico	-	✓
ClearCARE, Acceso Remoto Soporte	-	✓
ClearCARE, Teléfono de Ayuda **1**	-	✓
Hybrid Cloud Services		
Google Apps Sincronización **2**	-	Aplicación de Pago
Sincronización de la cuenta **2**	-	Aplicación de Pago
Terceros Aplicaciones y Servicios		
Zarafa Community Edition	Aplicación de Pago	Aplicación de Pago
Edición Zarafa Pequeños Negocios **2**	-	Aplicación de Pago
Antimalware Premium, impulsado por Kaspersky **2**	-	Aplicación de Pago
ClearCenter Aplicaciones y Servicios 3		
Conector de Active Directory **2**	-	Aplicación de Pago
Intrusos Protección	Aplicación de Pago	✓

Continua

Firmas y actualizaciones		
Filtro de contenido de lista negra y actualizaciones	Aplicación de Pago	✓
Auditoría de seguridad remota	Aplicación de Pago	✓
Copia de seguridad del servidor remoto	Aplicación de Pago	✓
Antimalware Actualizaciones	Aplicación de Pago	✓
Antispam Actualizaciones	Aplicación de Pago	✓
Monitor del sistema remoto	Aplicación de Pago	✓
VPN dinámica	Aplicación de Pago	✓

Fuente: (ClearCenter, 2014)

1.4.3. Estándar ISO-27001

1.4.3.1. Conceptos

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, publica o privada, grande o pequeña.

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema

de gestión de seguridad de la información (SGSI) basado en ISO 27001. (ISO 27000 , 2013)

La certificación ISO 27001 avala la adecuada implantación, gestión y operación de todo lo relacionado con la implantación de un SGSI, siendo la norma más completa que existe en la implantación de controles, métricas e indicadores que permiten establecer un marco adecuado de gestión de la seguridad de la información para las organizaciones.

Activo.- Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma, que tenga valor para la organización.
Confidencialidad.- Acceso a la información por parte únicamente de quienes estén autorizados.
Disponibilidad.- Acceso a la información y los sistemas de tratamiento de la misma, por parte de los usuarios autorizados cuando lo requieran.
Integridad.- Mantenimiento de la exactitud y completitud de la información y sus métodos de procesos. (uladech.edu.pe, 2013)

1.4.3.2. Gestión de la Seguridad de la Información.

El sistema de gestión de seguridad de la información comprende la política, estructura organizativa, procedimientos, procesos y recursos necesarios para implantar la SGSI, el cual se implanta de acuerdo a los estándares de seguridad como el ISO 27001 basado en el código de buenas prácticas y objetivos del control ISO 17799, el cual se centra en la preservación de las características de CONFIDENCIALIDAD, INTEGRIDAD y DISPONIBILIDAD. (uladech.edu.pe, 2013)

La implantación de un SGSI se basa en la norma UNE ISO/IEC 27001:2007. Esta norma nos presenta un sistema de gestión basado en el ciclo de Deming: Plan, Do, Check, Act, conocido como PDCA y que traducido al castellano sería Planificar, Hacer, Comprobar y Mejorar.

Figura 8. Ciclo PDCA

Fuente: (Rivas, 2010)

El ciclo PDCA supone la implantación de un sistema de mejora continua que requiere una constante evolución para adaptarse a los cambios producidos en su ámbito y para tratar de conseguir la máxima eficacia operativa.

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

I. Planificar

En esta fase tiene lugar la creación del SGSI, con la definición del alcance y la Política de Seguridad. El núcleo fundamental de esta fase y del SGSI es la realización de un análisis de riesgos que refleje la situación actual de la entidad. A partir del resultado de este análisis se definirá un plan de tratamiento de riesgos que conlleva la implantación en la organización de una serie de controles de seguridad con el objetivo de mitigar los riesgos no asumidos por la Dirección.

II. Hacer:

Esta fase cubre la implantación del plan de tratamiento de riesgos, su ejecución. Incluye también la formación y concienciación de los empleados en materia de seguridad y la definición de métricas e indicadores que sirvan para evaluar la eficacia de los controles implantados.

III. Comprobar:

Durante esta fase se realizan diferentes tipos de revisiones para comprobar la correcta implantación del sistema. Entre ellos, se realiza una auditoría interna independiente y objetiva, así como una revisión global del SGSI por Dirección, con el objetivo de marcarse nuevas metas a cubrir en el próximo ciclo del SGSI.

IV. Mejorar:
El resultado de las revisiones debe reflejarse en la definición e implantación de acciones correctivas, preventivas y de mejora para avanzar en la consecución de un SGSI eficaz y eficiente.

1.4.3.3. Fases del sistema de seguridad de la información

Establecer y Administrar el SGSI.

a) **Definir el alcance y límites del SGSI.**
   Debe ser en relación con las características de la empresa, la organización, su ubicación, bienes y tecnología. El alcance del SGSI tiene que estar bien definido y completo.

b) **Definir una política del SGSI.**
   La dirección aprobará la política del SGSI, que incluirá una base para fijar los objetivos, dar la dirección para la administración y la acción, determinar el contexto de gestión de riesgos y los criterios contra los cuales el riesgo será valorado.

c) **Definir el enfoque sistemático para la evaluación de riesgos.**
   La empresa tiene que incluir en sus criterios para la aceptación de riesgos y la identificación de los niveles aceptables del riesgo.

d) **Identificar los riesgos.**

Identificar los riesgos a los bienes tomando en cuenta las amenazas y las vulnerabilidades relacionadas con estos bienes y los impactos de las pérdidas de la confidencialidad, integridad y disponibilidad, puedan tener sobre los bienes.

e) **Analizar y Valorar los riesgos.**

Basado en la información procesada en la identificación de riesgos, se incluirán todas las áreas de control como procesos, operaciones, personas, legalidad, reglamentos y contratos, instalaciones de procesamiento. Esto permite evaluar el daño a la empresa como resultado de una falla de seguridad y la probabilidad de tal falla. La organización necesita calcular el nivel de riesgo y determinar si lo acepta o lo trata (establece controles).

f) **Identificar y valorar las alternativas para el tratamiento de los riesgos.**

En cuanto la organización ha identificado, evaluado y comprendido el impacto que los riesgos podrían tener sobre la empresa, se puede tomar acciones y tratar los riesgos.

Las acciones pueden ser: poner controles apropiados, evitar los riesgos, transferir los riesgos y aceptar el riesgo.

g) **Selección de los objetivos de control y los controles para tratar los riesgos.**

Los controles entre los que la empresa puede seleccionar están contenidos en el Anexo A de la ISO 27001:2005.

La selección de controles tiene que ser eficaz en costos, el costo de implantar un control no debe exceder el impacto en las finanzas de los riesgos que son previstos reducir.

h) **Preparar una declaración de aplicabilidad.**

El Soja (Statment of Aplicablity) es un requisito obligatorio para las empresas que quieren obtener la certificación ISO 27001. Presenta

los objetivos de control y controles que han sido seleccionados en base a los resultados de la evaluación y tratamiento de riesgos.

Figura 9. Fases SGSI.

Fuente: (ISO 27001 , 2013)

1.4.3.4. Ventajas de la implementación las políticas se SGSI en TeamSourcing Cía. Ltda. Según el estándar ISO-27001.

- Establecimiento de una metodología de gestión de la seguridad de la información clara y bien estructurada.
- Reducción de riesgos de pérdida, robo o corrupción de la información.
- Los usuarios tienen acceso a la información de manera segura, lo que se traduce en confianza.
- Los riesgos y sus respectivos controles son revisados constantemente.
- Las auditorias externas e internas permiten identificar posibles debilidades del sistema.
- Continuidad en las operaciones del negocio tras incidentes de gravedad.
- Garantizar el cumplimiento de las leyes y regulaciones establecidas en materia de gestión de información.

- Incrementa el nivel de concientización del personal con respecto a los tópicos de seguridad informática.
- Proporciona confianza y reglas claras al personal de la empresa.

2. CAPÍTULO II

Políticas de Administración y mantenimiento de la red Interna de TeamSourcing Cía. Ltda., basadas en el Estándar ISO-27001.

2.1. Análisis y evaluación de riesgos.

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), cumple define los procedimientos que sirven como guía para el establecimiento de la protección necesaria de los sistemas de información para todo tipo de empresas. Además de cumplir con objetivos primordial de garantizar la seguridad de la información, identificando problemas y definiendo políticas que lo eviten, además de cumplir con los objetivos específicos de TeamSourcing, enfocados a la realización de un análisis de riesgos dentro de la empresa.

2.1.1. Administración de riesgos.

Es importante hacer notar a los directivos de la empresa las actividades más importantes a ser desarrolladas, midiendo el cumplimiento de las metas y determinando la manera en que se va a desarrollar en IT los objetivos relacionados con la seguridad de la información , con el objetivo de encontrar un balance entre el manejo de los riesgos encontrados y los beneficios.

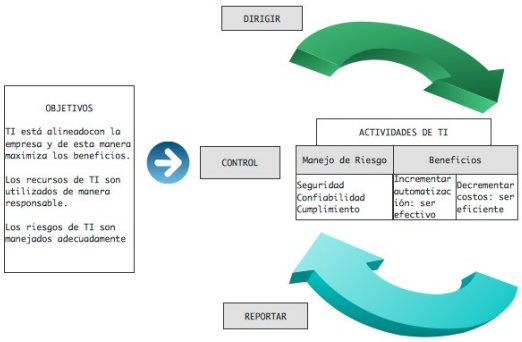


Figura 10. Esquema base para la administración de riesgos.

Fuente: (ISO 27000, 2013)

2.1.2. Análisis de riesgos.

Este análisis nos permite determinar los puntos críticos de la empresa y estimar su nivel de exposición a los riesgos presentes, entre los cuales se debe tener en cuenta tres elementos fundamentales:

- Activos

  Se debe valorar los elementos del sistema de información que aportan valor a la empresa.

- Amenazas

  Se enfoca en todo lo que pueda provocar en una vulnerabilidad. La probabilidad de amenaza, el grado de vulnerabilidad y la severidad del impacto de relacionan entre si para emitir un criterio a cerca del riesgo a tratar.

- Salvaguardas

  Se debe seleccionar las contramedidas o salvaguardas y una evaluación de su efectividad. El análisis de riesgos permite analizar los riesgos de forma metódica para llegar a conclusiones basadas en un fundamento.

2.1.3. Control de activos.

Se definen como activos aquellos recursos que son considerados como esenciales para o que tengan relación con el correcto funcionamiento de la red y que alcance los objetivos propuestos por su gerencia.

Tabla 7. Valoración de activos.

Valoración de Activos			
Valor	**Disponibilidad**	**Integridad**	**Confidencialidad**
5	Este nivel abarca toda información, instalación o recurso cuya disponibilidad siempre debe garantizarse. Su pérdida es considerada como catastrófica para la institución	Este nivel abarca toda información, instalación o recurso en el cual la integridad es en extremo importante y debe garantizarse bajo cualquier circunstancia. Su pérdida es considerada como catastrófica.	Este nivel abarca toda información, instalación o recurso calificado como de uso confidencial. Solo puede ser utilizado con autorización explícita.
4	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por algunas horas.	Este nivel abarca toda información, instalación o recurso en el cual la integridad es muy importante y debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso restringido. Solo puede ser utilizado por personal autorizado.
3	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por 24 horas máximo.	Este nivel abarca toda información, instalación o recurso en el cual la integridad es de importancia media y debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso semi-restringido. Solo puede ser utilizado por personal interno.
2	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por 48 horas máximo.	Este nivel abarca toda información, instalación o recurso en el cual la integridad no es muy importante pero debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso interno. Solo puede ser utilizado por personal interno o usuarios/clientes.
1	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por varios días sin causar consecuencias.	Este nivel abarca toda información, instalación o recurso en el cual la perdida de integridad es insignificante.	Este nivel abarca toda información, instalación o recurso calificado como de uso público.

Fuente: (Mendoza, 2010)

El activo principal dentro de nuestra empresa, es la información contenida en nuestros servidores de base de datos, al igual que el de los computadores del equipo de TI y los funcionarios de alto rango, los cuales pueden ser vulnerables por virus o intromisiones fraudulentas.

- Servicios: Que se pueden prestar gracias a aquellos datos y los servicios que se necesitan para poder gestionar dichos datos.

- Software: Que permitan manejar los datos.
- Hardware: Que permitan alojar datos, aplicaciones y servicios.
- Soporte de información Son dispositivos de almacenamiento de datos.
- Equipos de Backup: Complementan a los equipos principales.
- Redes de comunicaciones: Permiten el envío y recepción de datos.
- Instalaciones: Donde se localizan los equipos informáticos y de comunicaciones.
- Personal: Aquellos que explotan y operan todos los elementos anteriormente citados.

2.1.3.1. Identificación de activos

a) Datos usados por los sistemas de información de TeamSourcing.

Tabla 8. Equipos existentes en TeamSourcing.

Cantidad	Descripción
2	Servidor HP ProLiant DL380 Gen 5
1	Servidor HP ProLiant DL140
1	Servidor HP ProLiant DL380 Gen 7
1	Servidor HP ProLiant MicroServer Gen 8
3	Access Point 3COM
2	Switch HP V1910-48G
1	Router Cisco 800 Series
1	Storage HP StorageWorks P2000
3	UPS Powercom VGD-6000

Servicios

Para nuestra empresa el departamento de TI producción brinda los siguientes servicios:

- Soporte de la Red LAN.
- Servicios de soporte.

  -Internet

  -Red Local

-Red Inalámbrica

-Antivirus

-Software

- Mantenimiento de Hardware.
- Soporte de aplicaciones de software

b) Aplicaciones informáticas

Tabla 9. Descripción de software utilizado en las distintas estaciones de trabajo

Aplicación	Descripción
Antivirus	ESET NOD 32 con licencia renovable para un año
Microsoft Windows 7 Professional edition	Con licencia para activación por internet
Centos	Versión 6.x.x
Postgres	Versión 9.x.x, para uso corporativo.
Microsoft Office Professional edition	Con licencia para activación por internet
Postgres Enterprise manager	Uso y administración de Base de datos.
Netbeans	Desarrollo en JAVA/PHP
win zip	
Central telefónica 3CX	Para uso de extensiones telefónicas en general.
Evolution	Para uso de Call center y softphone en general
skype	
hangouts	
putty	
SSH Secure File Transfer	Para uso general de transferencia de archivos de Windows hacia los servidores.

c) Soporte de Información / Backups.

Dentro de TeamSourcing existen varios tipos de soporte para el respaldo de información, nombraremos los siguientes:

- Servidores que replican la información cada cierto tiempo formado respaldos.

- Bancos de discos duros, conectados a la red en donde se almacena gran cantidad de información.

d) Equipamiento auxiliar.

Tabla 10. Descripción de equipos auxiliares.

Equipos	Descripción
UPS	2 UPS Centrales (KVA). Ubicados en el cuarto de equipos
Generados Eléctrico.	Proporcionado para todo el edificio, con mantenimiento preventivo y correctivo, otorgado por la administración del mismo.
Impresora láser	1 HP 550
Impresoras multifunción	2 Canon MP-1140
Impresora matriciales	1 HP

e) Redes de comunicaciones

Tabla 11. Redes de comunicaciones de TeamSourcing.

Red	Descripción
Red Local	Red local compuesta por subredes en cada uno de los departamentos.
Red Wireless	Red inalámbrica compuesta por 3 Access Point, un en cada oficina.

f) Instalaciones.

Tabla 12. Ubicación de instalaciones de TeamSourcing.

Instalaciones	Ubicación
Área Comercial	Oficina 501
TI	Oficina 502
Producción/Operaciones	Oficina 503

g) Personal.

Tabla 13. Personal de áreas en general de TeamSourcing.

Personal	Descripción
Gerente General	Gerente de TeamSourcing, y jefes de las áreas comercial/administrativas.
Gerentes de Proyectos	Jefes de Proyectos, Arquitectura, QA, desarrolladores.
Jefe de Producción	Jefes de Producción, Infraestructura y Operaciones.
Analistas	Analistas, operadores de Call center, usuarios en general.

2.1.3.2. Valoración de activos de TeamSourcing.

Para evaluar los activos se debe tomar en cuenta parámetros de Disponibilidad (D), Integridad (I), Confidencialidad (C).
Para dicha valoración se tomará en cuenta las siguientes observaciones:

- Valoración comprendida entre 5 y 1, en la cual 1 es el número para especificar aquellos activos que en el caso de producirse algún tipo de falla no provoquen daños considerables.
- Cada activo debe ser evaluado por cada uno de los tres aspectos relacionados.
- El valor acumulado se definirá del promedio de los valore propios de Disponibilidad, Integridad y Confidencialidad de cada activo.
- No todos los activos pueden ser evaluados en los tres aspectos definidos, por lo que en ese caso se deberá representar esto con un guión medio (-).

Tabla 14. Valor de activos de TeamSourcing.

Cantidad	Descripción	Valor Propio			V.Acumulado
		D	I	C	
2	BD Postgres	5	5	5	5
1	Antivirus	5	-	4,5	4,75
1	Microsoft Windows 7 Professional edition	5	-	4,5	4,75
1	Centos	5	5	-	5

Continua

1	Microsoft Office Professional edition	5	5	4,5	4,83
1	Postgres Enterprise manager	5	5	5	5
1	Netbeans	5	3	3	3,67
1	win zip	4	-	-	4
1	Central telefónica 3CX	5	-	5	5
1	Evolution	5	-	5	5
1	Generador eléctrico	5	3	1	3
35	Pc de Escritorio	5	5	5	5
15	Computadores Portátiles	5	5	5	5
1	Impresora láser	5	-	-	5
2	Impresoras multifunción	5	-	-	5
1	Impresora matriciales	5	-	-	5
2	Servidor HP ProLiant DL380 Gen 5	5	-	5	5
1	Servidor HP ProLiant DL140	5	-	5	5
1	Servidor HP ProLiant DL380 Gen 7	5	-	5	5
1	Servidor HP ProLiant MicreServer Gen 8	5	-	5	5
3	Access Point 3COM	5	-	5	5
2	Switch HP V1910-48G	5	-	5	5
1	Router Cisco 800 Series	5	-	5	5
1	Storage HP StorageWorks P2000	5	-	5	5
3	UPS Powercom VGD-6000	5	-	5	5
1	Área de Operaciones	5	-	-	5
1	Área de Producción	5	-	-	5
1	Área Comercial	5	-	-	5
50	Analistas y usuarios en general	5	-	-	5

2.1.4. Control de amenazas.

Las amenazas se definen como cosas o sucesos que pueden ocurrir y pueden ocasionar daños a los activos de la empresa. Para lo cual se los puede dividir en naturales, como: inundaciones, terremotos, etc. Y desastres del tipo industrial, en lo cual se podría citar a casos como: la contaminación, fallos eléctricos, entre otros, en los cuales los sistemas de información es una víctima pasiva.

De la misma manera existen amenazas del tipo intencional, u ocasionadas por personas, que pueden ir desde un error de usuario, hasta un ataque con fines mal intencionados.

2.1.4.1. Valoración de amenazas.

Para determinar cuan dañina puede ser una amenaza se debe estimar cuan vulnerable es el activo, tomando en cuenta parámetros de:

- Degradación: cuan perjudicado resulta el activo.

Nota: La degradación mide el daño causado por un incidente en el caso de que suceda y se suele caracterizar como una fracción del valor del activo.

- Frecuencia: cada que tiempo se materializa la amenaza.

Tabla 15. Degradación de activos.

Degradación del activo		
Descripción	**Degradación %**	**Valor**
Baja	25	1
Media	50	2
Alta	75	3
Total	100	4

Fuente: (Mendoza, 2010)

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de consecuencias fatales pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acumular un daño considerable. La frecuencia se modela como una tasa anual de ocurrencia, siendo valores típicos.

Para la representación de la frecuencia basados en una tasa anual se detalla la siguiente tabla, en donde la frecuencia esta expresada en un tiempo (t), según lo indica la metodología MAGERIT.

Tabla 16. Valores representativos de frecuencia de amenazas de activos.

Valor	Tasa	Ocurrencia	Tiempo
4	100	Muy frecuente	A diario
3	10	Frecuente	Mensualmente
2	**1**	**Normal**	**Una vez por año**
1	1/10	Poco frecuente	Cada varios años

Fuente: (Mendoza, 2010)

2.1.4.2. Valoración de riesgo.

Se expresa el nivel de riesgo mediante un valor numérico, entendiéndose el valor más alto como el valor más expuesto a amenazas dentro de la empresa.

Tabla 17. Niveles de valoración de riesgo.

Nivel de factor de riesgo	Valor	Porcentaje %
Bajo	1 - 32	1 - 25
Medio	33 - 63	25 - 50
Alto	64 -94	51 - 75
Muy alto	95 - 125	76 - 100

Fuente: (Mendoza, 2010)

2.1.4.2.1. Ecuaciones de cálculo de riesgo.

Para estimar el nivel de riesgo al que esta expuesto un activo se debe tomar en cuenta la siguiente ecuación:

$$Riesgo = Valor_{activo} * Degradación * Frecuencia$$

Ecuación 1. Ecuación de cálculo de riesgo.

Fuente: (Mendoza, 2010)

Donde:

- $Valor_{activo}$ (%): Es el valor de importancia del activo para el desarrollo de actividades del personal dentro de la empresa.
- Degradación (%): Indica el valor de perjuicio que sufre u activo, si una amenaza llega a materializarse.
- Frecuencia (t): Representa el valor de frecuencia con la que un activo se ve amenazado.

El cálculo de riesgo respectivo para cada uno de los activos materiales está disponible en el ANEXO 1, en el cual se detalla el resultado de aplicar la *Ecuación 1* y se debe de interpretar según la *Tabla 17* para determinar el nivel del factor de riesgo.

2.1.4.2.2. Cálculo del riesgo inicial en TeamSourcing.

Para determinar el riesgo actual o inicial dentro de nuestra empresa se necesita calcular el valor de riesgo de los activos considerados como esenciales y aplicar la fórmula respectiva al cálculo de riesgo. En este cálculo se debe tomar en cuenta únicamente los activos materiales de la empresa, ya que se va a evaluar la degradación de un activo en un tiempo determinado. Se considera el valor de degradación igual a 2 según la *Tabla 15*, debido a que este tipo de activos se encuentran fuera del alcance del personal externo de la empresa, además de estar protegidos contra amenazas de índole natural como del personal de TeamSourcing. En el caso de la frecuencia de ocurrencia de una amenaza se toma como valor el número 3, descrito en la *Tabla 16*, considerando que puede existir al menos una acción mal intencionada en el plazo de un mes en la empresa.

Entonces, una vez obtenido el valor de riesgo de cada uno de los activos materiales, se establece el valor promedio de riesgo, aplicando la siguiente ecuación:

$$Riesgo_{inicial} = \frac{R1 + R2 + \cdots + Rn}{Total\ de\ activos\ materiales}$$

Ecuación 2. Ecuación general de cálculo de riesgo.
Fuente: (Mendoza, 2010)

Donde:

- R1,R2,…Rn: Valor de riesgo de cada uno de los activos materiales.
- Total de activos materiales: es el número de activos analizados.

Entonces:

$$Riesgo_{inicial} = \frac{30 + 30 + 30 + 30 + 30 + 30 + 30 + 27 + 30 + 30 + 12 + 12 + 12}{13}(\%)$$

$$Riesgo_{inicial} = \frac{133}{13}(\%)$$

$$\boldsymbol{Riesgo_{inicial}} = \mathbf{25.61}(\%)$$

$$Riesgo_{inicial} = Medio$$

Ecuación 3. Cálculo total del riesgo inicial.
Fuente: (Mendoza, 2010)

Tabla 18. Nivel de factor de riesgo calculado.

Nivel de factor de riesgo	Valor	Porcentaje %	Porcentaje Calculado%
Bajo	1 - 32	1 - 25	
Medio	33 - 63	25 - 50	**25.61**
Alto	64 -94	51 - 75	
Muy alto	95 - 125	76 - 100	

Fuente: (Mendoza, 2010)

Si tenemos un valor inicial de riego de **25.61%**, como se puede ver en la tabla anterior, estaríamos entre los valores aceptables es decir en un nivel medio de factor de riesgo de 33 a 63, lo que nos indica que la madurez de nuestra empresa, de acuerdo a la siguiente tabla:

Tabla 19. Cuadro indicativo del nivel de madurez de la empresa.

Eficiencia	Nivel de Madurez	Descripción
0 - 9	0	Inexistente
10 - 49	**1**	**Inicial**
50 - 89	2	Intuitivo
90 - 94	3	Definido
95 - 99	4	Gestionado
100	5	Optimizado

Fuente: (Mendoza, 2010)

Para este caso y según los datos de la tabla anterior se tiene que nuestra empresa con un 25.61%, es igual a 1, equivalente a un nivel inicial y se caracteriza por procesos, manuales, políticas y estándares de seguridad inexistentes, lo que se traduce que para cierto casos como Seguridad de la Información no se tiene un sistema centralizado y los usuarios de TI tienen todos los permisos y privilegios sobre la información.

La empresa debe definir sus políticas de seguridad y con base a ellas, crear los procedimientos asociados.

2.1.5. Determinación del impacto.

El impacto es considerado como la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos y la degradación que causan las amenazas, se determina el impacto que estas tienen sobre el sistema.

En la siguiente tabla se detalla el valor del impacto de una amenaza materializada tomando en cuenta la degradación expresado en porcentaje tanto para Disponibilidad e Integridad.

Tabla 20. Valoración de impactos.

Valoración de Impactos				
	Amenaza		Degradación	
	Aplicaciones		Servidores/Equipos	
	Confidencialidad	Disponibilidad	Confidencialidad	Disponibilidad
Incidentes	0	0	5	10
Accesos no autorizados	5	0	5	5

Fuente: (Mendoza, 2010)

2.1.5.1. Impacto acumulado

Se obtiene del cálculo sobre un activo, tomando en cuenta: Su valor acumulado y las amenazas a las que está expuesto.

Se lo calcula para cada activo, por cada amenaza y en cada dimensión de valoración, cuan mayor sea el valor propio o acumulado sobre un activo, el impacto será mayor.

Al calcularse el impacto acumulado sobre los activos que soportan el peso del sistema de información, nos permite determinar las salvaguardas que deberían existir par proteger los activos, y se lo puede determinar aplicando la siguiente fórmula:

$$Impacto_{acum}\% = Valor_{acum} * Degradación$$

Ecuación 4. Ecuación de cálculo del impacto acumulado.

Cálculo del impacto acumulado en los activos de TeamSourcing.

Tabla 21. Valores del impacto acumulado en los activos Dependientes

Fuente: (Mendoza, 2010)

Activos Dependientes	Incidentes			Accesos no Autorizados		
	D	C	T	D	C	T
PCs de Escritorio	4*0.05=0.20	5*0.1=0.5	0.70	4*0.05=0.20	5*0.05=0.25	045
Computadores Portátiles	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
Impresora láser	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
Impresoras multifunción	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
Impresora matriciales	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
Servidor HP ProLiant DL380 Gen 5	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
Servidor HP ProLiant DL140	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
Servidor HP ProLiant DL380 Gen 7	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
Servidor HP ProLiant MicreServer Gen 8	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
Access Point 3COM	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
Switch HP V1910-48G	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
Router Cisco 800 Series	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
Storage HP StorageWorks P2000	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
UPS Powercom VGD-6000	5*0.05=0.25	5*0.1=0.5	0.75	5*0.05=0.25	5*0.05=0.25	0.5
	Total		**0.74**	**Total**		**0.49**

Donde:

- Los incidentes no provocados causan un impacto del 74 % en activos.
- Los accesos no autorizados provocan un impacto del 49 % a los activos.

Tabla 22. Valores del impacto repercutido en los activos independientes

Activos independientes	Incidentes			Accesos no Autorizados		
	D	C	T	D	C	T
Antivirus	5*0=0	5*0=0	0	5*0=0	5*0.5=0.25	0.25
Microsoft Windows 7 Professional edition	2*0.05=0.1	0*0.1=0	0.1	2*0.05=0.1	0*0.5=0	0.1
Centos	5*0=0	5*0=0	0	5*0=0	5*0.5=0.25	0.25
Postgres	5*0=0	5*0=0	0	5*0=0	5*0.5=0.25	0.25
Microsoft Office Professional edition	2*0.05=0.1	0*0.1=0	0.1	2*0.05=0.1	0*0.5=0	0.1
Netbeans	2*0.05=0.1	0*0.1=0	0.1	2*0.05=0.1	0*0.5=0	0.1
Central telefónica 3CX	2*0.05=0.1	0*0.1=0	0.1	2*0.05=0.1	0*0.5=0	0.1
Información Privada	4*0=0	5*0=0	0	4*0=0	5*0.5=0.25	0.25
Información Pública	5*0=0	5*0=0	0	5*0=0	5*0.5=0.25	0.25
	Total		**0.038**	**Total**		**0.17**

Dónde:

- Los incidentes no provocados causan un impacto del 3.8% en activos.
- Los accesos no autorizados provocan un impacto del 17% a los activos.

2.1.6. Determinación del riesgo

El riesgo lo definíamos como el daño probable sobre un sistema de información. Conociendo el impacto de las amenazas sobre los activos, se puede determinar el riesgo, tomando en cuenta, la frecuencia con que esto ocurra. La siguiente tabla nos muestra los riesgos más comunes a los que pueden estar expuestos los activos de TeamSourcing.

Tabla 23. Determinación del riesgo en TeamSourcing.

TIPO DE ACTIVO / AMENAZA		SERVICIOS			DATOS			APLICACIONES			EQUIPOS INFORMÁTICOS			SOPORTES DE INFORMACIÓN			EQUIPAMIENTO AUXILIAR			INSTALACIONES			PERSONAL		
Código	Descripción	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C	I
ORIGEN: NATURAL																									
N1	Fuego										✓			✓			✓			✓					
N2	Daño por agua										✓			✓			✓			✓					
N*	Desastres naturales										✓			✓			✓			✓					
ORIGEN: INDUSTRIAL																									
I1	Fuego										✓			✓			✓			✓					
I2	Daño por agua										✓			✓			✓			✓					
I3	Contaminación mecánica										✓			✓			✓								
I4	Contaminación electromagnética										✓			✓			✓								
I5	Avería de origen físico o lógico							✓			✓			✓			✓								
I6	Corte de suministro eléctrico										✓			✓			✓								
I7	Condiciones inadecuadas de temperatura/humedad										✓			✓			✓								
I8	Interrupción de otros servicios y suministros																✓								
I9	Degradación de los soportes de almacenamiento													✓											
I10	Emanaciones electromagnéticas												✓												
I*	Desastres industriales													✓			✓								
ORIGEN: ERRORES																									
E1	Errores de usuarios	✓	✓		✓	✓		✓	✓																
E2	Errores de administrador	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓												
E3	Errores de monitoreo				✓	✓	✓																		
E4	Errores de configuración	✓	✓	✓				✓	✓	✓	✓	✓	✓												
E5	Deficiencias de la organización																						✓		
E6	Difusión de software maligno							✓	✓	✓															
E7	Errores de encaminamiento		✓	✓					✓	✓															
E8	Errores de secuencia		✓						✓																
E9	Escapes de información						✓			✓															

Continua

E10	Alteración de información					✓																	
E11	Introducción de información incorrecta					✓																	
E12	Degradación de información					✓																	
E13	Destrucción de información				✓																		
E14	Divulgación de información						✓																
E15	Vulnerabilidades de programas							✓	✓	✓													
E16	Errores de mantenimiento/actualización de programas							✓	✓		✓												
E17	Errores de mantenimiento/actualización de equipos										✓												
E18	Caída del sistema por agotamiento de recursos	✓																					
E19	Indisponibilidad del personal																					✓	
ORIGEN: ATAQUES																							
A1	Manipulación de la configuración	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓										
A2	Suplantación de identidad del usuario		✓	✓				✓	✓														
A3	Abuso de privilegios de acceso		✓	✓				✓	✓		✓	✓											
A4	Uso no previsto	✓						✓			✓			✓			✓						
A5	Difusión de software dañino							✓	✓	✓													
A6	Re-encaminamiento de mensajes		✓	✓					✓	✓													
A7	Alteración de secuencia		✓						✓														
A8	Acceso no autorizado		✓	✓		✓	✓		✓	✓		✓	✓		✓	✓		✓	✓				
A9	Intercepción de información						✓			✓			✓										
A10	Modificación de información					✓																	
A11	Introducción de falsa información					✓																	
A12	Corrupción de la información					✓																	
A13	Destrucción de información				✓																		
A14	Divulgación de información						✓		✓	✓													
A15	Manipulación de programas																						
A16	Negación de servicio	✓									✓												
A17	Robo										✓		✓	✓		✓	✓		✓				
A18	Ataque destructivo										✓			✓			✓			✓			
A19	Ocupación enemiga										✓		✓	✓		✓	✓		✓	✓	✓		
A20	Indisponibilidad del personal																					✓	
A21	Extorsión																						✓ ✓
A22	Ingeniería social																						✓ ✓

2.1.6.1. Riesgo acumulado

El riesgo debe ser calculado para cada activo, por cada amenaza y en cada dimensión de valoración, para lo cual se toma en cuenta: El impacto acumulado sobre un activo debido a una amenaza y la frecuencia de la misma, para lo cual tenemos la siguiente fórmula:

$$Riesgo_{acum} = Impacto_{acum} * Frecuencia$$

Ecuación 5. Ecuación de cálculo del riesgo acumulado.

Fuente: (Mendoza, 2010)

- **Cálculo del riesgo acumulado en los activos de TeamSourcing.**

Para el caso de ocurrencia de incidentes se toma como referencia un valor de frecuencia igual a 2 según la *Tabla 16*, debido a que no son comunes este tipo de sucesos.

En base a esto se puede determinar el riesgo acumulado provocado por incidentes en los activos de TeamSourcing, aplicando la *Ecuación 5*.

El cálculo del riesgo acumulado debido a incidentes y a accesos no autorizados en los activos de TeamSourcing se muestra en las siguientes dos ecuaciones.

$$Riesgo_{acum} = 7.4 * 2 = 14.8\%$$

Ecuación 6. Cálculo de riesgo acumulado debido a incidentes en los activos.

Fuente: (Mendoza, 2010)

$$Riesgo_{acum} = 4.9 * 3 = 14.7\%$$

Ecuación 7. Cálculo del riesgo acumulado debido a accesos no autorizados en los activos.

Fuente: (Mendoza, 2010)

2.1.6.2. Riesgo repercutido.

Para determinar el riesgo repercutido es necesario aplicar la siguiente ecuación, tomando en cuenta, el impacto repercutido sobre un activo debido a una amenaza y la frecuencia de la amenaza:

$$Riesgo_{rep} = Impacto_{rep} * Frecuencia\ \%$$

Ecuación 8. Ecuación de cálculo del riesgo repercutido.

Fuente: (Mendoza, 2010)

- **Cálculo del riesgo repercutido en los activos de TeamSourcing.**

Para esto se debe tomar en cuenta el mismo valor utilizado para calcular el riesgo acumulado, es decir, igual a 2.

$$Riesgo_{rep} = 0.4 * 2 = 0.8\%$$

Ecuación 9. Cálculo del riesgo repercutido debido a incidentes en los activos de TeamSourcing.

Fuente: (Mendoza, 2010)

Para el caso de los accesos no autorizados, se utiliza un valor de frecuencia igual a 3, según la *Tabla 16*.

$$Riesgo_{rep} = 1.7 * 3 = 5.1\%$$

Ecuación 10. Cálculo del riesgo repercutido debido a accesos no autorizados en los activos de TeamSourcing.

Fuente: (Mendoza, 2010)

Para este tipo de casos se debe tomar en cuenta que le valor más alto, que es el producido por incidentes, pero se debe tomar en cuenta la inexistencia de medidas que permitan contrarrestar a este tipo de riesgos.

2.1.7. Salvaguardas

Para esto es necesario recalcar que TeamSourcing tiene medidas de seguridad de la información implementadas por Rack Space, para todos nuestros datos y conexiones con los distintos países, operadoras, y empresas con los que tenemos relaciones comerciales, pero no implementadas dentro de nuestro firewall, como seguridad perimetral para salvaguardar la información de nuestros funcionarios.

Por lo cual es necesario planificar un conjunto de salvaguardas pertinentes, para determinar tanto el impacto como el riesgo, reduciendo la degradación de los activos, o reduciendo la frecuencia de amenaza.

Para esto es necesario:

1. Establecer una política de la empresa al respecto, es decir, directrices generales de quién es responsable de cada actividad.
2. Establecer objetivos a satisfacer para poder asegurar que la amenaza ha sido minimizadas.
3. Establecer procedimientos, de que es lo que se debe hacer.
4. Definir salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para minimizarlas.
5. Definir controles que permitan saber que todo lo anterior está funcionando según lo previsto.

Tabla 24. Niveles iniciales para el cálculo de riesgos.

Niveles iniciales para el cálculo de Riesgos		
Ítem	**valor**	**Descripción**
Degradación del activo	2	Media
Nivel de factor de riesgo	25.61%	Medio
Frecuencia de amenazas de activos	2	Normal

Tabla 25. Resumen General del establecimiento de Controles sobre las Políticas.

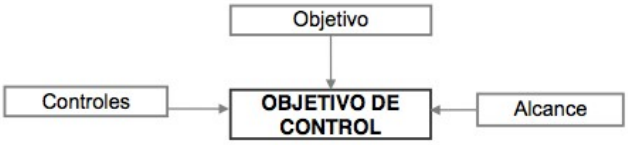
Controles ISO 27001:2005		Controles Excluidos	Controles Actuales	Controles Seleccionados y su Justificación				Comentarios
				RL	OC	RN/ABP	RER	
Clausula	**Objetivo de Control/Control**							
POLÍTICA DE SGURIDAD	**Política de Seguridad de la Información**							
	Documento de política de seguridad de la Información					✓		Documento presentado para aprobación de la Gerencia, y posteriormente publicado y comunicado para todos los empleados de TeamSourcing.
	Organización de la seguridad de la Información.						✓	Definir claramente todas las responsabilidades para la ejecución de la seguridad de la información.
	Gestión de Activos					✓		Clasificar los activos más importantes en relación a su valor, requisitos legales, sensibilidad y criticidad para el desempeño de actividades dentro de la empresa.
	Seguridad física y ambiental (entorno físico de activos)		✓					Verificar que el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios estén protegido contra posibles intercepciones o daños.
	Gestión de las comunicaciones y operaciones.					✓		Documentar y mantener los procedimientos de operación y ponerlos a disposición de los usuarios que los necesiten.
	Control de acceso.				✓	✓		Establecer, documentar y revisar periódicamente las políticas establecidas para el control de acceso en las distintas áreas.
	Adquisición, desarrollo y mantenimiento de los sistemas de información.					✓		Evitar errores humanos, pérdidas, modificaciones no autorizadas o mal uso de la información en aplicaciones.
	Gestión de incidentes en la seguridad de la información.				✓			Comunicar los eventos o incidentes de seguridad de la información lo más rápido posible.
	Gestión de la continuidad comercial.			✓	✓			Desarrollar e implantar planes de mantenimiento o recuperación de las operaciones para asegurar la disponibilidades de la información y los servicios, tras una interrupción o fallo de los procesos críticos de la empresa.
	Cumplimiento.							Proteger los registros importantes, de la pérdida, destrucción y falsificación de acuerdo a las normas establecidas en esta política.
	Revisión de la política de seguridad de la Información	✓						Se debería posponer para la próxima revisión de SGSI.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	**Organización Interna**							
	Compromiso de la Gerencia con la seguridad de la información					✓		La Gerencia apoya activamente la seguridad de la información dentro de la empresa, con una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información.
	Coordinación de la seguridad de la información					✓		Se debe involucrar la cooperación y colaboración de gerentes, usuarios, empleados y personal de seguridad.
	Asignación de responsabilidades relativas a la seguridad de la información					✓		Se realizará de acuerdo con la política de seguridad de la información y estar claramente definida.
	Proceso de autorización de recursos para el procesado de la información	✓						Se debe tratar este tema en la siguiente revisión del SGSI
	Acuerdos de confidencialidad	✓						Se debe tratar este tema en la siguiente revisión del SGSI
	Contacto con las autoridades	✓						Se debe tratar este tema en la siguiente revisión del SGSI
	Contacto con grupos especiales de interés	✓						Se debe tratar este tema en futuras revisiones del SGSI
	Revisión independiente de la seguridad de la información	✓						Se debe tratar este tema en futuras revisiones del SGSI
	Terceros							
	Identificación de los riesgos derivados del acceso de terceros	✓						Se debe tratar este tema en futuras revisiones del SGSI
	Tratamiento de la seguridad en contratos con los clientes	✓						Se debe tratar este tema en futuras revisiones del SGSI
	Tratamiento de la seguridad en la relación con terceros	✓						Se debe tratar este tema en futuras revisiones del SGSI

Leyenda(para Controles Seleccionados y su Justificación)
RL: Requisito Legal
OC: Obligaciones Contractuales.
RN/ABP: Requisitos de Negociación/Adopción de Buenas Prácticas.
RER: Resultado de la Evaluación de Riesgos.

2.2. Diseño del SGSI

El diseño del SGSI debe estar alineado a los 9 objetivos de control, y cada uno debe cumplir con los requisitos que se muestra en la siguiente figura



Fuente: (iso27000.es)

2.2.1. Políticas de seguridad basadas en objetivos de control

Las políticas de seguridad basadas en objetivos de control tienen como finalidad brindar una guía de procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños.

Los beneficios de un sistema de seguridad con políticas claramente concebidas y bien elaboradas son inmediatos, ya que TeamSourcing trabajará sobre una plataforma confiable. Con la implementación de las políticas se logran los objetivos de control indicados en el diseño del SGSI.

A continuación se listan los objetivos de control:

1. Política de Seguridad.
2. Organización de la seguridad de la información.
3. Gestión de activos.
4. Seguridad física y ambiental (Entorno físico de los activos).
5. Gestión de las comunicaciones y operaciones.
6. Control de acceso.
7. Adquisición, desarrollo y mantenimiento de los sistemas de información.
8. Gestión de incidentes en la seguridad de la información.

9. Gestión de la continuidad comercial.
10. Cumplimiento.

2.2.1.1. Política de seguridad.

Tabla 26. Políticas de Seguridad

Objetivo:	Proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requerimientos de la institución y a las leyes y regulaciones vigentes dentro de TeamSourcing.
Alcance	**Controles**
a) Proteger los recursos de información de TeamSourcing y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.	TeamSourcing debe establecer una política clara y que estén acorde a los objetivos de la institución y demostrar su apoyo y compromiso con la seguridad de la información mediante la publicación y mantenimiento de una política de seguridad de la información para toda la organización.
b) Asegurar la implementación de las medidas de seguridad comprendidas en esta política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.	
c) Mantener la Política de Seguridad de TeamSourcing actualizada, a efectos de asegurar su vigencia y nivel de eficacia.	

Fuente: (iso27000.es, 2011)

- **Políticas Diseñadas.**

Acceso a la información

- El personal que presta sus servicios a TeamSourcing debe tener acceso sólo a la información necesaria para el desarrollo de sus actividades.
- En el caso de personas ajenas a TeamSourcing, la persona

responsable de generar la información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación. Este proceso debe ser documentado.

- El otorgamiento de acceso a la información debe regularse mediante las Normas y procedimientos definidos para tal fin.
- Todos los privilegios para el uso de los sistemas de información de la Institución deben terminar inmediatamente después de que el trabajador deje de prestar sus servicios a la Institución. El proceso de eliminación de privilegios debe estar regulado por una norma y procedimiento apropiado. Los proveedores o terceras personas solamente deben tener privilegios durante el período del tiempo requerido para llevar a cabo las funciones aprobadas.
- Para dar acceso a la información se tendrá en cuenta la clasificación asignada por la empresa.
- Se debe efectuar un registro de los eventos acontecidos a los diversos recursos informáticos de la plataforma tecnológica
- Basándose en el registro anterior, se debe hacer un seguimiento a los accesos realizados por los usuarios tanto a los sistemas, como a los datos.

2.2.1.2. Organización de la seguridad de la Información.

Tabla 27. Políticas de la seguridad de la Información.

Objetivo:	Gestionar la seguridad de la Información dentro de TeamSourcing.
Alcance	**Controles**
a) Se debe establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro TeamSourcing.	Los miembros de la Gerencia deben respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Empresa.

Continua

b) La Gerencia debe aprobar la política de seguridad de la información, asignar los roles de seguridad, coordinar y revisar la implantación de la seguridad en toda la Empresa.	Se debe definir claramente todas las responsabilidades para la seguridad de la información.
c) Si fuera necesario, se debe establecer y facilitar el acceso a una fuente especializada de consulta en seguridad de la información.	Identificar y revisar regularmente en los acuerdos aquellos requisitos de confidencialidad o no divulgación que contemplan las necesidades de protección de la información de la institución.
d) Debe fomentarse un enfoque multidisciplinario de la seguridad de la información que implique la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en áreas como la gestión de seguros y la gestión de riesgos.	

Fuente: (iso27000.es, 2011)

- **Políticas de seguridad.**

Administración de cambios.

Aquí se detalla lo referente al desarrollo de aplicaciones y a los cambios en configuraciones de los servidores.

- Todo cambio, creación y modificación de programas, módulos, reportes, etc. Que afecte los recursos informáticos, debe ser solicitado por los usuarios y aprobado formalmente por el responsable de la administración del área afectada.
- Cualquier cambio, desde su solicitud hasta su implementación, debe de ser documentado formalmente.
- No se podrá bajo ningún motivo permitir que un cambio pueda ser aprobado, realizado e implantado por la misma persona o área.

- La documentación servirá como una herramienta para efectuar el seguimiento y garantizar el cumplimiento de los procesos definidos.
- Todo cambio, sea este, de software, modificación de accesos o configuraciones será implementado siempre y cuando no disminuya la seguridad ya existente.

2.2.1.3. Gestión de activos.

Tabla 28. Políticas de Gestión de activos.

Objetivo:	Alcanzar y mantener una protección adecuada de los activos de TeamSourcing, asegurando que se apliquen un nivel de protección de acuerdo a la información.
Alcance	**Controles**
a) Todos los activos deben ser justificados y tener asignado un usuario responsable.	Todos los activos deben estar claramente identificados manteniendo un inventario con los más importantes. La información debe clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Empresa.
b) Se debe identificar a los usuarios responsables para todos los activos y asignarles la responsabilidad del mantenimiento y controles adecuados.	

Fuente: (iso27000.es, 2011)

- **Políticas Diseñadas**

Administración de seguridad

- El análisis de riesgos para los Recursos informáticos debe ejecutarse al menos una vez por año.

- Cualquier mejora, actualización o cambios asociados a los recursos tomados en cuenta en el análisis de riesgos, deben ser precedidos por una nueva evaluación del riesgo.
- Cualquier brecha de seguridad o sospecha de mala utilización en el Internet o la Intranet, de los recursos informáticos a cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial al personal de Seguridad Informática.
- El personal que realiza labores de administración es responsable de los controles sobre los activos.
- El personal encargado de la Seguridad de Información es el encargado de divulgar los estándares, políticas y procedimientos en dicha materia.
- El personal encargado de la Seguridad de Información es responsable de darle seguimiento a las políticas de relacionadas con dicha materia y reportar al Jefe del Departamento. En caso de detectarse un incumplimiento, el personal encargado de la Seguridad Informática reportará al Jefe del Departamento.

2.2.1.4. Seguridad física y ambiental (Entorno físico de los activos).

Tabla 29. Políticas de seguridad física y ambiental.

Objetivo:	Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización. Evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la empresa.
Alcance	**Controles**

Continua

a) Los servicios de procesamiento de información sensible deben ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deben estar protegidas físicamente contra accesos no autorizados, daños e interferencias.	Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deben utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.
b) Debe protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.	Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado.
c) Así mismo, se debe considerar la ubicación y la baja de los equipos.	Se debe proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles intercepciones o daños.

Fuente: (iso27000.es, 2011)

- **Políticas diseñadas.**

Seguridad Física

- Se deben implementar mecanismos de control de acceso a puertas de seguridad, sistema de alarma y circuitos cerrados de televisión inteligentes en las dependencias criticas (por ejemplo, local de los servidores y puertas de entrada principales).
- Si un trabajador se encuentra a un visitante en un área restringida, el visitante debe ser cuestionado acerca de su propósito en el área y se debe informar a los responsables de la seguridad del edificio.
- En el local de los servidores se debe implementar un sistema automatizado para eliminar los incendios.
- Los locales desde donde se tiene acceso al cableado deben ser catalogados como zonas de alto riesgo, limitando el acceso a los mismos. Se debe registrar el ingreso y salida de todas las

computadoras, módems y otros equipos de comunicaciones ajenos a la empresa.

- Los equipos no deben moverse o reubicarse sin la aprobación previa.
- Los empleados de la empresa se comprometen a NO utilizar la red regulada de energía para conectar otros equipos que no sean su estación de trabajo y/o la impresora que se le haya asignado.
- El personal ajeno a la empresa no está autorizado a utilizar los recursos informáticos de la empresa.

2.2.1.5. Gestión de las comunicaciones y operaciones.

Tabla 30. Políticas de gestión de las comunicaciones y operaciones.

Objetivo:	Asegurar la operación correcta y segura de los recursos de tratamiento de información. Proteger la integridad del software y de la información.
Alcance	**Controles**
a) Se deben establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos para el tratamiento de la información.	Se debe documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten.
b) Esto incluye el desarrollo de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias.	Se debe controlar los cambios en los sistemas y en los recursos de tratamiento de la información.
c) Se requieren ciertas precauciones para prevenir y detectar la introducción de código malicioso.	La separación de los recursos para el desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.

Fuente: (iso27000.es, 2011)

- **Políticas diseñadas.**

Seguridad en comunicaciones.

- La topología de red (direccionamiento IP, configuraciones, información relacionada con las medidas de seguridad, etc.) debe considerarse como información RESERVADA.
- Todas las conexiones a otras redes de datos deben protegerse mediante cifrado, detección de intrusos, autenticación y control de acceso.
- La salida de información hacia otras Instituciones o Empresas debe estar amparada por un acuerdo de confidencialidad.
- Las comunicaciones con equipos externos se realizaran utilizando conexiones seguras.
- Toda la información con un nivel de sensibilidad igual o superior a CONFIDENCIAL que se transmita por las redes de la Institución e Internet debe ser cifrada.

Almacenamiento y respaldo.

- La información que genera y soporta la infraestructura de tecnología informática de TeamSourcing deberá ser almacenada y respaldada, garantizando su disponibilidad.
- Se debe definir el procedimiento de crear las copias de respaldo, así como los tiempos de retención y rotación de dichas copias.
- El personal es responsable de la información generada y almacenada en sus estaciones de trabajo, así como, el respaldo de la misma.
- El Departamento de Sistemas es el ente autorizado a realizar el seguimiento y control del cumplimiento de las políticas relacionadas con los respaldos.

2.2.1.6. Control de acceso.

Tabla 31. Políticas de control de acceso.

Objetivo:	Controlar los accesos a la información.
Alcance	**Controles**
a) Se debe controlar los accesos a la información, los recursos de tratamiento de la información y los procesos importantes en base a las necesidades de seguridad de TeamSourcing.	Se debe establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad de la empresa.
	Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.

Fuente: (iso27000.es, 2011)

2.2.1.7. Adquisición, desarrollo y mantenimiento de los sistemas de información.

Tabla 32. Políticas de adquisición, desarrollo y mantenimiento de los sistemas de información.

Objetivo:	Garantizar que la seguridad de la información es parte integral de los sistemas de Información.
Alcance	**Controles**
a) Dentro de los Sistemas de la Información se incluye: sistemas operativos, infraestructura, aplicaciones propias de la empresa, aplicaciones de terceros o de usos generalizados, servicios y aplicaciones desarrolladas por usuarios de la empresa. Los pre-requisitos de seguridad deben de ser identificados y establecidos previamente al desarrollo e implantación de los sistemas de información.	Evitar errores humanos, de pérdidas, modificaciones no autorizadas o mal uso de la información en aplicaciones.

Fuente: (iso27000.es, 2011)

- **Políticas diseñadas.**

Contraseñas

- Capacitar a los usuarios en la creación de contraseñas.
- Garantizar que las contraseñas cumplan con las características siguientes:
    - Utilizar al menos 8 caracteres.
    - Utilizar letras mayúsculas, minúsculas, símbolos y números.
    - Los usuarios deben cambiar las contraseñas cada 120 días.
    - Los administradores deben cambiar las contraseñas cada 90 días. No deben reutilizarse contraseñas.
- Aplicar cada 60 días revisiones de la calidad de las contraseñas

Control de acceso.

- Cada usuario debe disponer de un nombre de usuario y contraseña única.
- Las contraseñas son responsabilidad de sus propietarios. Dichas contraseñas serán generadas por el administrador y entregadas al usuario. Las contraseñas solo deben ser conocidas por su propietario. Los usuarios son responsables de las actividades llevadas a cabo con su nombre de usuario y/o contraseña.
- Las contraseñas deben tener una fecha de caducidad definida en base a la sensibilidad de la información a proteger. Para los sistemas de acceso a las estaciones de trabajo, se recomienda cambiarlas cada 90 días. Las claves de administración deben cambiarse cada 60 días.
- Los nombres de usuario no deben estar basados en las funciones de trabajo. Los nombres de usuario identifican a personas específicas. Para la asignación de nombres de usuario se toma en cuenta la primera letra del nombre y el apellido completo del usuario, por ejemplo:
    - Giacomo Orizzonte: gorizonte, Edgar Pilacuán: epilacuan

- Se deben tener definidos los perfiles de usuario de acuerdo a la función y cargo de los usuarios.
- El nivel de administrador de los sistemas críticos debe estar controlado, es decir, las actividades realizadas por alguien con nivel/privilegio de administrador, deben ser supervisadas.
- Antes de diseñar o adquirir un sistema, se deben especificar los requerimientos de seguridad necesarios. Los ambientes de desarrollo, pruebas y producción deben ser independientes.

2.2.1.8. Gestión de incidentes en la seguridad de la información.

Tabla 33. Políticas de gestión de incidentes.

Objetivo:	Garantizar que los eventos y debilidades en la seguridad, asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas.
Alcance	**Controles**
a) Se deben establecer las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados.	Se debe comunicar los eventos en la seguridad de información lo más rápido posible.
b) Se debe aplicar un proceso de mejora continua en respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de información.	Todo el personal, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.

Fuente: (iso27000.es, 2011)

- **Políticas diseñadas.**

Contingencia

- Se debe preparar, actualizar y validar periódicamente el plan de contingencias. Dicho plan debe garantizar la continuidad de operaciones en caso de desastres como terremotos, explosiones, actos terroristas, inundaciones etc.
- En dicho plan se describirán los procedimientos de neutralización y recuperación ante cualquier evento que afecte la confidencialidad, integridad y disponibilidad de la información.
- Partiendo de los resultados obtenidos en el análisis de riesgos, se determinarán las acciones a realizar para minimizar el riesgo.

2.2.1.9. Gestión de la continuidad comercial.

Tabla 34. Políticas de gestión de la continuidad comercial.

Fuente: (iso27000.es, 2011)

Objetivo:	Reaccionar a la interrupción de actividades y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.
Alcance	**Controles**
a) Se debe implantar un proceso de gestión para reducir, a niveles aceptables, la interrupción causada por los desastres y fallos de seguridad mediante una combinación de controles preventivos y de recuperación.	Se debe identificar los eventos que puedan causar interrupciones a los procesos junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.
b) Se deben analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio, disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos.	Se debe desarrollar e implantar planes de mantenimiento o recuperación de las operaciones para asegurar la disponibilidad de la información, tras la interrupción o fallo de los procesos críticos de negocio.

- **Políticas diseñadas.**

Seguridad para los servicios informáticos.

- No se utilizarán servicios externos de correo electrónico.
- La empresa se reserva el derecho de acceder a todos los mensajes enviados por medio del correo electrónico. Para este efecto, cada usuario autorizará por escrito a la empresa a que realice las revisiones y/o auditorías respectivas directamente o a través de terceros.
- La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la Institución. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, códigos fuentes, documentación y otros materiales.
- El personal no debe utilizar versiones escaneadas de firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico o cualquier otro tipo de comunicación electrónica haya sido firmada por la persona que la envía.
- El personal que haya recibido aprobación para tener acceso a Internet, deberá aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.
- Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar a la oficina de informática, no utilizar el computador y desconectarlo de la red.

2.2.1.10. Cumplimiento.

Tabla 35. Políticas de cumplimiento.

Objetivo:	Evitar imcumplimientos de ley, estatuto, regulación u obligación establecida dentro de la empresa.
Alcance	**Controles**

Continua

a) El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad vigentes. Los requisitos legales específicos deben ser advertidos por los asesores legales de la organización o por profesionales adecuadamente cualificados.	Los registros importantes se deben proteger de la pérdida, destrucción y falsificación, de acuerdo al reglamento establecido y que esté en vigencia dentro de la empresa.

Fuente: (iso27000.es, 2011)

- **Políticas diseñadas.**

Registros

Se definen los documentos de registro que se requieran para el control de la actividad, de acuerdo a los lineamientos del sistema de seguridad diseñado, considerando entre otros los siguientes:

- Registro de inspecciones.
- Registro y control de los soportes.
- Registro de software de nueva adquisición.
- Registro de entrada, salida y movimiento de tecnologías de información.
- Registro de incidencias de la Seguridad Informática.

Registros disponibles en el **Anexo 2** de este proyecto.

Software utilizado.

- El software utilizado debe garantizar la integridad de los datos en su totalidad.
- Se debe crear una cultura en los usuarios de la empresa sobre las implicaciones del uso de software ilegal.
- Se mantendrá un inventario de las licencias de software en la empresa que permita su administración y control. El uso de este inventario permitirá detectar el uso de software no licenciado.

- Se establecerá un reglamento que limite el uso de software de demostración en las estaciones de la empresa.

Actualización de hardware.

- Cualquier cambio de hardware (procesador, memoria, tarjetas adicionales, etc.) debe ser autorizado por el personal responsable de los recursos.
- La reparación de los equipos que implique la apertura de los mismos será realizada solo por personal autorizado.
- El movimiento y/o re-ubicación de equipos (PC, servidores, equipamiento activo) debe estar debidamente autoriado y documentado.

Listado de usuarios con acceso a redes de alcance global

- Se dispondrá de un Listado de Usuarios autorizados, especificando
- Nombre, Apellidos y Cargo que ocupa en la Institución, así como los Servicios para los que está autorizado.

3. CAPÍTULO III

Análisis y diseño de una solución firewall para una red corporativa.

ClearOS nace como una necesidad de brindar mayor seguridad en lo que tiene que ver a seguridad perimetral en los sistemas de información existentes en TeamSourcing, se toma en cuenta varias premisas para decidir que éste es la mejor opción, ya que además de su capacidad de instalarse bajo equipos con requerimientos bajos, nos brinda una seguridad robusta y manejable para el administrador de la red, además de contar con una extensa fuente de consulta propia y de terceros, que lo hace mucho más fácil para desarrollar requerimientos adicionales.

3.1. Análisis de los requerimientos de seguridad en una red corporativa.

3.1.1. Seguridad que emplea la red.

El objetivo principal de la administración de una red de datos es la de permitir la comunicación entre distintos tipos de usuarios, pero así mismo, no debe de estar disponible todo el tiempo ni para cualquier tipo de usuarios, por lo que se deben crear distintos tipos de reglas o parámetros para permitir o negar el acceso a las redes de datos. Pero además de proteger el acceso a información confidencial, es importante también estar protegido contra otro tipo de amenazas, tales como pueden ser: los ataques a los servicios o a la disponibilidad de los equipos y puntos críticos dentro de nuestra red, los cuales pueden dejarlos sin disponibilidad y consecuentemente esto se vería reflejado en pérdida de datos, insatisfacción de los usuarios o falta de credibilidad.

Como ya se había hablado en el desarrollo de las políticas de seguridad perimetral para TeamSourcing, *tabla 25,* se debe tomar en cuenta los tres parámetros básicos de la seguridad de la información:

- Confidencialidad.- La información debe de estar protegida por accesos no autorizados.
- Integridad.- La información no debe de ser alterada o eliminada de ninguna manera, deben establecerse formas de restricción para los distintos tipos de usuarios, así como los permisos de modificación de información.
- Disponibilidad.- La información debe de estar siempre disponible y accesible para los usuarios autorizados, en el momento en que la requieran. En caso de presentarse inconvenientes con el funcionamiento de algún servicio de la red, este debe tener una recuperación lo más rápida posible según las capacidades de equipos y personal humano.

Términos importantes a tomar en cuenta dentro de este capítulo:

- Identificación.- Proceso de diferenciar una entidad de otra o determinar la identidad de una entidad con quien se está comunicando.
- Autenticación.- Proceso de verificar la identidad de una entidad, probar que es quien dice ser.
- Autorización.- Controlar los permisos o accesos de una entidad o usuario hacia un sistema y verificar los privilegios que ella tiene.
- No repudio.- Prevenir que una entidad niegue la realización de un evento, como envío , recibo, acceso o alteración de información o archivos.

Seguridad de acceso

En la capa de acceso se permite realizar un enlace físico real con los medios y enviar paquetes IP sobre la red. Detallaremos algunos de los protocolos que se debe tomar en cuenta para este diseño, ya que en esta capa se

incluyen detalles de la tecnología LAN, WAN, capa física y de enlace de datos, según el modelo OSI.

- ATM (Asíncronos Transfer Mode) .- Esta tecnología, orientada a la conexión de red, nos provee de seguridad como integridad, autenticación, alta seguridad puno-multipunto y VPN, las cuales son vitales en lo que tiene que ver en confidencialidad en el internet.

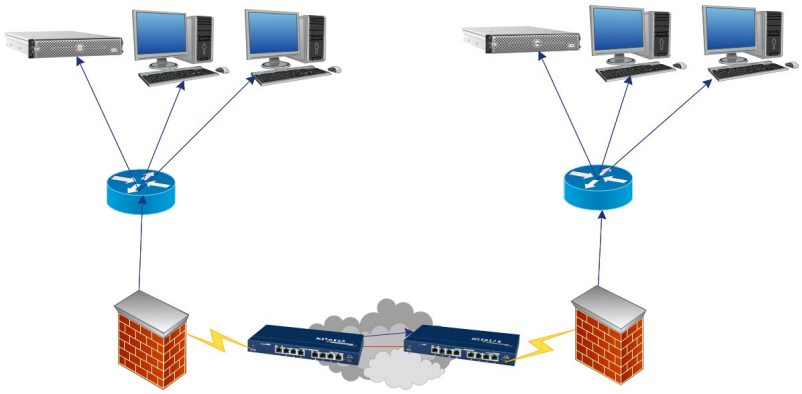


Figura 12. Red ATM

- L2TP.- Opera sobre la capa de enlace de datos del modelo OSI, por lo que su implementación se realiza punto a punto en la red, transporta en un túnel tráfico PPP sobre varias redes como IP, ATM, etc. El tipo de seguridad que nos puede ofrecer L2TP es a nivel de autenticación y cifrado proporcionado por PPP y dependiendo del tipo de red que estemos tratando se podrá ofrecer otro tipo de seguridad.

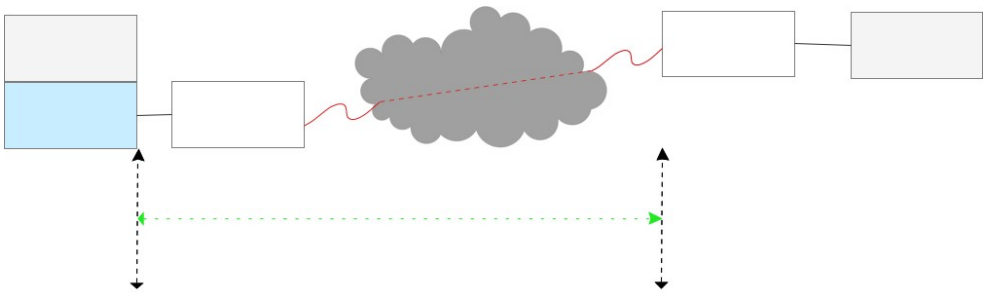


Figura 13. Tipo de red L2TP.

Seguridad en la capa de internetworking.

En esta capa se selecciona la mejor ruta para la distribución de paquetes y la conmutación de los mismos, entre los mecanismos de seguridad a mencionar se tiene los siguientes:

- Filtros de paquetes o Firewalls.- Se define como un limitador de paquetes, es decir, todos los paquetes tienen negado su paso a menos que cumplan con las reglas establecidas.
- Filtros basados en Direcciones IP.- Se basa en la dirección de origen y destino de un paquete para permitir o negar su paso.

Tabla 36. Reglas de filtraje basadas en direcciones IP.

Regla	IP Origen	IP Destino	Acción
1	72.32.191.*	201.218.12.*	Permitir
2	201.218.12.*	72.32.191.*	Permitir
3	*	*	Negar

- Filtros basados en direcciones IP y número de puertos.

Tabla 37. Reglas de filtraje basadas en direcciones IP y puertos TCP/UDP.

Regla	Conexión	Tipo	IP Origen	IP Destino	Puerto fuente	Puerto destino	Acción
1	entrada	tcp	externa	interna	>=1024	25	permitir
2	entrada	tcp	interna	externa	25	>=1024	permitir
3	salida	tcp	interna	externa	>=1024	25	permitir
4	salida	tcp	externa	interna	25	>=1024	permitir
5	*	*	*	*	*	*	negar

Donde:

Conexión de entrada: Es indicada desde un cliente sobre un host externo.

Conexión de salida: Es indicada desde un cliente sobre un host interno.

Otras acciones como la autenticación de usuario o cifrado pueden ser implementadas adicionales a permitir o negar una conexión.

- NAT (Network Address Traslation).- Es un mecanismo que nos ayuda a reemplazar una dirección IP (poder ser externa o pública) de un paquete por otra (que puede ser interna o privada). Por lo general esto se implementa en equipos de borde o gateways como un firewall o routers.

Tabla 38. Traducción de direcciones de red.

Red Interna		NAT	Red Externa	
IP Origen	IP Destino		IP Origen	IP Destino
201.218.12.*	192.168.63.1	➔	192.168.63.1	201.218.12.*
192.168.63.1	201.218.12.*	➔	201.218.12.*	192.168.63.1

En complemento al párrafo anterior se puede decir que la dirección IP de origen de un paquete se traduce de una IP privada a una dirección pública, y de la misma manera sucede con los paquetes de respuesta. Esto nos ayuda no solamente para mantener una cierta seguridad de a los dispositivos de la intranet, ya que la dirección IP pública permanece oculta, sino que también permite una conservación de IPs, las cuales son limitadas.

- IPSec (Internet Protocol Security).- Se refiere a una extensión de IP que asegura su comunicación, para lo cual utiliza una serie de protocolos de seguridad y algoritmos, también provee integridad de datos, autenticación y confidencialidad. Es muy usado para la implementación de VPNs en la intranet e internet por su asociación de seguridad y administración de llaves.
- Seguridad para DNS.- Domain Name Server, por sus siglas en inglés, se trata de un sistema que asocia direcciones IP, con nombres de dominio de host. La mayoría de ataques hacia un DNS se trata de direccionar el tráfico de datos a un sitio incorrecto, una de las formas de conseguir este objetivo es ingresar al registro DNS y modificarlo y así la respuesta del servidor DNS será una dirección IP incorrecta.
- NIDS (Network Based Intrusion Detection System).- Un sistema de detección de intrusos debe proveer los siguientes mecanismos de defensa:

- Detección.- Identificar los ataque maliciosos sobre recursos de la red y el host.
- Prevención.- Detener la ejecución del ataque detectado.
- Reacción.- Inmunizar el sistema de futuros ataques de fuentes maliciosas.

Un IDS está formado por uno o varios sensores y un analizador, que pueden trabajar solos o en conjunto, para lo cual el analizador examina la información aplicando algunos de los métodos de detección de intrusos, los cuales se resumen en “detección de anomalías” y “detección de sus indebidos”.

Para lo cual un NIDS inspecciona el tráfico entrante o saliente a nivel de red, si detecta una acción maliciosa realiza una acción correctiva propia, si está configurada, o a su vez notifica al administrador del sistema para que sea él quien realice dicha acción correctiva.

Seguridad en la capa de transporte

En esta capa se proporcionan servicios de transporte de datos desde un host de origen hacia uno de destino, la cual forma una conexión lógica entre los extremos de la comunicación.

- Proxy a nivel de circuito.- Se define como un servidor, que está entre un servidor real y un cliente, permitiendo una comunicación controlada, la limitación de esto, es que el cliente debe de ejecutar un software de cliente especial para que el proxy a nivel de circuito funcione.

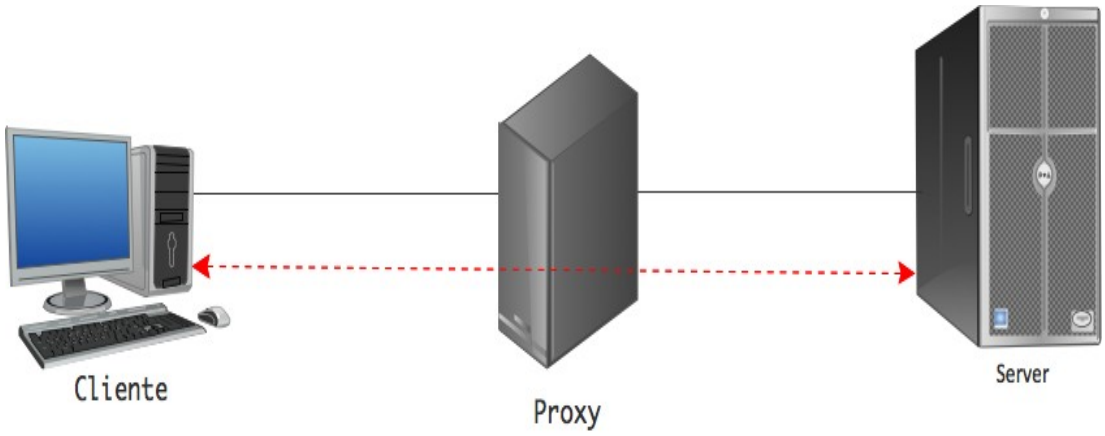


Figura 14. Conexión proxy base en capa de transporte.

- Filtros de contenidos.- Son programas que se ejecutan sobre el firewall y analizan el tráfico en base a las reglas en el nivel de aplicación.
- Controles de acceso y autorización.- Son puntos de acceso a la red y a sus recursos, por lo cual son el punto principal de seguridad de redes, siendo los más renombrados protocolos de autenticación “RADIUS” y/o “TACACS” los cuales se implementan en la mayoría de firewalls.
- Seguridad en sistemas operativos.- La mayoría de ataques van dirigidos a la accesibilidad a host o servidores , por lo que se deben tomar en cuenta algunos mecanismos de seguridad en los mismos:

    - Configurar el monitoreo de logs, logs fallidos y toda la actividad de la red y e cada uno de sus dispositivos, en especial en sistemas críticos como servidores.
    - Revisar continuamente el archivo de logs, si es posible una vez por día.
    - Respaldar los archivos de logs periódicamente, una copia impresa por mes sería una buena opción, ya que algunas copias digitales podrían ser alteradas.

- Definir y controlar los niveles de acceso a los privilegios de uso en las aplicaciones en cada sistema.
- Utilizar mecanismos de cifrado sobre información de administración y monitoreo.
- Instalar únicamente los programas necesarios para la ejecución y buen desempeño de cada equipo.
- Actualizar las versiones de los sistemas operativos.

- HIDS (Host Based Intrusion Detection System).- Detecta algún tipo de actividades o acciones maliciosas dentro de un solo host, para lo cual revisa los logs del host y del sistema.

3.1.2. Tráfico trasmitido

La cantidad y el tipo de tráfico que atraviesan la red son los factores más importantes al momento de implementar nuevos sistemas de seguridad.
La cantidad de tráfico nos da una idea de cómo diseñar una red, ya que de acuerdo a esto tendremos que dimensionar de manera coherente la distribución física y lógica de los equipos, para lo cual se utiliza una fórmula matemática, la cual se denomina “Teoría de Colas” la cual en sencillas palabras, hace uso de modelos capaces de representar el comportamiento óptimo de una red frente a volúmenes de tráfico deseados, es decir, que en función a esta herramienta se deberían diseñar parámetros como por ejemplo capacidades de enlaces, servidores o equipos en general, el siguiente análisis se enfoca en resultados de tráfico para una red corporativa pequeña.

Dentro de una red corporativa pequeña debemos tomar en cuenta los siguientes aspectos básicos:

- Telefonía.- La red interna de TeamSourcing tiene alrededor de 50 usuarios, de los cuales no todos tienen una extensión de línea

telefónica, por lo que únicamente los jefes de cada área, personal del departamento comercial, personal de recepción, y esencialmente el personal de Call-center, tienen acceso a softphones o teléfonos virtuales, en cada una de sus estaciones, todos ellos controlados por la central telefónica de voz sobre IP 3CX.

- Servicio Web.- TeamSourcing, por ser una empresa dedicada al desarrollo de software, utiliza mucho este recurso, ya que la mayoría de proyectos y nuevos productos que se están llevando a cabo están desarrollados sobre PHP, por lo que el consumo o ejecución de páginas web aplicativos sobre Web Services, pero solo a nivel de desarrollo, es de muy alta demanda, ya que los servicios o productos ya en producción se ejecutan en servidores localizados en Rackspace, fuera de nuestra red interna.

- Servicio de transferencia de archivos.- Dentro de TeamSourcing se tiene un servidor dedicado para este fin, por lo que los usuarios podrán descargar desde nuestra intranet los archivos que sean de sus necesidades.

- Tráfico de control como DHCP, DNS, entre otros.

- Se debe tomar en cuenta también las descargas que los usuarios de la intranet hagan desde el internet.

3.2. Diseño de una solución de firewall para una red corporativa

3.2.1. Análisis de hardware.

El diseño de una red corporativa incluye muchos tipos de tecnologías y topologías físicas y lógicas, los cuales se van a describir o analizar el mejor

desempeño de cada una de ellas en este capítulo, para lo cual se dividirá a los usuarios como: Usuarios de poder y Usuarios de no poder.

Usuarios de poder.- Son aquellos que tendrán comunicación con todos los servidores y también con los usuarios de no poder, los cuales aparte de esto tendrán libre acceso y navegación a internet así como acceso a una extensión de línea telefónica.

Usuarios de no poder.- Este tipo de usuarios no tienen la necesidad de tener acceso al stack de servidores internos, es decir, tendrán permiso de lectura, pero no de escritura, por lo que la documentación contenida en la intranet será accesible para su uso, pero ellos no podrán subir ningún archivo, y también se dispondrán limitaciones en la navegación de internet, la cual será restrictiva.

Usuarios de Poder.- Tendrán todas la facilidades y privilegios de navegación y acceso a toda la red

Ya en términos de hardware para generar la conectividad dentro de la empresa, se debe tomar en cuenta los equipos existentes, que en su mayoría son routers, switch y un servidor que nos servidor como equipo para alojar al firewall ClearOS.

Para la distribución de IPs dentro de TeamSourcing se tomará en cuenta los dos grupos asociados en Usuarios de poder y Usuarios de no poder, además de los equipos de almacenamiento de bases de datos internas situados en una zona llamada Hot LAN, de uso exclusivo de ClearOS, los cuales serán distribuidos de la siguiente manera:

Tabla 39. Distribución de zonas e interfaces físicas.

Grupo	VLAN	IP
Hot LAN	eth3	192.168.61.X
Usuarios no poder	eth2	192.168.62.X
Usuarios de poder	eth1	192.168.63.X

Hot LAN.- Las interfaces designadas como Hot LAN tienen NAT aplicada a ellos, pero no tienen acceso a las redes LAN. Especificando el uso de una Hot LAN para las redes que se consideran restringido pero aún necesitan acceso a Internet.

Tabla 40. Tipos de redes en ClearOS y su enrutamiento.

From/To	External	LAN	HotLAN	DMZ
External	Pass	FW/PF/1:1NAT	FW/PF/1:1NAT	DMZ Firewall
LAN	Pass	Pass	Pass	Pass
HotLAN	Pass	Block	Pass	Pass
DMZ	Pass	Blocks/Pinholes	Block	Pass

Fuente: (ClearOS Guides, 2013)

Enfocándonos en el uso de un router que nos permita la conectividad entre las distintas áreas, para este proyecto lo haremos con ClearOS, que a su vez funcionará como router de borde, ya que nos permitirá tener conexión a internet, funcionará como firewall y proporcionará a nuestra red interna de algunos servicios típicos, para ello, la empresa ha destinado el siguiente equipo para este software firewall:

- Servidor HP ProLiant DL380 Gen 7
- Procesador Intel(R) Xeon(R) CPU E5405 @ 2.00GHz
- 15,57 GB de RAM
- 60 GB en Disco Duro

3.2.2. Análisis de los servicios.

Mediante la implementación de ClearOS, podremos tener servicios típicos dentro de una red como: DHCP, DNS, NAT, QoS, SSH, http.

DHCP.- Se trata de un servicio TCP/IP el cual se encarga de la administración y configuración IP de los equipos de nuestra red, ClearOS nos ofrece una configuración bastante fácil e intuitiva en lo que tiene que ver a este servicio, aparte de darnos una oportunidad de autenticación, por así decirlo, manual para cada host y así ser un filtro adicional, además de los que más adelante mencionaremos.

DNS.- Utilizado para asignar a los equipos un nombre equivalente a su dirección IP, para lo cual este servicio es transparente al usuario, y el cual es configurado dentro de la interfaz gráfica de ClearOS sin muchos pasos a seguir.

NAT.- Como ya lo definimos anteriormente, este servicio nos ofrece la posibilidad de traducir direcciones IP, algo muy necesario dentro de nuestro sistema implementado con ClearOS para que las distintas áreas tengan salida al internet, y debido a que ClearOS, en la configuración en si se deberá tomar en cuenta que interfaz Eth, Vlan o bond se desea dar el servicio.

QoS.- ClearOS trabaja con la prioridad de paquetes que se haya configurado para cada área, es decir, que dará paso al paquete que esté marcado como prioritario antes que a los que tienen una prioridad mayor, y así mismo dividirá o asignará el ancho de bando dependiendo de los usuarios que lo necesiten, es decir, los usuarios de poder y de no poder.

HTTP y SSH.- ClearOS nos permite tener acceso a una interfaz gráfica mediante una página web, la cual es de mucha ayuda al momento de revisar

configuraciones y reportaría de una manera más ágil y amigable con el administrador del firewall, y también se podrá acceder vía ssh si así se requiere y se desea, por lo que una línea de comandos también estará disponible para nosotros.

3.2.3. Diseño de la topología física y lógica.

Para esto como ya se había mencionado en ocasiones anteriores se dividirá a la red en tres áreas, a las cuales de aquí en adelante las denominaremos como zonas, las cuales son:

- Usuarios de Poder
- Usuarios de no poder
- Hot LAN

Que son las que típicamente se encuentra en una empresa, y cuyas características físicas se detallan a continuación.

- Zona de usuarios de no poder
  Capacidad de hasta 100 usuarios
  Conexión a internet con limitaciones
  Conexión con la zona Hot LAN

- Zona de usuarios de poder
  Capacidad de hasta 100 usuarios
  Conexión a internet sin limitaciones de acceso
  Conexión con los usuarios de la zona de no poder
  Conexión con la zona Hot LAN

- Conexión a la zona de Hot LAN
  Capacidad de hasta 10 servidores.
  Conexión a internet

A continuación se detalla la topología física básica de nuestra red corporativa:

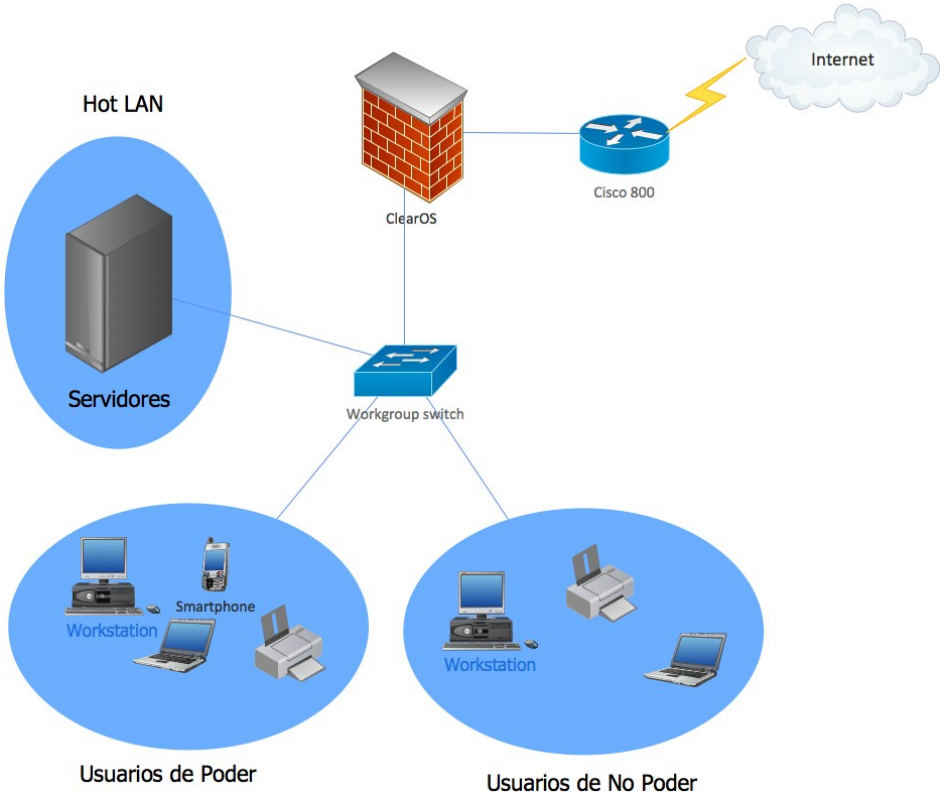


Figura 15. Diagrama esquemático de la red corporativa.

Los dispositivos críticos de la red los mantendremos en una subred, para dar un poco más de robustez al acceso a ellos en términos de acceso. El diseño de la red lógica se refleja en diagrama de capa 3, por lo que no necesariamente tienen que tener coherencia con el diseño físico de la red, así lo denotaremos a continuación.

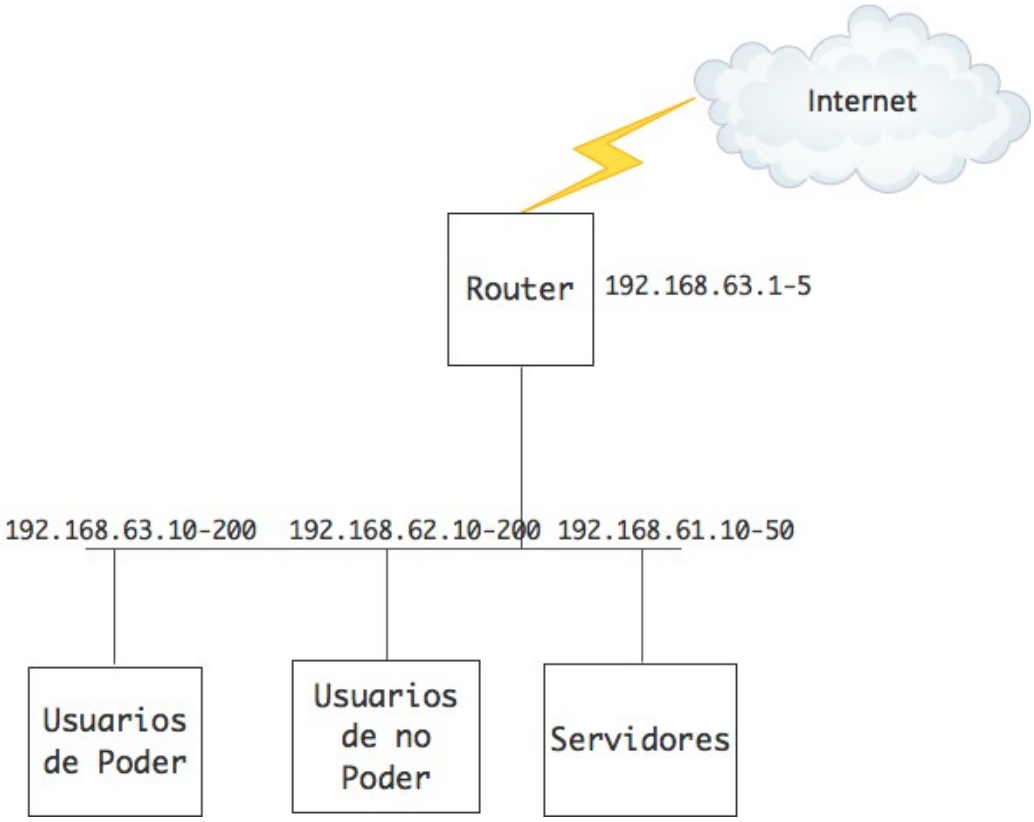


Figura 16. Diseño lógico de la red corporativa.

Nuestra red ahora es funcional, para lo cual los componentes necesarios están dispuestos según nuestra necesidad.
La primera consideración a tomarse en cuenta, es las direcciones IP, para lo cual asignaremos IPs de carácter privado, es decir de clase C.

Como el título del proyecto reza, esta red necesita la seguridad necesaria para la red interna de la empresa, por lo que se procederá con la instalación y configuración de nuestro firewall, ClearOS, para proveer a la red de seguridad de alto nivel hacia la internet.

ClearOS será conectado directamente a la internet, y luego a los dispositivos de distribución, es decir, switch conectados en cascada, para dar paso a toda la intranet hacia el internet, el firewall será instalado en un servidor dedo de baja para los servicios corporativos de la empresa, el cual funciona perfectamente y tiene condiciones más que suficientes para el correcto

funcionamiento de ClearOS y además estará únicamente dedicado a este objetivo.

Teniendo una topología final a partir de las configuraciones anteriores, delimitando las distintas etapas y para dar conectividad a las zonas antes citadas, tendríamos la siguiente imagen:

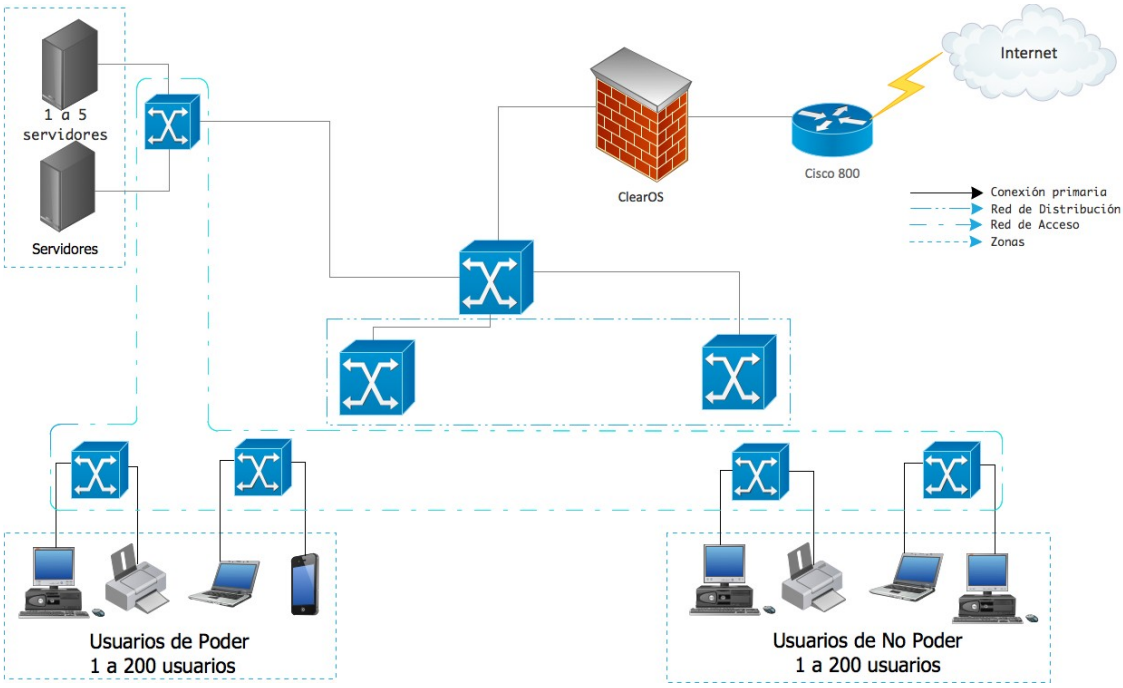


Figura 17. Configuración de la red corporativa de TeamSourcing.

4. CAPÍTULO IV

Implementación de la solución de firewall para la red corporativa de TeamSourcing.

4.1. Implementación de la solución de firewall para la red corporativa de TeamSourcing.

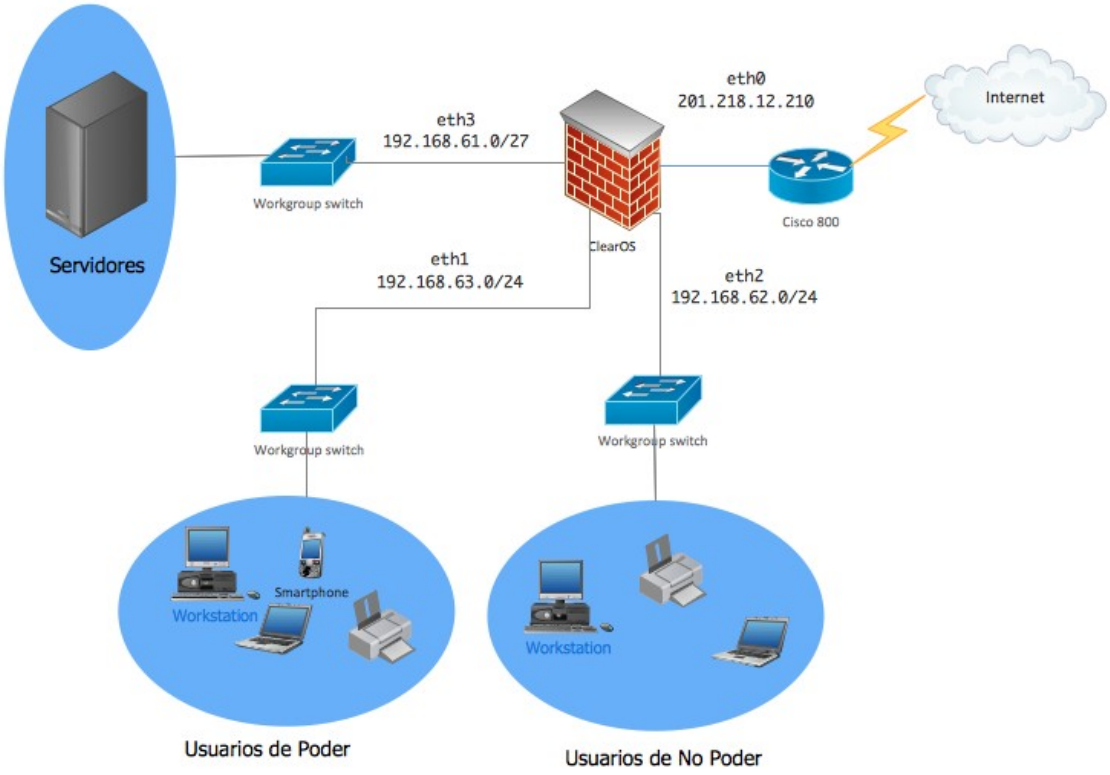


Figura 18. Topología a implementar.

Para la topología de la red se ha establecido el siguiente direccionamiento IP, el cual se detalla a continuación:

Tabla 41. Topología de red propuesta

Interfaz		Máscara	Especificaciones	
	ClearOS			
LAN	Eth 1	192.168.63.0/24	192.168.63.0	Dirección de red
			192.168.63.1	Dirección ClearOS
			192.168.63.10 192.168.63.200	Intervalo usuarios de poder
			192.168.63.255	Broadcast
	Eth 2	192.168.62.0/24	192.168.62.0	Dirección de red
			192.168.62.1	Dirección ClearOS
			192.168.62.10 192.168.62.200	Intervalo usuarios de no poder
			192.168.62.255	Broadcast
	Eth 3	192.168.61.0/27	192.168.61.0	Dirección de red
			192.168.61.1	Dirección ClearOS
			192.168.61.10 192.168.62.29	Intervalo para Servidores
			192.168.62.31	Broadcast

4.2. Configuraciones iniciales de ClearOS.

Colocamos nuestro usuario y contraseña que configuramos durante la instalación y podremos acceder al siguiente dashboard.

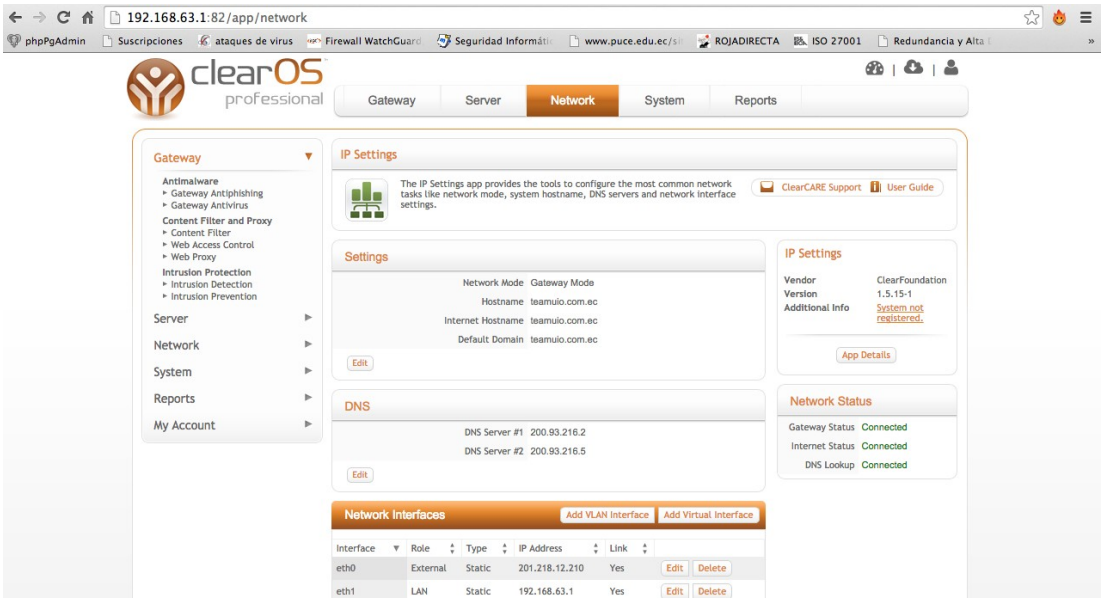


Figura 19. Dashboard inicial de ClearOS.

En la gráfica anterior podemos ver algunos parámetros de los configurados durante la instalación, los cuales los ampliaremos en la siguiente imagen:

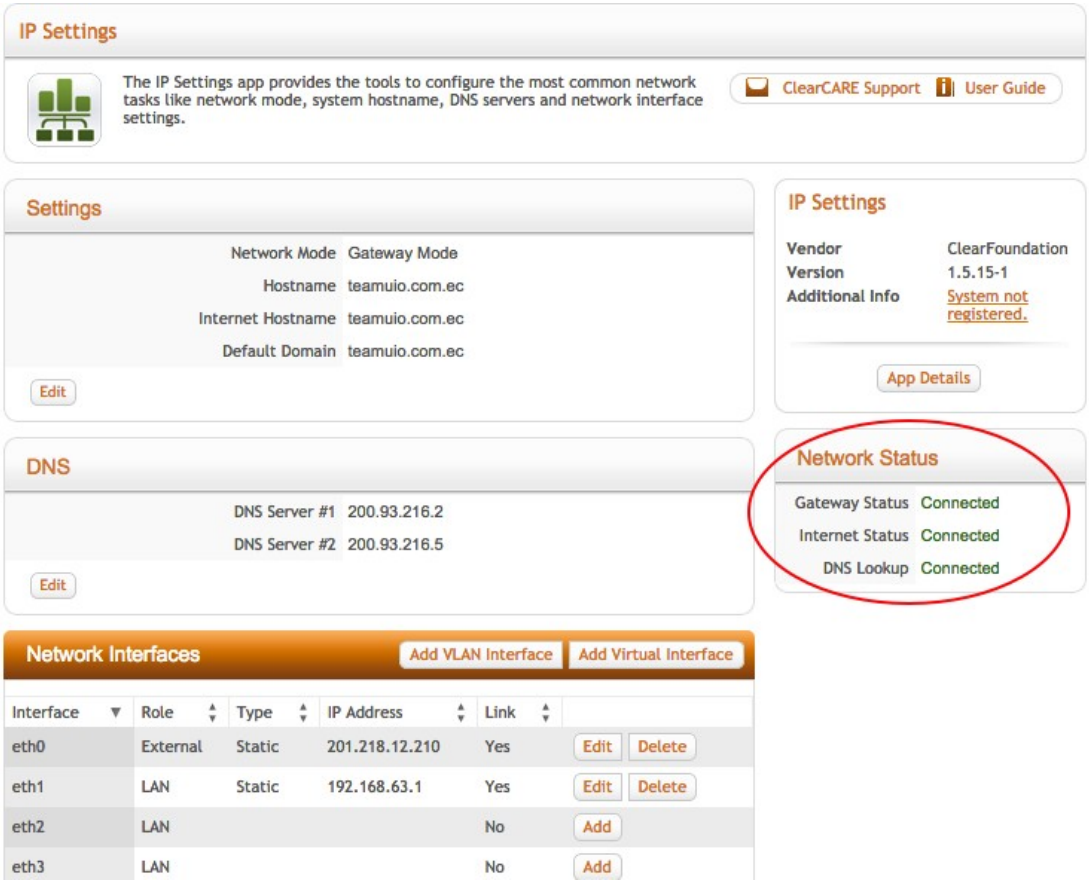


Figura 20. Parámetros configurados durante la instalación y mostrado en la interfaz web.

Analizando la figura anterior podemos observar en el estado de la red que estamos en estado “conectado” a el modo Gateway, Internet y DNS, por lo que hasta ahora todo funcionaría de una manera correcta, y se podría ya navegar por internet, debido a que se estaría asignando DHCP de una manera dinámica, es decir, todo aquel que se conecte a nuestra red, y en el caso de los APs se autentiquen, estarían con una IP asignada aleatoriamente.

En la siguiente figura se puede apreciar el reporte del sistema, es decir, la capacidad del equipo que estamos utilizando y la versión del sistema operativo de ClearOS que estamos utilizando, cabe mencionar que esta versión se ha actualizado a la más reciente, he aquí el por que no coincide

con la versión de instalación que se había mencionado en párrafos anteriores.

Entre los ítems de información que nos ofrece este reporte están:

- La versión del Sistema Operativo
- Versión del kernel
- Hora y fecha del sistema
- Modelo de Procesador
- Desde cuando está arriba el sistema

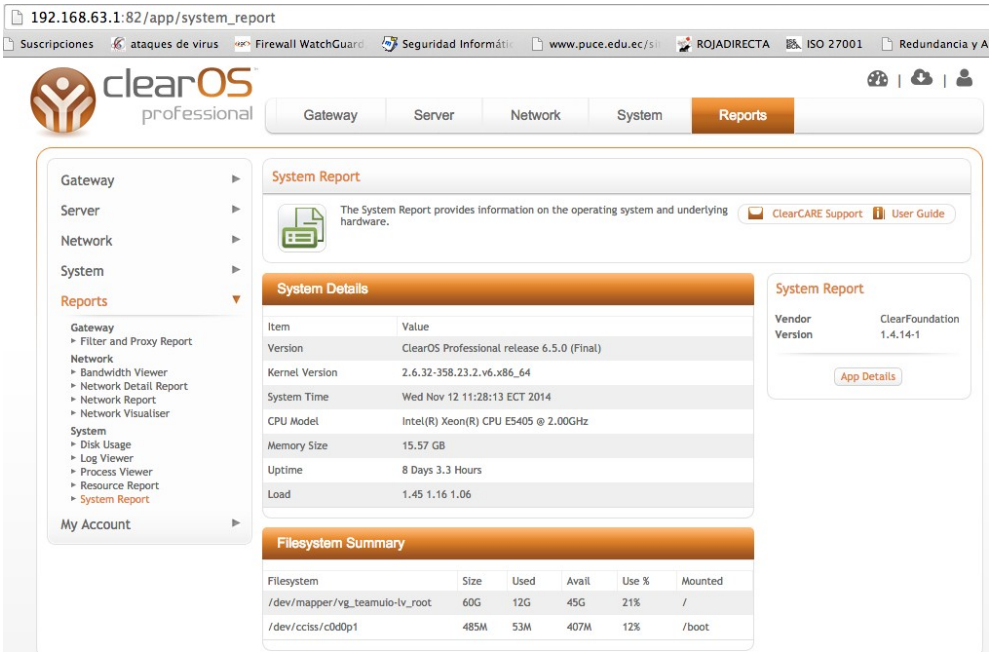


Figura 21. Reporte del sistema de ClearOS.

Como se puede apreciar en la siguiente imagen, ClearOS tiene dos tipos de menús que en sí despliegan la misma información, o por así decirlo, las mismas opciones, las mismas que para que aparezcan tienen que ser descargadas e instaladas del market-place, en donde podremos encontrar aplicaciones gratuitas así como de pago, con opción a que sean por un año o algunas que sean instaladas ya con el paquete que hayamos seleccionado al momento de comprar.

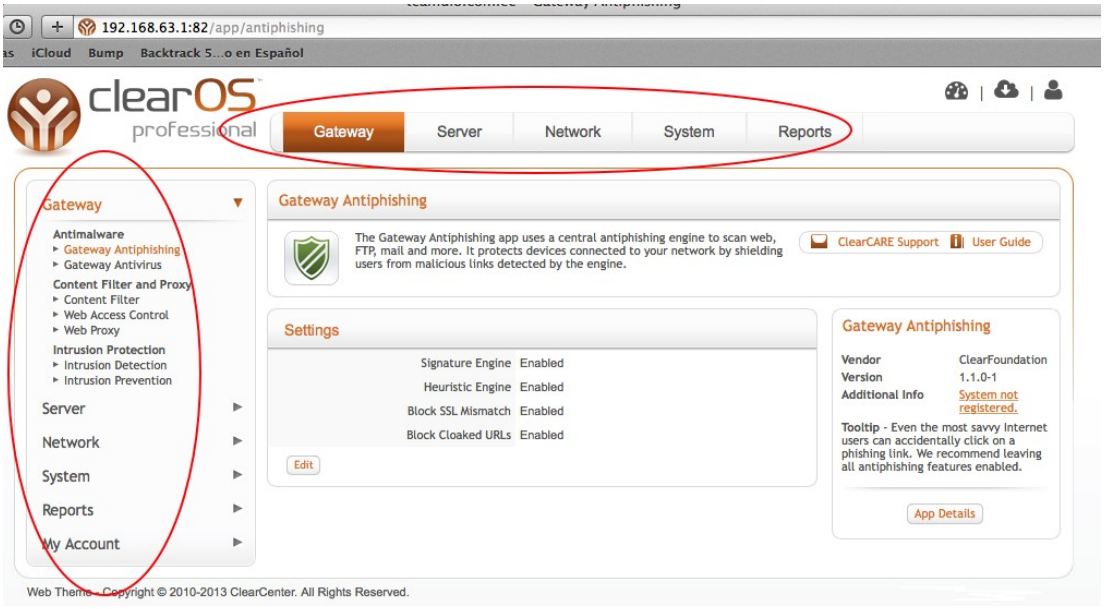


Figura 22. Menús de ClearOS.

Algunas de las funcionalidades más interesantes dentro de ClearOS, se encuentra en el menú: Network-> IP Settings-> Network Interfaces, donde encontraremos opciones de crear VLANS o a su ver Interfaces virtuales, como podemos ver a continuación.

Figura 23. Network Interfaces.

Se procederá a configurar el acceso vía ssh para nuestro firewall, para tener otra opción de configuración aparte de la interfaz gráfica, por lo que

realizaremos lo siguiente: Iremos al menú Network-> Infraestructure-> SSH Server y encontraremos la siguiente pantalla:

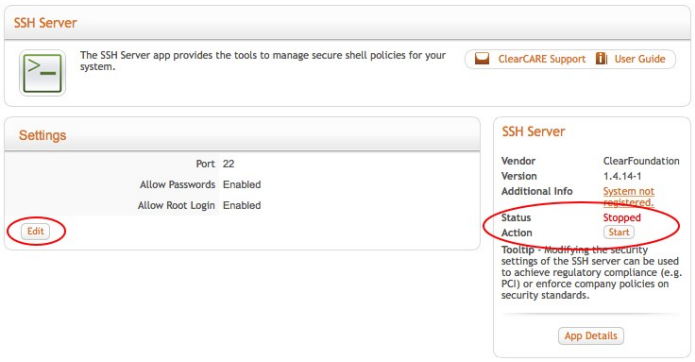


Figura 24. Configuración del servidor de SSH.

Damos click en el botón editar y colocaremos el puerto por donde queremos conectarnos, que por default se encuentra en 22 y habilitaremos las opciones de permitir contraseñas y del acceso de “Root” y luego daremos click en update.

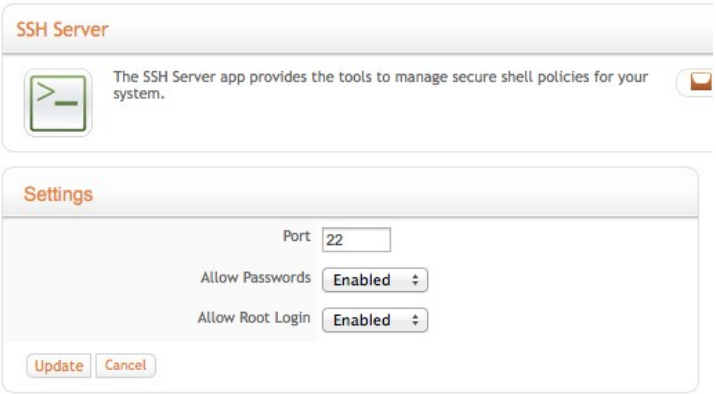


Figura 25. Parámetros para habilitación del acceso vía SSH.

Luego de esto damos click en el botón start, descrito en la Figura 36, y probamos el acceso por consola.

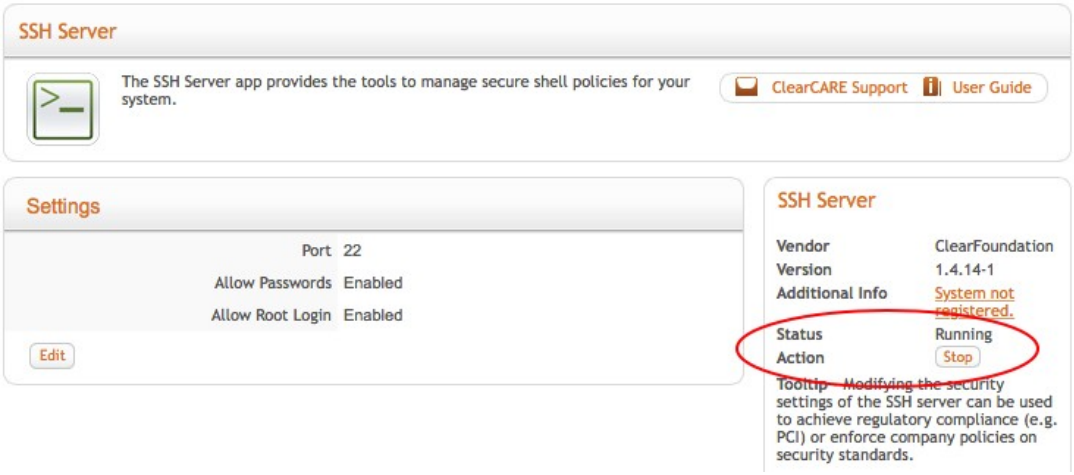


Figura 26. Habilitación del acceso vía SSH.

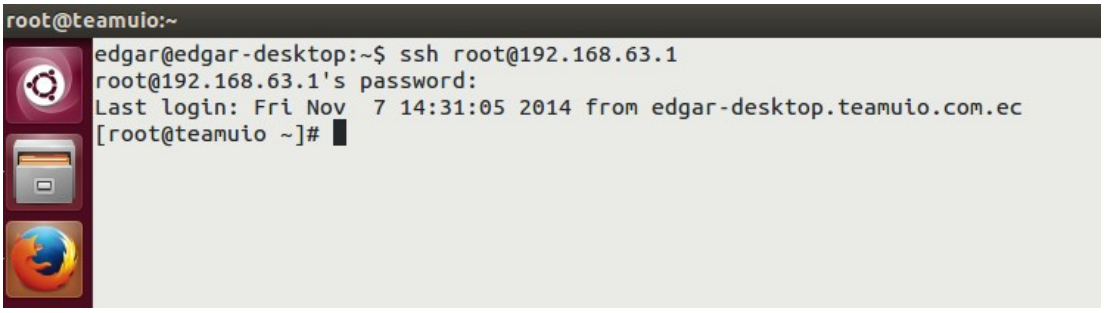


Figura 27. Prueba de acceso vía SSH, consola, desde un host dentro de la red.

4.3. Configuración del Servidor de DHCP.

Al momento de definir los distintos pools de direcciones a entregar en las diferentes áreas, es necesario recordar que habrá equipos que por su distribución en la red, tendrán que tener una IP fija, ya que para acceso o configuración de servidores, estas IPs no deberán cambiar nunca, ni deberán ser tomadas por otros equipos, por lo que en algunos casos los rangos de direcciones entregadas automáticamente serán reducidos, o en algunos casos nulos, y si alguien desea tener alguna de esas direcciones deberá ser gestionado manualmente.

Para la configuración del servidor DHCP dentro de ClearOS, nos dirigiremos a las siguientes opciones: Network-> Infraestructure -> DHCP Server -> Subnets, en esta parte tomamos una de las redes que hemos creado, para

este ejemplo será la subred 192.168.63.0/24 y le daremos click en edit, como muestra la siguiente figura:

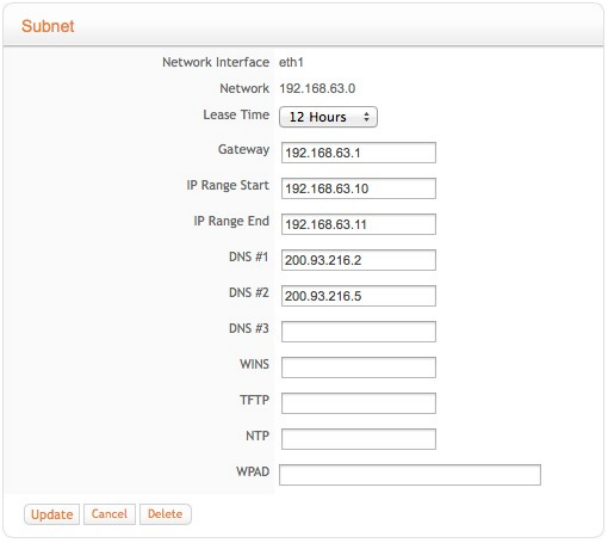


Figura 28. Configuración de DHCP en la subred 192.168.63.0.

Como vemos podemos ver algunas opciones, las cuales son configurables según nuestras necesidades, y para este caso colocaremos los parámetros detallados en la imagen anterior, en la cual señalaremos que función cumplen cada uno:

Lease time (tiempo de concesión): 12 horas (el tiempo mínimo)
Gataway: 192.168.63.1
IP Range Start (IP inicial): 192.168.63.10
IP Range End (IP final): 192.168.63.11
DNS #1: 200.93.216.2
DNS #2: 200.93.216.5

De los parámetros anteriores notamos que la IP de inicio y final del rango para esta subred, no tiene nada que ofrecer a algún dispositivo que se haya unido a la red, por lo que si alguien quiere tener acceso a internet tendrá que pedírselo al administrador de la red.

De igual manera para que no haya confusión con los DNSs colocamos los mismos que nos ofrece nuestra compañía proveedora de internet y así no tendremos problemas.

Cabe mencionar que los usuarios no tendrán que hacer alguna configuración adicional en sus equipos o dispositivos, sino que el administrador de la red será quien configure las direcciones MAC de los equipos para las IPs respectivas, por lo que tan solo con unirse a algún Access Point con la respectiva clave obtendrá una dirección IP de clase B como esta: 169.254.x.x, la cual es usada cuando no hay un servidor DHCP disponible, y en cuanto el administrador de la red haya registrado la dirección MAC en el servidor DHCP de ClearOS se le asignará una IP válida, para esto iremos a la opción “Leases” del menú anterior, Network-> Infraestructure -> DHCP Server y daremos click en el botón “Add”:

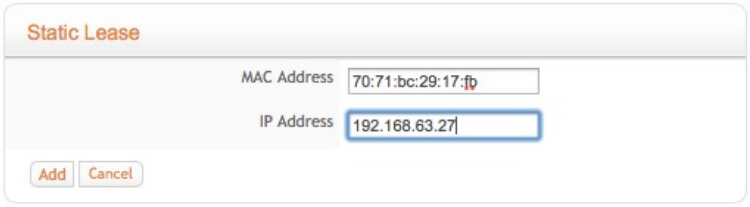


Figura 29. Agregar IPs manualmente.

Damos click en el botón “Add” y luego buscamos nuestra IP dentro del reporte y le damos en “Edit”

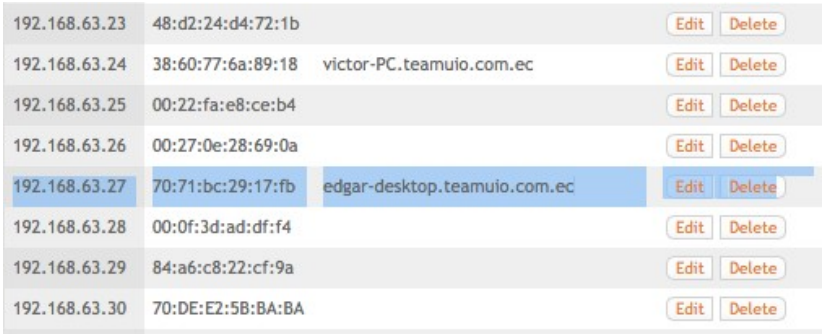


Figura 30. Reporte de IPs con DHCP

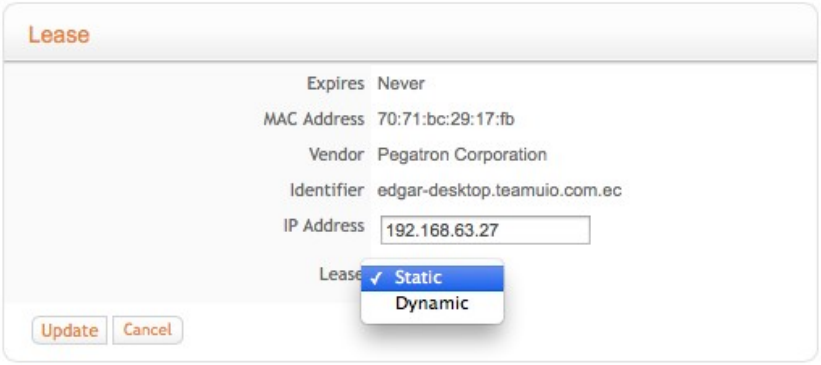


Figura 31. Tipo de concesión.

Como podemos ver las opciones que se nos presentan son: cambio de IP y el tipo de concesión, por lo que la colocaremos en “Static” y así ClearOS no le asignará a nadie más la IP 192.168.63.27, además de mostrarnos información como el nombre del equipo seguido del dominio que configuramos para ClearOS, el vendedor o marca de la tarjeta de red y el tiempo en el que expira la concesión, estos datos pueden estar presentes solo en algunos equipos, o a su vez no aparecer más información que solo la IP y MAC del equipo.

Debido a que nuestro servidor que estamos utilizando como equipo físico tiene la disponibilidad de cuatro interfaces físicas, no vamos a hacer uso de la configuración de VLANs, sino que se utilizaremos dichas interfaces para un mejor funcionamiento de nuestra red.

Tabla 42. Distribución de interfaces físicas según las zonas respectivas

Grupo	Interfaz	IP
Hot LAN	eth3	192.168.61.X
Usuarios no poder	eth2	192.168.62.X
Usuarios de poder	eth1	192.168.63.X

Se procederá a crear las redes correspondientes según nuestro diseño.

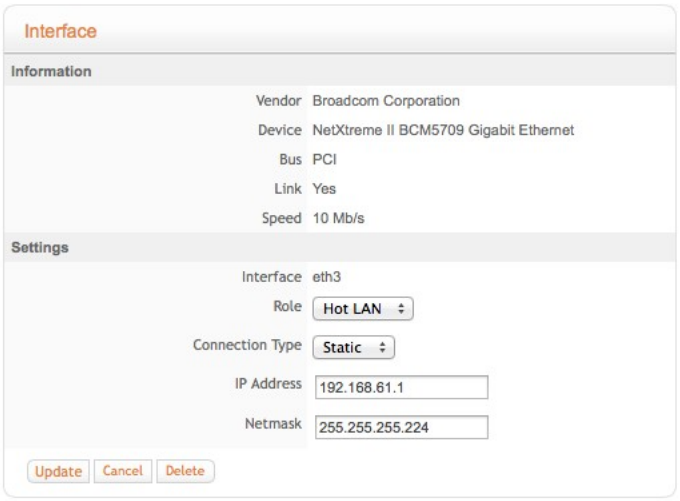


Figura 32. Creación de interfaces según nuestro diseño.

Realizaremos el mismo proceso para las demás redes y tendremos lo siguiente:

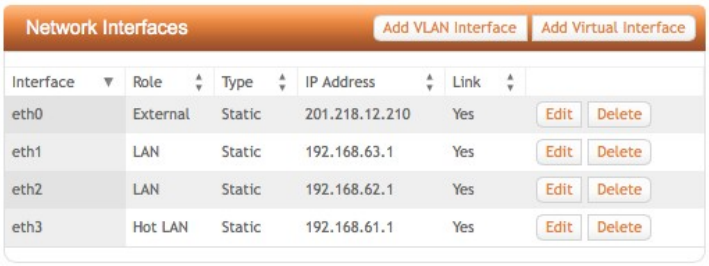


Figura 33. Interfaces creadas según el diseño propuesto.

Para las demás zonas tendremos que seguir los mismos pasos para signar el servicio de DHCP, el cual será acorde a las necesidades de cada LAN.

4.4. Configuración de reglas de acceso al Firewall.

A pesar de que la interfaz web de ClearOS nos ofrece muchas posibilidades de uso del firewall como tal, también tiene la opción de aceptación y negación de acceso mediante “iptables” para lo cual nos dirigiremos a la siguiente opción: Network -> Custom Firewall -> Rules, dentro de esta opción encontraremos la el botón “Add” para añadir una regla, esto lo haremos para algunos de los dispositivos que deben estar unos bloqueados y otros con salida desde nosotros hacia ellos, por lo que por ejemplo configuraremos la siguiente regla para la Central Telefónica de la empresa:

Figura 34. Reglas de firewall con iptables.

Como vemos no hay más opciones que configurar, la regla a negar en este caso desde el exterior y una etiqueta que identifique la regla de la que se trata, hacemos click en “Update” y podremos ver la regla creada, la cual al dar click sobre ella, nos aparecerá toda la regla, como se puede ver a continuación:

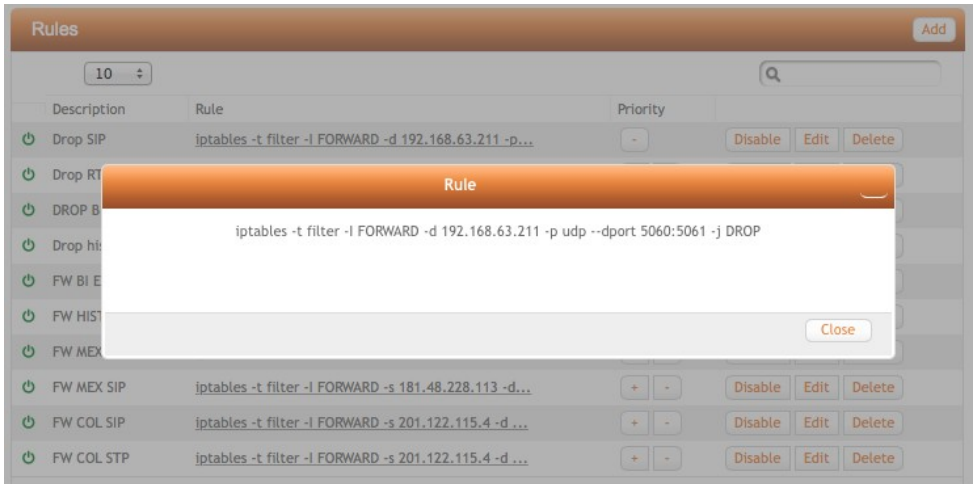


Figura 35. Descripción de la regla configurada.

Debido a que TeamSourcing maneja distintas sucursales en distintos países unas más grandes que otras según la operación que se esté llevando a cabo, se han configurado reglas para acceso del Call-center desde el exterior, en su mayoría México y Colombia, para que las operadoras de Ecuador puedan atender requerimientos de consultas o requerimientos de estos países, es por eso que tenemos algunas reglas configuradas para ese fin.

Todo esto diseñado y alineado a las Políticas de gestión de las comunicaciones y operaciones, descritas en la *tabla 30* y sus consecuentes ítems, los cuales nos dan normas a seguir para el cuidado de IPs, topologías y direccionamiento según las necesidades de la empresa.

4.4.1. Reglas de acceso a redes sociales

Como en toda empresa sucede, las redes sociales en la actualidad son los sitios web más visitados durante todo el día, para lo cual según estadísticas

arrojan que el medio más usual para hacerlo es vía aplicaciones móviles, gastando al nivel mundial 700 billones de minutos en Facebook por mes teniendo un promedio de contactos de 130, con lo cual se puede definir que dentro de una empresa, donde el ancho de banda sea limitado y haya usuarios con un promedio de edad, de entre: 18 a 35, estaríamos bastante expuestos a dedicar un ancho de banda considerable al momento de navegar, es por eso que ClearOS nos ofrece filtros en nuestro firewall para poder acceder o no a las redes sociales o a cualquier dominio en internet que no sea llamado a la productividad. (Granja, 2014)

Para lo cual iremos al menú Network-> Firewall-> Egress Firewall y seleccionaremos en el recuadro “Destination Domain” el botón “add”, en donde añadiremos un Nick para la regla y el dominio a bloquear, de la siguiente manera.

Figura 36. Reglas de firewall de salida.

Daremos click en “add” y añadiremos todos los sitios que queramos bloquear y quedará de la siguiente manera:

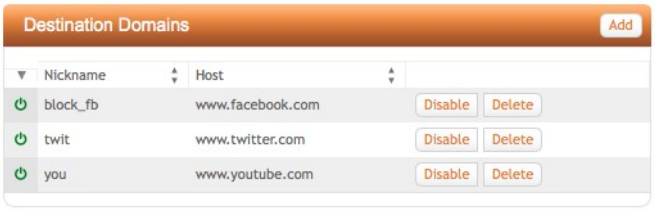


Figura 37. Reglas para redes sociales.

En este mismo menú nos ofrece también la posibilidad de bloquear puertos para bloquear el acceso total a estos, para lo cual nos ofrece la posibilidad de bloquear, por servicio, por puerto, o por rango de puertos, para lo cual bloquearemos el puerto de HTTPS, 443, de manera didáctica, ya que funcionalmente no es muy recomendable hacerlo.

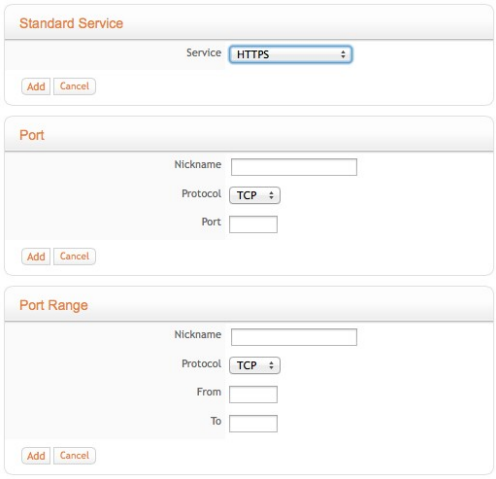


Figura 38. Bloqueo de puertos y servicios.

Figura 39. Bloqueo del servicio de HTTPS.

4.5. Configuración de administración de Ancho de Banda y QoS

4.5.1. Administración de Ancho de Banda

El gestor de ancho de banda es una herramienta utilizada para priorizar o establecer una política de tráfico entrante y saliente de nuestro firewall, y así obtener un mejor desempeño de nuestra red en las áreas que más se necesita, para esto ClearOS puede limitar el uso de ancho de banda la dirección IP, un determinado rango de direcciones IP y puertos.

Esta opción se encuentra disponible dentro del menú Network -> Bandwidth and QoS -> Bandwidth.

Para poner en práctica una mejor utilización de esta herramienta es necesario definir los tipos de criterios que se pueden tomar en cuenta para un mejor desempeño, los cuales son:

- **Limit**.- Límite del tráfico de baja prioridad, en un esfuerzo por mejorar las velocidades del tráfico de alta prioridad.
- **Reserve**.- Ancho de banda de reserva para el tráfico de alta prioridad que dejará el tráfico de baja prioridad a un lado.

Es imposible determinar a ciencia cierta cual será el tráfico de baja prioridad, por lo que es más fácil y práctico fijarnos a que tipo de tráfico se le debe asignar un ancho de banda fijo, como puede ser en cualquier empresa, la voz sobre IP, dedicado a un central telefónica o un Call-center, por lo que esa sería una de nuestras premisas de alta prioridad.

Las tasas de ancho de banda de subida o de bajada en la interfaz de red conectada a nuestro ISP deben estar establecidas de una manera lo más real posible, ya que si establecemos un valor menor al que nos brinda la empresa proveedora de internet, pues este será un limitante para nuestra red interna. Para esto tendremos la siguiente interfaz:

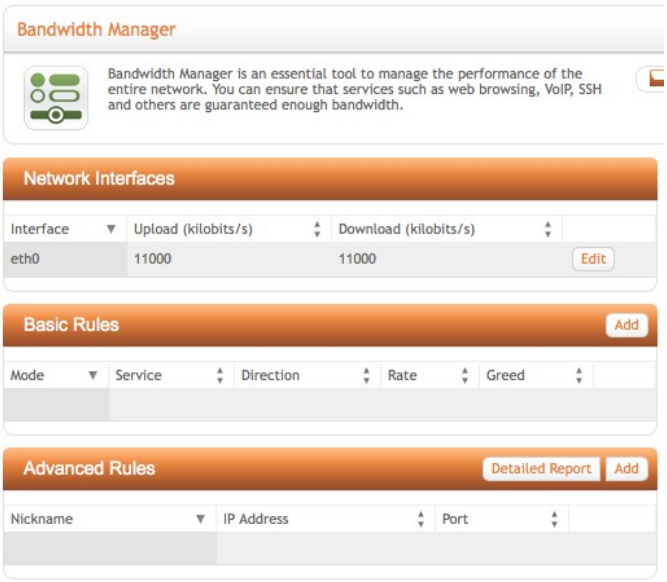


Figura 40. Administrador de Ancho de Banda.

Como podemos ver en la figura anterior, ya se ha establecido un ancho de banda de subida y de bajada, la cual TeamSourcing tiene por contrato 10MB, y es por esa razón que dichos valores los hemos colocado en 11000Kbits/s

En este panel también hay opciones de “Reglas Básicas” y “Reglas Avanzadas”, las cuales deberemos implementar con cierto cuidado, ya que podríamos causar el malestar de usuarios los cuales necesitan recursos

importantes de velocidad de internet, para esto, daremos click en el botón "Add" de la Opción "Basic Rules" y configuraremos lo siguiente:

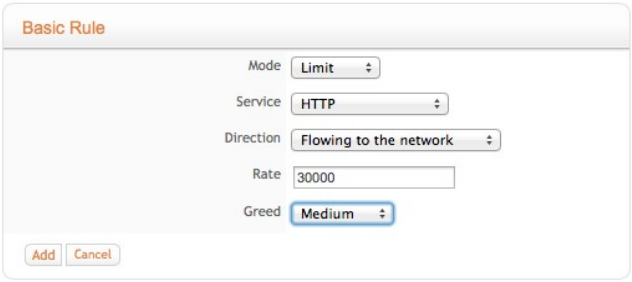


Figura 41. Ejemplo de regla básica de límite de ancho de banda.

Haremos lo mismo para el tráfico HTTP que sale de la red y tendremos lo siguiente:

Figura 42. Reglas básicas para navegación web

Como reglas un poco más exhaustivas o dedicadas a un host en específico por ejemplo que está consumiendo demasiado ancho de banda o con muchas descargas, podríamos hacer una regla para este host o para un pool de direcciones, denotándolas estas de la siguiente manera:

- Hacia una IP específica: 192.168.63.27.
- Hacia un grupo de direcciones: 192.168.63.10 : 192.168.63.200
- Hacia todo el pool de direcciones: 192.168.63.0/24

Para estos casos específicos dentro de la opción "Advance Rueles" daremos click en el botón "Add" y configuraremos lo siguiente:

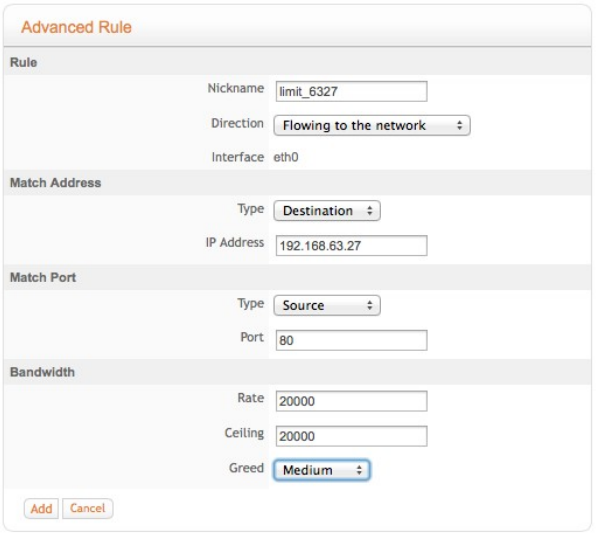


Figura 43. Ejemplo de Regla Avanzada para un host específico.

Para lo cual tendremos la siguiente regla:

Figura 44. Regla avanzada con restricción hacia la web.

Si deseamos un reporte de la regla más detallado daremos click en el botón “Detailed Report” y nos mostrará lo siguiente:

Figura 45. Reporte detallado de reglas avanzadas.

Es importante dar a notar que todas las reglas deben estas habilitadas para que su funcionamiento surja efecto, por lo que deberemos dar click en el botón “Enable” para que esto suceda, además de tener un botón dedicado a hacer que el Gestor de Ancho de Banda funcione, el botón “Start/Stop” el cual nos indicará el estado de esta funcionalidad, lo encontraremos en el recuadro de la parte derecha de la pantalla.

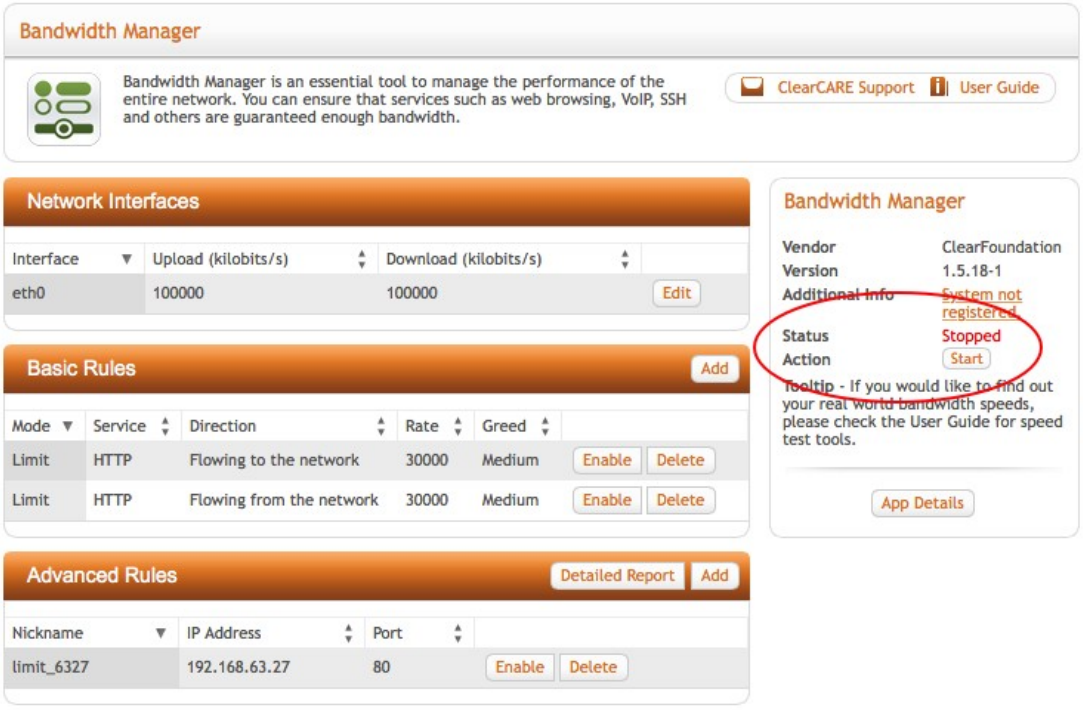


Figura 46. Interfaz de gestión de ancho de banda.

4.5.2. QoS (Calidad de Servicio)

La aplicación de calidad de servicio se encuentra todavía en una versión Beta, por lo que solo explicaremos un poco de su funcionamiento y como nos podría ayudar con el desempeño de la red y como un adicional a lo antes descrito en la parte sección de Administración de Ancho de Banda.

Para encontrar esta función iremos al menú Network -> Bandwidth and QoS -> QoS y se nos desplegará la siguiente pantalla:

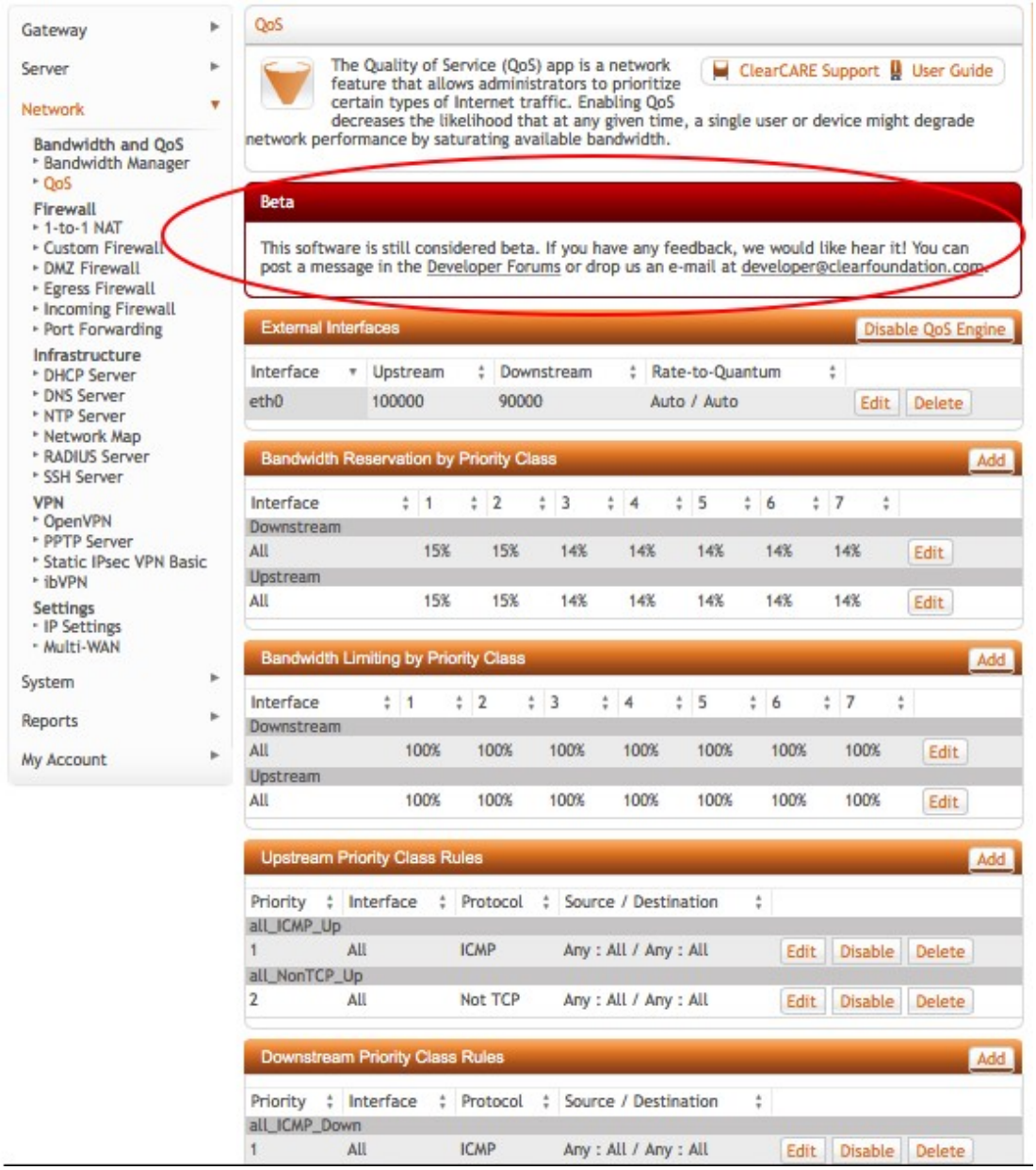


Figura 47. Interfaz de QoS.

Como podemos ver en el recuadro señalado, nos advierte que esta software todavía lo consideran como una versión Beta, por lo que no nos ofrecería las garantías reales de que podamos filtrar el tráfico en las distintas interfaces y con las distintas prioridades del caso, pero en todo caso se mantendrá al tanto de las versiones resientes del ClearOS para poder implementar esta funcionalidad en el futuro.

4.6. Reportes

En esta sección tenemos varias opciones que nos pueden ayudar a visualizar estadísticas en tiempo real desde el funcionamiento del equipo que aloja a ClearOS hasta reportería que nos puede ayudar a determinar posibles causas de navegación lenta o de intermitencias en la red, así como también nos presentará una lista de usuarios que pueden estar acaparando el ancho de banda y así poder tomar acciones.

NOTA:
Se debe tomar muy en cuenta que tal como lo describe la *tabla 30* y sus ítems consecuentes, esta información debe de ser de acceso exclusivo del administrador de la red en turno o del personal que este lo delegue, siempre tomando en cuenta su capacidad para administrar el Sistema.

El menú de reportes tiene las siguientes opciones:

Figura 48. Opciones de reportes de ClearOS.

Resource Report.

De las cuales solo haremos referencias a las más relevantes, dentro del menú Reports -> System -> Resource Report, tenemos reportes de:

- Carga del Sistema.
- Memoria RAM
- Memoria SWAP
- Procesos
- Tiempo activo

De los cuales tenemos las siguientes imágenes:

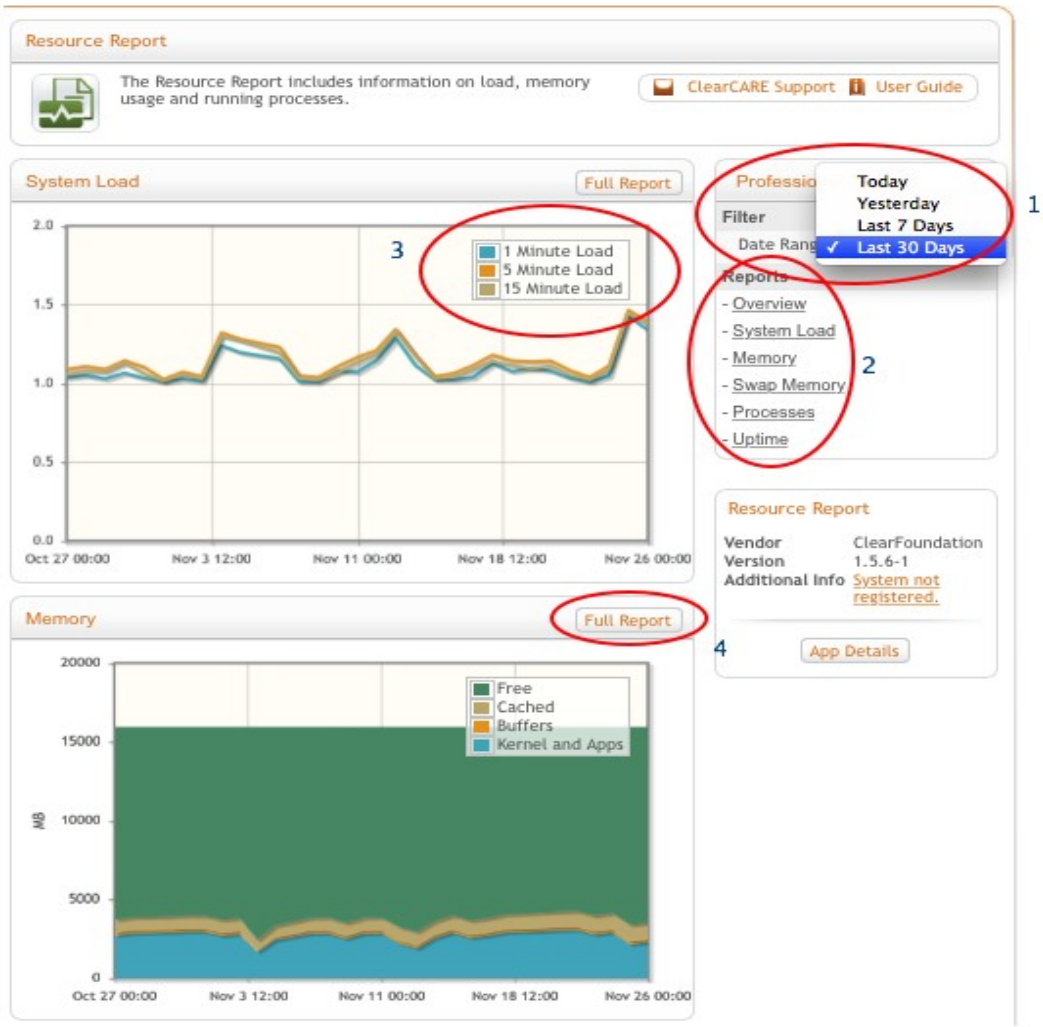


Figura 49. Reportes del Sistema.

En donde podemos ver algunos detalles que están presentes en algunos reportes, tales como:

1) Date Range: El rango de fechas a visualizar en el o los reportes en general.
2) Reports: Reportes disponibles a visualizar, que van desde el resumen, hasta visualizarlos a cada uno por separado.
3) Leyendas: Explicación del significado de cada color según el reporte.
4) Full Report: La opción de visualizar un reporte detallado además de las gráficas ya presentadas, con datos según el rango que se elijan.

Reporte de Uptime.

De este menú podemos destacar el reporte de “Uptime” del sistema, el cual en este último mes ha tenido un comportamiento muy normal, excepto en el día 04/11/2014, en el que se tuvo que hacer un reinicio del sistema, razón por la cual se presenta un pico bajo en el reporte detallado, como en la gráfica en sí.

Figura 50. Gráfica de tiempo de actividad de ClearOS

Network Visualiser

En el menú Reports -> Network -> Network Visualiser, podremos encontrar información que nos será muy útil en el día a día, ya que nos enseña el consumo de ancho de banda de cada IP, organizándola de la manera que más nos convenga, como veremos en la siguiente figura.

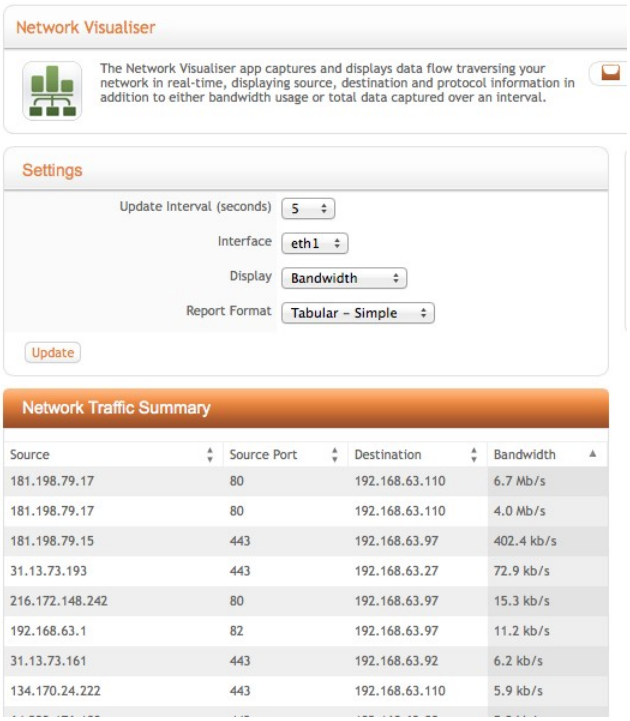


Figura 51. Visualizador de red.

En este reporte tenemos como opciones el intervalo de tiempo en el que tomará los datos, la interface a analizar, que en este caso será la eth1 para visualizar el tráfico de nuestra red local, que es lo que queremos visualizar, en este caso será el ancho de banda, aunque también tiene como opción las transferencias totales, y el formato del reporte que en este caso hemos seleccionado en tabulaciones simples, aunque también se tiene las opciones de tabulaciones detalladas y un reporte gráfico.

Si escogemos la opción “Tabular Detailed”, nos mostrará la IP que más paquetes ancho de banda ha consumido durante el día, así como muestra la siguiente gráfica.

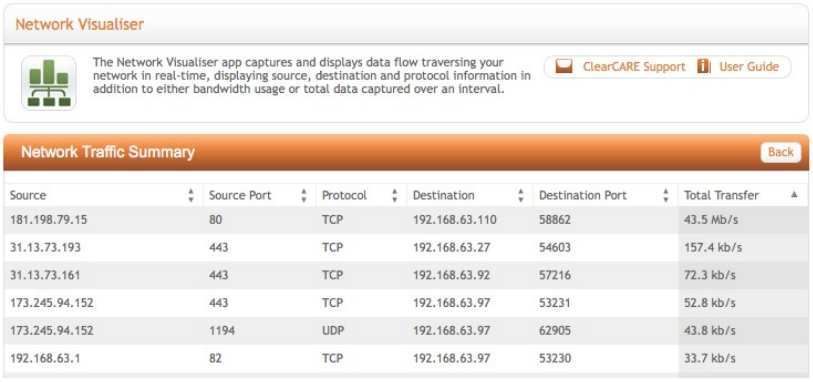


Figura 52. Reporte de red detallado.

Network Detailed Report

Este reporte lo podemos encontrar en el menú Report -> Network -> Network Detail Report, el cual nos brinda una visión histórica de información de la red por tipos de IP, usuario y dispositivo, este tipo de informe nos es de mucha ayuda ya que nos ayuda en el monitoreo de la red, así como el uso y abuso de la misma.

En su totalidad los reportes se presentarán en gráficas que nos dan un top ten de los datos según sea el reporte, a continuación haremos énfasis en el reporte de Top IPs, el cual nos indica las IPs que más ancho de banda han consumido, esto puede ser filtrado, por día, semana, o los últimos 30 días, como veremos en la siguiente figura.

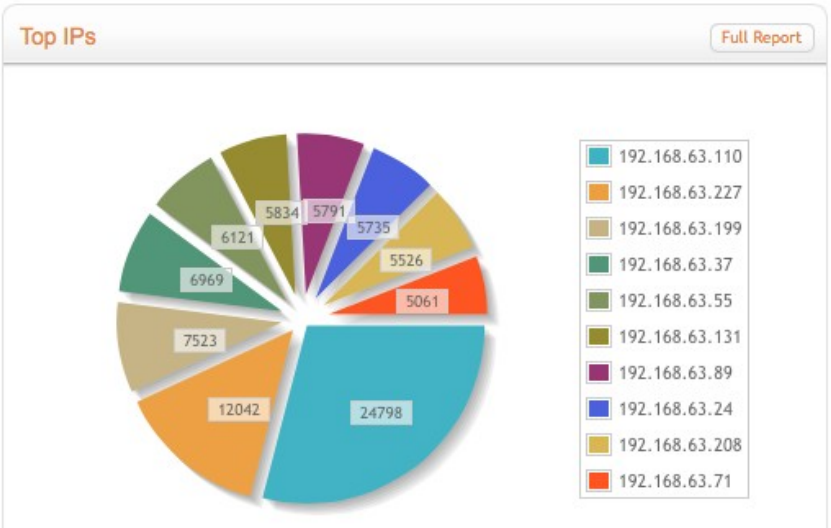


Figura 53. Reporte Top IPs

Si damos click en “Full Report” nos ofrecerá la información completa de esta opción, como podemos ver la IP: 192.168.63.110, correspondiente al Administrador de Base de Datos, es el equipo que más paquetes ha subido y bajado desde y hacia el internet.

Report Data

All

IP Address	Hostname	Download Size	Download Packets	Upload Size	Upload Packets
192.168.63.110	dbateam-PC.teamuio.com.ec	24798	18904715	1010	10862453
192.168.63.227	iMac-Any.teamuio.com.ec	12042	9898231	1229	5168543
192.168.63.199	192.168.63.199	7523	5983463	267	3584512
192.168.63.37	iPhone-de-Cesar.teamuio.com.ec	6969	5692242	317	3185750
192.168.63.55	lex-PC.teamuio.com.ec	6121	5577165	342	3531632
192.168.63.131	RRHH.teamuio.com.ec	5834	5250658	474	3328527
192.168.63.89	Intel-PC.teamuio.com.ec	5791	5229725	1099	2934626
192.168.63.24	victor-PC.teamuio.com.ec	5735	6183967	849	4023123
192.168.63.208	192.168.63.208	5526	4168824	98	1729860
192.168.63.71	MBPdeGiacomo652.teamuio.com.ec	5061	5301730	1392	3537704
192.168.63.87	MININT-QH437ER.teamuio.com.ec	4693	4050542	276	2303231
192.168.63.11	Jenny-PC.teamuio.com.ec	4686	4077116	272	1937903
192.168.63.27	iPhone-de-Alex.teamuio.com.ec	4360	6511321	619	5711722
192.168.63.147	192.168.63.147	3835	2797959	93	1505588
192.168.63.83	MBPdeGiacomo652.teamuio.com.ec	3744	3388451	213	2862349
192.168.63.72	iPaddeGrizzonte.teamuio.com.ec	3712	2620583	87	1604952
192.168.63.85	Kary-PC.teamuio.com.ec	3668	3422572	294	2032301

Figura 54. Reporte detallado de Top IPs

5. CAPÍTULO V

Pruebas y evaluación de ClearOS

5.1. Pruebas de funcionamiento de ClearOS

Para la realización de las pruebas a realizarse a continuación, se establecerán escenarios donde se pueda demostrar el correcto funcionamiento y desempeño de las funcionalidades de ClearOS, instaladas y configuradas, para lo cual se utilizarán herramientas de software libre.

5.1.1. Pruebas de funcionamiento de DHCP

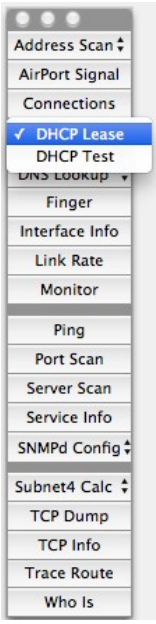


Figura 55. IPNetMonitorX

Para probar el funcionamiento y desempeño de DHCP en ClearOS utilizaremos el programa de distribución libre IPNetMonitorX, el cual tiene algunas funcionalidades que nos ayudarán a determinar el tiempo en el que el servidor es capaz de responder a una petición de IP, de un dispositivo que

previamente haya sido registrado su dirección MAC en ClearOS, como ya lo habíamos plateado anteriormente.

En la opción “DHCP Lease” encontramos la información actual, de nuestro equipo, que en este caso será la IP: 192.168.63.97, como se muestra en la siguiente figura.

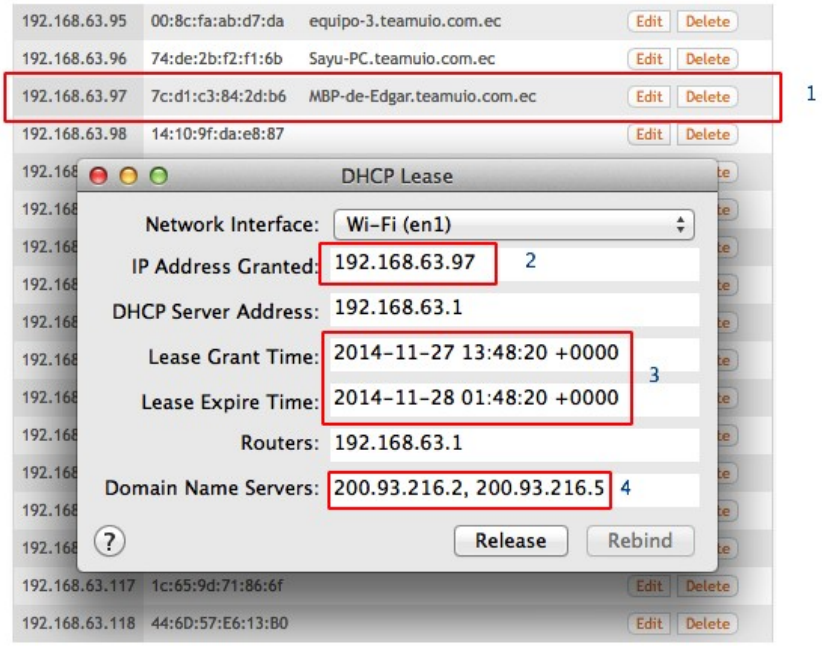


Figura 56. DHCP Lease

De donde:

1. Muestra en ClearOS la IP asignada manualmente para el dispositivo con id “MBP-de-Edgar.teamuio.com.ec”.
2. Se muestra la misma IP: 192.168.63.97, como IP asignada en la herramienta IPNetMonitorX.
3. Se muestra el tiempo cuando fue concesionada la IP y el tiempo en el que expira la misma, el cual previamente configuramos para que sea cada 12 horas, esto con el fin de que se liberen las IPs de equipos invitados cuando así se lo requiera.
4. Nos muestra los DNSs asignados, los cuales son los mismos que nos entregó nuestro proveedor de internet, para que no haya conflicto de DNSs.

Para determinar el tiempo en el que ClearOS asigna direcciones IP, utilizaremos la funcionalidad de “DHCP Test”, como se muestra en la siguiente figura.

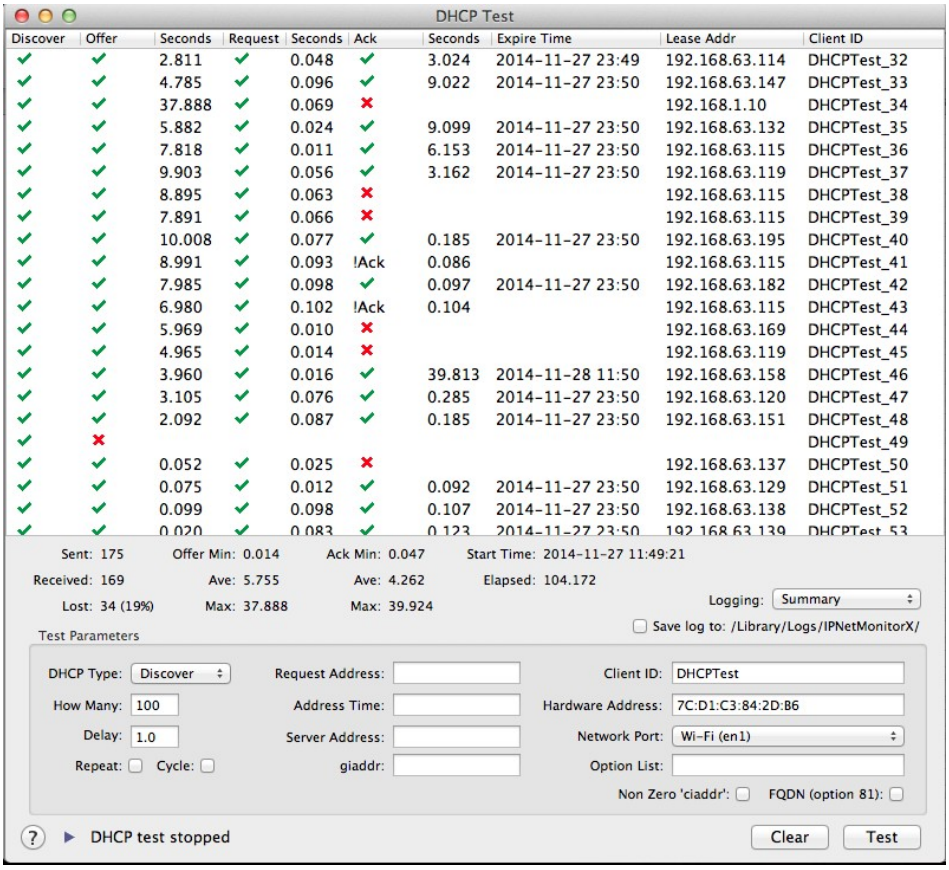


Figura 57. Interfaz de DHCP Test.

Como podemos ver en la figura anterior, se descubren direcciones IP en nuestra red todas bajo el un segundo de su petición, lo que es muy bueno considerando que son aproximadamente 150 host en total a diario en la empresa.

5.1.2. Pruebas de funcionamiento de DNS

Para probar el desempeño del Servidor del servidor de nombres, colocaremos como escenario el acceso o ping a una página web la cual deberá responder con rapidez a nuestra herramienta de IPNetMonitorX,

"Name Server Query" la cual nos da una información mucho más detallada que solo usar el comando "nslookup".

Name Server Query, nos muestra una información más completa del Servidor de Nombres de Domino de Internet, enviando peticiones al servidor de nombres por defecto.

Las respuestas obtenidas por la herramienta, resultaron exitosas, ya que en la información presentada en la siguiente figura, se detalla desde que servidor fue respondida la petición, así se comprueba que el dominio ha sido almacenado en el cache de ClearOS, por lo que nos dará una impresión de responder mucho más rápido a esta página la siguiente vez que vayamos a ingresar.

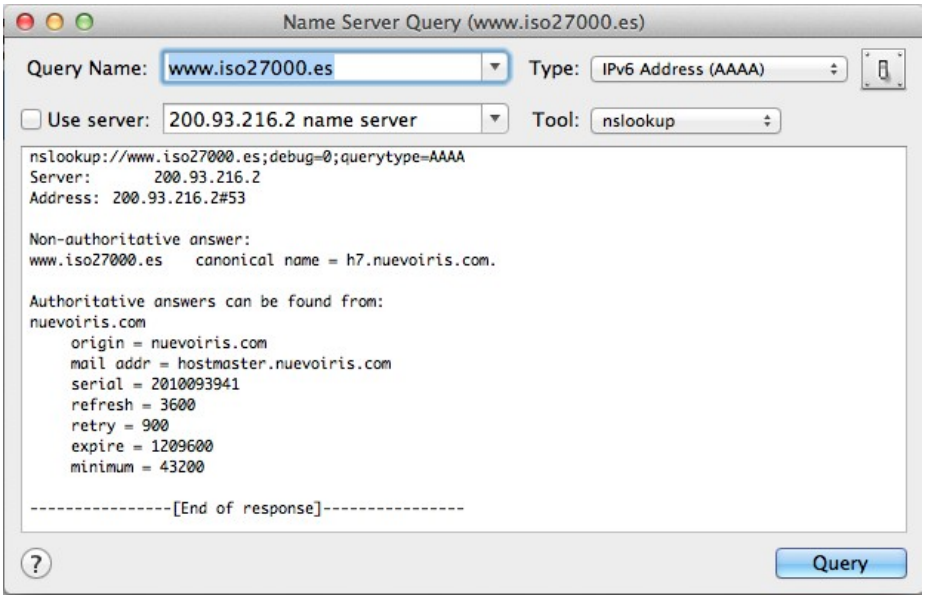


Figura 58. Pruebas de funcionamiento de DNS.

Como ya hemos notado en la herramienta de DHCP de ClearOS la mayoría de host registrados y asociados a nuestro sistema tienen como dominio "teamuio.com.ec", el cual es el dominio que nosotros asignamos a nuestra red local, por lo cual en el sistema, por ejemplo: "karen-PC", por defecto lo visualizaremos como:

192.168.63.41	74:e5:43:2a:33:18	JoseEspoz.teamuio.com.ec	Edit Delete
192.168.63.42	64:20:0C:68:53:06	iPadMarioNoboa.teamuio.com.ec	Edit Delete
192.168.63.43	1c:65:9d:71:81:f0	TEAM-PC1.teamuio.com.ec	Edit Delete
192.168.63.44	78:dd:08:e6:81:bf		Edit Delete
192.168.63.45	9c:b7:0d:74:02:f7	GabrielAlvarez.teamuio.com.ec	Edit Delete
192.168.63.46	60:36:DD:BA:BF:FD		Edit Delete
192.168.63.47	fc:75:16:86:f8:9b	karen-PC.teamuio.com.ec	Edit Delete
192.168.63.48	F8:1A:67:5E:44:34		Edit Delete
192.168.63.49	38:60:77:6a:89:31	Intel-PC.teamuio.com.ec	Edit Delete
192.168.63.50	B4:18:D1:42:90:6A	iPhone-de-Alex.teamuio.com.ec	Edit Delete
192.168.63.51	B8:88:e3:1d:5f:a6		Edit Delete
192.168.63.52	fc:75:16:86:f8:a8		Edit Delete
192.168.63.53	c8:0a:a9:26:e0:01		Edit Delete
192.168.63.54	20:68:9d:90:7c:2f	AlexDeLaTorre.teamuio.com.ec	Edit Delete
192.168.63.55	38:60:77:6a:89:30	lex-PC.teamuio.com.ec	Edit Delete

Figura 59. Servidor de Nombres de Dominio.

Con esto se demuestra que el servidor DNS está funcionando correctamente, si usaríamos un poco más a ClearOS como una herramienta de comunicación configurable para lo que es un servidor de mail o ActiveDirectory nos fuera de mucha ayuda, ya que complementaría s uso dentro de la empresa, pero para esto TeamSourcing cuenta con la ayuda de Google, por lo cual para este tipo de requerimientos se los administra de una manera diferente.

5.1.3. Medidas de tráfico local y hacia el internet.

Para este tipo de pruebas nos valdremos de nuestro proveedor de internet, Telconet, el cual nos ha proporcionado un usuario y contraseña para acceder a las gráficas que ofrece “Cacti”, el cual es un gestor dedicado a una visualización intuitiva mediante gráficas que denotan velocidad de conexión de internet, temperatura, velocidad, voltaje, número de impresiones, etc., tomando en cuenta rangos de fechas que van desde la última media hora atrás hasta los últimos dos años, si este fuera el caso,

pero con la condición que se podrá obtener datos desde el momento en que se haya activado Cacti para nuestra red.

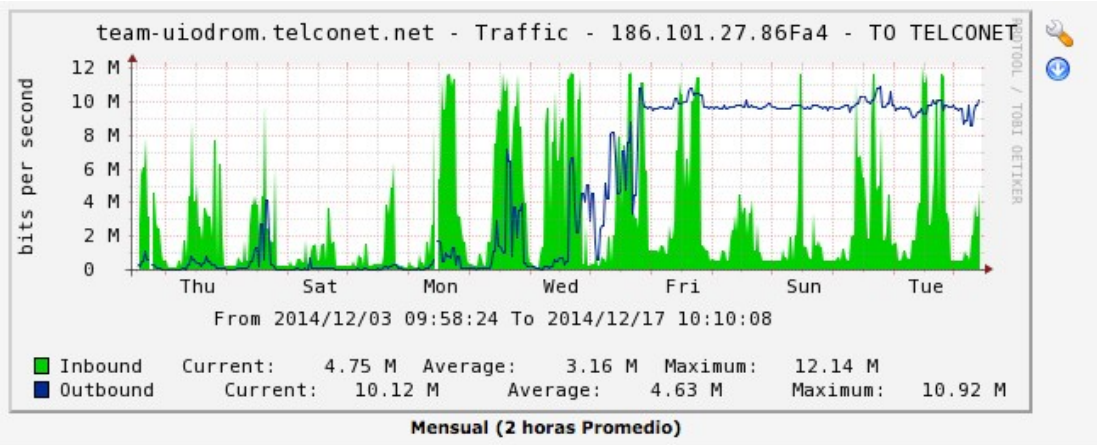


Figura 60. Mediciones del enlace de internet existente entre TeamSourcing y Telconet

Donde claramente se nota los picos más altos, que son entre las 09h00 y las 11h00 en la mañana y en la tarde desde las 14h00 y las 18h00, horas hábiles, en donde incluso los niveles de necesidad de internet, exceden el ancho de banda contratado, que es de 10MB/s

ClearOS desde su herramienta de reportería nos muestra información similar a la de Cacti, en donde podemos ver los picos altos y bajos de consumo de internet, localmente, es decir, en la interface LAN eth1.

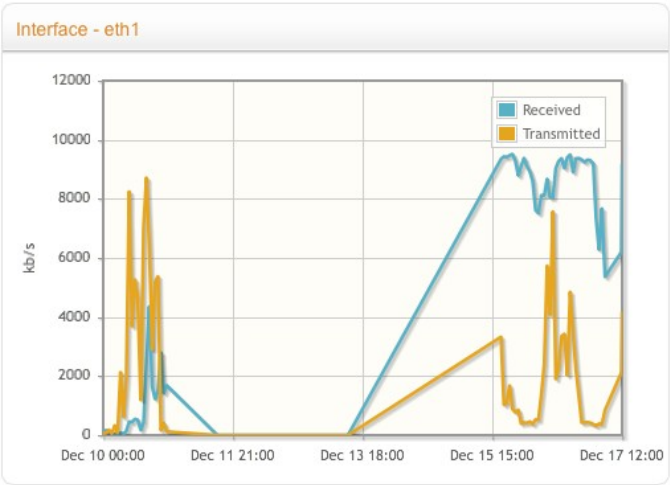


Figura 61. Mediciones de Ancho de Banda desde ClearOS.

5.1.4. Pruebas desde entre las distintas zonas.

Entre las distintas zonas deben de haber restricciones de permisos de acceso entre ellas, para lo cual, de ha delimitado tres zonas:

Tabla 43. Distribución de redes y zonas en TeamSourcing.

Grupo	Interfaz	IP
Hot LAN	eth3	192.168.61.X
Usuarios no poder	eth2	192.168.62.X
Usuarios de poder	eth1	192.168.63.X

Para esto haremos los siguientes escenarios:

- Conectividad entre las distintas zonas.

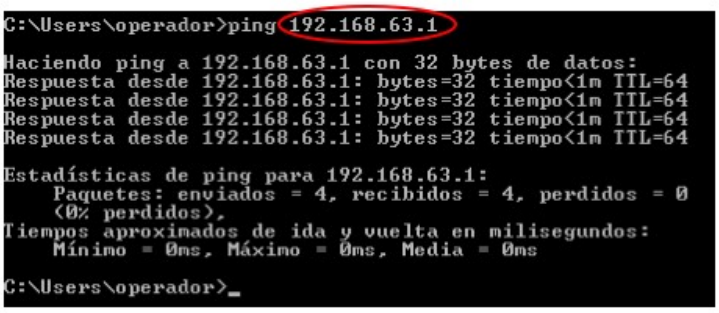


Figura 62. Conectividad hacía el gateway de la zona de Poder desde la zona de No Poder

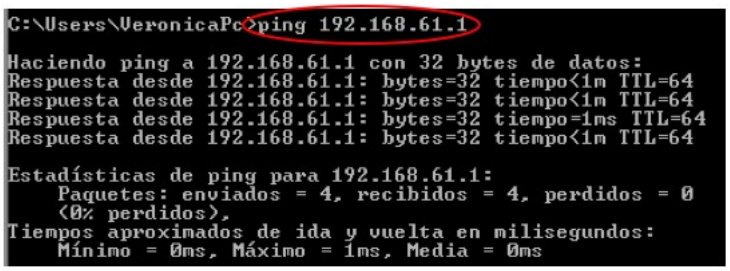


Figura 63. Conectividad hacía el gateway de la zona de Hot LAN desde la zona de No Poder

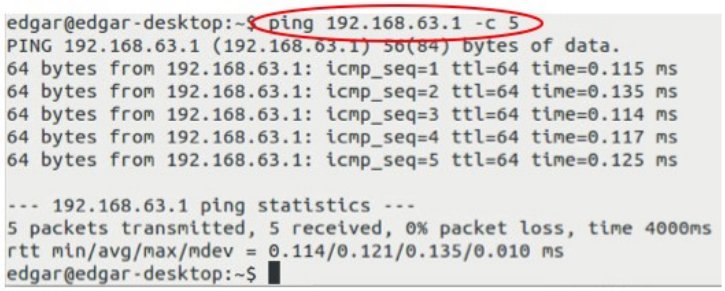


Figura 64. Conectividad hacía el gateway de la zona de Poder.

- Acceso desde la red de Poder a todos los servicios, usuarios y zonas

Se tiene los servicios de http, https, web, es decir sin restricciones:

```
MacBook-Pro-de-Edgar:~ Usuario$ ping www.facebook.com
PING star.c10r.facebook.com (31.13.73.1): 56 data bytes
64 bytes from 31.13.73.1: icmp_seq=0 ttl=84 time=66.774 ms
64 bytes from 31.13.73.1: icmp_seq=1 ttl=84 time=61.643 ms
64 bytes from 31.13.73.1: icmp_seq=2 ttl=84 time=66.820 ms
64 bytes from 31.13.73.1: icmp_seq=3 ttl=84 time=67.228 ms
64 bytes from 31.13.73.1: icmp_seq=4 ttl=84 time=63.924 ms
64 bytes from 31.13.73.1: icmp_seq=5 ttl=84 time=62.023 ms
64 bytes from 31.13.73.1: icmp_seq=6 ttl=84 time=62.003 ms
^C
--- star.c10r.facebook.com ping statistics ---
7 packets transmitted, 7 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 61.643/64.345/67.228/2.351 ms
```

Figura 65. Acceso a Redes Sociales.

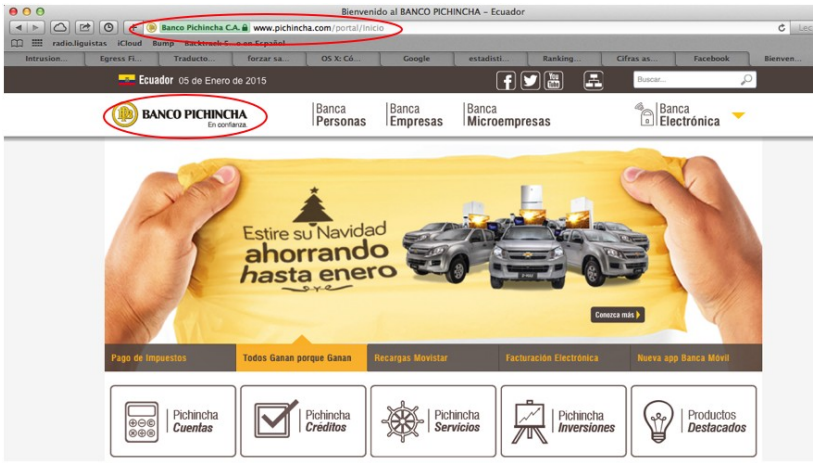


Figura 66. Acceso a Paginas https.

- Acceso de la red de No Poder solo a ciertas ventajas de navegación más.

```
C:\Users\VeronicaPc>IPCONFIG

Configuración IP de Windows

Adaptador de LAN inalámbrica Conexión de área local* 1:

   Estado de los medios. . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

   Estado de los medios. . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . : teamuio.com.ec

Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . : teamuio.com.ec
   Vínculo: dirección IPv6 local. . . : fe80::b4c9:823a:899b:e5ff%12
   Dirección IPv4. . . . . : 192.168.62.13
   Máscara de subred . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . : 192.168.62.1

Adaptador de túnel Conexión de área local* 8:

   Estado de los medios. . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de túnel Teredo Tunneling Pseudo-Interface:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv6 . . . . . : 2001:0:5ef5:79fd:4ef:2a97:3f57:c1f2
   Vínculo: dirección IPv6 local. . . : fe80::4ef:2a97:3f57:c1f2%18
   Puerta de enlace predeterminada . . . . . : ::

Adaptador de túnel isatap.teamuio.com.ec:

   Estado de los medios. . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . : teamuio.com.ec

C:\Users\VeronicaPc>
```

Figura 67. Prueba con el Host 192.168.62.13

- No navegación en redes sociales:

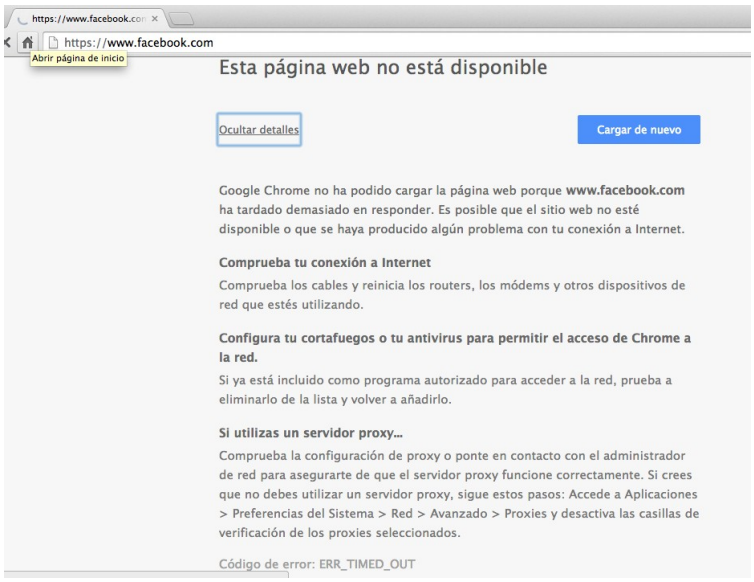


Figura 68. No acceso a redes sociales.

- El no acceso a la zona de Servidores desde las demás zonas.

Figura 69. No acceso a la zona de servidores desde la zona de No Poder.

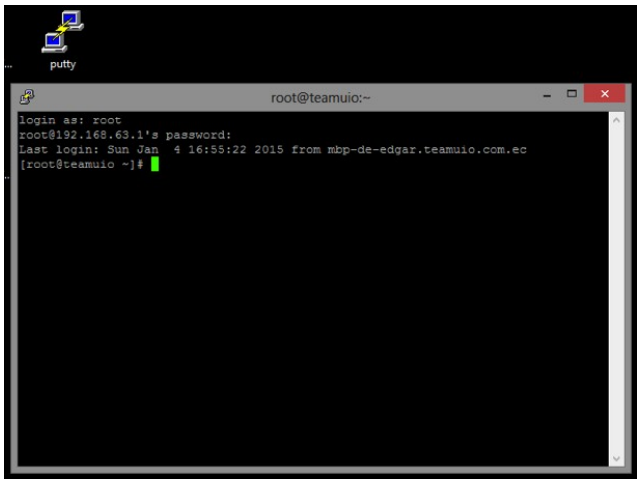


Figura 70. Acceso desde la zona de Poder.

- Conectividad hacia el internet.

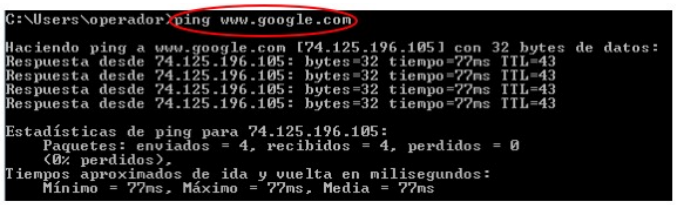


Figura 71. Conectividad hacia el internet desde la zona de No Poder

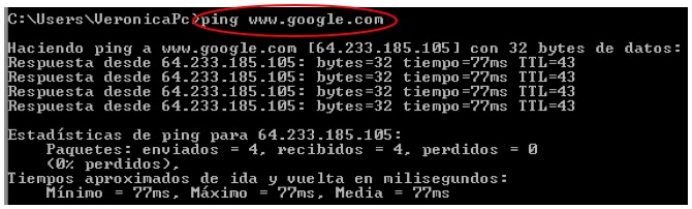


Figura 72. Conectividad hacia el internet desde la zona de Poder

5.1.5. Pruebas de reglas implementadas en el firewall para redes sociales.

Para esta prueba se habilitará las reglas implementadas en “Egress Firewall” y se tratara de acceder a dichas páginas vía web y con pruebas de conectividad, Ping.

Figura 73. Reglas configuradas.

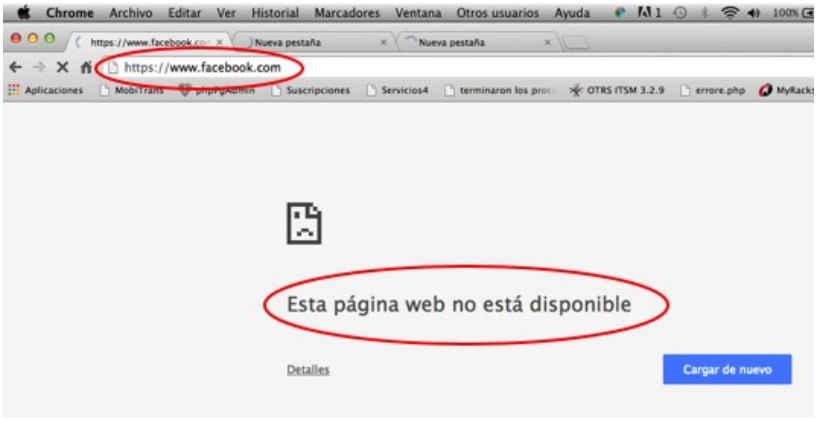


Figura 74. Bloqueo de Facebook en navegación

```
MacBook-Pro-de-Edgar:~ Usuario$ ping www.facebook.com
PING star.c10r.facebook.com (31.13.73.1): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
^C
--- star.c10r.facebook.com ping statistics ---
7 packets transmitted, 0 packets received, 100.0% packet loss
```

Figura 75. Bloqueo de Facebook en consola.

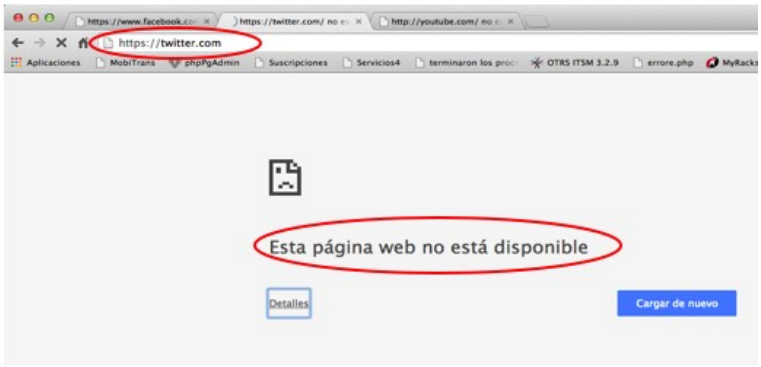


Figura 76. Bloqueo de Twitter en navegación.

```
MacBook-Pro-de-Edgar:~ Usuario$ ping www.twitter.com
PING twitter.com (199.16.158.8): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
^C
--- twitter.com ping statistics ---
7 packets transmitted, 0 packets received, 100.0% packet loss
```

Figura 77. Bloqueo de Twitter en consola.

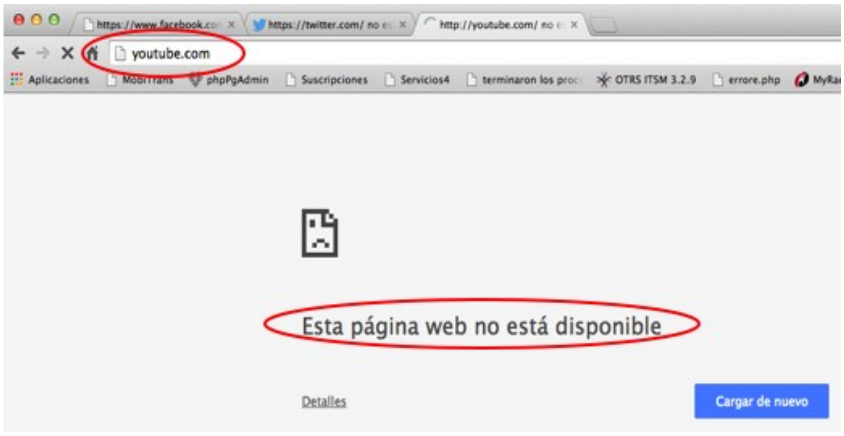


Figura 78. Bloqueo de Youtube en navegación.

```
MacBook-Pro-de-Edgar:~ Usuario$ ping www.youtube.com
PING youtube-ui.l.google.com (173.194.125.70): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
^C
--- youtube-ui.l.google.com ping statistics ---
7 packets transmitted, 0 packets received, 100.0% packet loss
```

Figura 79. Bloqueo de Youtube en consola.

5.1.6. Comparativa y bondades de ClearOS frente al firewall anterior.

Como se mencionó en los antecedentes de este proyecto, TeamSourcing tenía como firewall a Vyatta, el cual también es un software de código abierto, el cual también tiene funcionalidades muy interesantes, pero para el parecer de TeamSourcing, con poco desarrollo en su interfaz gráfica, por lo que siempre se tendrá que hacer algún cambio desde consola.

Haremos una comparativa desde algunos ámbitos para detallar en como ClearOS nos da una mejor o una limitación en comparación a su predecesor.

Tabla 44. Comparativa de ClearOS vs Vyatta.

	ClearOS	Vyatta
Instalación	Similar a la instalación de cualquier sistema operativo.	Similar a la instalación de cualquier sistema operativo.
Interfaz Gráfica	Desarrollada en su totalidad para cumplir con todas las funcionalidades que puedan implementarse en ClearOS, mediante menús perfectamente determinados según la utilidad que queramos configurar o visualizar.	Desarrollada en una estructura de subcarpetas, en las cuales se pueden observar de manera jerárquica las opciones que se pueden realizar, aunque en su mayoría no se pueden desarrollar muchos cambios de manera gráfica.
Consola	Completamente accesible mediante el puerto 22 o en su defecto por el puerto que nosotros queramos configurarlo ejemplo: el puerto 22222, por consola podemos manejarnos como en un servidor normal con Linux o RedHat, por lo cual, cambios más complicados en cuanto a configuración no los podremos realizar si no se tiene un conocimiento de Linux avanzado.	Ofrece una gran variedad de comandos, los cuales van desde visualizar las opciones ya configuradas, hasta poder hacer cambios complejos, como creación de VLANs, VRRP, o QoS, para ver todas sus configuraciones se presenta en forma jerárquica, similar a un archivo de texto con instrucciones de código, para los cuales hay una infinidad de tutoriales disponibles en su mayoría en inglés
Configuración de IPs	Se puede hacerlo desde la configuración inicial durante la instalación para su funcionamiento base, o desde la interfaz web, en donde además se pueden agregar varias opciones, se puede visualizar todo de una manera fácil e intuitiva.	Se le tiene que hacer mediante consola con el comando set, y seguido de la interface e IPs que van a ser asignadas respectivamente, las cuales pueden ser editadas después según las necesidades del caso, para que cada cambio surja efecto, es necesario digitar el comando "commit".

Continua

Aplicaciones	Mediante el "Market Place" podemos encontrar muchas aplicaciones con distintas funcionalidades, para el engrandecimiento y robustez de nuestro firewall, las cuales son gratuitas según la versión que elijamos, y de pago, con planes anuales de renovación.	No existen aplicaciones que nos ofrezcan los desarrolladores de este Software Firewall.
Configuración de VLANs	Completamente configurable desde el menú: Network -> Settings-> IP Settings -> Add VLAN Interface.	Configurable mediante el comando, por ejemplo: set vif 50 Address 192.168.0.238/28, con lo cual también tendremos que establecer para esta 'vif" la descripción y la interface en donde se va a alojar.
Configuración de DHCP	Configurable en el menú: Network-> DHCP Server-> Subnets-> edit, en la interface que queramos asignar un rango de IPs según nuestras necesidades.	Configurable mediante el comando: set service dhcp-server shared-network-name zona 192.168.0/28 start 192.168.60.10 stop 192.168.60.200. Además de continuar configurando las opciones de gateway y DNS, con el mismo comando después de la IP a la que pertenece, y al final con el comando "commit" para que comience a funcionar.
Configuración de QoS	Aplicación todavía considerada como "Beta", por lo que se ha configurado la mayoría de reglas en la Administración de Ancho de Banda.	Configurable mediante el comando por ejemplo: set traffic-policy-shaper LAN class 20 Bandwidth 45%, y complementando con las demás opciones, como prioridades, reserva y total de ancho de banda que va a pasar por nuestra red LAN.
Reportería	Reportería detallada en su totalidad en el menú Reportes, donde podremos encontrar información desde el estado del sistema, hasta datos puntuales de consumo de ancho de banda y páginas visitadas filtrado por IP.	No posee reportería propia, se debería complementar este software con algún gestor que nos de algún tipo de información.

Continua

Logs	Disponibles en el menú: Reports-> System-> Log Viewer, donde podremos elegir el log a visualizar, de manera simplificada o en su totalidad y al cual los podremos filtrar por IP o todos según nuestras necesidades.	Disponible mediante el path /var/log/, en el cual se podrán ver y crear logs del sistema y del tráfico de nuestra red.
Soporte	Disponible en la página oficial de ClearOS, Clear Center, secure.clearcenter.com, en donde podremos encontrar información oficial de los desarrolladores del sistema y foros con problemas comunes compartidos en la comunidad de ClearOS, además de tener un canal de soporte incluido según la versión de ClearOS adquirida.	Al momento la página oficial de Vyatta, vyatta.org, no está disponible, pero se puede encontrar mucha información, foros, configuraciones, howtos, y más en la página: openredes.com

6. CAPÍTULO VI

Conclusiones y Recomendaciones.

6.1. Conclusiones

6.1.1. Políticas de Seguridad de la Información.

- El Sistema de Gestión de Seguridad de la Información (SGSI), fundamentado en el estándar ISO-27001, mantiene una filosofía basada en los procesos de mejora continua, que consiste en Planear-Hacer-Verificar-Actuar, (Plan, Do, Check, Ack), también se basa en se basa en la norma ISO-27002:2005.
- Para realizar políticas de acuerdo al SGSI se tiene que tener en cuenta las 4 reglas del proceso de mejora continua antes mencionados, al igual que la gestión eficiente de la información, la cual nos permita siempre asegurar la Integridad, confidencialidad y disponibilidad de la información.
- Podríamos definir a una Política, como la forma de comunicar a los usuarios los parámetros o reglas que deben seguirse para tener una convivencia eficiente con los recursos y servicios tecnológicos disponibles en nuestra empresa.
- El socializar las Políticas de Seguridad de la información, debe tomarse como una campaña de alta prioridad, ya que los bienes informáticos y en sí, los servicios que ofrece como empresa TeamSourcing, pueden verse afectados no solo en el tiempo que podemos perder en recuperar información por ejemplo, sino también en términos económicos al traducirse en gastar tiempo es igual a gastar dinero.
- El alcanzar una “seguridad total de la información”, se traduce en un imposible, debido a los constantes cambios y retos que suponen establecer políticas que sean infalibles, y también tomando en cuanto a factor humano en el que la sociabilización y difusión de las políticas

lleguen con efectividad, pero con la mejora continua, se establecen parámetros que nos permiten tener niveles de seguridad aceptables y que aplicadas correctamente pueden reducir el riesgo dentro de la red.

- El uso de herramientas de “Open Source”, incrementa la productividad en todo tipo de empresas, ya sean estas públicas o privadas, en donde la tónica también puede conllevar a la modificación o desarrollo de nuevas tecnologías a partir de otras ya existentes.
- La asignación de personas a cargo de los cambios necesarios para la planeación y ejecución de las políticas definirá el tiempo en que se podrán ver resultados tangibles a largo plazo, tomando en cuenta que para algunas empresas el mantener el aseguramiento de la información resulta ser mucho más prioritario que para otras.

6.1.2. ClearOS

- La conclusión más importante en este proyecto es que el Sistema ClearOS, se establece como una solución, o una alternativa muy útil a falta de un dispositivo dedicado o físico, como son los equipos Cisco o 3Com, los cuales tiene precios que para una pequeña empresa serían demasiado cuestionables de acuerdo al tipo de negocio al que se dedique dicha empresa.
- Se debe tomar en cuenta que ClearOS posee grandes características en su versión libre, pero si se hace un esfuerzo por adquirir una licencia por un año o más, pues se tendrá muchos más beneficios de control y configuración a nivel local.
- El precio que establecido por ClearOS para versiones de pago no es demasiado elevado, además de ofrecer planes con descuento según el tiempo que se lo adquiera, es decir, si se contrata por dos años se tendrá un descuento del 20% o del 30% si se lo hace por los tres años seguidos.

- La configuración de todas y cada una de las funcionalidades que posee ClearOS se realizan mediante la interfaz web que nos ofrece este sistema, además del acceso por consola (ssh), por lo que se tiene una interactividad con el administrador de la red muy fluida y con muchos recursos para los fines que se propongan, en relación a e software anterior, Vyatta, en el cual la única fuente de configuración era mediante consola.
- El soporte de ClearOS, se define según el tipo de versión del sistema que hayamos adquirido, pero cabe mencionar que en “Clear Care”, http://www.clearcenter.com/, se puede encontrar la configuración básica de cada una de las funcionalidades de ClearOS, y en la misma página, los foros con FAQs que nos pueden ser de mucha ayuda o plantear inquietudes propias.
- En el caso del desempeño de DHCP y DNS se puedo comprobar que efectivamente se estaban obteniendo respuestas efectivas acorde a la normalidad del correcto funcionamiento y de tiempos de respuesta que se puedan esperar dentro de un rango aceptable.
- Para el caso de DHCP puntualmente, se puede destacar que este servicio cumple un desenvolvimiento muy estable, de acuerdo a nuestras exigencias, además de ofrecer tiempos de concesión que nos permiten tener un control del rango de IPs libres para nuevos dispositivos.
- Es de mucha utilidad que ClearOS nos brinde información detallada en su reportería, ya que de esa manera el administrador de la red podrá tomar decisiones de acuerdo a las circunstancias y exigencias de la red y tener un desempeño más eficiente de la misma.

6.2. Recomendaciones

6.2.1. Políticas de Seguridad de la Información.

- Las política de seguridad deben llevar a cabo un proceso de adaptación y socialización con los usuarios de la empresa a partir de un enfoque integral sobre todos las áreas involucradas.
- La Gerencia en su afán de apoyar a este proyecto debe proporcionar las herramientas y recursos necesarios para la ejecución y difusión de las Políticas de la Seguridad de la Información en TeamSourcing.
- La socialización de las políticas debe de ser de una manera organizada, ordenada y detallada a usuarios administradores y jefes de área, además de cumplir y utilizar dichas políticas con el afán de proteger los activos físicos y digitales de nuestra empresa.
- Se debe de utilizar los formularios respectivos de acuerdo a las acciones que se vayan a realizar, lo cual nos ayudará a mantener una información clara y actualizada.
- Es importante definir que en cada cambio que se haga en IT se debe actualizar un análisis de riesgos, para poder tratar a tiempo problemas que se puedan presentar a futuro.

6.2.2. ClearOS

- ClearOS y la configuración desarrollada durante este proyecto, se alinean de acuerdo a las políticas de seguridad de la información también desarrolladas aquí, por lo que se recomienda realizar un análisis de riesgo luego de un año de operaciones de ClearOS.
- Se debe tomar en cuenta que la versión free de ClearOS nos ofrece aplicaciones básicas de desempeño y administración de una red corporativa, para lo que, si se va a montar esta versión en una Pyme por ejemplo, resultará muy básico para el tipo de desempeño y control que se quiera tener.

- Se puede decir que lo que se considera una Pyme, es decir, una empresa que tiene de 50 a 99 empleados y puede tener como patrimonio máximo $120000 de capital fijo, la versión de pago estándar cuyo valor es $480 por año, no es un capital muy alto como para tener una mejor administración y desempeño de nuestra red, por lo que se recomienda utilizar la versión de pago, por lo menos para las empresas que estén ligadas a un sector de la industria con esas características.

BIBLIOGRAFÍA

ISO 27000. (2013). Obtenido de www.iso2700o.es: http://www.iso27000.es/download/doc_iso27000_all.pdf

Apablaza, F. (10 de 2011). *Calidad de redes y servicios de telecomunicaciones.* Obtenido de http://es.scribd.com/: http://es.scribd.com/doc/68277122/Apuntes-Confiabilidad-y-Disponibilidad-de-Redes#scribd

Apablaza, F. (s.f.). CALIDAD DE REDES Y SERVICIOS DE TELECOMUNICACIONES. http://es.scribd.com/doc/68277122/Apuntes-Confiabilidad-y-Disponibilidad-de-Redes.

Clear Foundation. (2014). *Clear Foundation, Forums*. Obtenido de clearfoundation.com: http://www.clearfoundation.com/component/option,com_kunena/Itemid,232/catid,37/func,view/id,36005/

ClearCenter. (2014). *ClearOS | Overview*. Obtenido de http://www.clearfoundation.com/: http://www.clearfoundation.com/Software/overview.html

ClearCenter. (2014). *ClearOS, comparison*. Obtenido de http://www.clearcenter.com: http://www.clearcenter.com/Software/clearos-comparison.html

ClearCenter. (2014). *www.clearcenter.com.* Obtenido de www.clearcenter.com: http://www.clearcenter.com/images/stories/MediaCenter/ClearCenter/ClearOS-Quick_Start_Guide.pdf

ClearFoundation. (2014). *ClearFoundation | Overview*. Obtenido de www.clearfoundation.com: http://www.clearfoundation.com/Foundation/overview.html

ClearOS Guides. (2013). *Network Types*. Obtenido de ClearCenter: http://www.clearcenter.com/support/documentation/clearos_guides/network_types_-_external_lan_hotlan_dmz

Corletti, A. (04 de 2006). ANÁLISIS DE ISO-27001:2005. Madrid, Espana. Obtenido de http://creangel.com: http://creangel.com/papers/analisis_ISO-27001.pdf

Definicion.de . (2014). *Definicion.de* . Obtenido de http://definicion.de/red-de-datos/#ixzz3EL5pidJo

Garcia, J. (02 de 2012). Instalacion y configuracion de cortafuegos. http://jgdasir2.files.wordpress.com/2012/02/ut04-instalacion-y-configuracion-de-cortafuegos.pdf.

Granja, M. (2014). *Cifras asombrosas de las redes sociales.* Vistazo.com, Blogs/Tecnologia.

ISO 27000 . (2013). ISO 27000 . http://www.iso27000.es/download/doc_iso27000_all.pdf.

ISO 27001 . (27 de 11 de 2013). *ISO 27001 Gestión de la Seguridad de la Información*. Obtenido de Normas ISO: http://www.normas-iso.com/iso-27001

iso27000.es. (16 de 01 de 2011). *ControlesISO27002-2005.* Obtenido de http://www.iso27000.es: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

iso27000.es. (s.f.). *ISO 27000,* . Recuperado el 2014, de iso27000.es: http://www.iso27000.es/sgsi.html#section2a

Massiah, J. (08 de 08 de 2010). *http://www.monografias.com*. Obtenido de Estadística básica aplicada al mantenimiento: http://www.monografias.com/trabajos62/estadistica-aplicada-mantenimiento/estadistica-aplicada-mantenimiento2.shtml

Matamala, M. (2012). *Apuntes de redes, lenguajes de marca, sistemas operativos, eguridad*. Obtenido de mauriciomatamala.net: http://www.mauriciomatamala.net/PAR/vyatta.php

Mendoza, R. (16 de 04 de 2010). *Sistema de Gestión para la seguridad de la información.* Obtenido de http://www.slideshare.net: http://www.slideshare.net/mmujica/mi-defensa

PriteshGupta.com. (2012). *iso27000.es*. Obtenido de www.iso27000.es: http://www.iso27000.es/sgsi.html#section2a

Rivas, H. M. (19 de 10 de 2010). *slideshare.net*. Obtenido de slideshare: http://www.slideshare.net/lalex20/historia-de-los-cortafuegos

Rojas, J. (02 de 2013). *www.buenastareas.com*. Obtenido de Historia Del Firewall: http://www.buenastareas.com/ensayos/Historia-Del-Firewall/7386302.html

TeamSourcing. (2014). *TeamSourcing*. Obtenido de www.teamsourcing.com.ec: http://www.teamsourcing.com.ec/webteam/index.php/empresa.html

uladech.edu.pe. (2013). *Norma NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de Información.* Obtenido de uladech.edu.pe:

http://files.uladech.edu.pe/docente/02659781/CAT/S06/06_lzy_iso27001.pdf

wikipedia. (30 de 01 de 2012). *es.wikipedia.org*. Obtenido de http://es.wikipedia.org/wiki/Curva_de_la_ba%C3%B1era