DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD UTILIZANDO EL FIREWALL IPCOP PARA EL CONTROL DEL ACCESO A INTERNET Y A LA RED DE DATOS DE LA UNIVERSIDAD DE CÓRDOBA

AUTORES

JULIO CESAR ÁLVAREZ CASTILLO

JAIR EMILIO CARUZO DOMÍNGUEZ

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES
MONTERÍA- CÓRDOBA
2015

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD UTILIZANDO EL FIREWALL IPCOP PARA EL CONTROL DEL ACCESO A INTERNET Y A LA RED DE DATOS DE LA UNIVERSIDAD DE CÓRDOBA

AUTORES

JULIO CESAR ÁLVAREZ CASTILLO

JAIR EMILIO CARUZO DOMÍNGUEZ

DIRECTOR

ING. MILTON HERNÁNDEZ ZAKZUK

COASESOR

P.HD. ANGEL DARIO PINTO MANGONES

TRABAJO DE GRADO PARA OPTAR AL TITULO DE INGENIERO DE SISTEMAS

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES
MONTERÍA- CÓRDOBA
2015

HOJA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____

_____
FIRMA PRESIDENTE DEL JURADO

_____
FIRMA DEL JURADO

_____
FIRMA DEL JURADO

Montería, Córdoba (Día___ Mes____ Año: 2015)

DEDICATORIA

A Dios por sus bendiciones y la fe que me dio para luchar por este sueño, A mi madre María Evangelina Castillo Anaya y mis abuelos Máximo José Castillo Avila y María Inés Anaya Flores por todo su esfuerzo y sacrificio por brindarme lo mejor de ellos en cada momento de mi vida, gracias a su sabiduría que influyo en mi madurez para lograr todos los objetivos en la vida, es para ustedes esta tesis en agradecimiento por todo su amor.

Julio Cesar Álvarez Castillo

DEDICATORIA

A Dios por permitirme llegar a este momento tan especial en mi vida, por los triunfos y los momentos difíciles que me han enseñado a valorarme cada día más.

A mis padres Jesús Salvador Caruzo López y Hilda Esther Dominguez Salgado por haberme educado y soportar mis errores. Gracias a sus consejos, por el amor que siempre me han brindado y por saberme inculcar el valor de la responsabilidad.

Jair Emilio Caruzo Domínguez

AGRADECIMIENTOS

Al Ingeniero Milton Hernández Zakzuk, asesor del proyecto de investigación.

Al Doctor Ángel Dario Pinto Mangones, coasesor del proyecto de investigación, por su valiosa orientación.

A la UNIVERSIDAD DE CÓRDOBA, por brindarnos la oportunidad de culminar con satisfacción los estudios de pregrado.

Todos los DOCENTES, de la Universidad por compartir sus conocimientos con nosotros.

TABLA DE CONTENIDO

TABLA DE FIGURAS

TITULO DEL PROYECTO

DISEÑO E IMPLEMENTACION DE UN SISTEMA DE SEGURIDAD UTILIZANDO EL FIREWALL IPCOP PARA EL CONTROL DEL ACCESO A INTERNET Y A LA RED DE DATOS DE LA UNIVERSIDAD DE CORDOBA

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Implementar un sistema de seguridad utilizando el firewall IPCOP para el control del acceso a Internet y a la red de datos de la Universidad de Córdoba.

1.2. OBJETIVOS ESPECÍFICOS

- Analizar el diseño de red existente en la Universidad de Córdoba para determinar posibles falencias en su diseño.
- Comparar las bondades del firewall IpCop con respecto a otros firewall existentes en el mercado.
- Identificar las principales amenazas en la red de la Universidad de Córdoba para establecer políticas de seguridad que garanticen la integridad de los datos.
- Implementar el firewall IpCop para controlar el acceso a la red y a sitios potencialmente peligrosos mediante políticas de control.

2. **INTRODUCCIÓN.**

En la actualidad la información de la UNIVERSIDAD DE CÓRDOBA se ha conocido como un activo valioso, ya que juega un papel muy importante a la hora de la toma de decisiones y definición de nuevas estrategias y a medida que se vayan integrando sistemas que apoyen cada vez más los procesos, se requiere contar con tácticas de un alto nivel para mantener la seguridad de los datos y así poder hacer control y administración de estos.

La seguridad informática, trata de minimizar los riesgos asociados al acceso y utilización de determinado sistema, de forma no autorizada y en general malintencionada, por tanto implica la necesidad de gestión de riesgo. (Galdámez, 2003)

Para ello, se deben realizar una evaluación y a la vez cuantificar los bienes a proteger, y en función de esto, implantar medidas preventivas y correctivas que eliminen los riegos.

La temática de estudio ha sido abordada a nivel internacional por autores como Vinueza, P. (2011) En Ecuador, este llevó a cabo una investigación denominada: "análisis para la seguridad de paquetes de datos y evitar ataques mediante sniffing". Esta menciona que: Sniffing, es una técnica que permite tener un ojo en el flujo de información, es decir tener acceso a la información que es enviada o recibida por A adaptadores de red, y algunas veces por computadoras. El objetivo principal de esta investigación se centra en el análisis de los paquetes de datos investigando protocolos, estándares de seguridad y medidas de protección de los datos que viajen a través de la red mediante sniffing, con ello evitar posibles ataques de hackers o intrusos, quienes puedan tener acceso a la información que se envíen usándolos de una manera indebida. Esta B provee un aporte a la investigación por pretender ser tema de estudio el análisis de información y la seguridad en los datos.

De la misma forma Ochoa, V. (2011). Con su trabajo titulado "el análisis y el tráfico de datos en la capa de enlace de una red LAN", para la detección de posibles

ataques o intrusiones sobre tecnologías Ethernet y Wifi 802.11, este proyecto de grado fue elabora en Sangolqui – Ecuador. La finalidad en sí, es detectar ataques que afecten la integridad/seguridad de la información de una Empresa u otros por medio del Análisis de Tráfico de Datos cursado en la Capa de Enlace en redes LAN sobre tecnologías Ethernet y WiFi 802.11.

En el 2010, Córdoba A., Durán G. & Flores V. realizaron un proyecto el cual denominaron “Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS configurado en un Sistema Operativo LINUX para una LAN”. Esta detalla en sus objetivos: Describir los conceptos básicos relacionados con la Seguridad Informática y el Control de Acceso, entender cómo funcionan las tecnologías inalámbricas existentes, así como los mecanismos de seguridad que se pueden enfocar a éstas y describir conceptos relacionados con la autenticación y el protocolo RADIUS, así como las especificaciones que faciliten su uso. Esta implementación es de gran aporte por que trata temas de acceso o servicios a la red y por qué se enfoca especialmente a la seguridad de la redes.

A nivel nacional se encuentran autores como, Díaz A., Collazos G., Lozano H., Ortiz L., & Herazo G. (2011). Quienes llevaron a cabo un artículo acerca de la implementación de un sistema de gestión de seguridad de la información (SGSI) en la comunidad nuestra señora de gracia, alineado tecnológicamente con la norma ISO 27001, este es resultado de un proyecto de investigación, adelantado por un grupo de estudiantes de ingeniería de sistemas con el fin de implementar un SGSI en la Comunidad Nuestra Señora de Gracia. Este sistema se basa en las directrices indicadas en la norma ISO/IEC 27001 y en el marco del mismo se generó un análisis de gap, que permitió evidenciar un nivel de brechas significativo en la mencionada Comunidad, con base en el cual se establecieron políticas y controles de mejoramiento de los procesos de seguridad de la información y se definieron las declaraciones de aplicabilidad que fortalecieron todo el análisis de riesgos efectuado.

En el 2007, Pérez, G. desarrollo un Modelo para describir el Comportamiento del tráfico de datos en una red local Ethernet y Wifi empleando geometría fractal. Se

recolectaron de muestras de encabezados de paquetes IP provenientes de dos redes red LAN con conexiones Ethernet e inalámbricas en dos laboratorios experimentales. El primero se ubicó en la Universidad Nacional de Colombia sede Medellín y se denominó ambiente experimental académico. El segundo en la entidad Bancaria Coltefinanciera S.A. como ambiente experimental comercial. El conjunto de muestras para cada uno de los laboratorios se filtraron y se escalaron con algoritmos construidos y obtuvieron los archivos que nos permitieron analizar las series de tiempos a diferentes escalas y buscar la caracterización propia de la geometría fractal bajo un modelo propuesto.

Esta investigación permitirá evaluar las vulnerabilidades en cuanto a la seguridad informática presentes en la Universidad de Córdoba, para así ofrecer alternativas de solución que conlleven a un sistema mucho más seguro y que permita retener los posibles ataques que se puedan presentar en la Universidad de Córdoba en las distintas dependencias Académico – Administrativas, mediante el estudio y análisis de esta fallas presentes se podrán ofrecer políticas de seguridad que ofrezcan unas alternativas de solución.

De la misma manera, fomentara las condiciones necesarias para que la incorporación de estas políticas de seguridad informática dentro de la estructura educativa, sea un instrumento para la protección de todos los datos que circulan tanto en la intranet como en el internet.

Metodológicamente incorpora modelos investigativos que pueden servir como aporte para solucionar problemas que se puedan presentar a la hora de implementar políticas de seguridad en una empresa, sirviendo de ejemplo para futuras investigaciones relacionadas con el tema de investigación, como otras áreas de trabajo, de igual forma se acude al instrumento de la observación, con lo cual su diseño podrá ser tomado como un modelo de recopilación de información para trabajos venideros.

El resultado de la investigación, aportara conocimiento al área de la seguridad en las redes telemáticas para la protección óptima de los datos y el uso adecuado de estos, de acuerdo a los objetivos planteados. De la misma forma ayudara a

encontrar soluciones a todos los problemas planteados anteriormente en la Universidad de Córdoba.

2.1.1 AMBIENTACION

Hoy en día, la seguridad informática ha tomado gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes para explorar más allá de las fronteras nacionales, situación que ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

La extensión de las redes de ámbito mundial que interconectan recursos de todo tipo, es la causante del aumento de los ataques informáticos a la información almacenada obligando a diseñar sistemas seguridad más robustos.

Las políticas de seguridad indican a los usuarios el uso correcto de los recursos informáticos con los que cuenta una organización y la forma como se deben afrontar los riesgos de seguridad que se presenten.

La protección en el uso de internet es unos de los principales punto a tener en cuenta.

Además, la navegación en ciertos sitios web que tienen contenido multimedia y que permiten la descarga de archivos de gran tamaño, reducen considerablemente el ancho de banda, lo que conlleva a la disminución en la velocidad de transmisión de los datos.

La ubicuidad inherente de internet también propicia la propagación de malware[1] de distintos propósitos, desde inundarnos con ventanas de anuncios, hasta los que buscan robar información redituable.

Hay diversos tipos de ataques informáticos:

[1] software Malicioso

Virus y Gusanos, Backdoor o Puerta Trasera, Drive-by Downloads, Rootkits, Troyanos, Hijackers, Keyloggers y Stealers, Botnets, Rogue software, Los Ransomware, Phishing, Grayware o greynet (Adware, Dialers y Spyware).

2.2. PROBLEMÁTICA

El problema de la seguridad informática, no es ajeno en nuestro país o a la región caribe, muchas empresas ven amenazada la integridad de su información y se hace necesario el diseño de sistemas que contemplen establecer políticas de seguridad y el uso de herramientas de software libre, que de una forma económica y viable pueden dar solución a estos problema.

En la Universidad de Córdoba, se ha hecho difícil mantener la integridad y la seguridad de la información institucional, debido al aumento y a la multiplicidad de dispositivos que acceden a la red institucional (portátiles, Tablet, Smartphone, entre otros medios), en todo el campus universitario, permitiendo que cualquier dispositivo pueda conectarse mediante este sistema, o a través de la red cableada, a la red de datos y al servicio de Internet.

Ya que actualmente se tiene un sistema bajo el soporte del Firewall Palo Alto 5020[2] que ofrece seguridad solo en cuanto al acceso a la red global, anotando la problemática que se está presentando en cuanto a la movilidad.

Las políticas de seguridad en la UNIVERSIDAD DE CÓRDOBA están en construcción y estarían enfocadas a endurecer el sistema de acceso al internet, descuidando a la red corporativa, ya que las políticas aplicadas actualmente para proteger la información han presentado muchas vulnerabilidades, (Ver **Figura 1**)

[2] Cortafuegos de próxima generación está diseñado para proteger los centros de datos, grandes puertas de enlace de Internet de la empresa y los entornos de proveedores de servicios, donde las demandas de tráfico dictan firewall predecible y rendimiento de prevención de amenazas.
(Fuente:http://www.ndm.net/firewall/Palo-Alto-Networks/pa-5020-series)

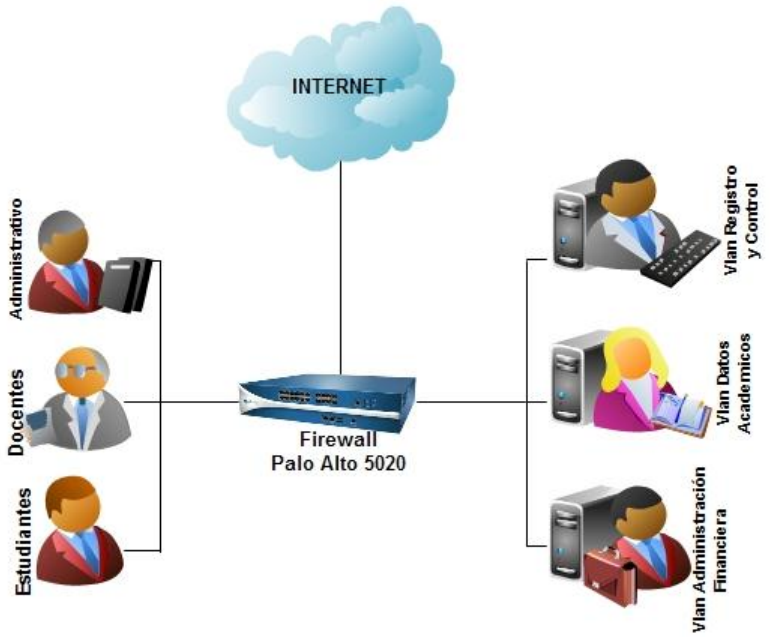


Figura 1: Distribución topológica de acceso a la red de la Universidad de Córdoba
Fuente: Elaboración Propia.

Por lo tanto se puede deducir que algunos de los ataques presentados en la red institucional y que han originado problemas de pérdida o modificación de algún tipo de información en la Universidad (ver **Figura 2**) se deben a la falta del endurecimiento de las políticas de seguridad actuales y la falta de Cultura informática.

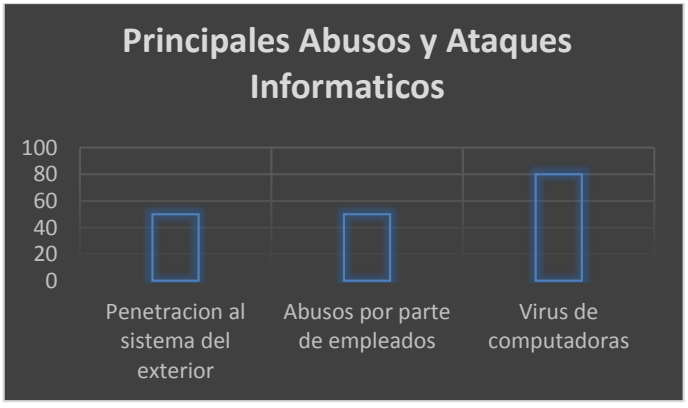


Figura 2: Abusos y Ataques Informáticos en la Universidad de Córdoba por Falta de Cultura informática.
Fuente: Elaboración Propia.

Los ataques que se han presentado en la Universidad de Córdoba han sido ataques de tipo activos porque se han presentado con algunas modificaciones en los datos, dentro de los sistemas afectados están: suplantación de identidad, esto se debe a que no se cuenta con un dispositivo que bloquee estos ataques informáticos.

Este es un tema de gran relevancia y significancia para cualquier organización y en especial para nuestro objeto de estudio, la UNIVERSIDAD DE CÓRDOBA, ya que si no se toman las medidas necesarias contra estos ataques, se tendrá un sistema que podría ser fácilmente vulnerado por piratas informáticos obteniendo accesos a la información que se encuentra almacena en los servidores de nuestra institución.

Por lo tanto es de suma importancia hacer un estudio de las posibles vulnerabilidades que se están presentando y que se pueden presentar a futuro con el objetivo de endurecer los sistemas informáticos de la institución y así protegerse de los siguientes personajes como son: los hacker, los cuales acceden a un sistema protegido como si se tratara de un reto personal, sin intentar causar daños. Los crackers, en cambio, tienen como principal objetivo producir daños que en muchos casos suponen un problema de extrema gravedad para el administrador del sistema. En cuanto a los piratas, su actividad se centra en la obtención de información confidencial y software de manera ilícita.

De igual forma cabe resaltar que un ataque informático es algo inesperado ya que este consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

De la siguiente propuesta se espera obtener un sistema seguro o fiable y que garantice tres aspectos importantes: que sea confidencial para brindar un acceso a la información solo mediante autorización y de forma controlada. Integridad donde se permita la modificación de la información solo mediante autorización y

disponibilidad el acceso al sistema, debe permanecer accesible mediante autorización.

Este problema se ha mitigado en otras partes estableciendo políticas de seguridad como la implementación del sistema de Gestión de la Seguridad de la Información (SGSI). El objetivo de un SGSI es proteger la información y para ello lo primero que debe hacer es identificar los activos de información que deben ser protegidos y en qué grado. Luego aplicaron el plan PDCA ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo. Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica y por ese motivo nunca se eliminan en su totalidad.

Un SGSI siempre cumple cuatro niveles repetitivos los cuales se muestran a continuación: PLANIFICAR (Plan): consiste en establecer el contexto en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad. HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles. VERIFICAR (Check): consiste en monitorear las actividades y hacer auditorías internas y ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

PREGUNTA DE INVESTIGACION

¿Cómo diseñar e implementar un sistema de seguridad utilizando el firewall IpCop para el control del acceso a internet y a la red de datos de la Universidad de Córdoba?

2.3. ANTECEDENTES

2.3.1. CONTEXTO INTERNACIONAL

In Vienna Zseby, T.(2015), proposed safety net for teaching redmétodos anomaly detection Traffic students of electrical engineering, project design follows a principle-oriented teaching research, allowing students to make their own discoveries in real network traffic data captured using a large monitor Darkspace IP operated at the University of California, San Diego (UCSD). Although traffic Darkspace not include two-way conversations (only attempts to set) containing traffic related to reality or perpetrate a variety of networks from attacks million Internet addresses worldwide. This breadth of coverage makes this data Darkspace an excellent choice for a practice in the study of detection techniques Internet attacks. In addition, data Darkspace is less privacy-critical than others redesrastros because it contains only unwanted network traffic and no legitimate communication.

En Ecuador, Vinueza, P. (2011), llevó a cabo una investigación denominada: análisis para la seguridad de paquetes de datos y evitar ataques mediante sniffing. Esta menciona que: Sniffing, es una técnica que permite tener un ojo en el flujo de información, es decir tener acceso a la información que es enviada o recibida por nuestros adaptadores de red, y algunas veces por el de otras personas computadoras también. El objetivo principal de esta investigación se centra en el análisis de los paquetes de datos investigando protocolos estándares de seguridad y medidas de protección, de los datos que viajen a través de la red mediante sniffing, con ello evitar posibles ataques de hackers o intrusos, quienes puedan tener acceso a la información que se envíen usándolos de una manera indebida. Esta nos provee un aporte a la investigación por pretender ser tema de estudio el análisis de información y la seguridad en los datos.

El análisis y el tráfico de datos en la capa de enlace de una red LAN, para la detección de posibles ataques o intrusiones sobre tecnologías Ethernet y Wifi 802.11, este proyecto de grado fue elabora en Sangolqui – Ecuador. Ochoa, V.

(2011). La finalidad en sí, es detectar ataques que afecten la integridad/seguridad de la información de una Empresa u otros por medio del Análisis de Tráfico de Datos cursado en la Capa de Enlace en redes LAN sobre tecnologías Ethernet y WiFi 802.11.

Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS configurado en un Sistema Operativo LINUX para una LAN. Hecho por Córdoba A., Durán G. & Flores V. (2010). Esta detalla en sus objetivos: Describir los conceptos básicos relacionados con la Seguridad Informática y el Control de Acceso, entender cómo funcionan las tecnologías inalámbricas existentes, así como los mecanismos de seguridad que se pueden enfocar a éstas y describir conceptos relacionados con la autenticación y el protocolo RADIUS, así como las especificaciones que faciliten su uso. Esta implementación es de gran aporte por que trata temas de acceso o servicios a la red y por qué se enfoca especialmente a la seguridad de la redes.

El desarrollo de un Sistema de Control de Acceso en Redes Wireless con el DNI electrónico por Yébenes, S. (2009). Como Proyecto Fin de Carrera realizado en la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid. En él se analiza, se documenta y se describe como diseñar y poner en funcionamiento un sistema de control de acceso, a redes WIFI o inalámbricas, con autenticación de los usuarios por medio del Documento Nacional de Identidad electrónico español (e-DNI).

Hooper, E. (2009). Intelligent strategies for secure complex systems integration and design, effective risk management and privacy. In the effective design of engineering complex integrated systems and systems-of-systems in engineering and network systems. This is largely due to the integration of complex large data transfers across multiple zones of systems and network integration. The increase in transmission of highly sensitive data and challenges of data protection and of privacy, data loss prevention has major significant implications for systems engineering, systems integration, and systems analysis, design and validation.

2.3.2. CONTEXTO NACIONAL

En Colombia, se llevó a cabo un artículo acerca de la implementación de un sistema de gestión de seguridad de la información (SGSI) en la comunidad nuestra señora de gracia, alineado tecnológicamente con la norma ISO 27001, este es resultado de un proyecto de investigación, adelantado por un grupo de estudiantes de ingeniería de sistemas con el fin de implementar un SGSI en la Comunidad Nuestra Señora de Gracia. Por Díaz A., Collazos G., Lozano H., Ortiz L., & Herazo G. (2011). Este sistema se basa en las directrices indicadas en la norma ISO/IEC 27001, y en el marco del mismo se generó un análisis de gap[3], que permitió evidenciar un nivel de brechas significativo en la mencionada Comunidad, con base en el cual se establecieron políticas y controles de mejoramiento de los procesos de seguridad de la información y se definieron las declaraciones de aplicabilidad que fortalecieron todo el análisis de riesgos efectuado.

Otro artículo donde se propone el firme propósito de brindar a los asociados de negocio la seguridad SEGURIDAD ACRÓPOLIS LTDA., tranquilidad y transparencia en sus procesos, se decide entonces implementar la certificación bajo la norma BASC. Desarrollada en Bucaramanga realizada por Romer, A. (2010).

En el 2007 se propone un Modelo para describir el Comportamiento del tráfico de datos en una red local Ethernet y Wifi empleando geometría fractal. Se recolectaron de muestras de encabezados de paquetes IP provenientes de dos redes red LAN con conexiones Ethernet e inalámbricas en dos laboratorios experimentales. Pérez, G. (2007). El primero se ubicó en la Universidad Nacional de Colombia sede Medellín y se denominó ambiente experimental académico. El segundo en la entidad Bancaria Coltefinanciera S.A. como ambiente experimental comercial. El conjunto de muestras para cada uno de los laboratorios se filtraron y se escalaron con algoritmos construidos y obtuvieron los archivos que nos

[3] Un análisis de gap, permite comparar los procesos actuales que tiene la organización con los lineamientos de cumplimiento de la norma ISO/IEC 27001 y establecer en qué áreas o procesos se debe priorizar y enfocar el esfuerzo para permitir incrementar la seguridad de la información. (Fuente: http://www.gapanalisis.com/)

permitieron analizar las series de tiempos a diferentes escalas y buscar la caracterización propia de la geometría fractal bajo un modelo propuesto.

2.4. JUSTIFICACIÓN

El estado colombiano expidió la ley 1273 de 2009[4] "**protección de la información y de los datos"** a través de la cual preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Dentro de los **Artículo 269A:** Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena

[4] Protección de la información y de los datos (Fuente: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf)

de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

La seguridad en los sistemas informáticos se ha convertido en una gran batalla contra aquellas amenazas que han ido creciendo a lo largo del gran auge que ha tenido la sistematización de los procesos, las vulnerabilidades en cuanto a la seguridad informática presentes en la Universidad de Córdoba, para ofrecer alternativas de solución que conlleven a un sistema mucho más seguro y que permita retener los posibles ataques que se puedan presentar en las distintas dependencias Académico – Administrativas, mediante el estudio y análisis de esta fallas presentes se podrán ofrecer políticas de seguridad que ofrezcan unas alternativas de solución.

La seguridad de tecnologías de la información se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y especialmente, la información circulante o que se almacena. Existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. Comprendiendo lo que es software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información de tipo confidencial llega a manos de otras personas, convirtiéndose en información privilegiada.

De la misma manera, fomentar las condiciones necesarias para que la incorporación de estas políticas de seguridad informática dentro de la estructura educativa, sea un instrumento para la protección de todos los datos que circulan tanto en la intranet como en el internet.

Metodológicamente incorpora modelos investigativos que pueden servir como aporte para solucionar problemas que se puedan presentar a la hora de implementar políticas de seguridad en una empresa, sirviendo de ejemplo para futuras investigaciones relacionadas con el tema de investigación, como a otras áreas de trabajo, de igual forma se acude al instrumento de la observación, con lo cual su diseño podrá ser tomado como un modelo de recopilación de información para trabajos venideros.

3. MARCO TEÓRICO

RED DE DATOS

Se denomina red de datos a aquellas infraestructuras o redes de comunicación que se han diseñado específicamente a la transmisión de información mediante el intercambio de datos. (Ecured, s.f.) **(Ver Figura 3).**

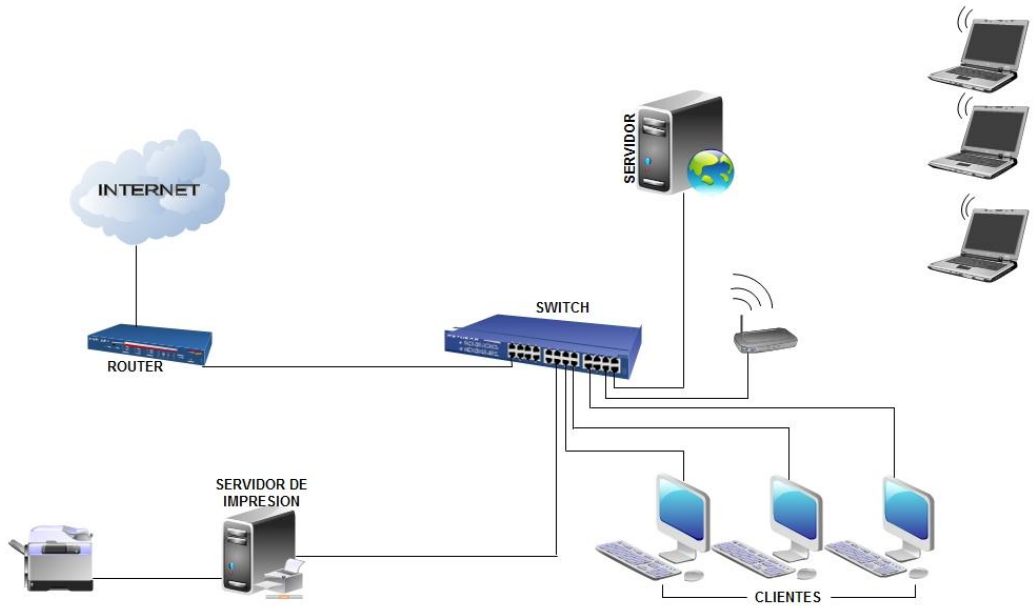


Figura 3. Red de Datos.
Fuente: Elaboración Propia. 2014.

Las redes de datos se diseñan y construyen en arquitecturas que pretenden servir a sus objetivos de uso, los cuales pueden ser:

- Compartir recursos, equipos, información y programas que se encuentran localmente o dispersos geográficamente.
- Brindar confiabilidad a la información, disponiendo de alternativas de almacenamiento.
- Obtener una buena relación costo / beneficio.
- Transmitir información entre usuarios distantes de la manera más rápida y eficiente posible.

La topología en las redes de datos puede ser enmarcada en dos tipos según el tipo de transmisión utilizada:

Redes de difusión: Donde se comparte el mismo medio de transmisión entre todos los integrantes de la red. Cada mensaje (típicamente llamado “paquete”) emitido por una máquina es recibido por todas las otras máquinas de la misma red. Cada paquete dispone de la información de “Origen” y “Destino” y de esta manera se discrimina quien debe procesar cada mensaje. Por ejemplo, Ethernet es una red de difusión. (Cyberprimo, 2008)

Redes punto a punto: Donde existen muchas conexiones entre pares individuales de máquinas. Para enviar mensajes hasta máquinas distantes, puede ser necesario pasar por varias máquinas intermedias. Por ejemplo, las conexiones por MODEM son redes punto a punto. (Cyberprimo, 2008).
En forma independiente la tecnología utilizada, las redes de datos pueden ser clasificadas según el alcance o tamaño de las mismas en los siguientes tipos:

- **LAN (Local Area Networks, Redes de Área Local):** Las redes de área local suelen ser una red limitada a la conexión de equipos dentro de un único edificio, oficina o campus, la mayoría son de propiedad privada. (wikitel, s.f.)

- **MAN (Metropolitan Area Networks, Redes de Área Metropolitana):** Las redes de área metropolitanas están diseñadas para la conexión de equipos a lo largo de una ciudad entera. Una red MAN puede ser una única red que interconecte varias redes de área local LAN’s resultando en una red mayor. Por ello, una MAN puede ser propiedad exclusivamente de una misma compañía privada, o puede ser una red de servicio público que conecte redes públicas y privadas. (wikitel, s.f.)

- **WAN (Wide Area Networks, Redes de Área Amplia):** Las Redes de área extensa son aquellas que proporcionen un medio de transmisión a lo largo de

grandes extensiones geográficas (regional, nacional e incluso internacional). Una red WAN generalmente utiliza redes de servicio público y redes privadas y que pueden extenderse alrededor del globo. (wikitel, s.f.).

SEGURIDAD INFORMATICA

La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios. (Alegsa, s.f.)

Técnicamente es imposible lograr un sistema informático ciento por ciento Seguro, pero buenas medidas de seguridad evitan daños y problemas que pueden ocasionar intrusos. (Alegsa, s.f.)

Existen dos tipos de seguridad con respecto a la naturaleza de la amenaza:

- Seguridad lógica: aplicaciones para seguridad, herramientas informáticas, etc.
- Seguridad física: mantenimiento eléctrico, anti-incendio, humedad, etc.

La seguridad de la información es un componente crítico de la estrategia de negocio de cualquier organización. Identificar las vulnerabilidades asociadas a la seguridad de la información que viaja dentro de la red, entender la importancia de definir políticas, procedimientos y estándares, de acuerdo a los requerimientos de la empresa, identificar las herramientas o productos tecnológicos que apoyen los controles, son elementos vitales que se deben analizar para reducir el riesgo y mejorar de esta manera la seguridad en la red. (Sisteseg, 2007)

Otros aspectos como: disponibilidad, desempeño, confidencialidad y control de acceso físico y lógico, deben tenerse en cuenta, de tal forma, que se pueda proponer un enfoque integral de acercamiento a la seguridad de la información que viaja por la red, de tal manera que se pueda combinar efectivamente la seguridad de la información en los diferentes sistemas hoy disponibles, sin afectar el desempeño de la red y mejorando a su vez la disponibilidad.

El análisis de riesgo involucra la determinación de qué es lo que se necesita proteger, de qué protegerlo y cómo protegerlo. Este es el proceso de determinar

todos los riesgos, clasificándolos por nivel de gravedad. Esto involucra tomar decisiones desde el punto de vista costo/beneficio, en relación con lo que se quiere proteger. No se debe gastar en proteger algo, más allá de su valor.

Existen dos elementos que se deben tomar en cuenta para analizar los riesgos como la Identificaciones de los bienes y la Identificación de las amenazas; para cada bien, los objetivos básicos de seguridad son: disponibilidad, confiabilidad e integridad. Para ello, cada amenaza debe ser analizada en función de su efecto en estos objetivos.

Identificación de los bienes

El primer paso en el análisis de riesgo, es identificar todo aquello que debe ser protegido. Algunos son obvios, como el valor de la propiedad de la información, la propiedad intelectual y los elementos de hardware, pero algunos no son considerados, como las personas que operan los sistemas. El punto esencial es listar todas aquellas cosas que podrían ser afectadas por un problema de seguridad. (Brevis, 2001)

Una lista de categorías deberá considerar los siguientes elementos:

Hardware: Cpu's, teclados, terminales, computadores personales, impresoras, unidades de discos, líneas de comunicación, servidores y equipos de comunicaciones.

Software: Programas fuente, programas objeto, utilitarios, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

Datos: En ejecución, almacenados en línea, archivados off-line, Backups, registros de auditoría, bases de datos, en tránsito sobre medios de comunicación.

Personas: Usuarios, administradores, mantenedores de hardware.

Una vez que se identifican los elementos que requieren protección, es preciso identificar y analizar las amenazas hacia ellos, para determinar de qué se está intentando proteger los elementos y los potenciales daños que puedan ocurrir.

Se entiende por amenaza, una condición del entorno del sistema de información (persona, máquina, suceso o idea), que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). (Informaticos, 2001)

La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario.

Un ataque no es más que la realización de una amenaza. Las cuatro categorías generales de amenazas o ataques son las siguientes:

- Interrupción: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros. (Informaticos, 2001)

- Intercepción: una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad). (Informaticos, 2001).

- Modificación: una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar

un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red. (Informaticos, 2001).

- Fabricación: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo. (Informaticos, 2001).

Estos ataques se pueden así mismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

Ataques pasivos: En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.

- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante. (Informaticos, 2001)

Ataques activos: Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- Suplantación de identidad: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

- Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

- Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.

- Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc. (Informaticos, 2001)

Las siguientes son amenazas clásicas que deben ser consideradas:

Acceso no autorizado a recursos y/o información: es conocido como "spoofing", en este caso, actualizaciones de ruteo falsas son enviadas a uno o más routers, ocasionando que los paquetes se desvíen de su lugar de destino. Esto difiere de un ataque por denegación de servicio sólo en el propósito existente en el ruteo falso. En la denegación de servicio, el objetivo es lograr que el router quede inutilizado; un estado que será rápidamente detectado por los usuarios de la red. En el "spoofing", la ruta falsa causará que los paquetes sean ruteados a un host, desde el cual un intruso puede monitorear los datos en los paquetes. Estos paquetes son entonces re-ruteados a su destino correcto. Sin embargo, el intruso podría haber ya alterado el contenido de los paquetes. (A., 2001)

Revelación involuntaria o no autorizada de información: Los problemas presentados en una red, generalmente son ocasionados por personas y hay tres factores que influyen en ellos: la ignorancia, la haraganería y la malicia.
La ignorancia puede ser solucionada fácilmente mediante cursos de capacitación internos, utilización de folletos informativos y mediante exámenes periódicos de la habilidad de los usuarios de la red; la haraganería o flojera, es un factor de riesgo muy común en las grandes empresas, donde las principales fallas en la seguridad se deben a la incompetencia de sus miembros, al no apagar su equipo cuando se retiran de su lugar de trabajo o al no cerrar sesión; y, la malicia, debe entenderse como la influencia de las emociones de las personas que utilizan la red y que tratarán por cualquier medio de ponerla a prueba o dañarla.

Denegación de servicio: En este caso, la red es llevada al estado en que no puede transportar datos a los usuarios. Existen dos formas comunes en que esto puede realizarse: atacando a los routers o inundando la red con tráfico extraño. El término router es usado como ejemplo de una gran clase de componentes activos de interconexión de redes, lo que incluye firewalls, servidores proxy, etc.

Un ataque a un router está destinado a provocar la detención del transporte de paquetes o enviarlos en forma indebida. El caso anterior se puede deber a una desconfiguración, la inserción de actualización de ruteo falsa o un "ataque de inundación" (es decir, el router es bombardeado con paquetes no ruteados, causando una degradación en su desempeño). Un ataque de inundación en una red es similar a un ataque de inundación en un router, excepto que los paquetes de inundación son transmitidos. Un ataque de inundación ideal debería ser a través de la inserción de un único paquete, el cual explota algunos defectos conocidos en los nodos de la red y provoca que ellos retransmitan el paquete o generen paquetes de error, cada uno de los cuales es atrapado y replicado por otro host. (Akamai, s.f.)

Los diversos tipos de ataques informáticos que se presentan en la red:

Virus y Gusanos: Éstos, son los tipos más conocidos de software maligno que existen y se distinguen por la manera en que se propagan. El término de virus informático se usa para designar un programa que al ejecutarse se propaga infectando otro software ejecutable de la misma computadora. Pueden tener un playload que realice otras acciones maliciosas en donde se borran archivos. Los gusanos son programas que se transmiten a sí mismos, explotando vulnerabilidades en una red de computadoras para infectar otros equipos. Su principal objetivo, es infectar a la mayor cantidad posible de usuarios y también puede contener instrucciones dañinas al igual que los virus. A diferencia que los gusanos, un virus necesita la intervención del usuario para propagarse, mientras que los gusanos se propagan automáticamente. (coreoneit, s.f.)

Backdoor o Puerta Trasera: Es un método para eludir los procedimientos habituales de autenticación al conectarse en una computadora. Una vez que el sistema ha sido comprometido, puede instalarse una puerta trasera para permitir un acceso remoto más fácil en el futuro de los atacantes. Los crackers suelen usar puertas traseras para asegurar el acceso remoto a una computadora, permaneciendo ocultos ante posibles inspecciones, utilizando troyanos, gusanos u otros métodos. (coreoneit, s.f.)

Drive-by Downloads: Son sitios que instalan spyware o códigos que dan información de los equipos. Generalmente se presentan como descargas que de algún tipo, se efectúan sin consentimiento del usuario, lo cual ocurre al visitar un sitio web, al revisar un mensaje de correo o al entrar a una ventana pop-up. El proceso de ataque Drive-by Downloads se realiza de manera automática mediante herramientas que buscan en los sitios web alguna vulnerabilidad e insertan un script malicioso dentro del código HTML. (coreoneit, s.f.)

Rootkits: Es un software que modifica el sistema operativo de la computadora, para permitir que el malware permanezca oculto al usuario, evitando que el proceso malicioso sea visible en el sistema. (coreoneit, s.f.)

Troyanos: Es un software malicioso que permite la administración remota de una computadora de forma oculta y sin el consentimiento del propietario. Generalmente están disfrazados como algo atractivo o inocuo que invitan al usuario a ejecutarlo. Pueden tener un efecto inmediato y tener consecuencias como el borrado de archivos del usuario e instalar más programas maliciosos. Son usados para empezar la propagación de un gusano, inyectándolo de forma local dentro del usuario. (coreoneit, s.f.)

Hijackers: Son programas que realizan cambios en la configuración del navegador web, cambiando la página de inicio por páginas con publicidad, pornográficas u otros re-direccionamientos con anuncios de pago o páginas de phishing bancario. Ésta es una técnica que suplanta al DNS, modificando archivos hosts, para redirigir el dominio de una o varias páginas a otras, muchas veces una web falsa que imita a la verdadera. Comúnmente es utilizada para obtener credenciales y datos personales mediante el secuestro de una sesión. (coreoneit, s.f.)

Keyloggers y Stealers: Estos programas están encaminados al aspecto financiero, la suplantación de personalidad y el espionaje. Los Keyloggers monitorizan todas las pulsaciones del teclado y las almacenan para realizar operaciones fraudulentas como son pagos desde cuentas de banco o tarjetas de crédito. La mayoría de estos sistemas son usados para recopilar contraseñas de acceso, espiar conversaciones de chat u otros fines. Los Stealers también roban información privada pero solamente la que se encuentra guardada en el equipo. Al ejecutarse comprueban los programas instalados y si tienen contraseñas recordadas, por ejemplo en los navegadores web la descifran. (coreoneit, s.f.)

Botnets: Son redes de computadoras infectadas, también llamadas “zombies”, que pueden ser controladas a la vez por un individuo y realizan distintas tareas. Este tipo de redes son usadas para el envío masivo de spam o para lanzar ataques contra organizaciones. En una Botnet cada computadora infectada por el malware se loguea en un canal de IRC u otro sistema de chat desde donde el atacante puede dar instrucciones a todos los sistemas infectados simultáneamente. Las botnets también pueden ser usadas para actualizar el malware en los sistemas

infectados manteniéndolos así resistentes ante antivirus u otras medidas de seguridad. (coreoneit, s.f.)

Rogue software: Hacen creer al usuario que la computadora está infectada por algún tipo de virus u otro tipo de software malicioso, esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones, pero el usuario no necesita ese software puesto que no está infectado. (coreoneit, s.f.)

Los Ransomware: También llamados criptovirus o secuestradores, son programas que cifran los archivos importantes para el usuario, haciéndolos inaccesibles, y piden que se pague un “rescate” para poder recibir la contraseña que permite recuperar los archivos. (coreoneit, s.f.)

Phishing: Es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta, que consiste en engañar al posible estafado, "suplantando la imagen de una empresa o entidad pública", de esta manera hacen "creer" a la posible víctima que realmente los datos solicitados proceden del sitio "Oficial" cuando en realidad no lo es. (internautas, 2005)

Grayware o greynet

Los Grayware o greynet son software malicioso que no es tan peligrosos como los malwares. Suelen utilizarse para clasificar las aplicaciones o programas de cómputo y se instalan sin la autorización de los usuarios. (coreoneit, s.f.)

Los tipos de Grayware que existen son:

Adware: Son programas que automáticamente se ejecutan y muestran publicidad web, después de instalar el programa o mientras se está utilizando la aplicación “Ad”, que se refiere a “advertisement” (anuncios) en idioma inglés. (coreoneit, s.f.)

Dialers: Son programas maliciosos que toman el control del módem, realizan una llamada a un número de teléfono de tarificación especial, muchas veces internacional, y dejan la línea abierta cargando el costo de dicha llamada al usuario infectado. La forma más habitual de infección suele ser en páginas web que ofrecen contenidos gratuitos pero que solo permiten el acceso mediante conexión telefónica. Suelen utilizar como señuelos videojuegos, salva pantallas, pornografía u otro tipo de material. Actualmente la mayoría de las conexiones a Internet son mediante ADSL y no mediante módem, lo cual hace que los Dialers ya no sean tan populares como en el pasado. (coreoneit, s.f.)

Spyware: Son creados para recopilar información sobre las actividades realizadas por un usuario, obteniendo datos sobre los sitios web que visita, direcciones de email a las que después se envía spam. La mayoría de los programas son instalados como troyanos. Otros programas spyware recogen la información mediante cookies de terceros o barras de herramientas instaladas en navegadores web. Generalmente se presentan como programas que muestran publicidad o ventanas emergentes (pop-up) que son aceptadas de forma involuntaria, afectando los sistemas del usuario. (coreoneit, s.f.)

POLITICAS DE SEGURIDAD

La toma de decisiones referidas a seguridad, qué se realiza (o no) como administrador, determina principalmente cuán segura o insegura es la red o cuánta funcionalidad ofrece y cuán fácil es de usar. Sin embargo, no se pueden tomar buenas decisiones en seguridad sin determinar cuáles son los objetivos de ella. Este es el primer paso, antes de hacer uso de las herramientas de seguridad, ya que se debe determinar para qué chequear y qué restricciones imponer. (A., Udec, 2001)

Los objetivos serán determinados por la siguiente combinación de factores:

- Servicios ofrecidos v/s seguridad provista: Cada servicio ofrecido a los usuarios, importa su propio riesgo de seguridad. Para algunos servicios, el

riesgo pesa más que el beneficio del servicio y el administrador puede determinar la eliminación de dicho servicio, más que intentar asegurarlo.

- Facilidad de uso v/s seguridad: Los sistemas de más fácil uso, deben permitir el acceso a cualquier usuario y no requerir de contraseñas, es decir, no habría seguridad. El requerimiento de contraseñas hace al sistema un poco menos conveniente, pero más seguro.

- Costo de seguridad v/s riesgo de pérdida: Existe el costo de adquirir hardware y software de seguridad tales como firewall y con facilidad de uso.

Mediante un conjunto de reglas de seguridad llamadas “Políticas de Seguridad”, se informa a los usuarios y administradores, cuales son los requisitos obligatorios a cumplir, para proteger los bienes de información y tecnología. La política debe especificar los mecanismos a través de los cuales se realiza. Otro propósito es proveer de una línea base a través de la cual adquirir, configurar y auditar sistemas computacionales y redes, en conformidad con la política. Por lo tanto, usar un conjunto de herramientas de seguridad en ausencia de por lo menos una política de seguridad implícita, es inconcebible.

La principal problemática de poner en marcha un plan de seguridad, es por supuesto, poner en marcha el plan. La mayoría de los usuarios tienen problemas para adaptarse con las nuevas disposiciones de seguridad, y tienden a desconfiar, cometer errores y reclamar por los problemas que tienen. La solución, por general es dar un periodo de tiempo para adaptarse y en el cual la red debe ser monitoreada de manera frecuente para ir resolviendo los diferentes problemas imprevistos en el plan de seguridad, y además para evitar posibles ataques externos que se aprovechen de la vulnerabilidad del sistema.

Para que una política de seguridad sea apropiada y efectiva, necesita tener la aceptación y el respaldo de todos los niveles de la organización. Es especialmente importante que la dirección de la organización respalde totalmente el proceso de la política de seguridad. La siguiente es una lista de individuos que deberían estar involucrados en la creación y revisión de documentos de políticas de seguridad:

- Administrador de seguridad.
- Personal técnico de tecnologías de información.
- Administradores de grandes grupos de usuarios dentro de la organización.
- Equipo de asistencia a incidentes de seguridad.
- Representantes de los grupos de usuarios afectados por las políticas de seguridad.
- Consejo legal (si es apropiado)

La lista anterior es representativa en muchas organizaciones, pero no es necesariamente completa. La idea es contar con representantes claves de la organización, administradores del presupuesto y de políticas de autoridad, personal técnico que sabe qué puede y no puede ser soportado y el consejo legal, que conoce las implicancias legales de la elección de las políticas. En algunas organizaciones puede ser necesario incluir personal de auditoría. El involucrar este grupo es importante si es que se alcanza la más amplia aceptación posible de las políticas.

Una buena política de seguridad debe tener las siguientes características:

- Debe ser implementable a través de procedimientos de administración de sistemas, publicando pautas directivas aceptables u otros métodos apropiados.
- Debe ser exigible con herramientas de seguridad si es preciso, y con sanciones, donde la prevención actual no es técnicamente factible.
- Debe definir claramente las áreas de responsabilidad de los usuarios, administradores y la dirección.

Además, los componentes de una buena política de seguridad incluyen:

- Pautas para adquisición de tecnología computacional con requerimientos específicos o características de seguridad deseadas. Estas deberían complementar pautas y políticas de adquisición existentes.

- Una política de privacidad que defina expectativas razonables de privacidad en temas tales como: monitoreo de correo electrónico, registros en teclado y acceso a archivos de usuarios.
- Una política de acceso que defina privilegios y derechos de acceso, para proteger los bienes de pérdida o divulgación, especificando pautas de uso aceptables por los usuarios, personal de operaciones y administradores. También debería proveer de pautas para conexiones externas, comunicación de datos, conexión de dispositivos a redes e incorporación de nuevo software al sistema.
- Una política de responsabilidad, que defina las responsabilidades de los usuarios, personal de operaciones y administradores. Esta debería especificar una capacidad de auditoría y proveer pautas para el manejo de incidentes, es decir, qué hacer y con quién contactarse si un posible intruso es detectado.
- Una política de autenticación que establezca confianza a través de una efectiva política de contraseñas y establezca pautas para autenticación en forma remota y el uso de dispositivos de autenticación.
- Una declaración de disponibilidad, que establezca expectativas de los usuarios acerca de la disponibilidad de los recursos. Esta debería localizar redundancias y recuperar elementos, también como especificar las horas de operación y los períodos de mantenimiento. También debería incluir información de contactos para el sistema de reportes y fallas en la red.
- Un sistema de tecnología de información y una política de mantenimiento de redes que describan cómo el personal de mantenimiento, tanto interno como externo, puede manejar y usar la tecnología. Un tópico importante que se indica aquí es si el mantenimiento remoto es permitido y cómo se controla dicho acceso.
- Una política de reporte de violaciones que indique qué tipo de violaciones (es decir, privacidad y seguridad, tanto interna como externa) deben ser reportadas y de quién son esos reportes. Una atmósfera no amenazante y la posibilidad de reportes anónimos, resultarán en una gran probabilidad que una violación será reportada si es que se detecta.

- Información de soporte que proveen los usuarios y administradores, con información de contacto para cada tipo de política de violación; pautas acerca de cómo manejar consultas acerca de incidentes de seguridad o información que pueda ser considerada confidencial y propietaria; referencias cruzadas a procedimientos de seguridad e información relacionada, tales como políticas de la compañía y leyes y regulaciones gubernamentales.
- Podría haber requerimientos regulatorios que afecten algunos aspectos de la política de seguridad (es decir, monitoreo en línea). Los creadores de la política de seguridad deberían considerar la búsqueda de asistencia legal en la creación de la política. Como mínimo, la política debería ser revisada por un consejo legal.
- Una vez que la política de seguridad ha sido establecida, debería ser claramente comunicada a los usuarios, staff y administradores. Habiendo todo el personal firmado una declaración que indique que han leído, comprendido y están de acuerdo en cumplir la política, es una parte importante del proceso.

MEDIDAS DE SEGURIDAD

Firewall: Una de las medidas y herramientas en la búsqueda de sistemas de seguridad más destacada y publicitada es el uso de Firewalls. Ellos proporcionan un nivel elevado de protección y son en general una forma de implementar políticas de seguridad en el nivel de red. El nivel de seguridad que proporciona un Firewall puede variar tanto como el nivel de seguridad de una máquina particular. Existe el tradicional balance entre seguridad, facilidad de uso, costo, complejidad, etc. (tripod)

Un Firewall es uno de los mecanismos usados para controlar y monitorear accesos hacia y desde una red, con el propósito de protegerla. Un Firewall actúa como un Gateway, a través del cual todo el tráfico fluye desde y hacia la red y/o sistema protegido. (tripod)

Un Firewall es generalmente una forma de construir una muralla entre una parte de una red, por ejemplo una red interna de la compañía y otra parte, por ejemplo la Internet global. La característica única de esta muralla es que necesita estar

concebida para tráfico con características particulares a transferir a través de puertas cuidadosamente vigiladas (gateways). La parte difícil es establecer el criterio por el cual los paquetes tienen acceso permitido o denegado a través de las puertas. (Luna, 2003)

Los Firewalls no son siempre una máquina individual. En lugar de ello, los Firewalls son a menudo una combinación de routers, segmentos de red y computadores hosts. Los Firewalls son comúnmente construidos usando dos componentes diferentes: routers de filtrado y servidores proxys. (Red Iris, 2002)

Routers de filtrado: son los componentes más fáciles de conceptualizar en un Firewall. Un router mueve datos de un lugar a otro entre dos o más redes. Un router normal toma un paquete de una red A y rutea este a su destino en la red B. Un router de filtrado hace lo mismo, pero no decide solamente cómo rutear el paquete, sino que considera si este paquete debe ser ruteado por él. Esto se logra instalando una serie de filtros a través de los cuales el router decide qué hacer con un paquete de datos. (Informatica, s.f.) (**Ver Figura 4**)

Figura 4. Filtrado mediante Router ACLs
Fuente: Elaboración Propia. 2014.

Servidores conectados directamente a Red Insegura: Son servidores que ofrecen servicios al exterior de la red y se encuentran conectados directamente al router y no al firewall, que protege la red interna. Toda la seguridad de los servidores depende de sí mismos, es decir, deben implementar diferentes mecanismos y técnicas de endurecimiento para soportar ataques desde la red insegura y continuar funcionando. Como recomendación deben tener el mínimo

de paquetes instalados y servicios habilitados, así como endurecimiento a nivel de sistema operativo y servicios. El acceso desde los servidores públicos hacia la red interna es estrictamente prohibido debido a que pueden ser utilizados como salto hacia la red interna. **(Ver Figura 5).**

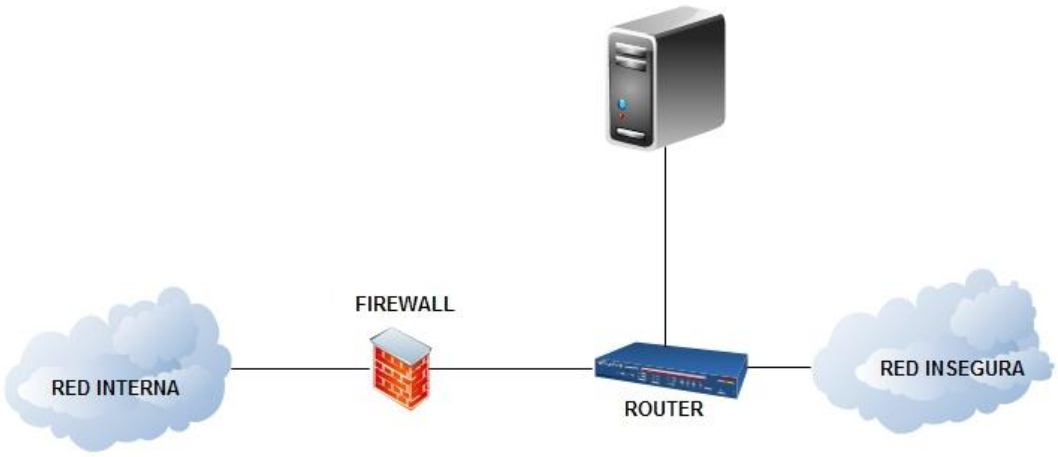


Figura 5. Servidores conectados directamente a red insegura
Fuente: Elaboración Propia. 2014

Demilitarized Zone (Single Firewall): Tanto los servidores públicos como la red interna son protegidos por un firewall. El área en la que se ubican los servidores públicos se conoce como zona desmilitarizada, que puede definirse como un área pública protegida que ofrece servicios al interior y exterior de la red. La red interna se comunica con la DMZ mediante enrutamiento (no deberían compartir el mismo segmento de red por razones obvias de seguridad). Este tipo de diseño es muy común, debido a su fácil implementación, seguridad y control del flujo de tráfico. **(Ver Figura 6).**

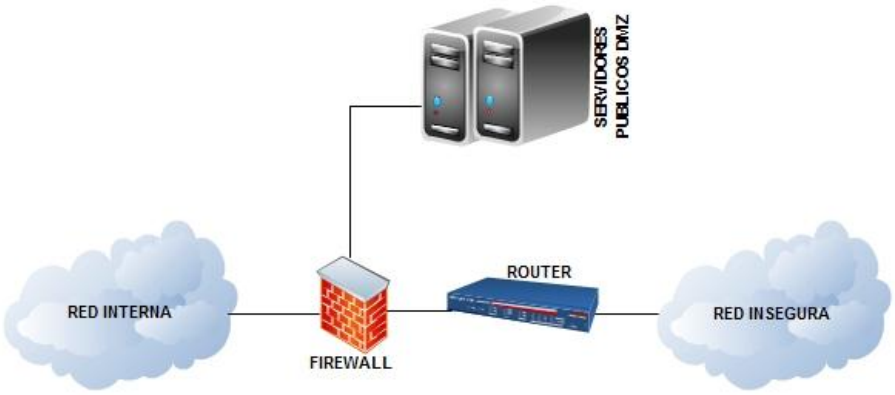


Figura 6. Demilitarized Zone (Single Firewall)
Fuente: Elaboración Propia. 2014.

Demilitarized Zone (Dual Firewall): El diseño de firewall dual adiciona un gateway firewall para controlar y proteger la red interna. Una de las razones es la protección de los servidores públicos frente a ataques provenientes de la red interna (como es bien conocido, la mayor cantidad de ataques son generados desde dentro de la red). Ofrece mayor seguridad para la red interna al no contar con un punto único de ataque como en las anteriores topologías. Como desventajas puede decirse que tiene mayor dificultad de configuración y monitoreo, así como mayores costos en hardware y software. Su implementación es adecuada para redes grandes en las que hay flujo de tráfico importante entre la red interna y la DMZ, donde también se demanda mayor seguridad para la red LAN.

Para esta arquitectura deberían implementarse dos tipos diferentes de firewalls (fabricantes distintos), debido a que si un atacante logra pasar el firewall exterior, ya tendría suficiente información para superar el firewall interno (asumiendo que es de la misma clase), ya que tendrían similar configuración al firewall ya violentado. **(Ver Figura 7).**

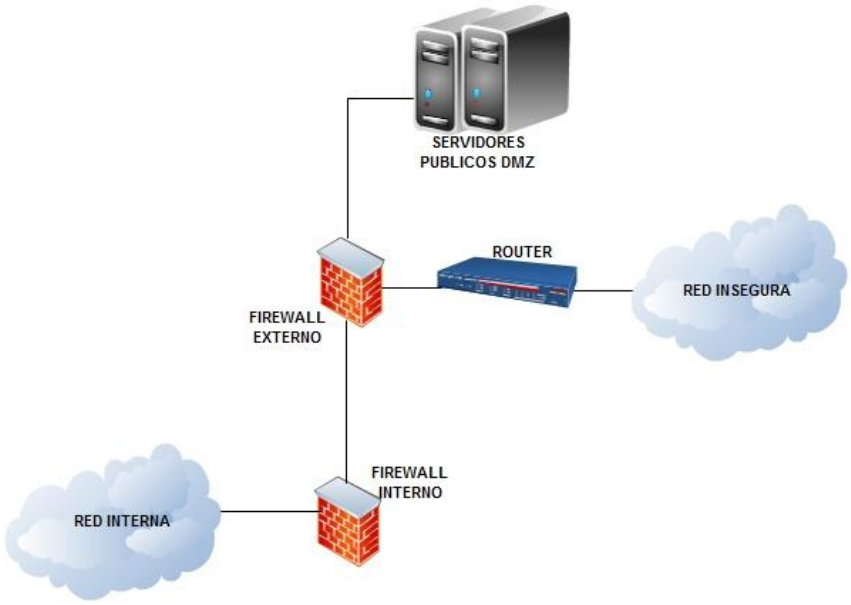


Figura 7. Demilitarized Zone (Dual Firewall)
Fuente: Elaboración Propia. 2014.

Proxy: un servidor proxy está hecho para concentrar los servicios de aplicación a través de una única máquina. Existe una única máquina (la máquina salvaguardia) que actúa como un servidor Proxy para una variedad de protocolos (Telnet, SMTP, Ftp, Http, etc.), pero pueden haber computadores host individuales para cada servicio. En vez de conectarse directamente a un servidor externo, el cliente se conecta al servidor proxy, el cual inicia una conexión al servidor externo requerido. Dependiendo del tipo de servidor proxy utilizado, es posible configurar clientes internos para ejecutar esta redirección en forma automática, sin conocer al usuario. Otros deben requerir que el usuario se conecte directamente al servidor proxy y entonces iniciar la conexión a través de un formato específico. (DesarrolloWeb, s.f.)

Existen significativos beneficios en seguridad, los cuales pueden ser derivados del uso de servidores proxys. Es posible agregar listas de control de acceso a protocolos, requiriendo a los usuarios o sistemas proporcionar algún nivel de autenticación, antes de que se confiera el acceso. Los servidores proxy más poderosos, algunas veces llamados Application Layer Gateways (ALGs) se

pueden escribir para que aprendan protocolos específicos y pueden ser configurados para bloquear sólo secciones del protocolo.

Los servidores proxy también pueden ser configurados para encriptar tramas de datos, basados en una variedad de parámetros. Una organización debe usar esta característica para permitir conexiones encriptadas entre dos ubicaciones cuyos únicos puntos de acceso están en Internet. **(Ver Figura 8).**

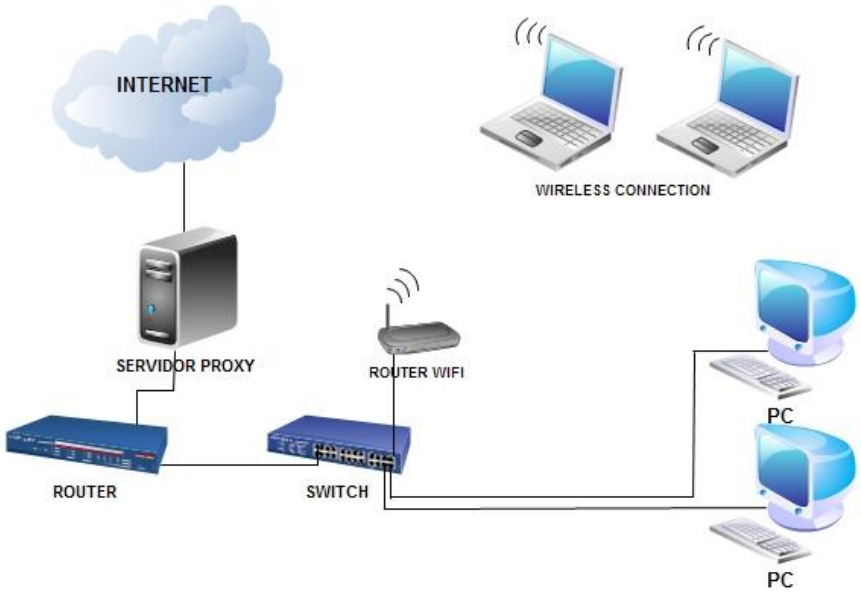


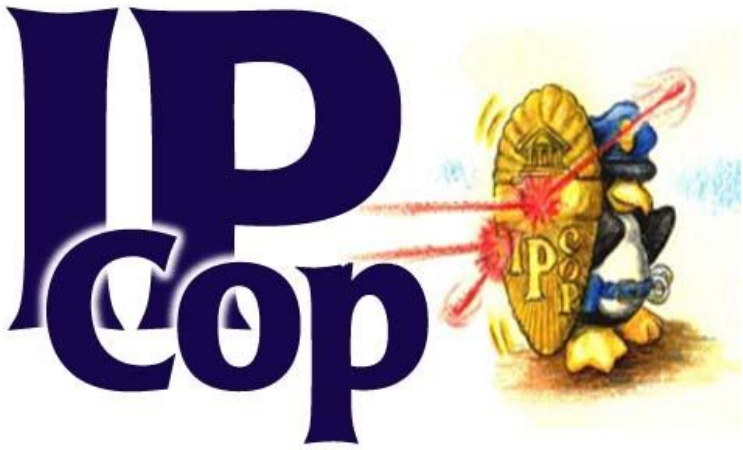
Figura 8. Servidor Proxy
Fuente: Elaboración Propia. 2014.

Los firewalls están concebidos como una manera de mantener fuera a los intrusos, pero a menudo son usados como una forma de legitimar a los usuarios dentro del sitio. El acceso a la Internet está a menudo disponible, pero puede ser a través de una máquina o red poco confiable. Un servidor proxy correctamente configurado permite a los usuarios legítimos acceder al sitio, mientras deniega acceso a los otros usuarios.

El mejor esfuerzo en técnicas Firewall, se encuentra usando una combinación de un par de routers protegidos con uno o más servidores proxys en una red entre los dos routers. Esta configuración permite a los routers externos bloquear

cualquier intento de uso bajo el nivel IP, para romper la seguridad, mientras el servidor proxy permite manejar potenciales brechas en la seguridad en los protocolos de nivel superior. El propósito de los router internos es bloquear todo el tráfico, excepto al servidor proxy. Si este setup es implementado en forma rígida, se puede alcanzar un nivel superior de seguridad.

HERRAMIENTAS TECNOLOGICAS



Ilustracion 9. IpCop
Fuente.http://www.networkset.net/wp-content/uploads/2011/05/IPCop.jpg

IPCop es un cortafuego; de principio, de final y siempre, Ipcop es una Distribución Linux especializada; completa, configurada y lista para proteger su red. IPCop es una comunidad; donde los miembros se ayudan entre sí, compartiendo para mejorar el proyecto y entre ellos. Esta ayuda va desde simples instrucciones y consejos del “Networking básico”, hasta ayudar a los miembros a personalizar su IPCop para cubrir una necesidad especial como los teléfonos IP (VoIP) o la integración de múltiples oficinas.

Es un proyecto GNU/GPL. Se trata de un firewall basado en Linux que brinda una interesante gama de posibilidades a la hora de conectar una red local a Internet. Requiere de un hardware dedicado y permite gestionar el acceso a Internet, la seguridad y la interacción de hasta cuatro redes distintas que, en la jerga del IPCop, se denominan GREEN, BLUE, ORANGE y RED. Las mismas tienen las siguientes características:

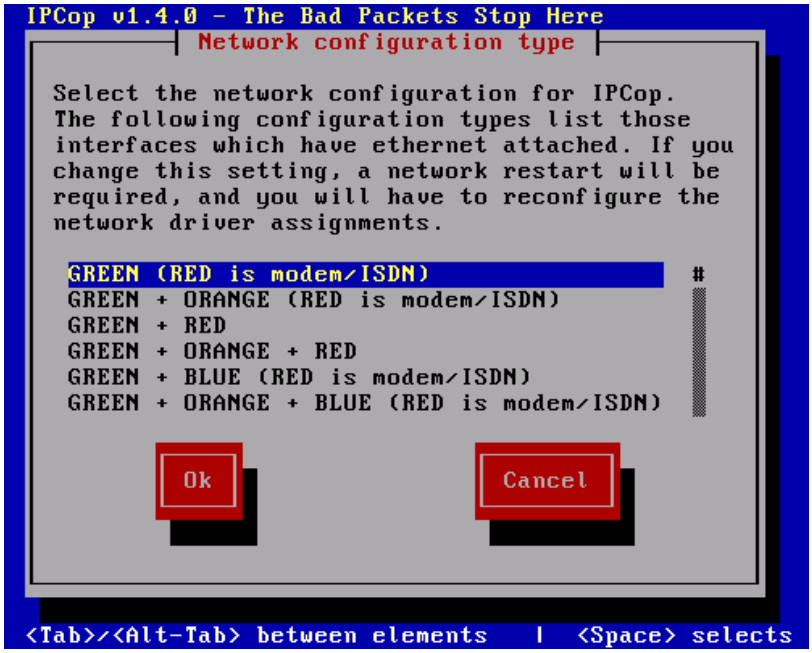


Figura 10. Interface configuration Green, Red, Blue and Orange of Ipcop
Fuente: http://www.ipcop.org/1.4.0/en/install/images/26-netcombo.png

GREEN: Esta es la interfaz de red de la LAN o red de área local. Aquí es donde se conectarán todos los equipos que necesiten mayor protección, como servidores que no tengan que tener presencia en Internet y puestos de trabajo. Los dispositivos que se encuentren conectados a esta interfaz tendrán acceso irrestricto a las interfaces RED, BLUE y ORANGE, o sea que podrán salir a Internet (y conectarse a los equipos que se encuentren en cualquiera de estas otras tres redes) por cualquier puerto, pero a su vez los equipos de la interfaz RED (equipos en Internet) no pueden iniciar conexiones a ningún equipo que se encuentre en las interfaces GREEN, BLUE y ORANGE. En otras palabras, estarán protegidos del exterior, en el sentido que no son accesibles desde Internet. (Infosertec, 2008)

BLUE: Es la interfaz que se asigna normalmente para conectar un access point de modo que se puedan conectar dispositivos inalámbricos. De todas maneras sirve para conectar cualquier otra red que se necesite, sea esta inalámbrica o no. Los dispositivos que se encuentren en esta red, no podrán iniciar una conexión a los dispositivos que se encuentren en la interfaz GREEN, pero salvo esta excepción, contarán con el mismo nivel de acceso y protección que cuentan los

dispositivos conectados a la interfaz GREEN. No es necesario activar esta interfaz en una instalación de IPCop si no se cuenta con más de una red, o no se va a utilizar un router inalámbrico. (Infosertec, 2008)

ORANGE: Esta es la interfaz que se utilizará para montar una DMZ o zona desmilitarizada. Principalmente se utiliza para montar servidores web, de correo, de ftp, etc. que deban tener presencia en Internet; o sea que sean accesibles desde Internet, pero que en el caso que se produzca alguna intrusión a algún equipo de esta red, eso no comprometa la seguridad de la red interna (GREEN). Los equipos que formen parte de la red ORANGE no podrán iniciar conexiones a ninguno de los dispositivos que se encuentren en las interfaces GREEN y BLUE. No es necesario activar esta interfaz en una instalación de IPCop si no se piensa utilizar una DMZ. (Infosertec, 2008)

RED: Es la interfaz de red que conectará directamente al proveedor de Internet. Puede ser una conexión ADSL, cable módem, una línea dedicada o hasta inclusive un módem telefónico común. Obviamente que por razones de ancho de banda esta última opción es desaconsejable, pero es perfectamente factible tenerla configurada para una contingencia en la cual el proveedor de Internet tenga inconvenientes para brindar el vínculo habitual, pero si esté operativo el acceso dialup. Cualquier instalación de IPCop contará con esta interfaz habilitada. (Soporta tanto dispositivos ethernet como USB). Como aclaración cabe destacar que los equipos que están en la misma red, ya sea esta GREEN, BLUE u ORANGE, tienen la posibilidad de iniciar conexiones entre ellos. (Infosertec, 2008)

En el caso de contar con un router wifi, si bien es conveniente, no es obligatorio que esté conectado a la interfaz blue, ya que se podrá conectar sin problemas a la interfaz GREEN.

Las características antes mencionadas de cada interfaz son las políticas de seguridad que IPCop implementa por defecto, pero existe la posibilidad de realizar modificaciones a estas políticas para adaptarlas a las necesidades que se tengan mediante las opciones de Port Forwarding y DMZ Pinholes.

Estas cuatro posibles redes no son más que cuatro placas de red en la misma PC. No es necesario utilizar las cuatro, sino que se puede configurar de diferentes maneras dependiendo de las necesidades que existan.

En la interfaz RED estará conectado el router o modem de acceso a Internet (ADSL, cablemodem, etc.), y en las otras tres interfaces puede montarse un switch si hace falta conectar más de un equipo en alguna de ellas.

FUNCIONALIDADES

IPCop brinda una amplia gama de funcionalidades que van más allá de las que ofrecen algunos firewalls comerciales. Sin pretender explicar cada una de ellas y solo a modo de numeración, se tienen:

- Acceso seguro por SSL a la interfaz de administración web.
- DHCP cliente / servidor
- DNS dinámico
- Lista de hosts seteable desde la interfaz web
- HTTP / FTP proxy (squid)
- Log local o remoto
- NTP cliente / servidor
- Servidor SSH (PSK o con password)
- Traffic shaping (en la interfaz RED)
- “Statefull” Firewall
- Port forwarding (redireccionamiento de puertos)
- DMZ pinholes
- Activar o desactivar ping en todas las interfaces
- VPN (IPSEC)
- Gráficos de monitoreo de CPU, RAM, swap, HD, tráfico de RED, etc.

Existen varios desarrolladores (sin vinculación con el equipo de desarrollo de IPCop) que han desarrollado paquetes con funcionalidad adicional, que se denominan addons, estos permiten una amplia gama de funcionalidades no incluidas originalmente en el producto. Los siguientes son ejemplos de la gran variedad de addons disponibles:

- **Copfilter**: Se trata de un excelente addon que permite integrar a IPCop funciones de antivirus y antispam. Para ello se vale de paquetes de software antivirus como ClamAV (se le puede agregar también F-Prot y AVG), y SpamAssasin para el caso del antispam. (Infosertec, 2008). **(Ver Ilustracion 11).**

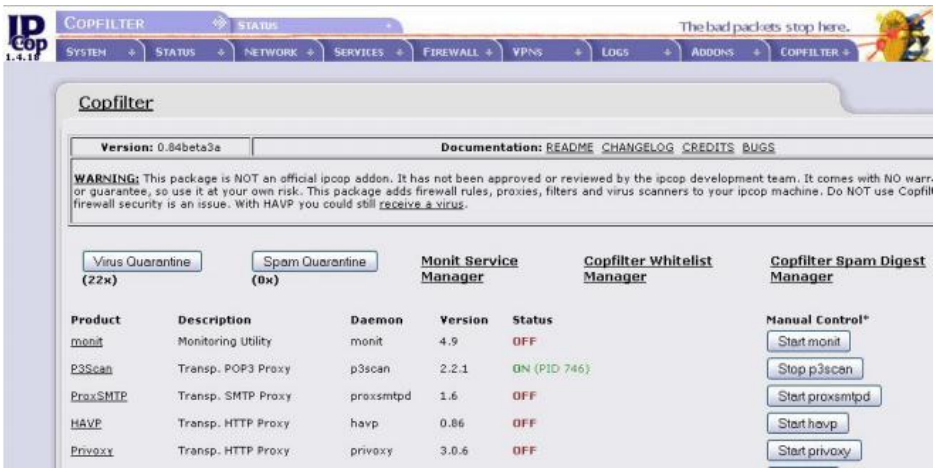


Figura 11. Interfaz de Copfilter
Fuente: http://infosertec.loquefaltaba.com/tuxinfo7baja.pdf

- ***Zerina****:* Si bien IPCop permite trabajar con una VPN por medio de IPSEC, este excelente addon da la posibilidad de agregar además OpenVPN. De esta manera es posible tener un excelente y robusto entorno de trabajo remoto accediendo por cualquiera de estas dos alternativas de VPNs, que permiten trabajar en cualquiera de los equipos internos de la red, tal como si se estuviera dentro de la red GREEN, pero trabajando tanto desde la red BLUE como la RED. (Infosertec, 2008). **(Ver Figura 12).**

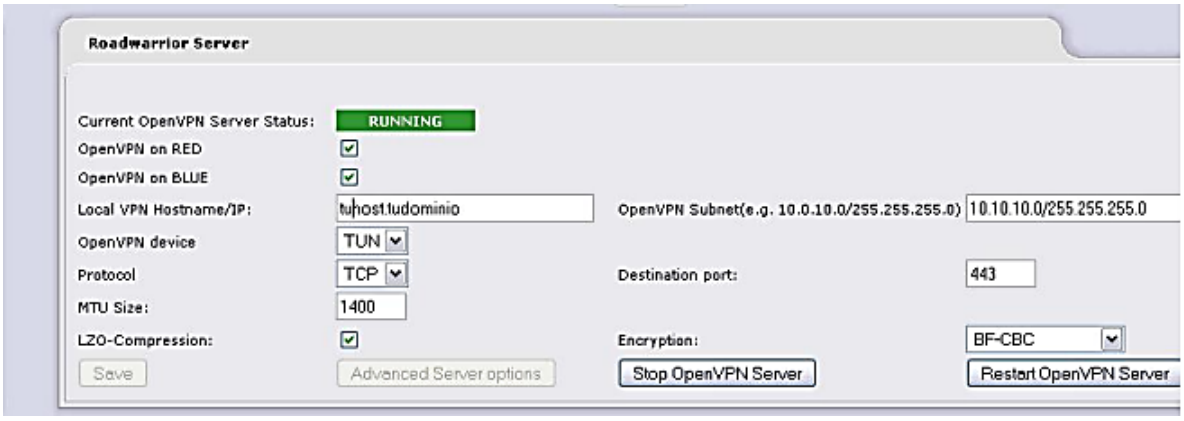


Figura 12. Interface Zerina
Fuente: http://infosertec.loquefaltaba.com/tuxinfo7baja.pdf

- **Addon Server:** Este addon es en realidad un servidor de addons que permite instalar en forma simple y desde la interfaz de administración web una variada lista de addons de diverso tipo para controlar el acceso desde la red GREEN hacia las otras tres, control horario de acceso a Internet, control de tráfico de cada red, mayor nivel de filtrado del tráfico. (Infosertec, 2008).

Otro punto importante es la facilidad de actualización que brinda, por la cual el propio IPCop avisará en la pantalla principal de su interfaz web, si hay actualizaciones disponibles, las cuales bastará con descargar a una PC y luego hacer el correspondiente upload de la misma para que se instale.

Cabe destacar que debido a que los addons no están oficialmente soportados, no es inusual que una actualización haga desaparecer algún Addon o algún punto de menú del mismo, por lo que debe prestarse especial atención a las actualizaciones, si es que se ha instalado algún addon al IPCop. **(Ver Figura 13).**

Figura 13. Interface Addon Server
Fuente: http://infosertec.loquefaltaba.com/tuxinfo7baja.pdf

CUADRO COMPARATIVO FIREWALL EN LINUX		
FIREWALL	**DEFINICION**	**CARACTERISTICAS**
IPCOP	IPCop es una distribución de servidor de seguridad de código abierto Linux, equipo IPCop está trabajando continuamente para ofrecer un estable, más seguro, el usuario del sistema de gestión de Firewall amable y altamente configurable a sus usuarios. IPCop proporciona una interfaz web bien diseñada para administrar el servidor de seguridad. Es muy útil y bueno para las pequeñas empresas y los PC locales. Puede configurar un PC antiguo como una VPN segura de proporcionar un entorno seguro en internet. También se mantiene un poco de información que se utiliza con frecuencia para ofrecer una mejor experiencia de navegación web a sus usuarios.	-Su interfaz web de código de colores le permite controlar los gráficos de rendimiento de CPU, memoria y disco, así como el rendimiento de red. -Se ve y rotación automática de registros. -Apoyar Soporte para múltiples idiomas. -Proporciona muy seguro actualización estable y de fácil implementación y añadir parches.
ENDIAN	Endian Firewall es otro firewall Stateful Inspection concepto de paquetes basado que puede ser desplegado como routers, delegación y puerta de enlace VPN con OpenVPN. Su originalmente desarrollado a partir de cortafuegos IPCop que también es un tenedor de Smoothwall.	-Firewall bidireccional -Prevención de intrusiones Snort -Puede asegurar servidor web con HTTP y FTP proxy, antivirus y URL lista negra. -Puede proteger los servidores de correo con SMTP y POP3 proxies, spam Auto-aprendizaje, lista gris. -VPN con IPSec -Registro de tráfico de red en tiempo real
IPTABLES	Iptables / Netfilter es el más popular firewall basado en la línea de comandos. Es la primera línea de defensa de la seguridad del servidor Linux. Muchos administradores de sistemas lo utilizan para el ajuste fino de sus servidores. Filtra los paquetes en la pila de red dentro del propio núcleo. Puede encontrar una descripción más detallada de Iptables aquí.	-En él se enumeran los contenidos Del conjunto de Reglas de Filtrado de paquetes. - Es rápido relámpago porque inspecciona sólo los encabezados de los paquetes. - Puede Añadir / Eliminar / Modificar Reglas de acuerdo a sus necesidades En los conjuntos de Reglas de Filtrado de paquetes. - Añadir / puesta a cero contadores de cada regla de los conjuntos de Reglas de Filtrado de paquetes. - Soporta copia de seguridad y restauración con los archivos.

SHOREWALL	Shorewall o Shoreline Firewall es otro servidor de seguridad de código abierto muy popular especializado para GNU / Linux. Está construido sobre el sistema Netfilter integrado en el kernel de Linux que también es compatible con IPv6.	-Utiliza las instalaciones de seguimiento de conexiones de Netfilter para el filtrado de paquetes de estado. -Soporta una amplia gama de aplicaciones de routers / cortafuegos / puerta de enlace. -Administración del cortafuegos centralizado. -Una interfaz gráfica de usuario con el panel de control de Webmin. -Apoyo ISP múltiple. -Soporta enmascaramiento y reenvío de puertos. -Soporta VPN
UFW	UFW es la herramienta de servidor de seguridad predeterminada para los servidores de Ubuntu, que está básicamente diseñado para menor la complejidad del firewall iptables y hace que sea más fácil de usar. Una interfaz gráfica de usuario de la UFW, Gufw también está disponible para los usuarios de Ubuntu y Debian.	-Soporta IPV6 -Extended Opciones de registro con On instalación / Off -Supervisión Del estado -Marco Extensible -Puede ser integrado con Las aplicaciones -Añadir / Eliminar / Modificar Reglas de acuerdo a sus necesidades.
PFSENSE	pfSense es otro de código abierto y un firewall muy fiable para los servidores de FreeBSD. Su basado en el concepto de filtrado de estado de paquetes. Ofrece amplias gamas de característica que normalmente está disponible en sólo firewalls comerciales caros.	-Altamente configurable y actualizado de su Web - interfaz basada. -Se puede desplegar como un servidor de seguridad perimetral, router, DHCP y DNS. -Configurado como punto de acceso inalámbrico y un punto final de VPN. -La asignación de tráfico y la información en tiempo real sobre el servidor. -Balanceo de carga entrante y saliente.
IPFIRE	IPFire es otro de los firewalls basados código abierto Linux para Small Office, Home Office (SOHO) entornos. Su diseñado con modularidad y altamente flexibilidad. Comunidad IPFire también se hizo cargo de la Seguridad y la desarrolló como un Stateful Packet Inspection (SPI).	-Puede ser desplegado como un firewall, un servidor proxy o una puerta de enlace VPN. -El filtrado de contenidos -Incorporado sistema de detección de intrusiones Soporta través Wiki, foros y chats -Hipervisores de apoyo como KVM, VMware y Xen para entornos de virtualización.

Figura 14. Cuadro Comparativo Firewall en Linux
Fuente: Elaboración Propia

SOFTWARE LIBRE

Entre los años 60 y 70 del Siglo XX, el software no era considerado un producto sino un añadido que los vendedores de las grandes computadoras de la época (las mainframes) aportaban a sus clientes para que éstos pudieran usarlos. En dicha cultura, era común que los programadores y desarrolladores de software compartieran libremente sus programas unos con otros. Este comportamiento era particularmente habitual en algunos de los mayores grupos de usuarios de la época, como DECUS (grupo de usuarios de computadoras DEC). A finales de los

70, las compañías iniciaron el hábito de imponer restricciones a los usuarios, con el uso de acuerdos de licencia.

En 1971, cuando la informática todavía no había sufrido su gran boom, las personas que hacían uso de ella, en ámbitos universitarios y empresariales, creaban y compartían el software sin ningún tipo de restricciones. Con la llegada de los años 80 la situación empezó a cambiar. Las computadoras más modernas comenzaban a utilizar sistemas operativos privativos, forzando a los usuarios a aceptar condiciones restrictivas que impedían realizar modificaciones a dicho software.

En caso de que algún usuario o programador encontrase algún error en la aplicación, lo único que podía hacer era darlo a conocer a la empresa desarrolladora para que esta lo solucionara. Aunque el programador estuviese capacitado para solucionar el problema y lo desease hacer sin pedir nada a cambio, el contrato le impedía que mejorase el software.

Richard Stallman, en el laboratorio donde trabajaba, había recibido una impresora donada por una empresa externa. El dispositivo, que era utilizado en red por todos los trabajadores, parecía no funcionar a la perfección, dado que cada cierto tiempo el papel se atascaba. Como agravante, no se generaba ningún aviso que se enviase por red e informase a los usuarios de la situación.

La pérdida de tiempo era constante, ya que en ocasiones, los trabajadores enviaban por red sus trabajos a imprimir y al ir a buscarlos se encontraban la impresora atascada y una cola enorme de trabajos pendientes. Richard Stallman decidió arreglar el problema, e implementar el envío de un aviso por red cuando la impresora se bloqueara. Para ello necesitaba tener acceso al código fuente de los controladores de la impresora. Pidió a la empresa propietaria de la impresora lo que necesitaba, comentando, sin pedir nada a cambio, qué era lo que pretendía realizar. La empresa se negó a entregarle el código fuente.

En 1984, Richard Stallman comenzó a trabajar en el proyecto GNU, y un año más tarde fundó la Free Software Foundation (FSF). Stallman introdujo la definición de free software y el concepto de "copyleft", que desarrolló para otorgar libertad a los usuarios y para restringir las posibilidades de apropiación del software.

El software libre sirve para reducir el déficit de los gobiernos que necesitan ahorrar. En tiempos de crisis económica como en los que estamos inmersos actualmente, se hace necesario el uso del software libre para ayudar a reducir costos, en especial en las instituciones gubernamentales. (Wikipedia, 2014).

4. MARCO CONCEPTUAL

FIREWALL: Se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. (MOTTA, 2011)

DNS: Es una base de datos distribuida, con información que se usa para traducir los nombres de dominio, fáciles de recordar y usar por las personas, en números de protocolo de Internet (IP) que es la forma en la que las máquinas pueden encontrarse en Internet. El DomainNameSystem (DNS), o Sistema de Nombres de Dominio, comprende personas, instituciones reguladoras, archivos, máquinas y software trabajando conjuntamente. (MOTTA, 2011)

FRECUENCIA: Frecuencia es una medida que se utiliza generalmente para indicar el número de repeticiones de cualquier fenómeno o suceso periódico en la unidad de tiempo. (MOTTA, 2011)

GATEWAY: Gateway (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

El gateway o «puerta de enlace» es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: NetworkAddressTranslation). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa. (MOTTA, 2011)

INTERFACE: Interfaz es la conexión entre dos ordenadores o máquinas de cualquier tipo dando una comunicación entre ambas. (MOTTA, 2011)

ISP: Proveedor de servicios de Internet (o ISP, por la sigla en inglés de Internet ServiceProvider) es una empresa que brinda conexión a Internet a sus clientes.

Un ISP conecta a sus usuarios a internet a través de diferentes tecnologías como DSL, Cable, módem, GSM, Dial-up, Wifi, entre otros. Muchos ISP también ofrecen servicios relacionados con Internet, como el correo electrónico, alojamiento web, registro de dominios, etc. (MOTTA, 2011)

SWITCHES: Un conmutador o switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local). (MOTTA, 2011)

POLITICAS DE SEGURIDAD DE RED: Los objetivos de la política de seguridad de red son establecer políticas proteger las redes y sistemas de ordenador del uso inadecuado. Los mecanismos de Políticas de Seguridad de Red ayudarán en la identificación y la prevención del abuso de sistemas de ordenador y redes. Las Políticas de Seguridad de Red proporcionan un mecanismo para responder a quejas y preguntas sobre verdaderas redes y sistemas de ordenador. Las Políticas de Seguridad de Red establecen mecanismos que protegerán y satisfarán responsabilidades legales a sus redes y conectividad de sistemas de ordenador al Internet mundial. Los mecanismos de Políticas de Seguridad de Red apoyarán los objetivos de existir políticas. La responsabilidad de la seguridad de los recursos de calcular descansa con los administradores de sistema que manejan aquellos recursos. (MOTTA, 2011)

CACHE: En informática, una cache es un conjunto de datos duplicados de otros originales, con la propiedad de que los datos originales son costosos de acceder, normalmente en tiempo, respecto a la copia en la caché. Cuando se accede por primera vez a un dato, se hace una copia en el caché; los accesos siguientes se realizan a dicha copia, haciendo que el tiempo de acceso medio al dato sea menor. (MOTTA, 2011)

LISTAS BLANCAS: Listas en donde los emisores de emails poseen buena Reputación. Ayudan a resolver el problema de la reputación. Estas listas son Creadas y mantenidas por los ISP. Contienen direcciones de IP y dominios que han ganado una buena reputación. (MOTTA, 2011)

LISTAS NEGRAS: Es una lista de direcciones IP (Protocolo de Internet) o dominios que son percibidos como fuentes emisoras de Spam (correo no solicitado). (MOTTA, 2011)

SPAM: Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La palabra ¨Spam¨ proviene de la segunda guerra mundial, cuando los familiares de los soldados en guerra les enviaban comida enlatada. Entre estas comidas enlatadas estaba ¨Spam¨ una carne enlatada, que en los Estados Unidos era y es muy común. (MOTTA, 2011)

VPN: Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. (MOTTA, 2011)

SERVER: Sistema que proporciona recursos (por ejemplo, servidores de ficheros, servidores de nombres). En Internet, este término se utiliza a menudo para designar los sistemas que proporcionan información a los usuarios de la red. (Definicion.org, s.f.)

LINUX: Es un sistema operativo de software libre (no es propiedad de ninguna persona o empresa), por ende no es necesario comprar una licencia para instalarlo y utilizarlo en un equipo informático. Es un sistema multitarea, multiusuario, compatible con UNIX, y proporciona una interfaz de comandos y una interfaz gráfica, que lo convierte en un sistema muy atractivo y con estupendas perspectivas de futuro. (Orozco, 2011).

REDES: es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos. Básicamente, la comunicación dentro de una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, emisor y receptor, que se van asumiendo y alternando en distintos instantes de tiempo. (redusers, 2013)

5. METODOLOGÍA

5.1. Tipo y diseño de la Investigación

Según el propósito de la investigación y en correspondencia a los objetivos planteados en la misma, el estudio es de tipo Descriptivo. De acuerdo con el tipo de diseño y apoyado por lo expuesto según Hernández, Fernández y Baptista (1999) esta investigación estará orientada a un diseño no experimental, dado que se realizara el estudio sin la manipulación de ningún parámetro que afecte las variables de estudios.

5.2. Diseño Metodológico

5.2.1. **Etapas del proyecto:**

5.2.2. **Identificación de bienes**: En esta etapa se hará la recolección de la información concerniente a los bienes tangibles de la entidad, tales como: cantidad de computadores, sistemas operativos, enrutadores, switches y software utilizado.

5.2.3. **Identificación de Amenazas**: Se identificarán las principales amenazas que acechan la seguridad de la red de datos y que comprometen la integridad de la información que se transporta mediante ella.

5.2.4. **Establecimiento de Políticas de Seguridad**: Se analizarán los distintos elementos que deben tenerse en cuenta al momento de establecer estas normas y se entregará un documento con Políticas de Seguridad que debe ser aprobado por las Directivas de la entidad y que deben ser presentadas a los usuarios de la red para su estricto cumplimiento.

5.2.5. **Diseño del sistema de seguridad**: Se hará el diseño lógico del sistema de seguridad para la red de datos y control de acceso a Internet en la Universidad de Córdoba.

5.2.6. **Implementación del Sistema de seguridad**: En esta fase, se realizará la instalación y configuración de los elementos de software que serán parte integral del sistema de seguridad de la red.

5.2.7. **Pruebas:** Se realizarán diferentes pruebas para verificar que se cumplan los mínimos requerimientos de seguridad y restricciones en el acceso a sitios web potencialmente peligrosos para la integridad, confidencialidad y disposición de la información.

5.3. Técnica de Recolección de los Datos

La técnica de recolección de los datos que se utilizó para el estudio fue la observación, definida por Busot (1991, P.182), como el proceso por el cual percibimos hechos o fenómenos, en forma directa o con auxilio del instrumento apropiado, bajo rigurosas condiciones de control que facilitan la confiabilidad deseada. Dentro de esta técnica se utilizara la guía de observación y nota finales de los alumnos.

5.3.1. Análisis de los Datos

Como primer paso se procedió a estudiar el material consultado procedente de diferentes fuentes bibliográficas, catálogos, de tesis de grado y páginas Web. Muy en especial el tema de la seguridad informática, discriminando la información según su importancia, enfoque y con la ayuda de especialistas en el área de seguridad y metodología de la investigación para abordar y dar un tratamiento adecuado.

Posteriormente se recopilara la información sobre las posibles fayas y vulnerabilidades en el sistema, procediendo después a llenar la guía de observación, donde cada ítem corresponde a los indicadores de la dinámica en cuestión. Para posteriormente analizar los datos.

5.4. Procedimiento de la Investigación

Inicialmente se realizó una revisión bibliográfica sobre tópicos referentes a telemática y seguridad en redes de datos de los cuales se tomaron los más interesantes según su aspecto innovador y científico y luego de la discusión de los mismo con los asesores y profesores se seleccionó el tema de la investigación y se redactó el título, el planteamiento del problema, objetivos de estudio, posterior

a esto se definió el objetivo general y los específicos, que al cumplirse darán respuesta al problema estudiado.

Seguidamente se realizó una revisión bibliográfica que consistió en la consulta y análisis de diferentes fuentes tales como, libros de autores reconocidos sobre el tema a estudiar, tesis de grado de doctorado y maestrías, pagina Web, una vez estructurado el marco teórico, se definió el tipo y diseño de la investigación, seleccionándose la población y la muestra objeto del estudio. Adicionalmente se eligió una guía de observación como instrumento de recolección de los datos la cual se diseñara y se aplicara.

Una vez se recopile la información se procederá a procesar los datos y realizar los análisis pertinente de los de los mismos. Los resultados arrojados de este análisis se interpretaron, analizaron y discutieron con el fin de garantizar los objetivos planteados al principio de la investigación.

Finalmente se obtendrán las conclusiones y se formularan las recomendaciones derivadas del estudio realizado. Lo cual constituirá una de los aportes principales que otorga relevancia de carácter científico y practica al trabajo de investigación presentado en este informe.

6. RESULTADOS

AMENAZAS A LA RED DE DATOS DE LA UNIVERSIDAD DE CORDOBA

- ✓ Ataques contra servidores.
- ✓ Seguridad y privacidad en Redes Sociales.
- ✓ Robo de archivos y no de base de datos.
- ✓ Seguridad en la nube.
- ✓ Introducción de virus.

POLITICAS DE SEGURIDAD DE LA UNIVERSIDAD DE CORDOBA.

Las Políticas de seguridad que se plantean a continuación, deben concientizar al personal de la Universidad de Córdoba (UNICORDOBA) acerca de la importancia y sensibilidad de la información y los servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permitan a la institución cumplir con su misión.

El proponer estas políticas de seguridad, requiere un alto compromiso con la institución, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dichas políticas en función del ambiente dinámico que la rodea.

La Sección de Sistemas de Información y Telemática, se encarga de brindar servicio directo al usuario, por el ámbito de competencia que tiene cada uno de ellos en materia de informática, desde el equipamiento, instalación, alteración, cambio de lugar, programación, etc. Por lo tanto, es necesario emitir políticas particulares para la Red-UNICORDOBA.

Todas aquellas Dependencias de la UNICORDOBA que soliciten, instalen, administren, operen o utilicen equipos y/o programas de cómputo y/o redes locales de computación deberán sujetarse, en la medida de lo posible, a las políticas de seguridad descritas a continuación.

Del equipo

De la instalación del equipo de cómputo.

- ✓ Todo equipo de cómputo que esté o sea conectado a la Red-UNICORDOBA, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe sujetarse a las normas y procedimientos de instalación que emite La Sección de Sistemas de Información y Telemática.

- ✓ La Sección de Sistemas de Información y Telemática en coordinación con el departamento de Control de inventarios, deberá tener un registro actualizado de todos los equipos propiedad de UNICORDOBA.

- ✓ El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de: seguridad física, las condiciones ambientales y alimentación eléctrica.

- ✓ Los responsables de las áreas de apoyo interno de los departamentos deberán en conjunción con La Sección de Sistemas de Información y Telemática dar cabal cumplimiento con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación, de adjudicación, sistema y misión.

- ✓ La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, a las autoridades correspondientes.

Del mantenimiento del equipo de cómputo.

- ✓ A la Sección de Sistemas de Información y Telemática de la UNICORDOBA, corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir las normas y procedimientos respectivos.

- ✓ Corresponde a la Sección de Sistemas de Información y Telemática dar a conocer las listas de las personas, que puedan tener acceso a los equipos y

brindar los servicios de mantenimiento básico, a excepción de los atendidos por terceros.

- ✓ Queda estrictamente prohibido dar mantenimiento a equipo de cómputo que no es propiedad de la institución.

De la actualización del equipo de cómputo.

- ✓ Todo equipo de cómputo y de telecomunicaciones que sean propiedad de la UNICORDOBA, debe procurarse ser actualizado tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño por parte del personal de soporte técnico interno.

De la reubicación del equipo de cómputo.

- ✓ La reubicación del equipo de cómputo se realizará satisfaciendo las normas y procedimientos que la Sección de Sistemas de Información y Telemática emita para ello.

- ✓ En caso de existir personal técnico de apoyo interno o externo, éste notificará de los cambios tanto físicos como de software de red que realice a la Sección de Sistemas de Información y Telemática

Del control de accesos

Del acceso a áreas críticas.

- ✓ El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta La Sección de Sistemas de Información y Telemática.

- ✓ En concordancia con la política de la institución y debido a la naturaleza de estas áreas se llevará un registro permanente del tráfico de personal, sin excepción.

- ✓ La Dirección de la Universidad deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.

- ✓ Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la institución.

Del control de acceso al equipo de cómputo.

- ✓ Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

- ✓ Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos a la Sección de Sistemas de Información y Telemática.

- ✓ Las áreas de cómputo de los departamentos donde se encuentre equipo cuyo propósito reúna características de imprescindible y de misión crítica, deberán sujetarse también a las normas que establezca la Sección de Sistemas de Información y Telemática.

- ✓ Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la Sección de Sistemas de Información y Telemática tiene la facultad de acceder a cualquier equipo de cómputo que no esté bajo su supervisión.

Del control de acceso local a la red.

- ✓ La Sección de Sistemas de Información y Telemática es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

- ✓ La Dirección de la **UNICORDOBA** es la responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.

- ✓ Dado el carácter unipersonal del acceso a la **Red-UNICORDOBA**, La Sección de Sistemas de Información y Telemática verificará el uso responsable, de acuerdo al Reglamento para el uso de la red.

- ✓ El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, etc.) conectado a la red es administrado por La Sección de Sistemas de Información y Telemática.

- ✓ Todo el equipo de cómputo que esté o sea conectado a la **Red-UNICORDOBA** o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite la Sección de Sistemas de Información y Telemática.

Del control de acceso remoto.

- ✓ La Sección de Sistemas de Información y Telemática es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.

- ✓ El usuario de estos servicios deberá sujetarse al Reglamento de uso de la **Red-UNICORDOBA** y en concordancia con los lineamientos generales de uso de Internet.

- ✓ El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emita La Sección de Sistemas de Información y Telemática.

Del acceso a los sistemas administrativos

- ✓ Tendrá acceso a los sistemas administrativos solo el personal de la **UNICORDOBA** que tenga la autorización del responsable si se trata de personal de apoyo administrativo o técnico.

- ✓ El manejo de información administrativa que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.

- ✓ La instalación y uso de los sistemas de información se rigen por el reglamento de uso de la **Red-UNICORDOBA** y por las normas y procedimientos establecidos por La Sección de Sistemas de Información y Telemática.

- ✓ Los servidores de bases de datos administrativos son dedicados, por lo que se prohíben los accesos de cualquiera, excepto para el personal de la Sección de Sistemas de Información y Telemática.

Del W.W.W.

- ✓ La Sección de Sistemas de Información y Telemática es la responsable de instalar y administrar el o los servidor(es) W.W.W.

- ✓ La Sección de Sistemas de Información y Telemática deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, del uso de la Intranet institucional, así como las especificaciones para que el acceso a estos sea seguro.

- ✓ Los accesos a las páginas de Web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan en el Reglamento de acceso a la **Red- UNICORDOBA.**

- ✓ El material que aparezca en la página de Internet de la **UNICORDOBA** deberá ser aprobado por la Dirección General, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

- ✓ La Sección de Sistemas de Información y Telemática tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información y conservar información del tráfico.

De la utilización de los recursos de la red

- ✓ Los recursos disponibles a través de la **Red-UNICORDOBA** serán de uso exclusivo para asuntos relacionados con las actividades específicas de la institución.

- ✓ La Sección de Sistemas de Información y Telemática es el responsable de emitir y dar seguimiento al Reglamento para el uso de la Red.
- ✓ Corresponde a la Sección de Sistemas de Información y Telemática, administrar, mantener y actualizar la infraestructura de la **Red-UNICORDOBA**.

Del Software

De la adquisición de software.

- ✓ En concordancia con la política de la institución, la Dirección General y La Sección de Sistemas de Información y Telemática, son los organismos

oficiales de la **UNICORDOBA** para establecer los mecanismos de procuración de sistemas informáticos.

- ✓ Se deberá establecerse un presupuesto para la adquisición de software con licencia.

- ✓ La Dirección General en conjunto con la Sección de Sistemas de Información y Telemática, propiciará la adquisición de licencias de sitio, licencias flotantes, licencias por empleado y de licencias en cantidad, para obtener economías de escala y de acorde al plan de austeridad del Gobierno de la República.

- ✓ De acuerdo a los objetivos globales de la Dirección General, se deberá propiciar la adquisición y asesoramiento en cuanto a software de vanguardia.

- ✓ En cuanto al software libre, deberá respetarse la propiedad intelectual intrínseca del autor.

- ✓ La Sección de Sistemas de Información y Telemática promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

De la instalación de software.

- ✓ Corresponde a la Sección de Sistemas de Información y Telemática emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.

- ✓ En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación

de software con licenciamiento apropiado y de acorde a la propiedad intelectual.

- ✓ La Sección de Sistemas de Información y Telemática es el responsable de brindar asesoría y supervisión para la instalación de software informático y de telecomunicaciones.

- ✓ La instalación de software que desde el punto de vista de la Sección de Sistemas de Información y Telemática pudiera poner en riesgo los recursos de la institución no está permitida.

- ✓ Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, privilegios de acceso, y otros que se apliquen).

- ✓ La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento a la Sección de Sistemas de Información y Telemática.

De la actualización del software.

- ✓ La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo a la programación que anualmente sea propuesta por la Dirección General.

- ✓ Corresponde a la Sección de Sistemas de Información y Telemática autorizar cualquier adquisición y actualización del software.

- ✓ Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo al plan de actualización desarrollado por la Sección de Sistemas de Información y Telemática.

Del software propiedad de la institución.

- ✓ Todo el software adquirido por la institución sea por compra, donación o cesión, es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera.

- ✓ La Sección de Sistemas de Información y Telemática en coordinación con el departamento de Control de inventario, deberá tener un registro de todos los paquetes de programación propiedad de la **UNICORDOBA**.

- ✓ Todo el software (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos del **UNICORDOBA** se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo.

- ✓ Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.

- ✓ Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados.

- ✓ Corresponderá a la Sección de Sistemas de Información y Telemática promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas programáticos.

- ✓ La Sección de Sistemas de Información y Telemática administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.

Sanciones

- ✓ Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la Sección de Sistemas de Información y Telemática.

- ✓ Las sanciones pueden ser: desde una llamada de atención o informar al usuario, hasta la suspensión del servicio, dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

- ✓ Corresponderá a la Sección de Sistemas de Información y Telemática las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la institución.

- ✓ Todas las acciones en las que se comprometa la seguridad de la **Red-UNICORDOBA** y que no estén previstas en esta política, deberán ser revisadas por la Dirección General y La Sección de Sistemas de Información y Telemática, para dictar una resolución sujetándose a las normas vigentes.

7. DESARROLLO

7.1. ARQUITECTURA DEL SISTEMA

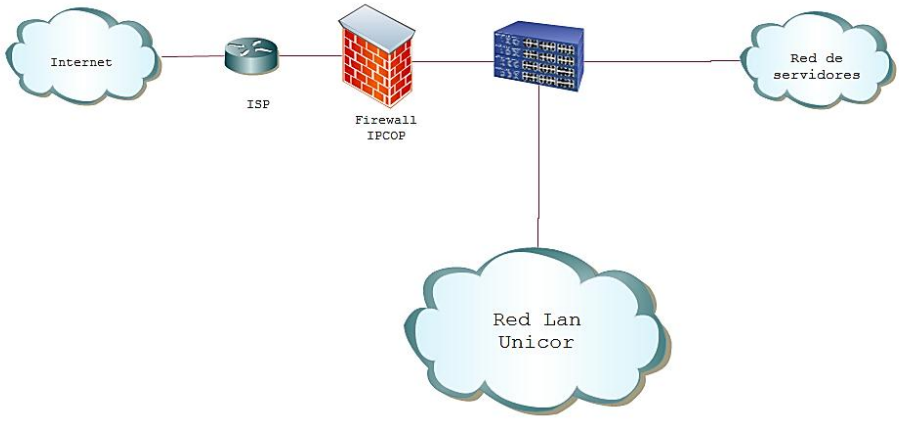


Figura 15. Arquitectura del Sistema.
Fuente: Elaboración Propia. 2015.

8. CONCLUSIONES

El principal factor de riesgo en una empresa es el factor humano. Como recurso siempre resultará indispensable, y la seguridad de una red dependerá siempre de cómo evaluar correctamente su grado de responsabilidad en el uso de la red.

Dentro de todo procedimiento, los niveles de responsabilidad de cada miembro deben ser considerados ante de emitir un juicio de quién debe usar un determinado recurso de la red y de qué manera.

Siempre debe mantenerse un control constante sobre el uso de los recursos de la red, para así evitar su colapso o la pérdida de su funcionalidad.

Se debe tener conocimiento de cuáles son las características de cada recurso (humano o máquina), controlar sus limitaciones, estar preparados para eventuales ataques y problemas internos, contar con herramientas de hardware y software adecuadas y mantener supervisión constante de los recursos de la red.

La seguridad de la red no se concentra en el firewall, aunque es parte importante de la misma, sino en políticas de seguridad coherentes que se adapten a la organización y su misión, en la que se tome la red como un todo y no como sub-sistemas independientes que dependen de un firewall para protegerse.

Las políticas de seguridad por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

IPCop es una excelente opción para brindar un muy buen nivel de seguridad y flexibilidad para instalaciones SOHO (Small Office Home Office). Existen algunas otras opciones, algunas con características más avanzadas, pero para las

necesidades más frecuentes de una instalación chica o mediana, IPCop resulta una de las propuestas más acertadas.

Referencias Bibliográficas

Alapont, V. (2003). Seguridad en redes inalámbricas. Consulta: documento en línea. Disponible en: http://www.uv.es/~montanan/ampliación/trabajo/SeguridadWireless.pdf. Consulta: 29/05/2014

A., Collazos G., Lozano H., Ortiz L., & Herazo G. (2011). Implementación de un sistema de gestión de seguridad de la información (SGSI) en la comunidad nuestra señora de gracia Documento en línea. Disponible en: http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf. -Consulta: 29/05/2014

Barahona E. & Gellibert P. (2011). Analizador de tráfico de red. Documento en línea. Disponible en: www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D91940.pdf -Consultado: 29/05/2014.

Cano, J. (2004). Pautas y recomendaciones para elaborar Políticas de Seguridad Informática (PSI). Documento en línea. Disponible en: http://www.derechotecnologico.com/estrado/estrado004.html. -Consultado: 30/05/2014.

Córdoba A., Durán G. & Flores V. (2010). Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS configurado en un Sistema Operativo LINUX para una LAN. Documento en línea. Disponible en: http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/6823/1/ESIMERADIUS.pdf -Consultado: 29/05/2014.

Documento CONPES (2011). Lineamientos de política para Ciberseguridad y Ciberdefenza. Documento en línea. Disponible en: http://www.slideshare.net/Derechotics/3701 -Consultado: 30/05/2014.

Esmoris, D. (2010). Implementación de Control de Acceso a Redes. Documento en línea. Disponible en: http://postgrado.info.unlp.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Esmoris.pdf -Consultado: 29/05/2014

Fernández, L. (2006). Desarrollo de un analizador de red Sniffer. Documento en Línea. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/454/1/38443tfc.pdf. -.Consulta: 29/05/2014

Hooper, E. (2009). Intelligent strategies for secure complex systems integration and design, effective risk management and privacy. Documento en línea. Disponible en: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4815808&queryText%3DCONTROL+OF+ACCESS+TO+INTERNET+AND+DATA+NETWORK Consultado: 26/05/2015

Hernández, R., Fernández, C., Batista, P. (1998) Metodología de la Investigación. (Segunda Edición). México, McGraw-Hill. -Consulta: 29/05/2014

Hurtado, J. (2007). El proyecto de Investigación. Quinta edición. Caracas. Ediciones Quirón-Sypal. -Consulta: 29/05/2014

Lerones L. (2006). Desarrollo de un analizador de red (sniffer).Documento en línea. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/454/1/38443tfc.pdf -Consultado: 29/05/2014.

Mieres, J. (2009). Ataques informáticos - Debilidades de seguridad comúnmente explotadas. Documento en línea. Disponible en: https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf -Consultado: 29/05/2014.

Mifsud, E. (2012). Introducción a la seguridad informática. Documento en línea. Disponible en: http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1. -Consultado: 29/05/2014.

Ochoa V. (2011). Análisis y el tráfico de datos en la capa de enlace de una red LAN, para la detección de posibles ataques o intrusiones sobre tecnologías Ethernet y Wifi 802.11. Documento en línea. Disponible en: http://repositorio.espe.edu.ec/bitstream/21000/4984/1/T-ESPE-032019.pdf - Consultado: 29/05/2014.

Pérez, G. (2007). Comportamiento del tráfico de datos en una red local Ethernet y Wifi empleando geometría fractal. Documento en línea. Disponible en: http://www.bdigital.unal.edu.co/12299/1/71612926.2007.Parte1.pdf. - Consulta: 29/05/2014.

Pfleeger. C. (2006). Security in Computing, Fourth Edition. - Pfleeger Consulting Group, Shari Lawrence Pfleeger. Prentice Hall. Consulta: 29/05/2014.

Pinilla, D. (2006). Diseño de un sistema automático de inspección remota (UAV). Documento en línea. Disponible en: http://eav.upb.edu.co/banco/sites/default/files/files/Tesistransmisioninalambricadatosmbricadatos.pdf. -Consulta: 29/05/2014

Romer, A. (2010). Documentación, implementación y verificación del sistema de gestion en control y seguridad (SGCS) a partir de la norma BASC (Business Alliance For Secure Commerce) a la empresa Seguridad. - Consulta: 29/05/2014 Acrópolis LTDA. Documento en línea. Disponible en: http://repository.upb.edu.co:8080/jspui/bitstream/123456789/1245/1/digital_19942.pdf. -Consulta: 29/05/2014

Sahagún, M. (2012). Seguridad Informática. Documento en línea. Disponible en:http://www.monografias.com/trabajos16/seguridadinformatica/seguridad-informatica.shtml -Consultado: 28/05/2014.

Taringa (2008). Conociendo e Instalando IPCOP. Documento en línea. Disponible en: http://www.taringa.net/posts/linux/1348427/Conociendo-eInstalando-IPCOP.html -Consultado: 30/05/2014.

Tanenbaum, Andrew (2005) Redes de Computadoras. Cuarta Edición. Prentice Hall Hispanoamericana.

Vinueza, P. (2011).Análisis para la seguridad de paquetes de datos y evitar ataques mediante sniffing. Ecuador. Documento en línea. Disponible en: http://186.42.96.211:8080/jspui/bitstream/123456789/509/1/TESIS%20FINAL%20-%20PABLO%20VINUEZA%20C.pdf -Consultado: 29/05/2014.

Yébenes, S. (2009). Sistema de Control de Acceso en Redes Wireless con el DNI electrónico. Documento en línea. Disponible en: http://oa.upm.es/1602/1/PFC_SERGIO_YEBENES_MORENO.pdf -Consultado: 29/05/2014.

Zseby, T. Iglesias Vazquez, F.; King, A.; Claffy, KC. (2015), Teaching Network Security With IP Darkspace Data. Viena. Documento en línea. Disponible en: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7086349&queryText%3Dnetwork+security+data Consultado en: 26/05/2015

A., L. B. (2001). *Universidad de Concepción.* Obtenido de http://www2.udec.cl/~ar-sc/arq-m-2001-1/brevis3.doc+&cd=1&hl=es&ct=clnk&gl=co

Cyberprimo. (2008). Obtenido de http://www.cyberprimo.com/2007/08/tipos-de-redes-informaticas.html

Informaticos, D. (2001). Delitos Informaticos. Obtenido de http://www.delitosinformaticos.com/seguridad/clasificacion.shtml

Infosertec. (2008). Obtenido de http://infosertec.loquefaltaba.com/tuxinfo7baja.pdf

Red Iris. (2002). Obtenido de http://www.rediris.es/cert/doc/unixsec/node23.html

Wikipedia.(2014).Obtenido http://es.wikipedia.org/wiki/M%C3%A1quina_virtual

Wikipedia. (2014). Obtenido de http://es.wikipedia.org/wiki/Software_libre

wikitel. (s.f.). wikitel. Obtenido de http://wikitel.info/wiki/Redes_de_datos.

ANEXOS

INSTALACION DE IPCOP.

Respecto al hardware necesario para su instalación, IPCOP corre en casi cualquier equipo disponible en la actualidad, ya que un Pentium con 32MB de RAM y unos cuantos cientos de MB en disco son más que suficientes para correr IPCop sin problemas

De todas formas si se quiere instalar algún addon, sería mejor que se utilice hardware más moderno, cuanto más potente mejor, sobre todo para que pueda correr sin problemas un addon como Copfilter que consume bastantes recursos de memoria y CPU.

Proceso de instalación y Configuración del Firewall IpCop

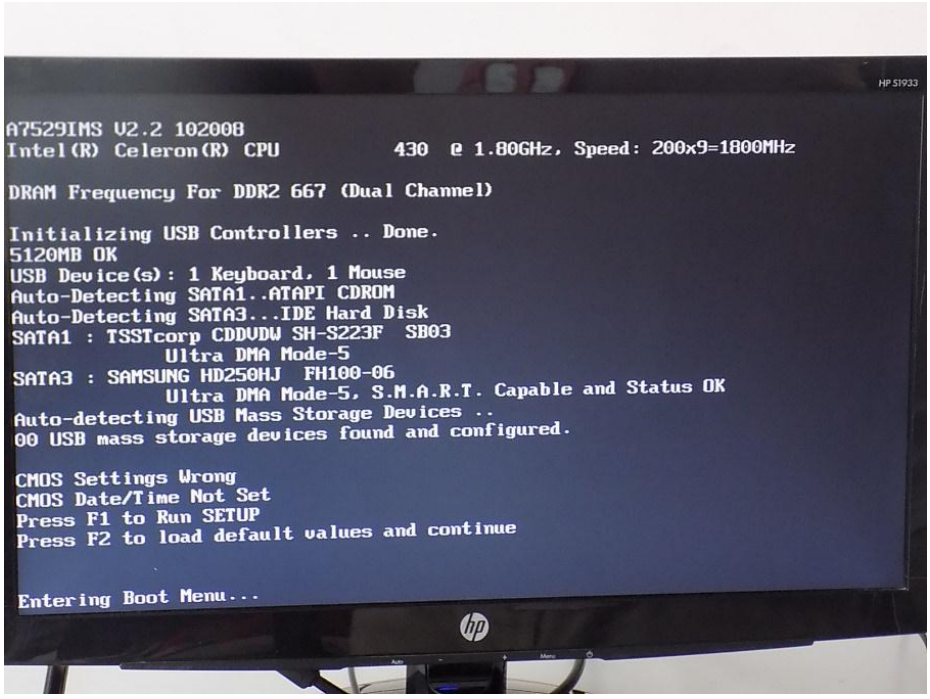


Figura 16. Inicio Boot menú para inicio desde la unidad de CD
Fuente: Elaboración Propia. 2015.

Figura 17. Copiado de archivos de instalación de IpCop
Fuente: Elaboración Propia. 2015.

Se ingresa el CD con el instalador de IpCop en la unidad de CD del equipo y se procede a iniciar desde el Boot Menu y se escoge la unidad de CD la instalación.

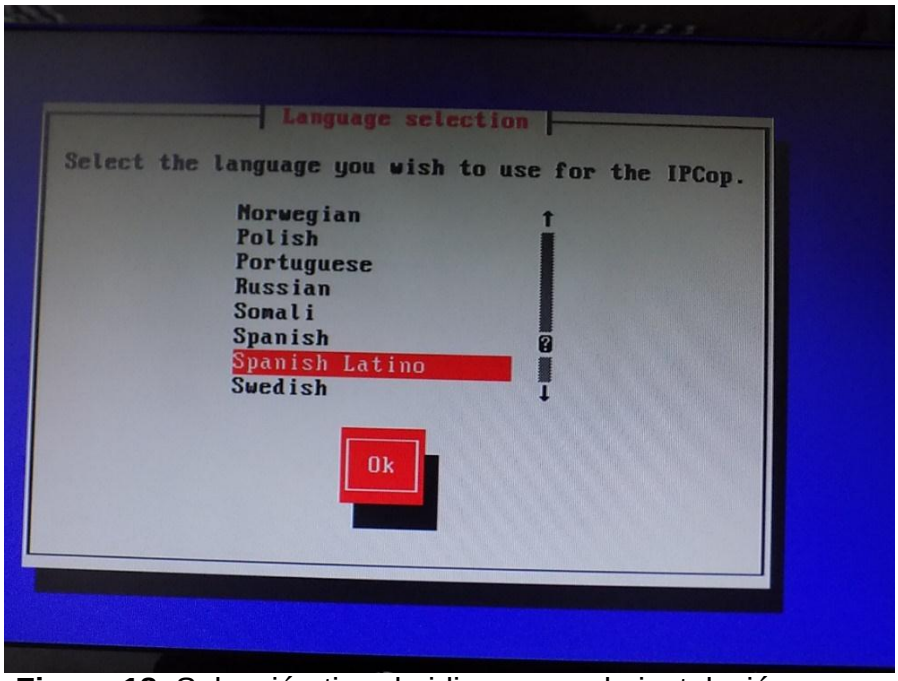


Figura 18. Selección tipo de idioma para la instalación
Fuente: Elaboración Propia. 2015.

.

Una vez finalizado el proceso de copiado de archivos y la inicialización de algunos procesos para la instalación, muestra un menú donde pide que se escoja el tipo de idioma.

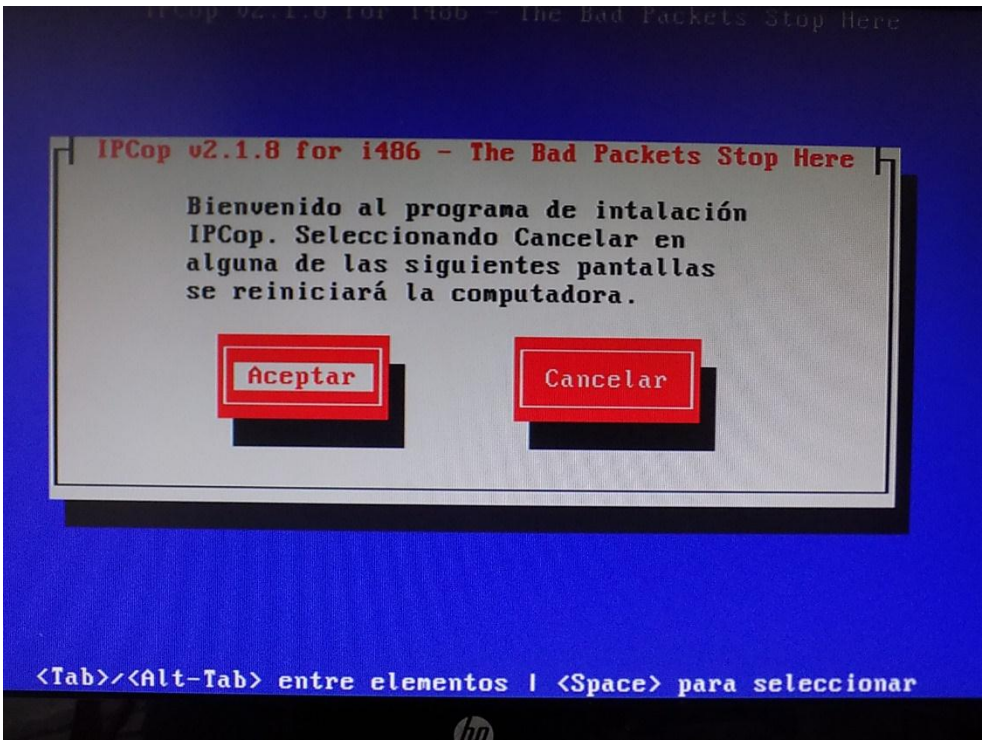


Figura 19. Bienvenida programa de Instalación de IpCop
Fuente: Elaboración Propia. 2015.

Da la bienvenida al proceso de instalación de IpCop y se da clic en aceptar.

.

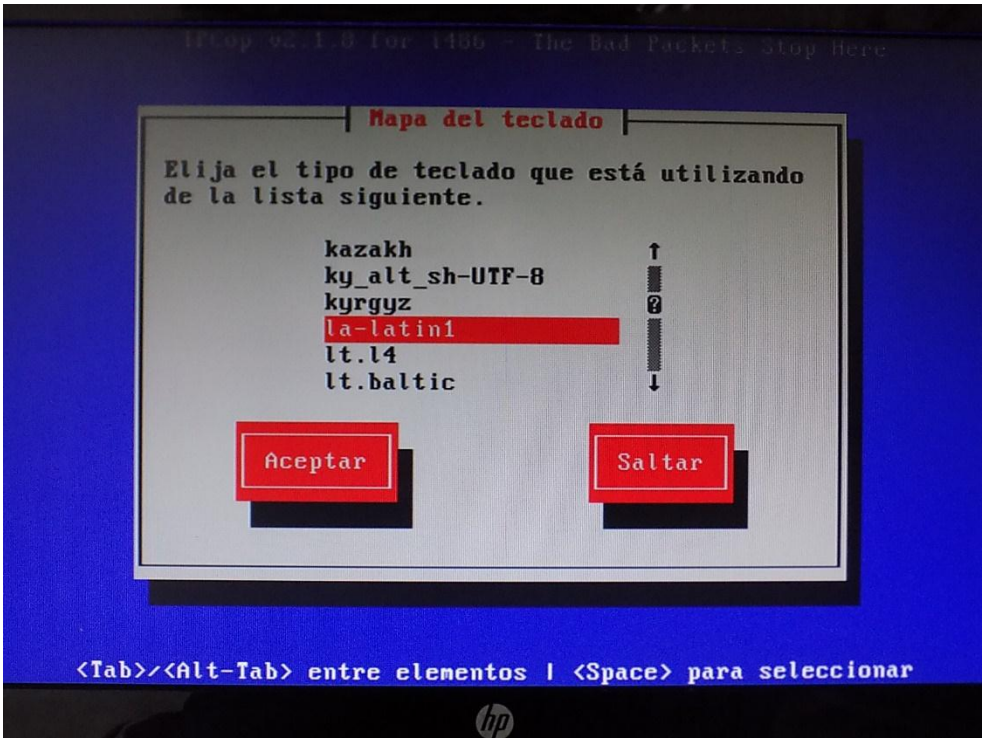


Figura 20. Selección del tipo de idioma del teclado
Fuente: Elaboración Propia. 2015.

Se elige el idioma del teclado que se desea utilizar, en este caso la-latino y se da clic en aceptar

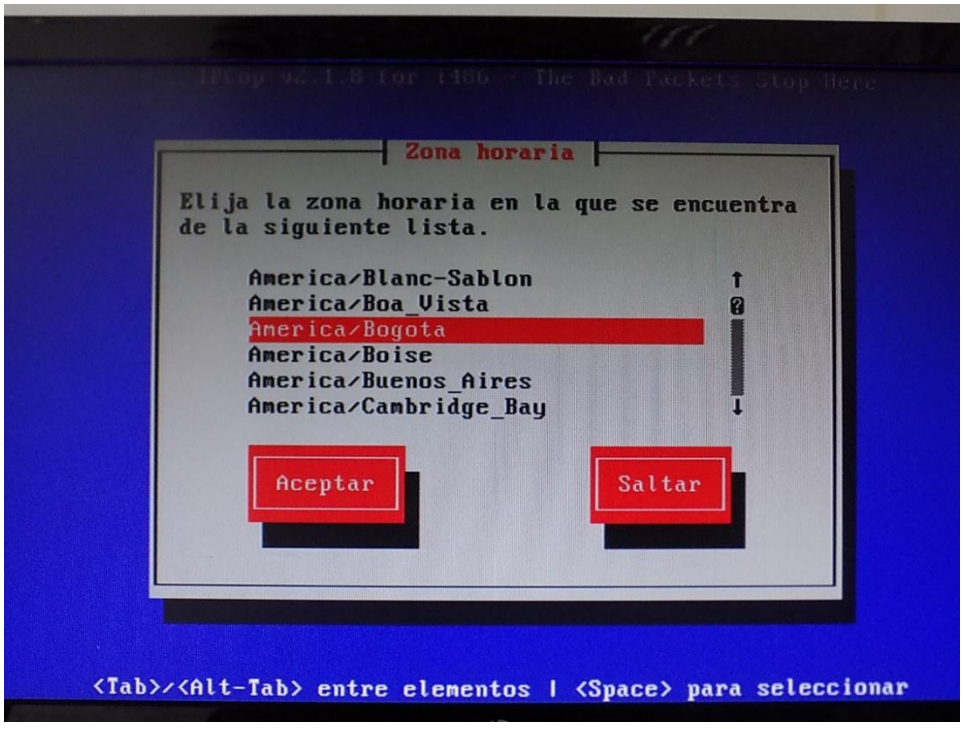


Figura 21. Selección zona horaria
Fuente: Elaboración Propia. 2015.

Luego se procede a escoger la zona horaria, en este caso sería América/Bogotá y se da clic en aceptar.

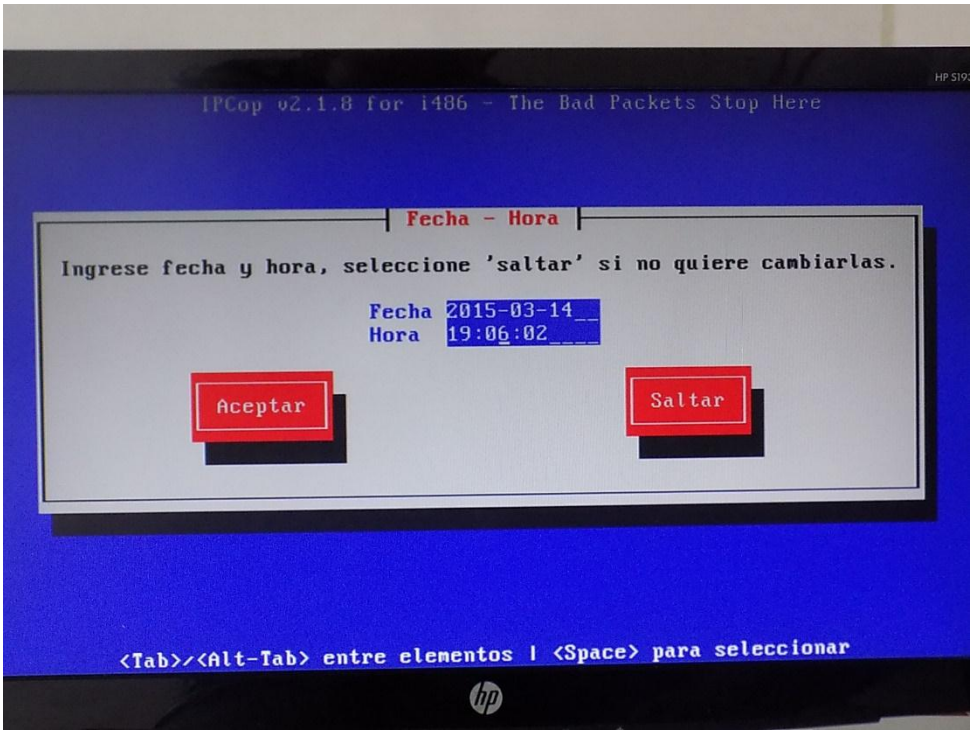


Figura 22. Configuración de hora y fecha
Fuente: Elaboración Propia. 2015.

Se procede a configurar la fecha y hora, se da clic en aceptar.

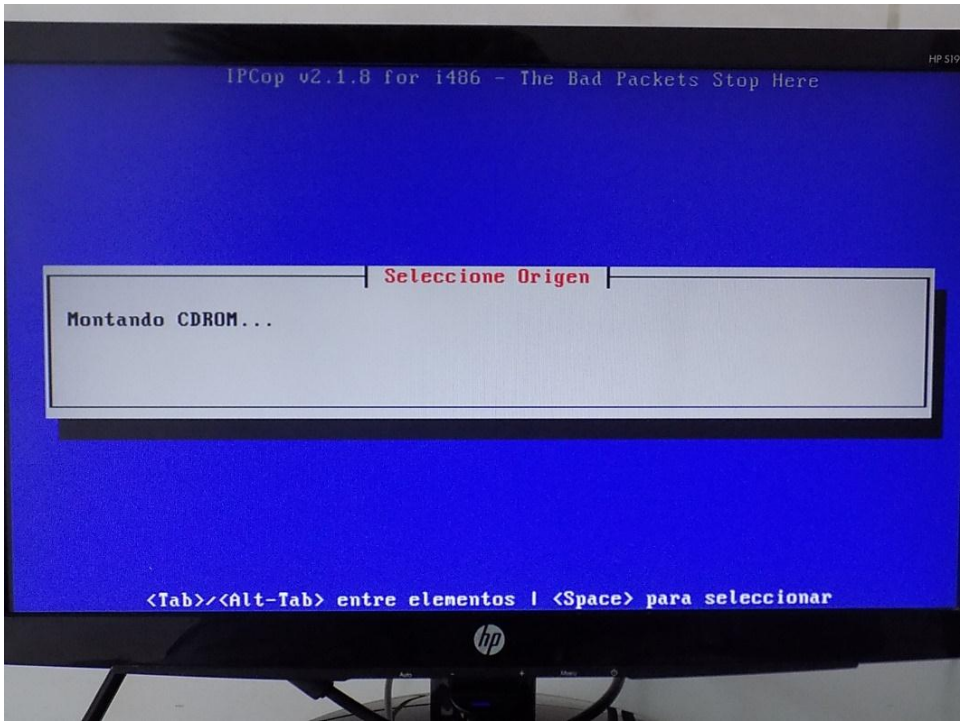


Figura 23. Montando unidad de CDROM
Fuente: Elaboración Propia. 2015.

Se espera que el sistema monte el CDROM y se pueda proceder con la instalación de IpCop.

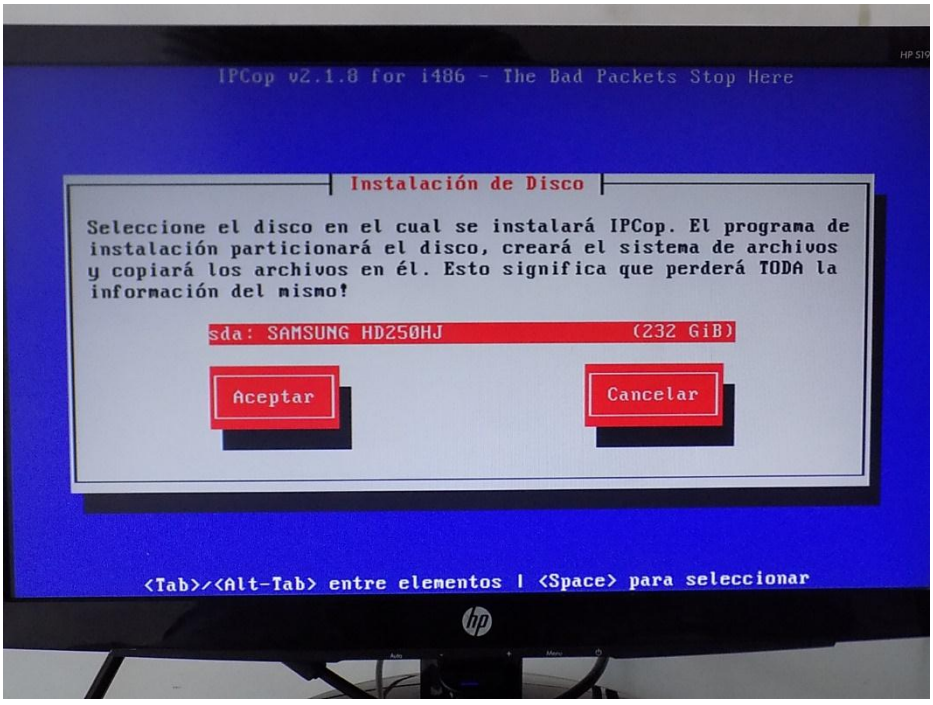


Figura 24. Selección del disco de instalación
Fuente: Elaboración Propia. 2015.

Una vez cargado la unidad y muestre los discos instalados en el equipo, se escoge el disco y se proceda a hacer la instalación de IpCop.

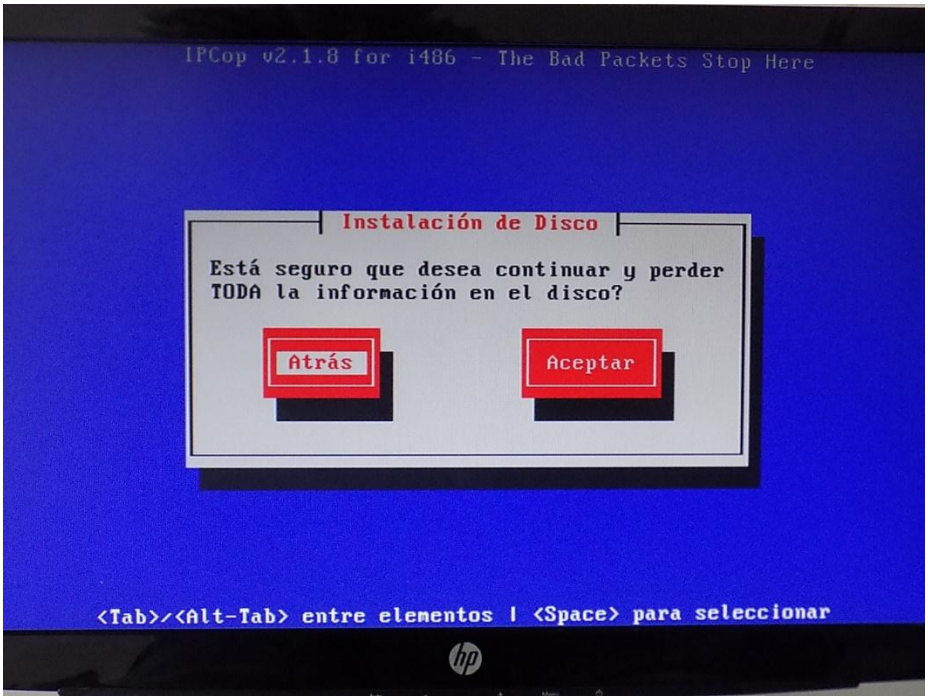


Figura 25. Permisos para instalación.
Fuente: Elaboración Propia. 2015.

Se procede a dar los permisos de continuar o no el proceso de instalación de IpCop.

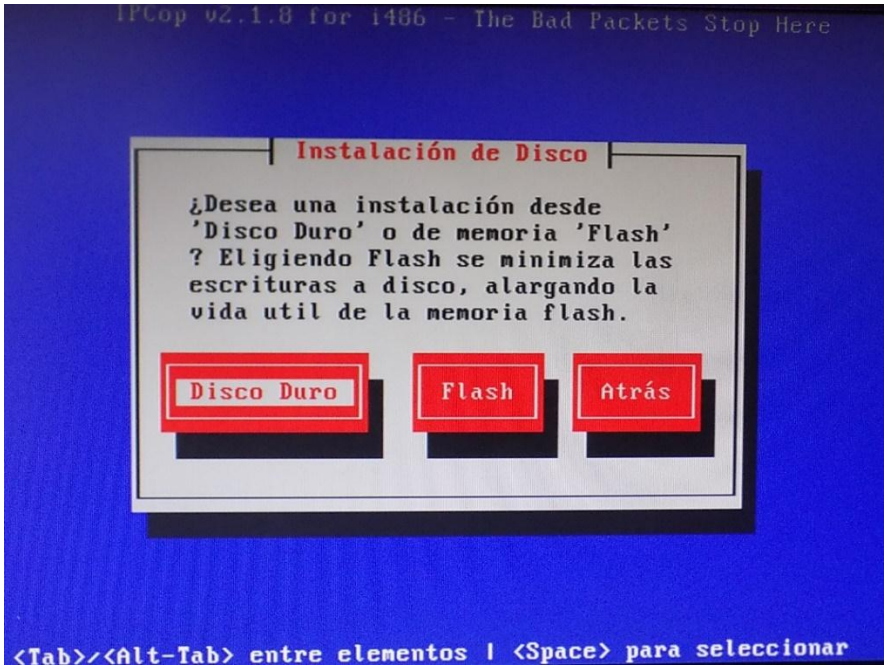


Figura 26. Instalación desde Disco Duro o flash
Fuente: Elaboración Propia. 2015.

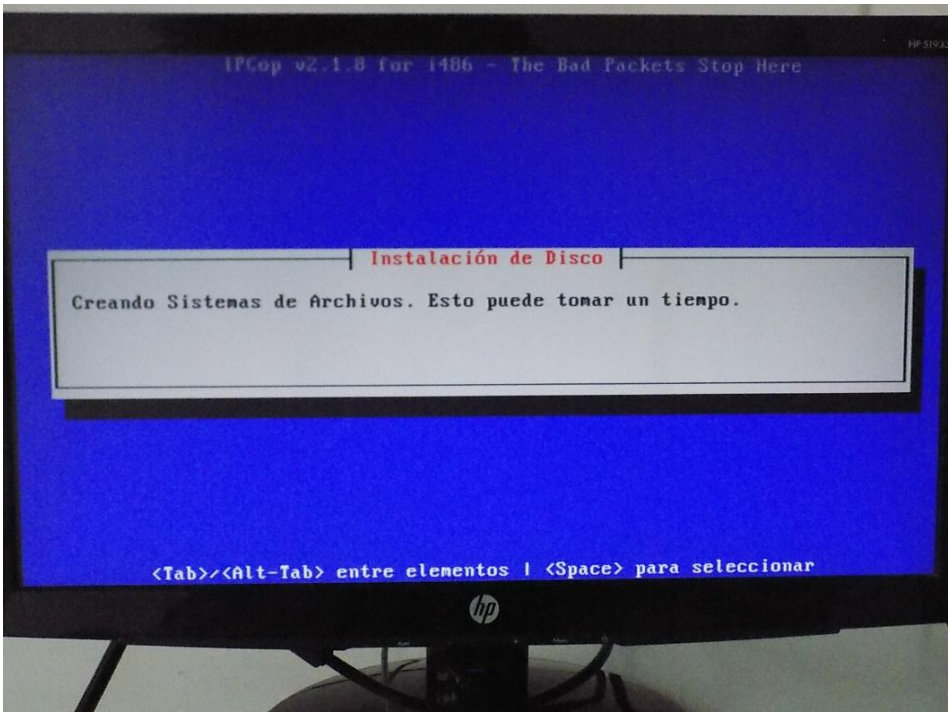


Figura 27. Creación del sistema de archivos
Fuente: Elaboración Propia. 2015.

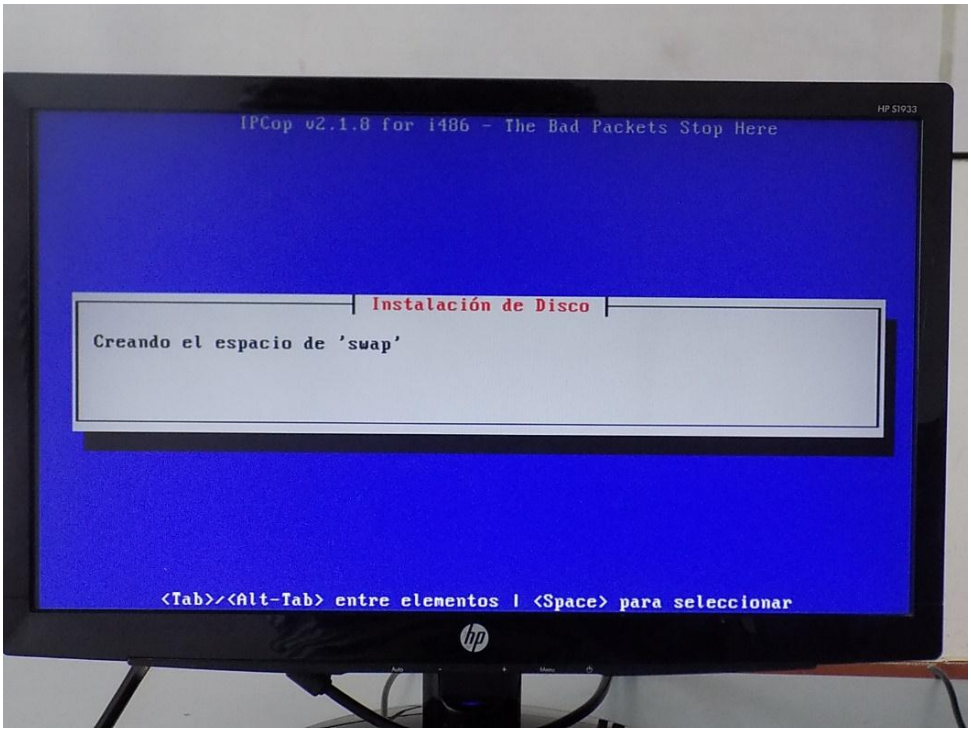


Figura 28. Creación del espacio de ‘swap`
Fuente: Elaboración Propia. 2015.

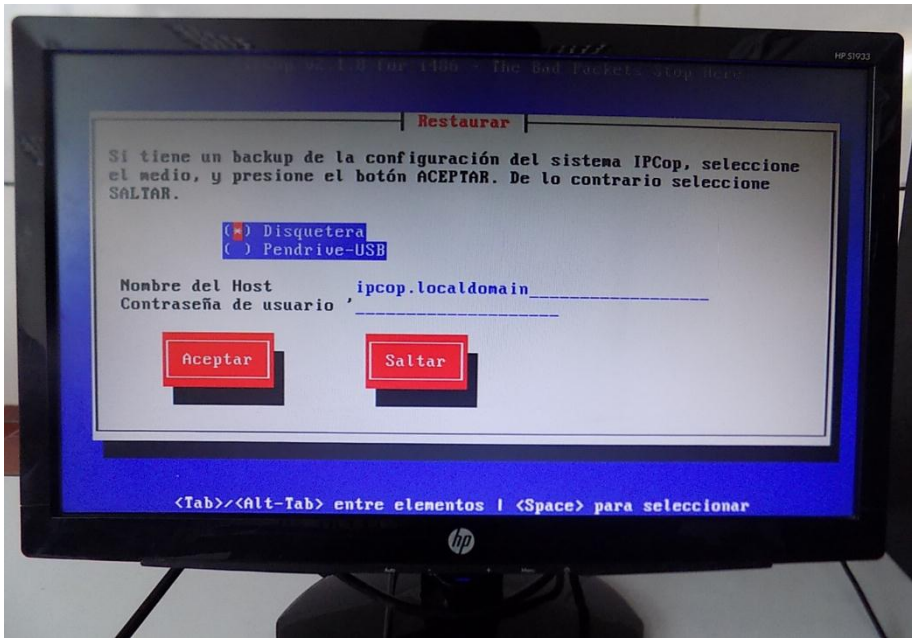


Figura 29. Configuración del Backup
Fuente: Elaboración Propia. 2015.

Se escoge la opción para el Backup y el medio de realizarlo y muestra el Nombre del Host y la contraseña de usuario.

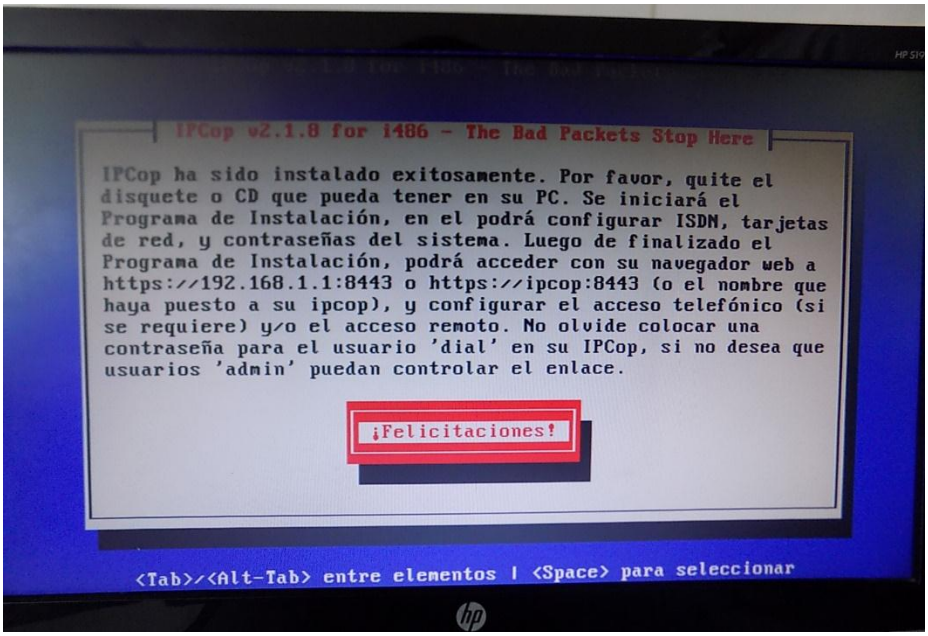


Figura 30. Finalización del proceso de Instalación
Fuente: Elaboración Propia. 2015.

Muestra un mensaje de finalización del proceso de instalación, donde ha finalizado exitosamente la instalación de IpCop.

Una vez finalizada la instalación se procede a la configuración de IpCop.

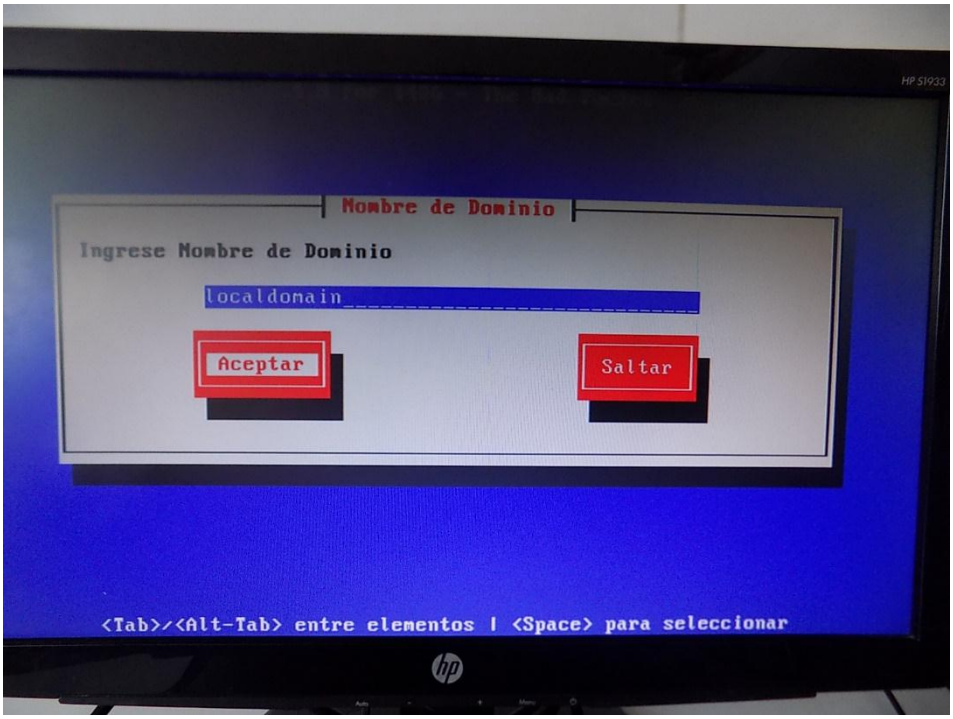


Figura 31. Ingreso del nombre del Dominio
Fuente: Elaboración Propia. 2015.

Se escribir el Nombre del Dominio, el cual se puede dejar tal cual aparece y se da clic en aceptar.

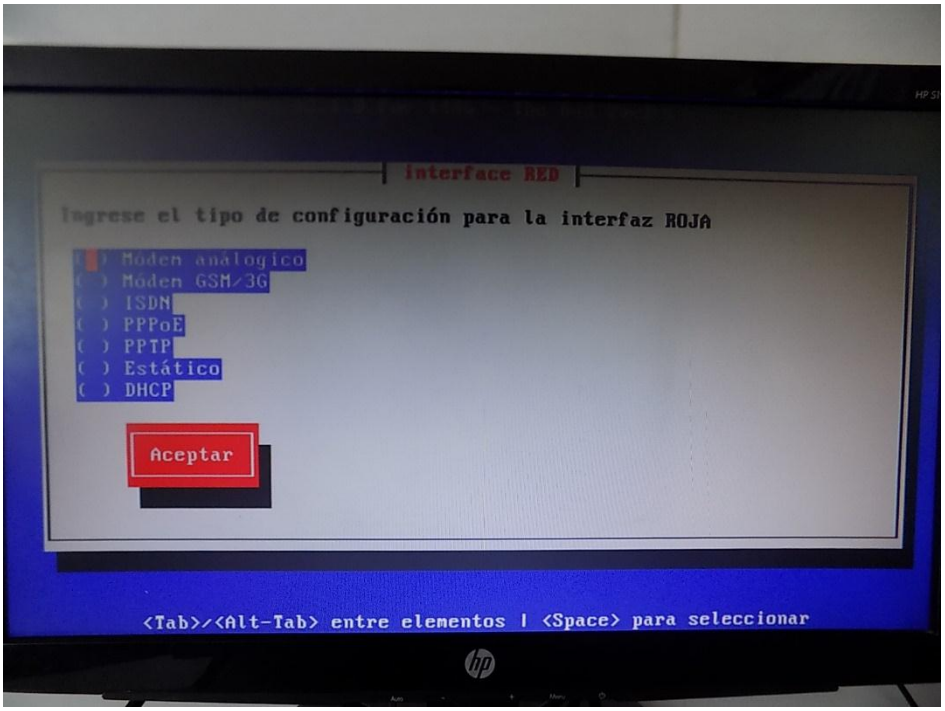


Figura 32. Tipo de configuración de interfaz roja
Fuente: Elaboración Propia. 2015.

Se escoge el tipo de interfaz de red que se va a utilizar y se da clic en aceptar.

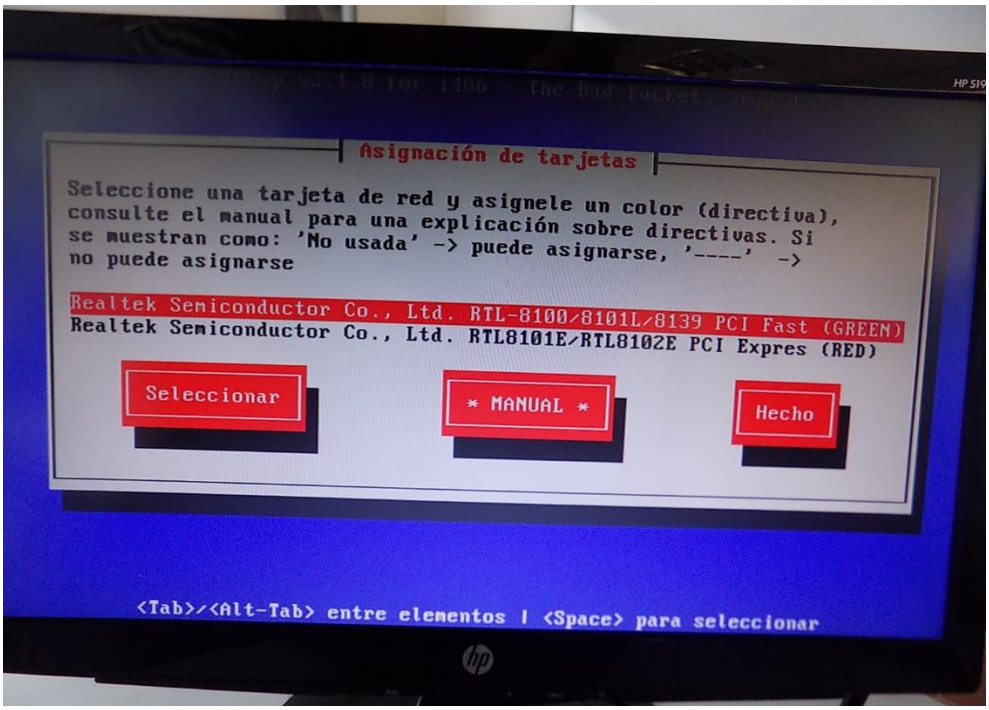


Figura 33. Asignación de colores a cada Tarjeta.
Fuente: Elaboración Propia. 2015.

Se procede con la asignación de tarjetas, en este caso a la tarjeta PCI Fast se le asignara el color GREEN y a la Tarjeta PCI Expres el color RED.

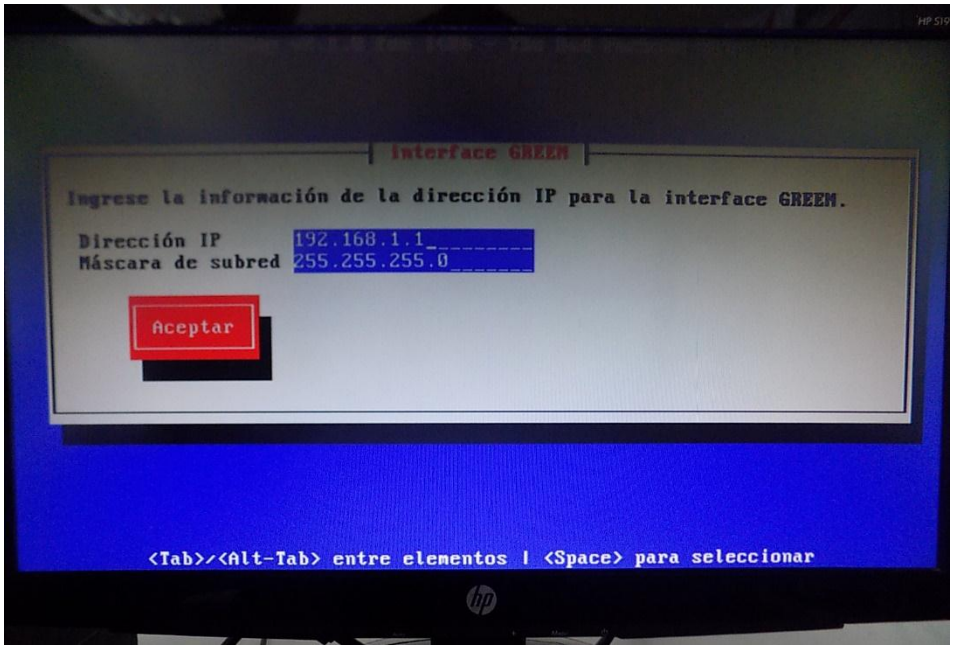


Figura 34. Configuración Interface GREEN.
Fuente: Elaboración Propia. 2015.

Figura 35. Configuración Interface RED.
Fuente: Elaboración Propia. 2015.

Se ingresa la información de la dirección IP para la interfaz GREEN y RED, dirección IP y Mascara de subred, se da clic en aceptar

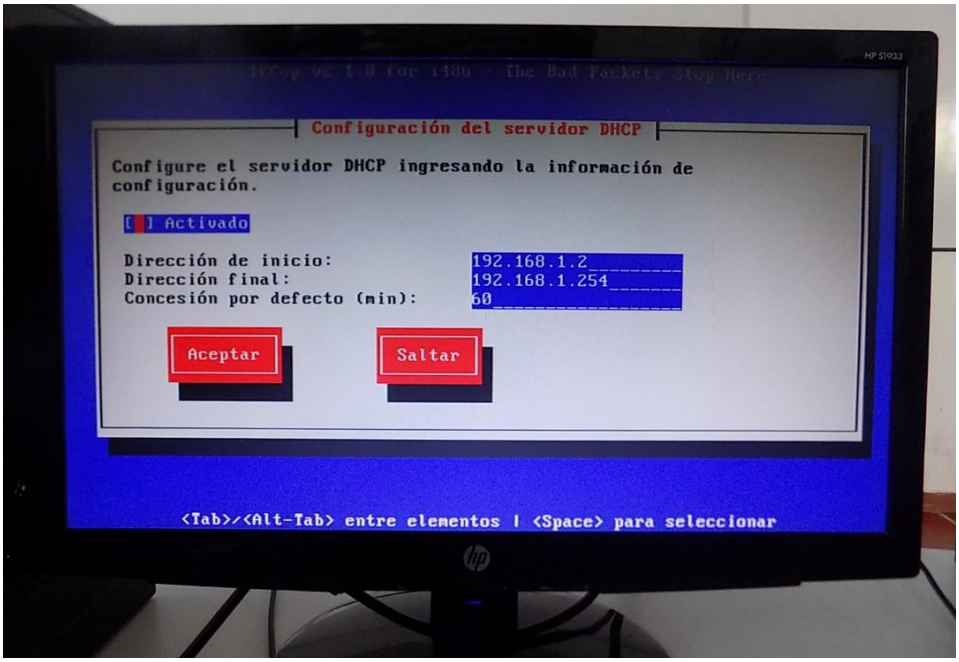


Figura 36. Configuración del Servidor DHCP.
Fuente: Elaboración Propia. 2015.

Se procede a hacer la activación del servidor DHCP, así como la dirección de inicio y la dirección final, y el número de concesión por defecto y clic en aceptar.

Figura 37. Ingreso de contraseña de usuario Root.
Fuente: Elaboración Propia. 2015.

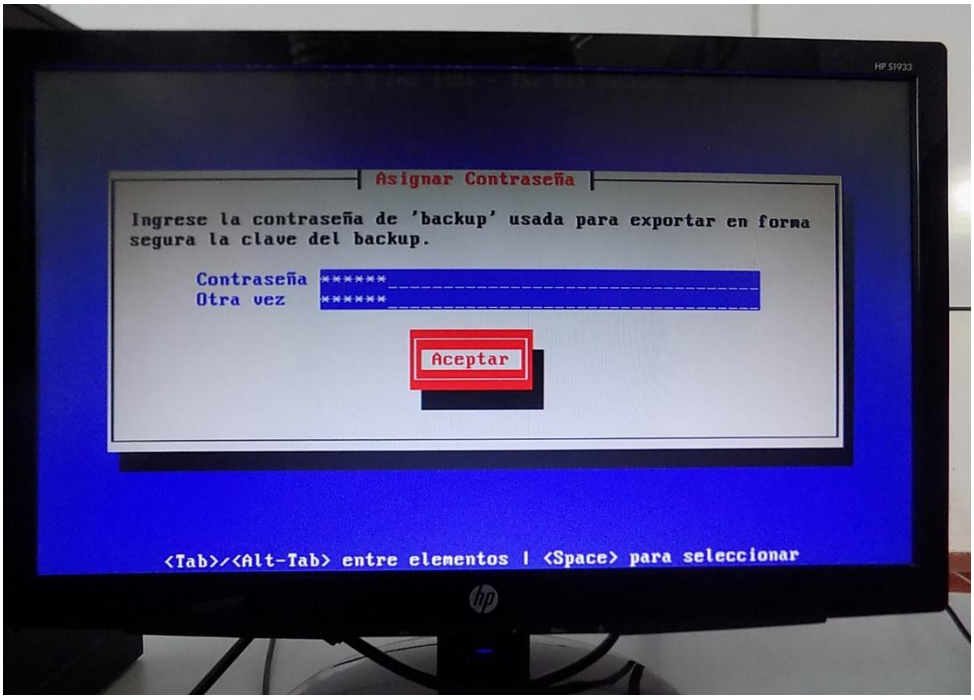


Figura 38. Ingreso de contraseña de Backup.
Fuente: Elaboración Propia. 2015.

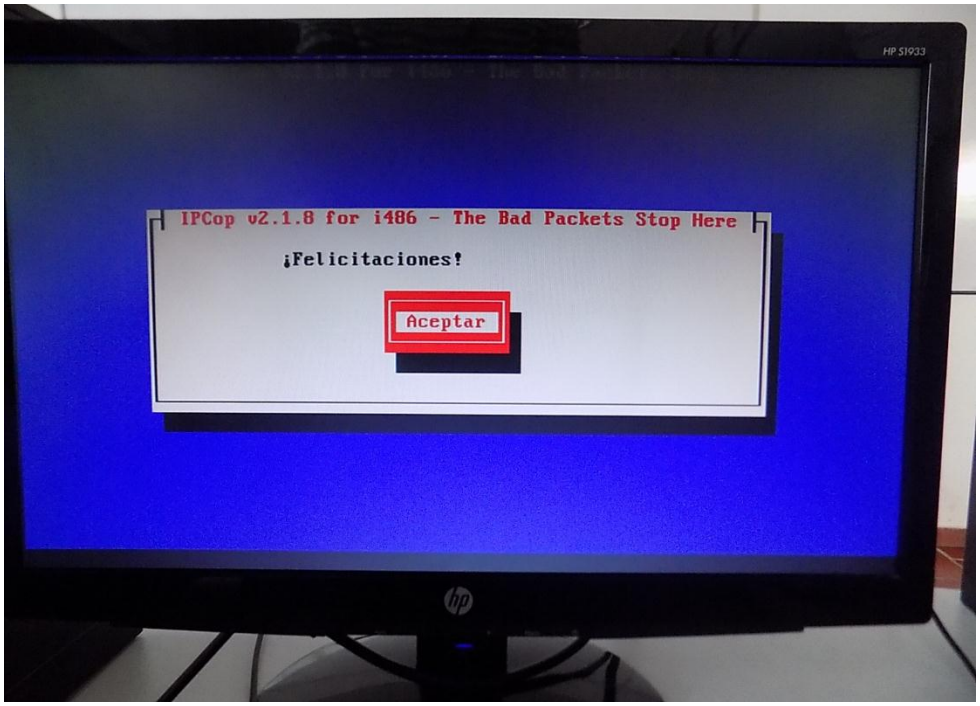


Figura 39. Finalización proceso de configuración del Firewall Ipcop.
Fuente: Elaboración Propia. 2015.

Una vez finalizado todo el equipo se reinicia y ya se puede ingresar como Usuario Root al sistema y hacer las configuraciones o modificaciones necesarias según sea el caso.

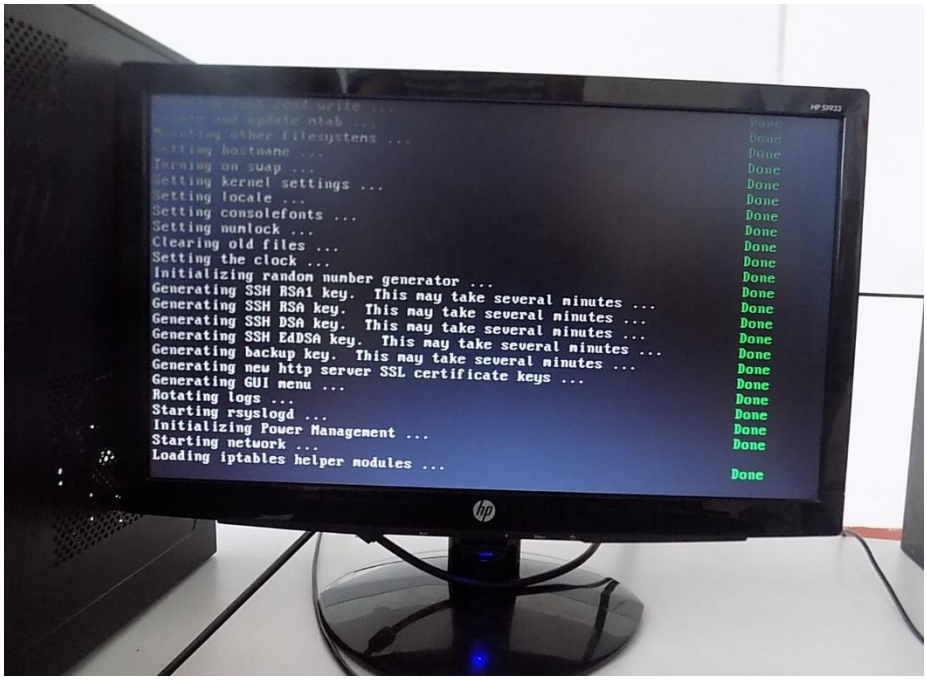


Figura 40. Pantalla de reinicio del sistema.
Fuente: Elaboración Propia. 2015.

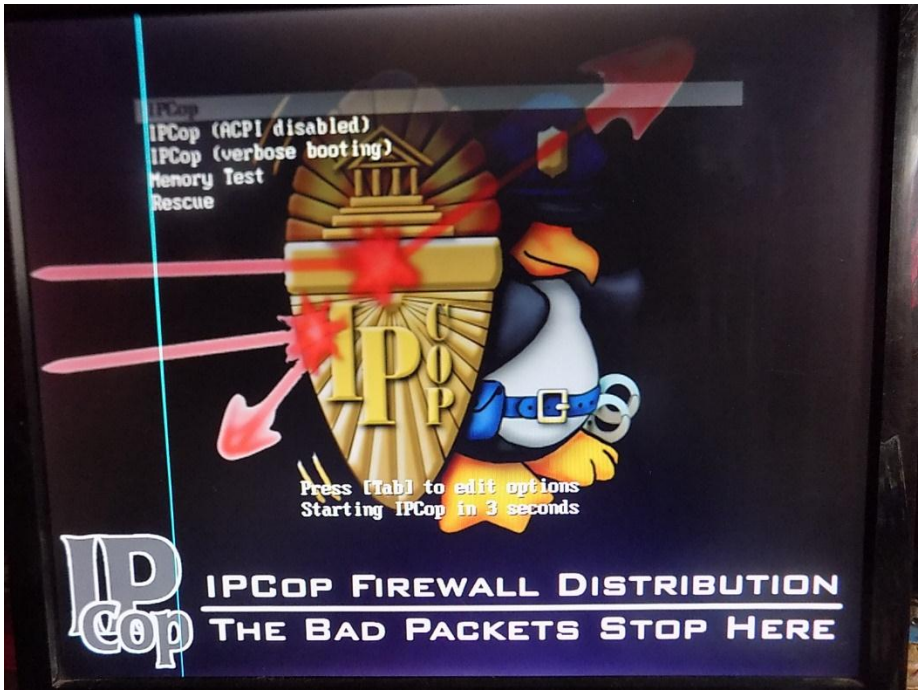


Figura 41. Pantalla de inicio de Ipcop.
Fuente: Elaboración Propia. 2015.

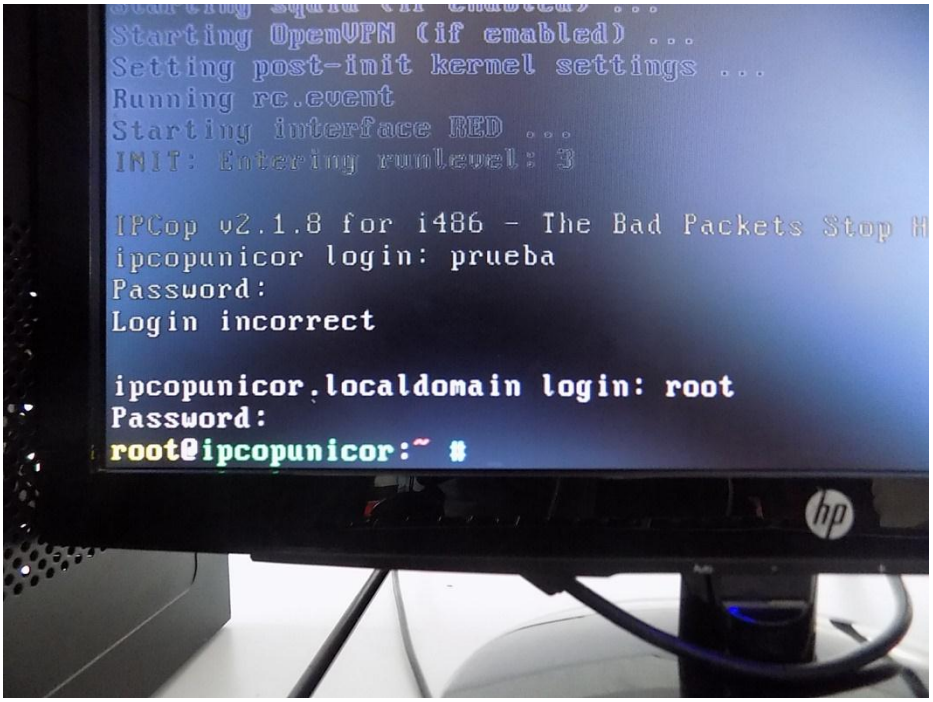


Figura 42. Ingreso al sistema mediante usuario Root
Fuente: Elaboración Propia. 2015.

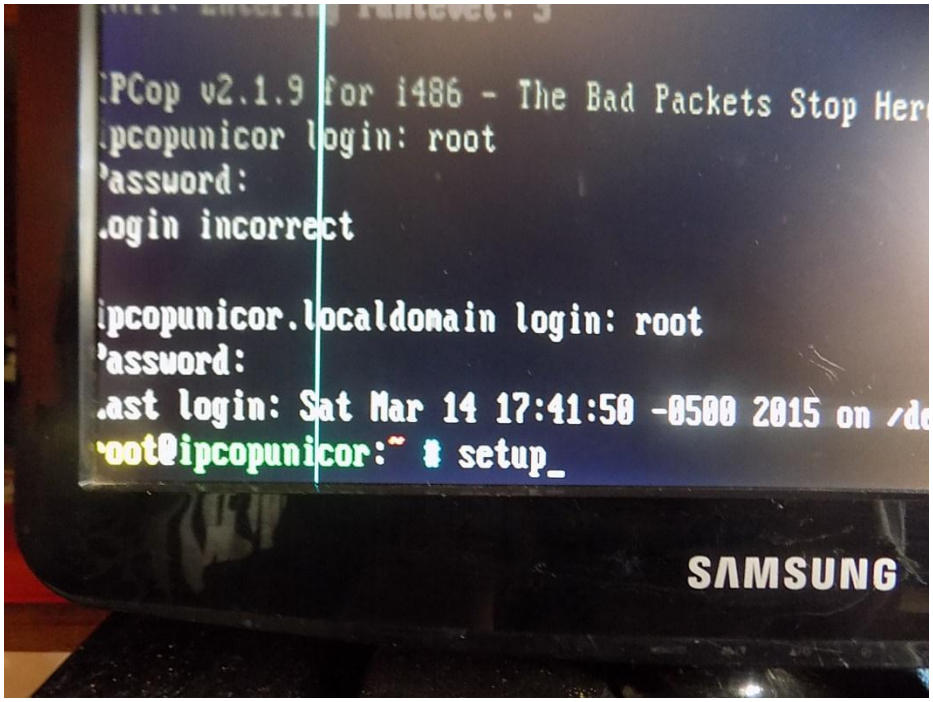


Figura 43. Ingreso a la Consola de Configuración
Fuente: Elaboración Propia. 2015.

Para acceder al menú de configuración de IpCop se escribe setup y se presiona la tecla enter. root@ipcopunicor:˜# setup

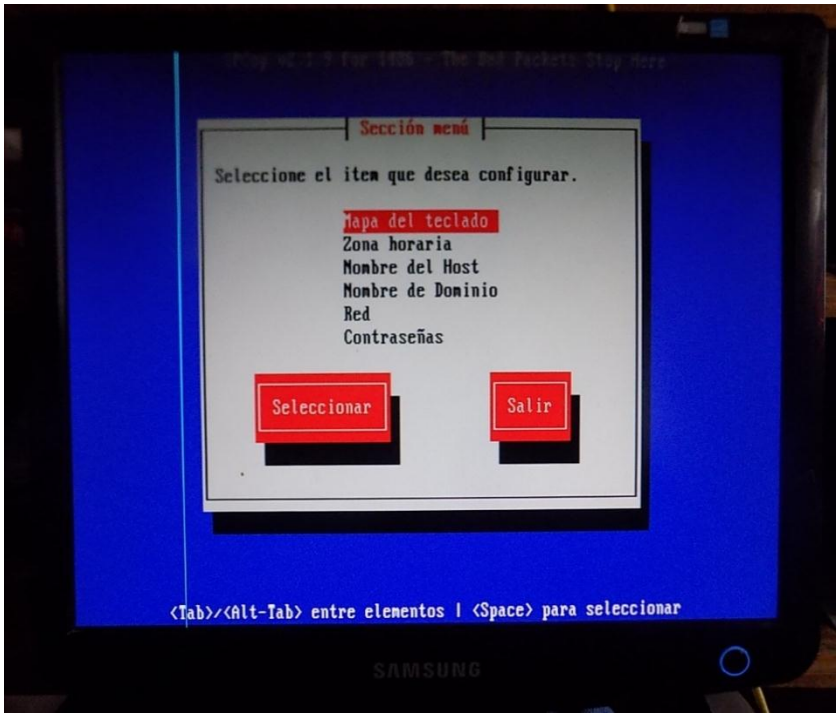


Figura 44. Menú de Configuración
Fuente: Elaboración Propia. 2015.

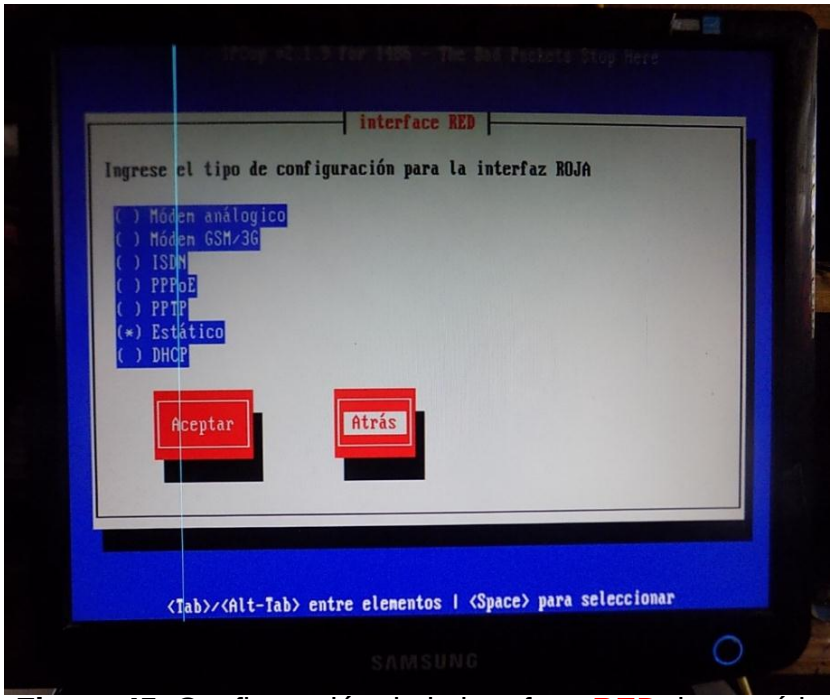
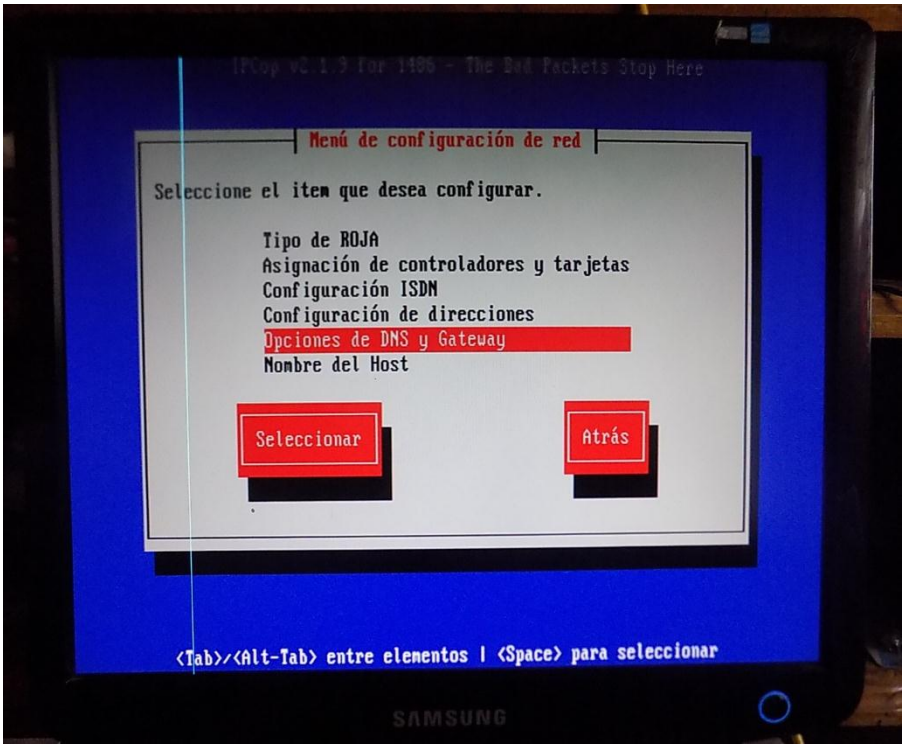


Figura 45. Configuración de la interface RED tipo estático
Fuente: Elaboración Propia. 2015.

Se selecciona el tipo de interfaz RED en este caso se selecciona de tipo estático y clic en aceptar.



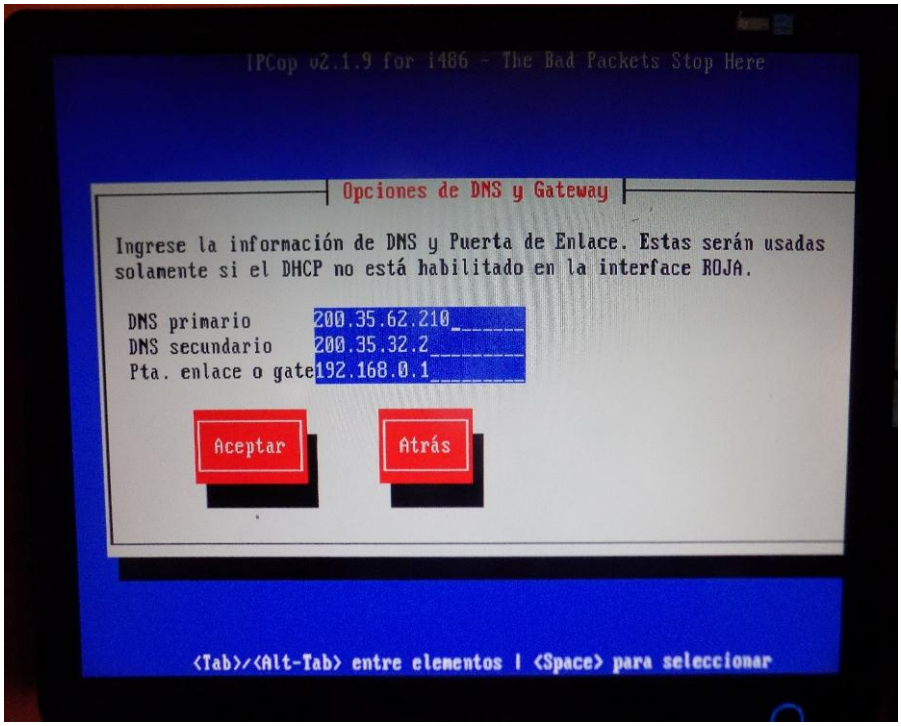


Figura 46. Configuración de DNS y Gateway
Fuente: Elaboración Propia. 2015.

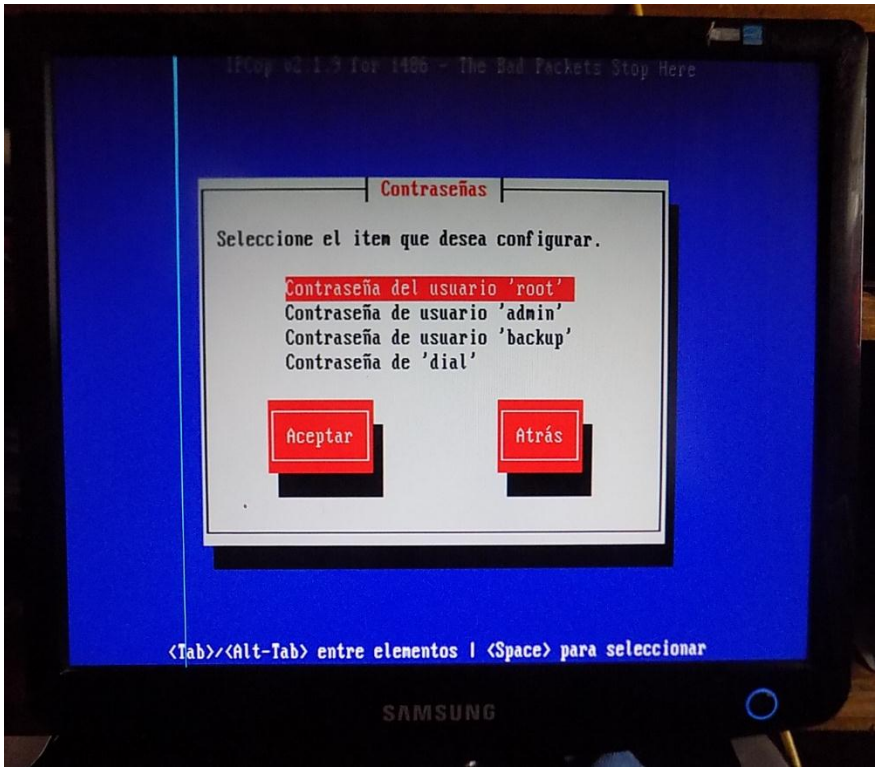


Figura 47. Configuración de las claves de los tipos usuarios.
Fuente: Elaboración Propia. 2015.

Se ingresa al Firewall por otra terminal de tipo grafico donde solicitará la identificación, por lo que se debe acceder con el usuario admin y su clave correspondiente, mediante la siguiente dirección https://192.168.1.1:8443

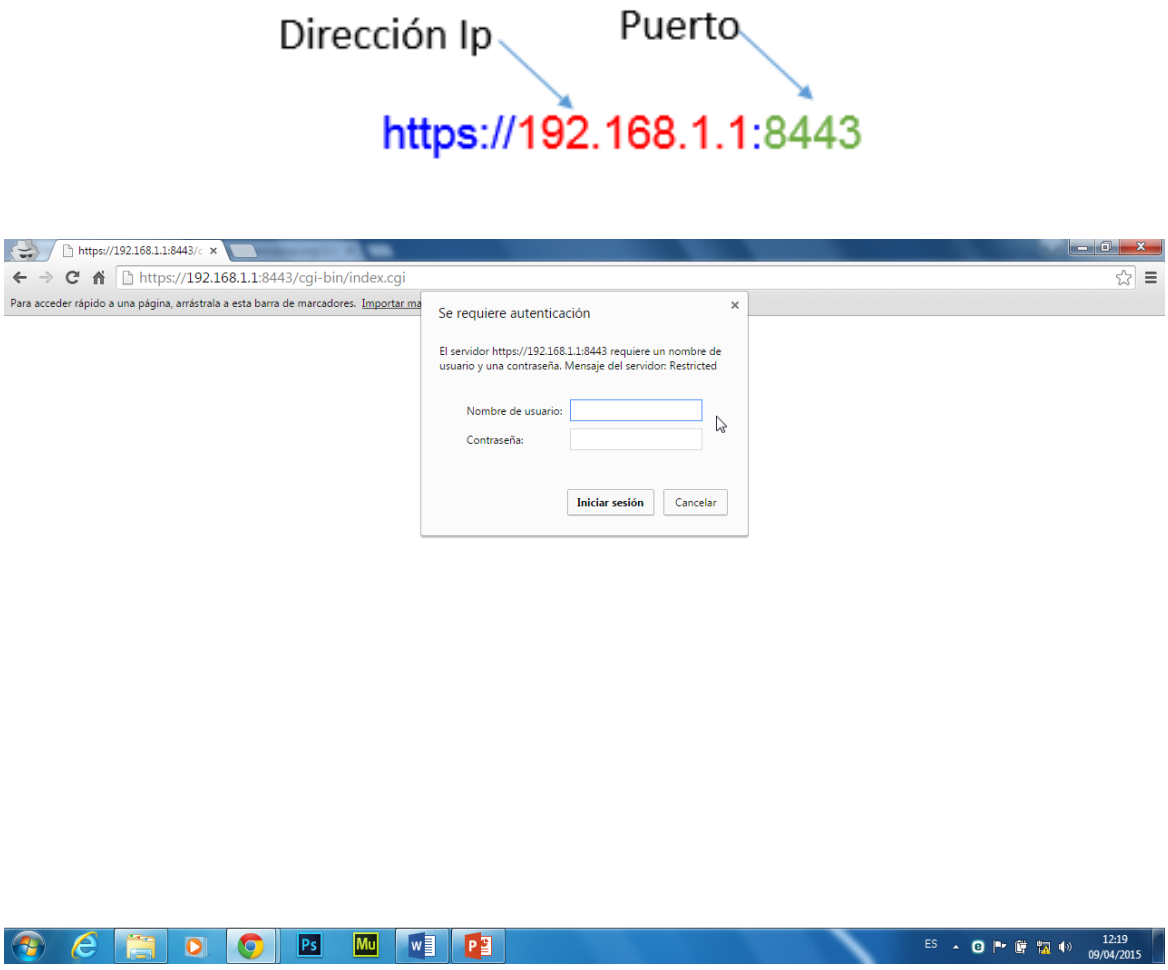


Figura 48. Ingreso a la configuración Web de IpCop.
Fuente: Elaboración Propia. 2015.

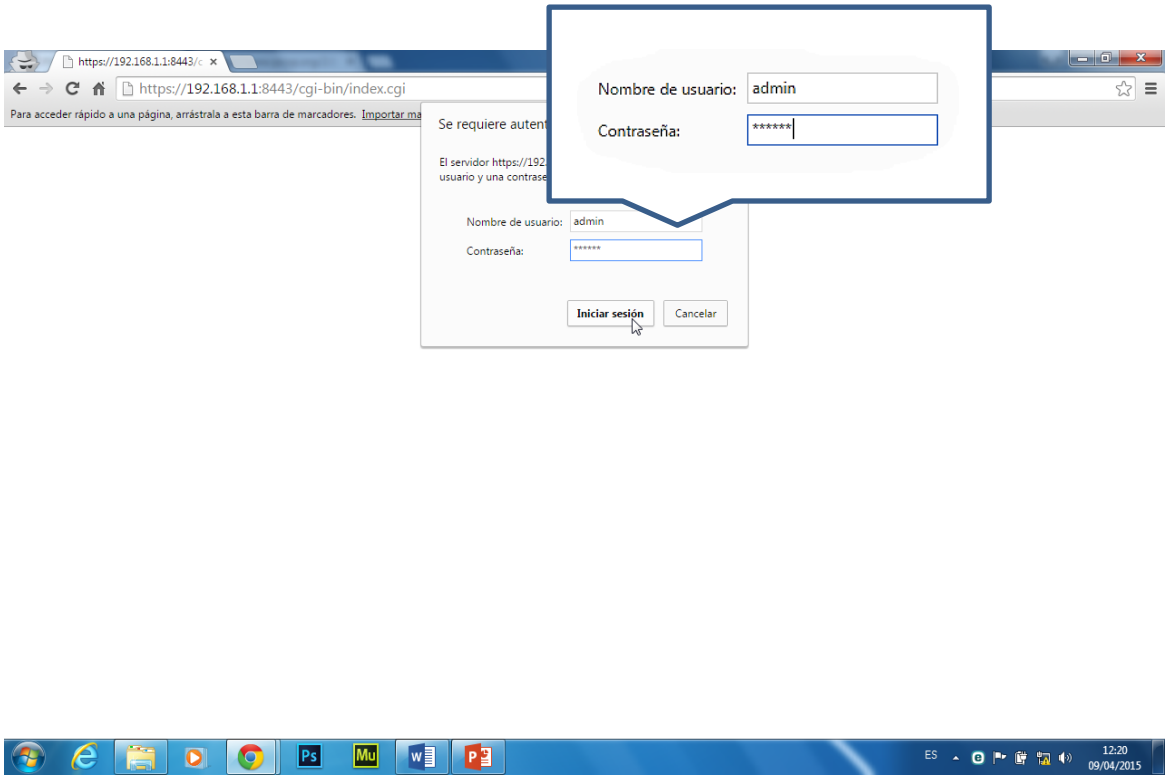


Figura 49. Ingreso de usuario y clave para logearse en el sistema
Fuente: Elaboración Propia. 2015.

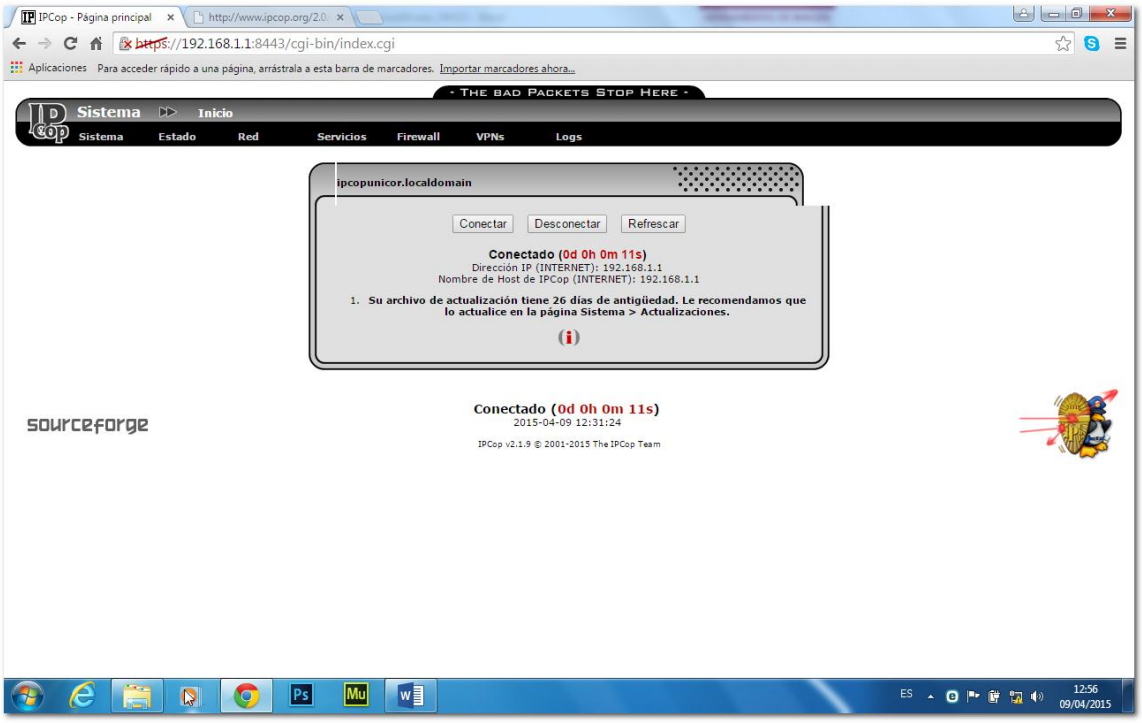


Figura 50. Página de Inicio de administración de IpCop
Fuente: Elaboración Propia. 2015.

Figura 51. Estado del sistema.
Fuente: Elaboración Propia. 2015.

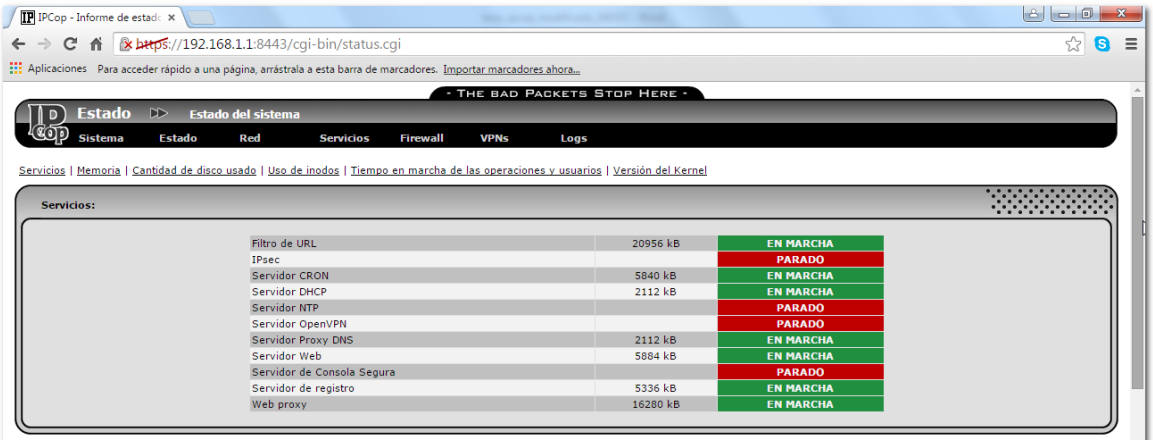


Figura 52. Servicios en marcha.
Fuente: Elaboración Propia. 2015.

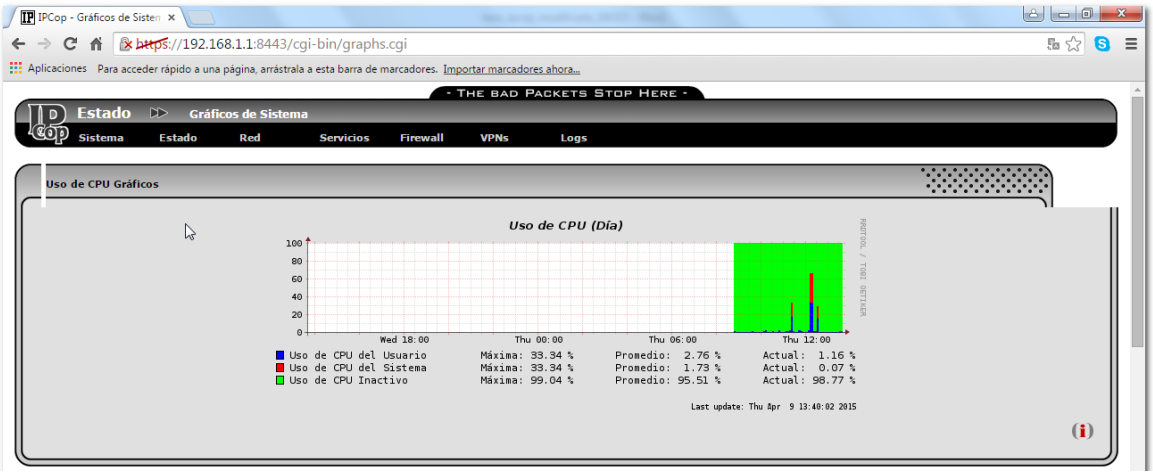


Figura 53. Grafico Uso de CPU
Fuente: Elaboración Propia. 2015.

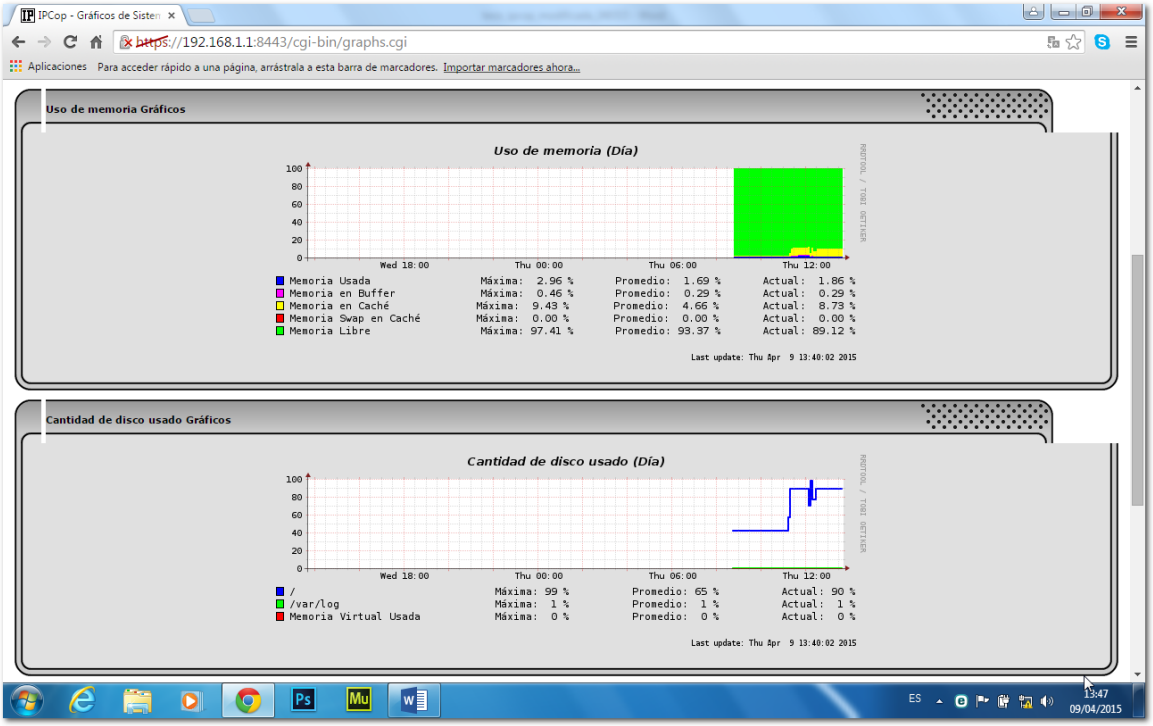


Figura 54. Grafico uso de Memoria y Disco
Fuente: Elaboración Propia. 2015.

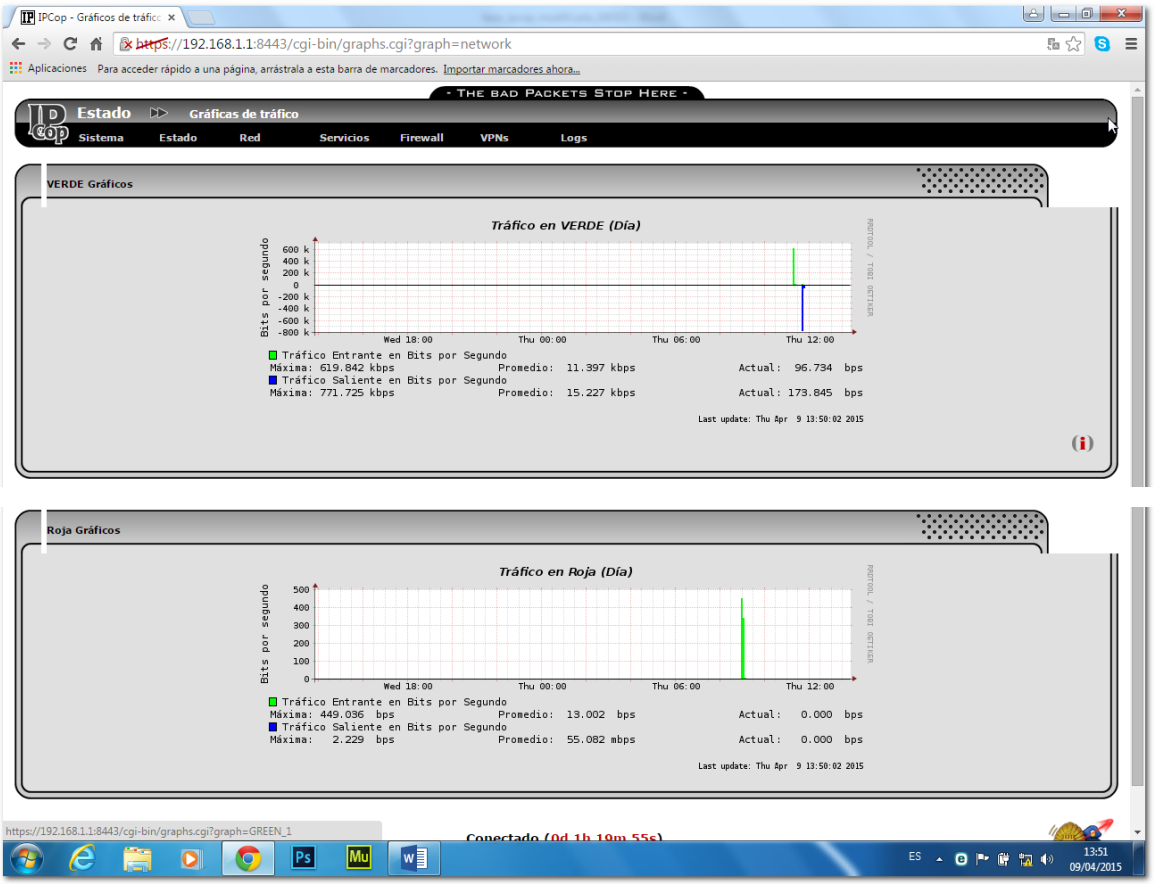


Figura 55. Grafica de tráfico en las tarjetas Green y Red.
Fuente: Elaboración Propia. 2015.

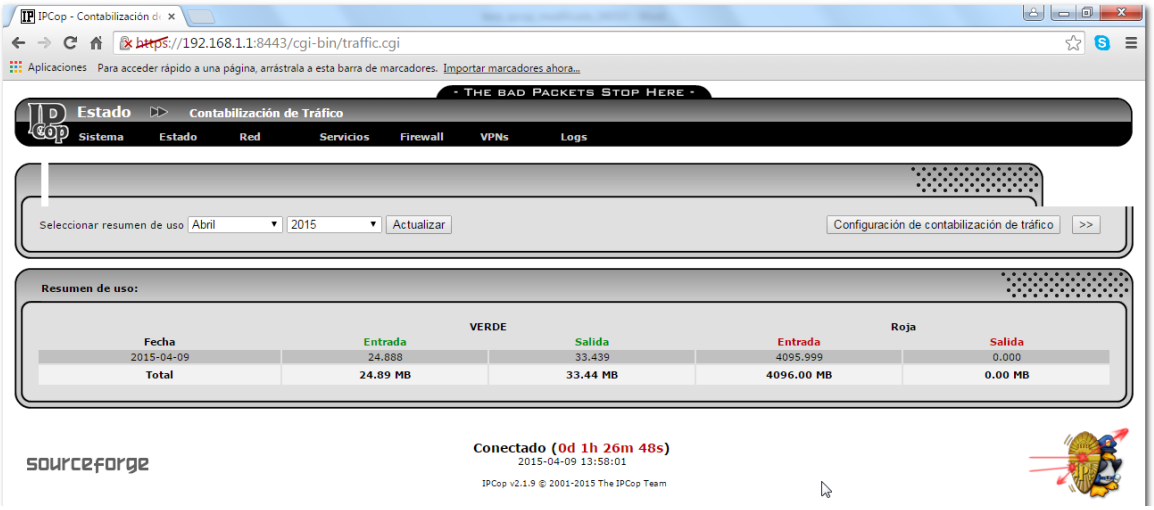


Figura 56. Contabilización del tráfico de entrada y salida en las tarjetas Green y Red
Fuente: Elaboración Propia. 2015.

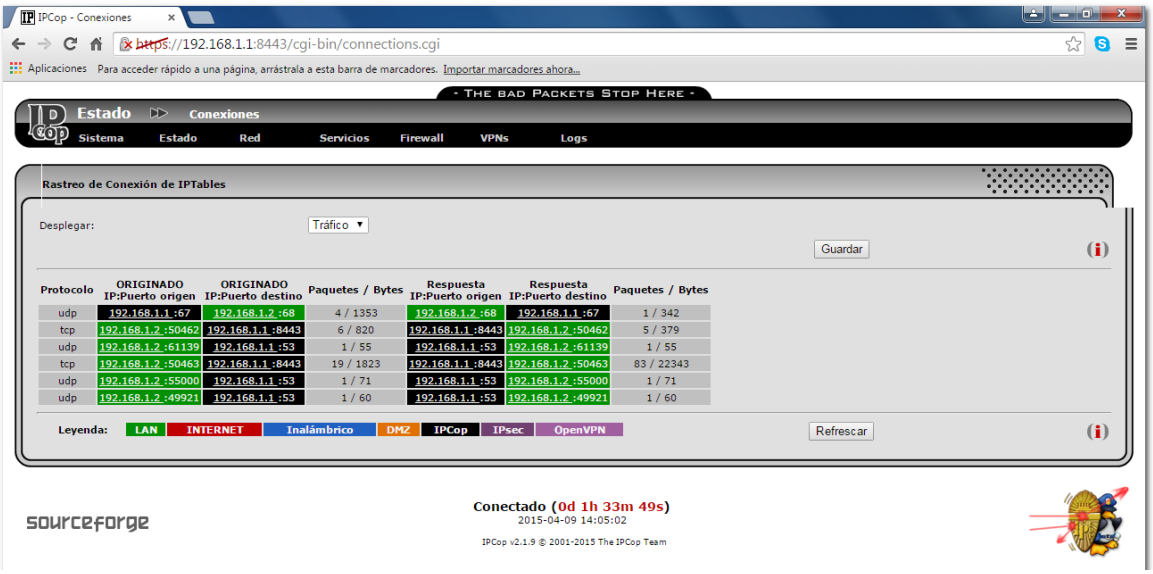


Figura 57. Rastreo de Conexión de IPTables
Fuente: Elaboración Propia. 2015.

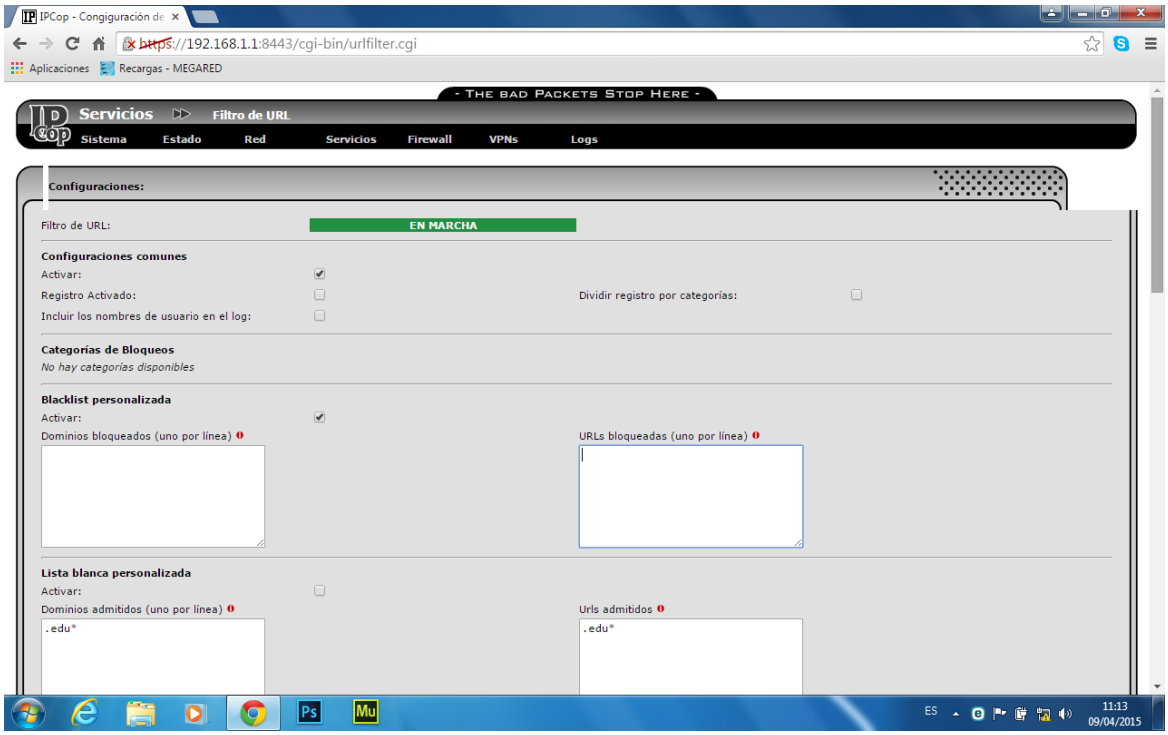
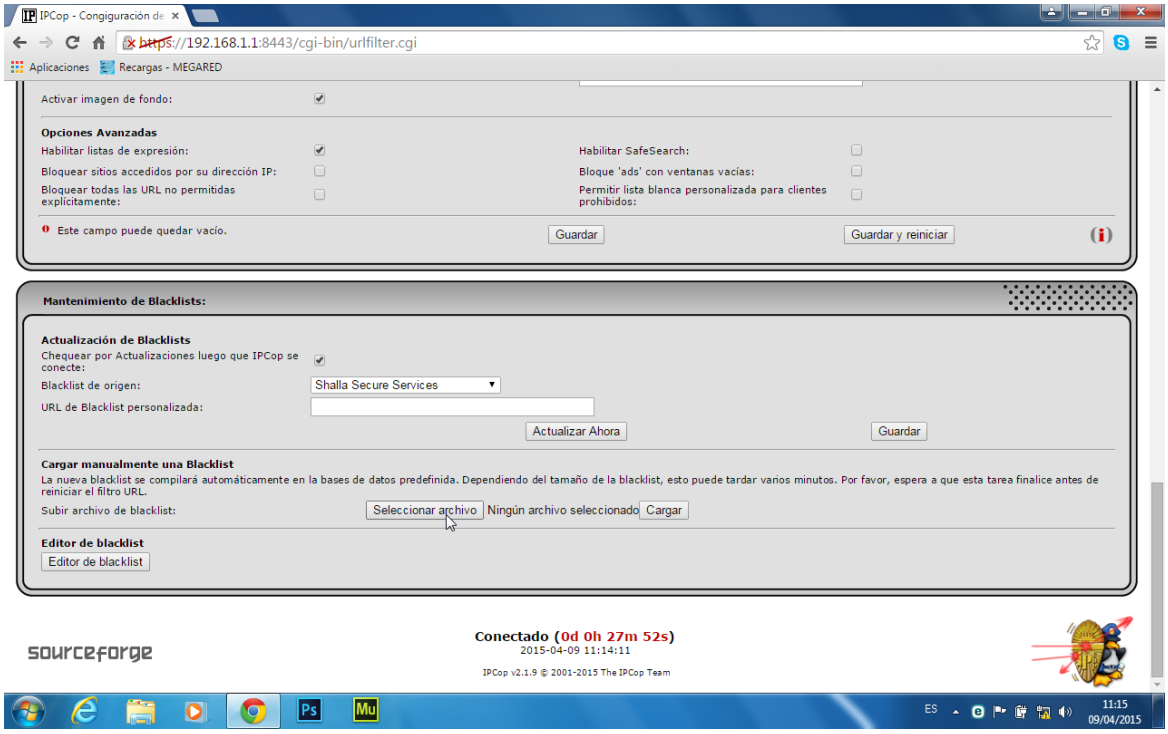
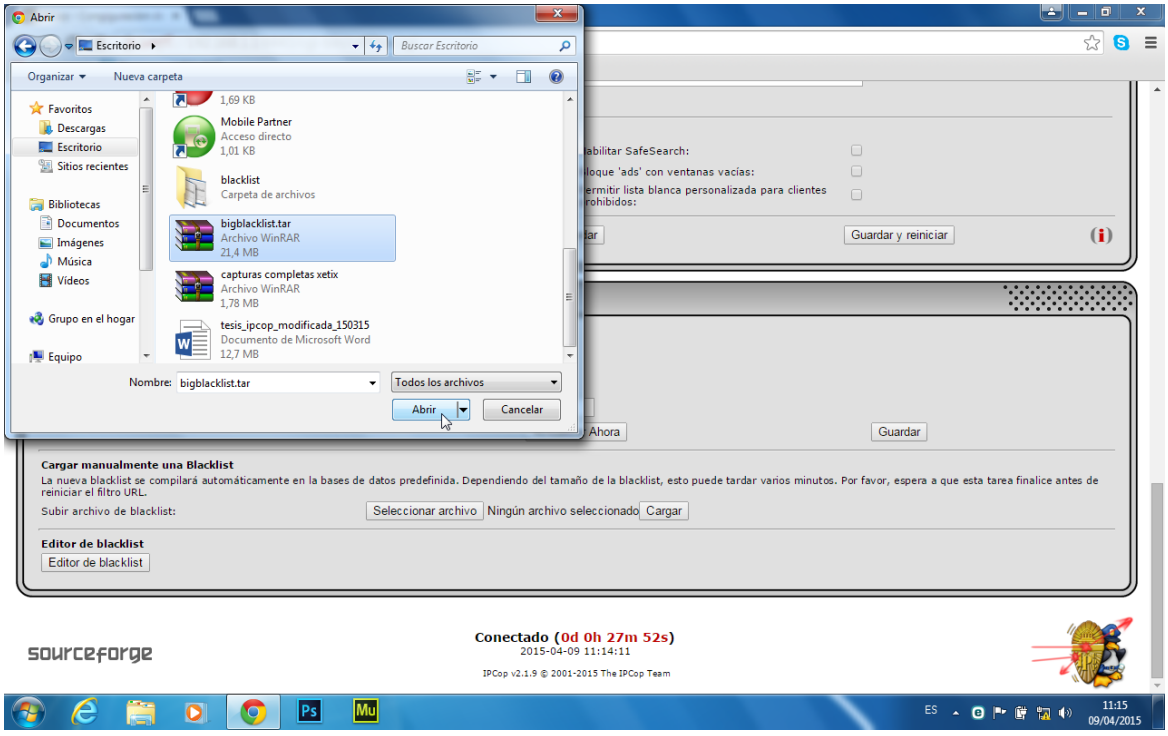


Figura 58. Filtrado de Url.
Fuente: Elaboración Propia. 2015.


IPCop - Congiguración de
https://192.168.1.1:8443/cgi-bin/urlfilter.cgi
Aplicaciones
Recargas - MEGARED
Activar imagen de fondo:
Opciones Avanzadas
Habilitar listas de expresión:
Habilitar SafeSearch:
Bloquear sitios accedidos por su dirección IP:
Bloque 'ads' con ventanas vacías:
Bloquear todas las URL no permitidas explícitamente:
Permitir lista blanca personalizada para clientes prohibidos:
Este campo puede quedar vacío.
Guardar
Guardar y reiniciar
Mantenimiento de Blacklists:
Actualización de Blacklists
Chequear por Actualizaciones luego que IPCop se conecte:
Blacklist de origen:
Shalla Secure Services
URL de Blacklist personalizada:
Actualizar Ahora
Guardar
Cargar manualmente una Blacklist
La nueva blacklist se compilará automáticamente en la bases de datos predefinida. Dependiendo del tamaño de la blacklist, esto puede tardar varios minutos. Por favor, espera a que esta tarea finalice antes de reiniciar el filtro URL.
Subir archivo de blacklist:
Seleccionar archivo
Ningún archivo seleccionado
Cargar
Editor de blacklist
Editor de blacklist
sourceforge
Conectado (0d 0h 27m 52s)
2015-04-09 11:14:11
IPCop v2.1.9 © 2001-2015 The IPCop Team
ES
11:15
09/04/2015


Abrir
Escritorio
Buscar Escritorio
Organizar
Nueva carpeta
Favoritos
Descargas
Escritorio
Sitios recientes
Bibliotecas
Documentos
Imágenes
Música
Vídeos
Grupo en el hogar
Equipo
1,69 KB
Mobile Partner
Acceso directo
1,01 KB
blacklist
Carpeta de archivos
bigblacklist.tar
Archivo WinRAR
21,4 MB
capturas completas xetix
Archivo WinRAR
1,78 MB
tesis_ipcop_modificada_150315
Documento de Microsoft Word
12,7 MB
Nombre:
bigblacklist.tar
Todos los archivos
Abrir
Cancelar
Guardar y reiniciar
Guardar
Cargar manualmente una Blacklist
Subir archivo de blacklist:
Seleccionar archivo
Ningún archivo seleccionado
Cargar
Editor de blacklist
Editor de blacklist
sourceforge
Conectado (0d 0h 27m 52s)
2015-04-09 11:14:11
IPCop v2.1.9 © 2001-2015 The IPCop Team
ES
11:15
09/04/2015

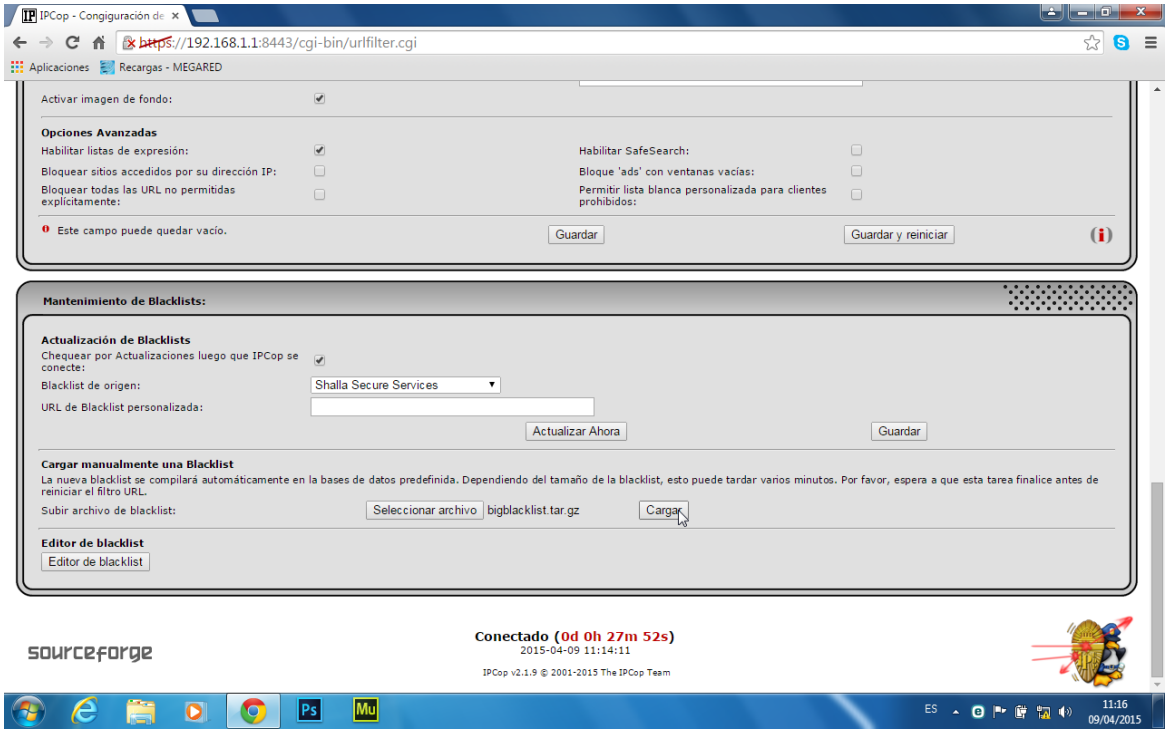


Figura 59. Carga archivo.tar.gz de Blacklist al sistema.
Fuente: Elaboración Propia. 2015.

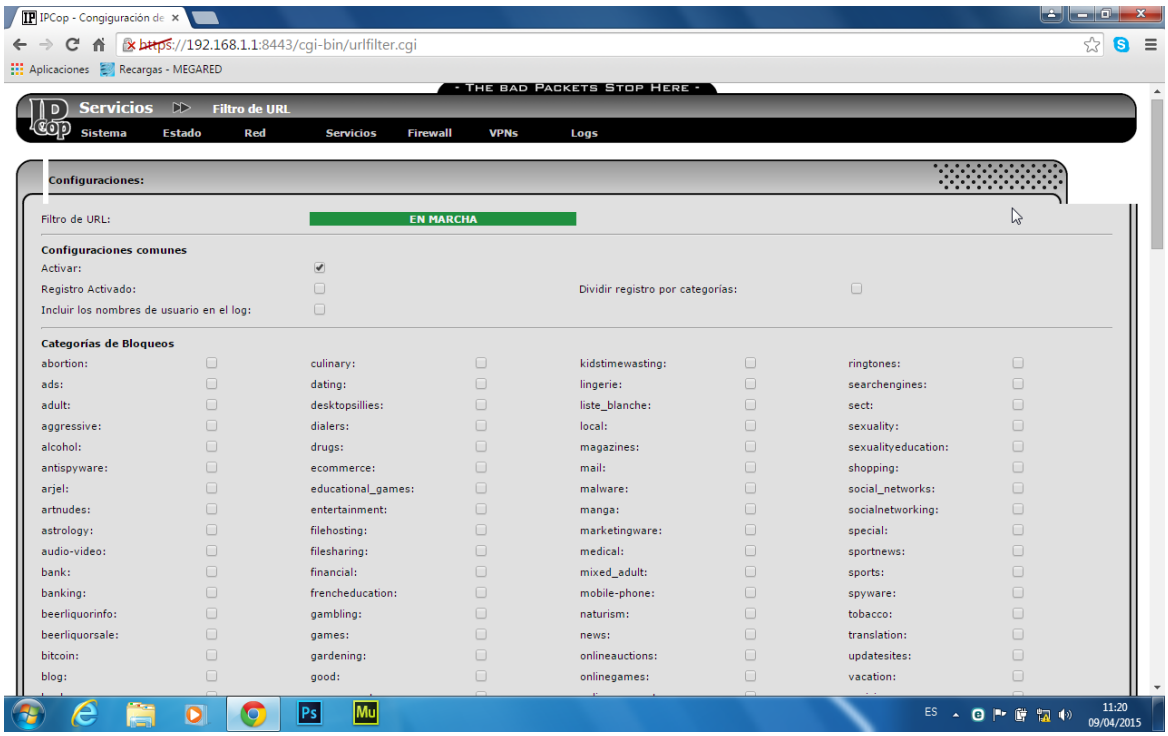


Figura 60. Categorías de Bloqueos de la Blacklist una vez cargada en el sistema.
Fuente: Elaboración Propia. 2015.

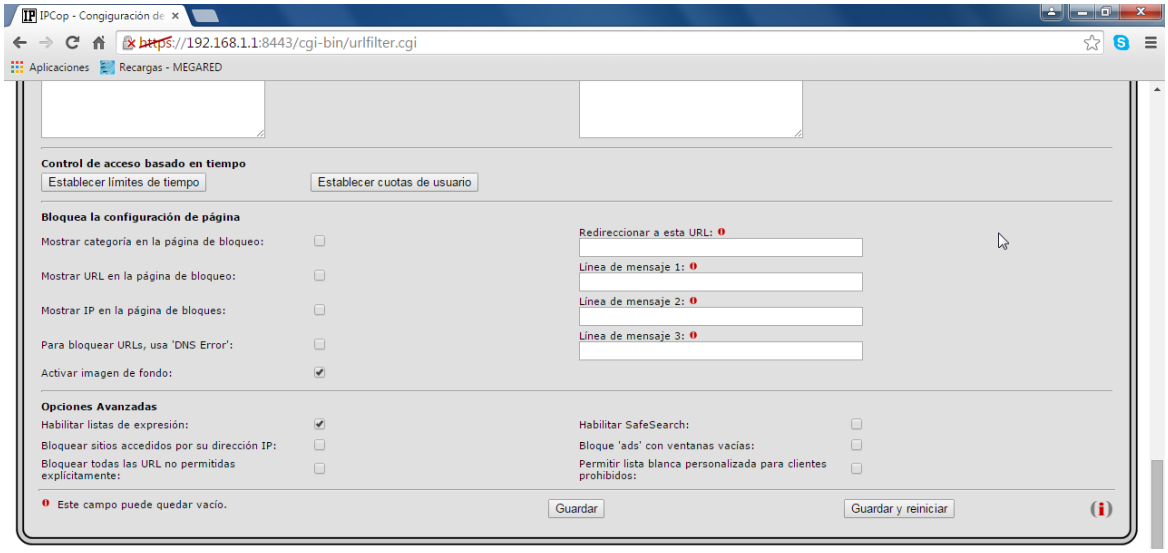


Figura 61. Bloqueo configuración de página.
Fuente: Elaboración Propia. 2015.

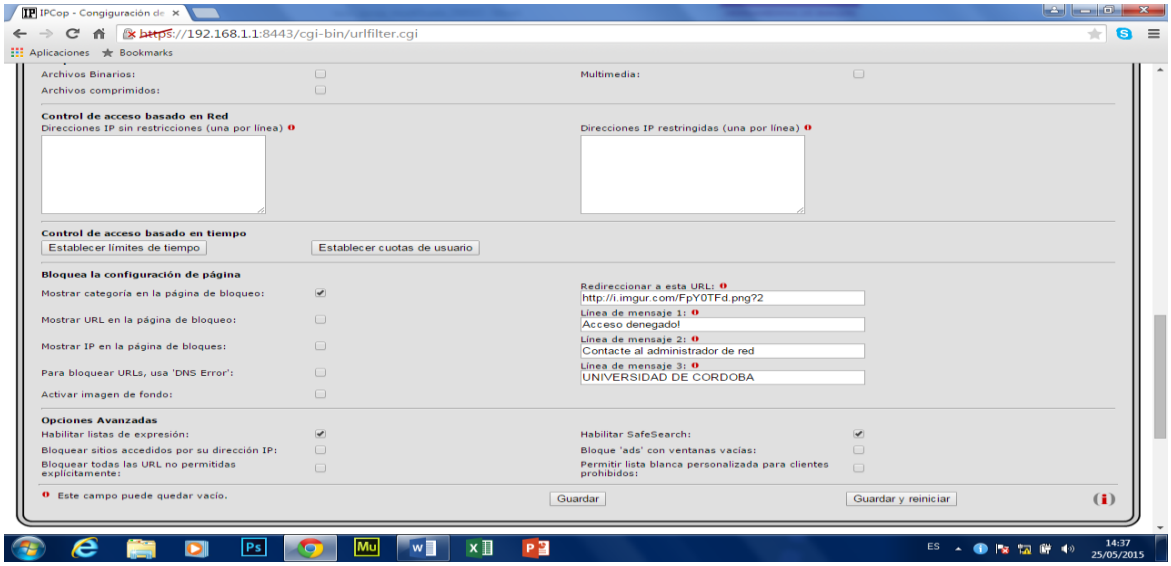


Figura 62. Mensaje de Bloqueo mediante Imagen Url.
Fuente: Elaboración Propia. 2015.

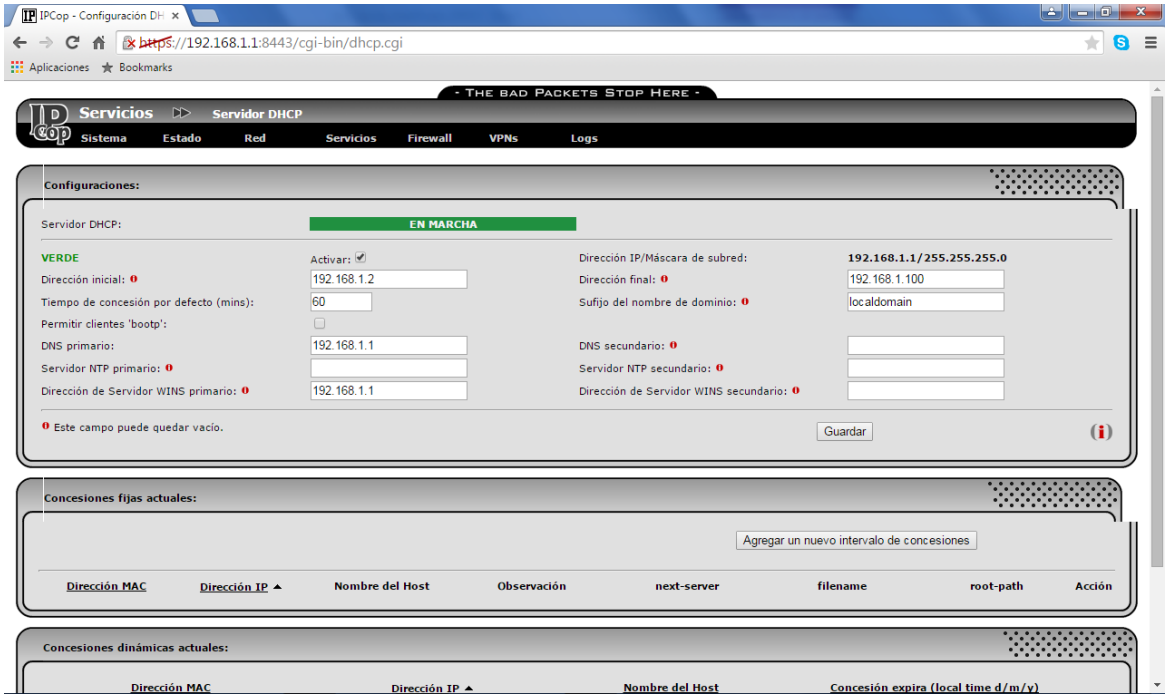


Figura 63. Configuración y puesta en marchar del servidor DHCP.
Fuente: Elaboración Propia. 2015.

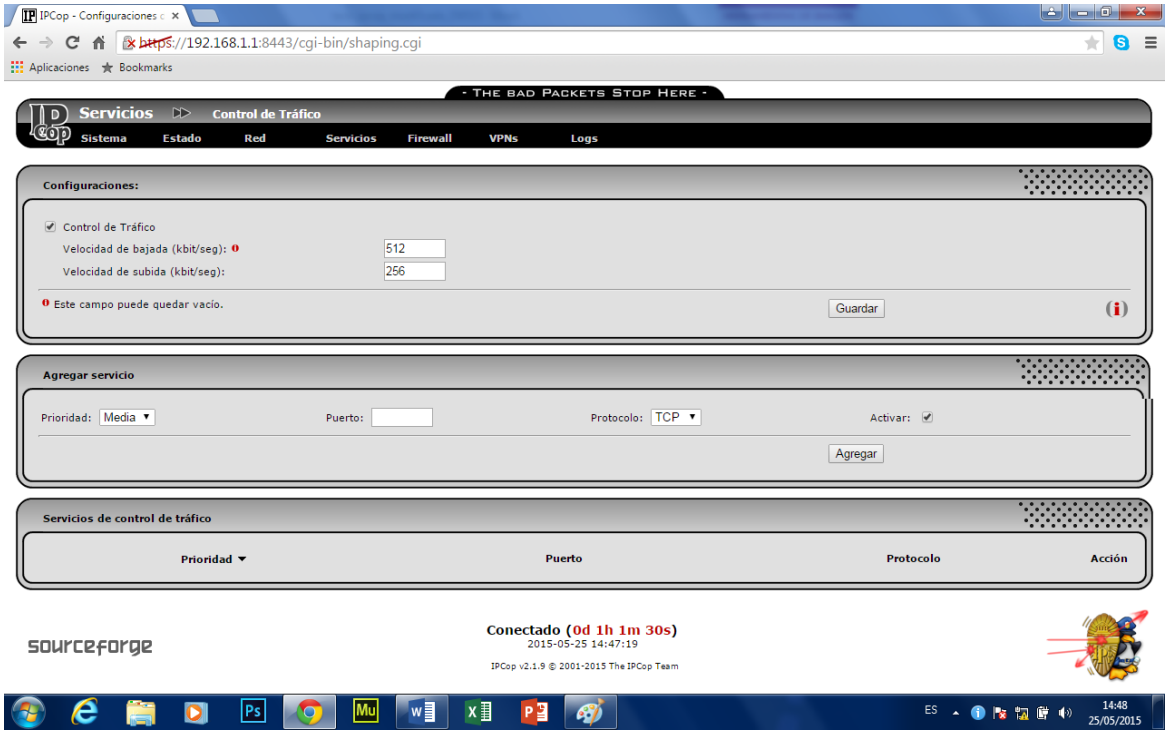


Figura 64. Control del tráfico.
Fuente: Elaboración Propia. 2015.

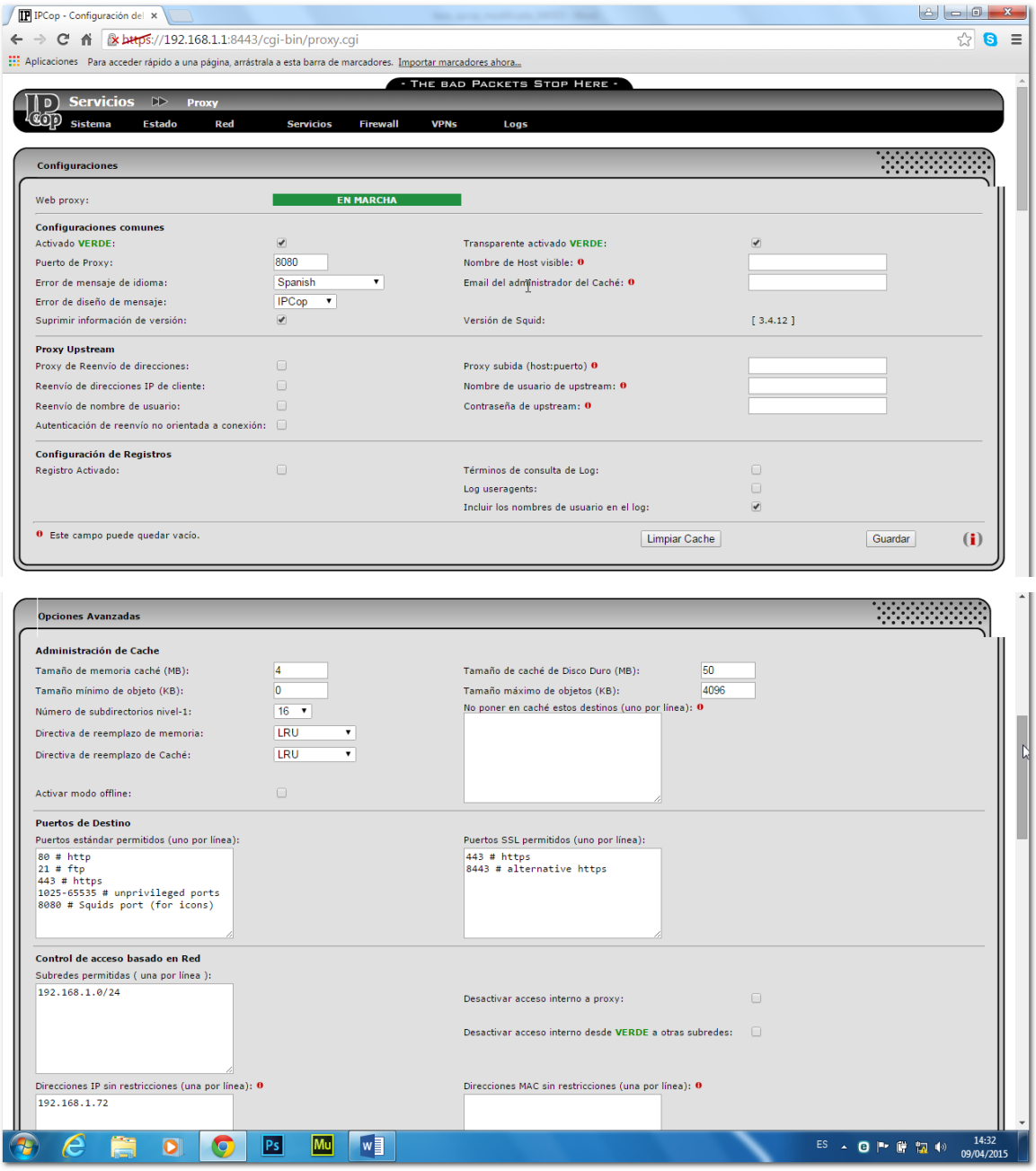


Figura 65. Configuración de Web Proxy.
Fuente: Elaboración Propia. 2015.

PRUEBAS

Realizamos el ingreso a distintas paginas para verificar que las políticas de seguridad establecidas en las restricciones de url que no son de tipo educativo.

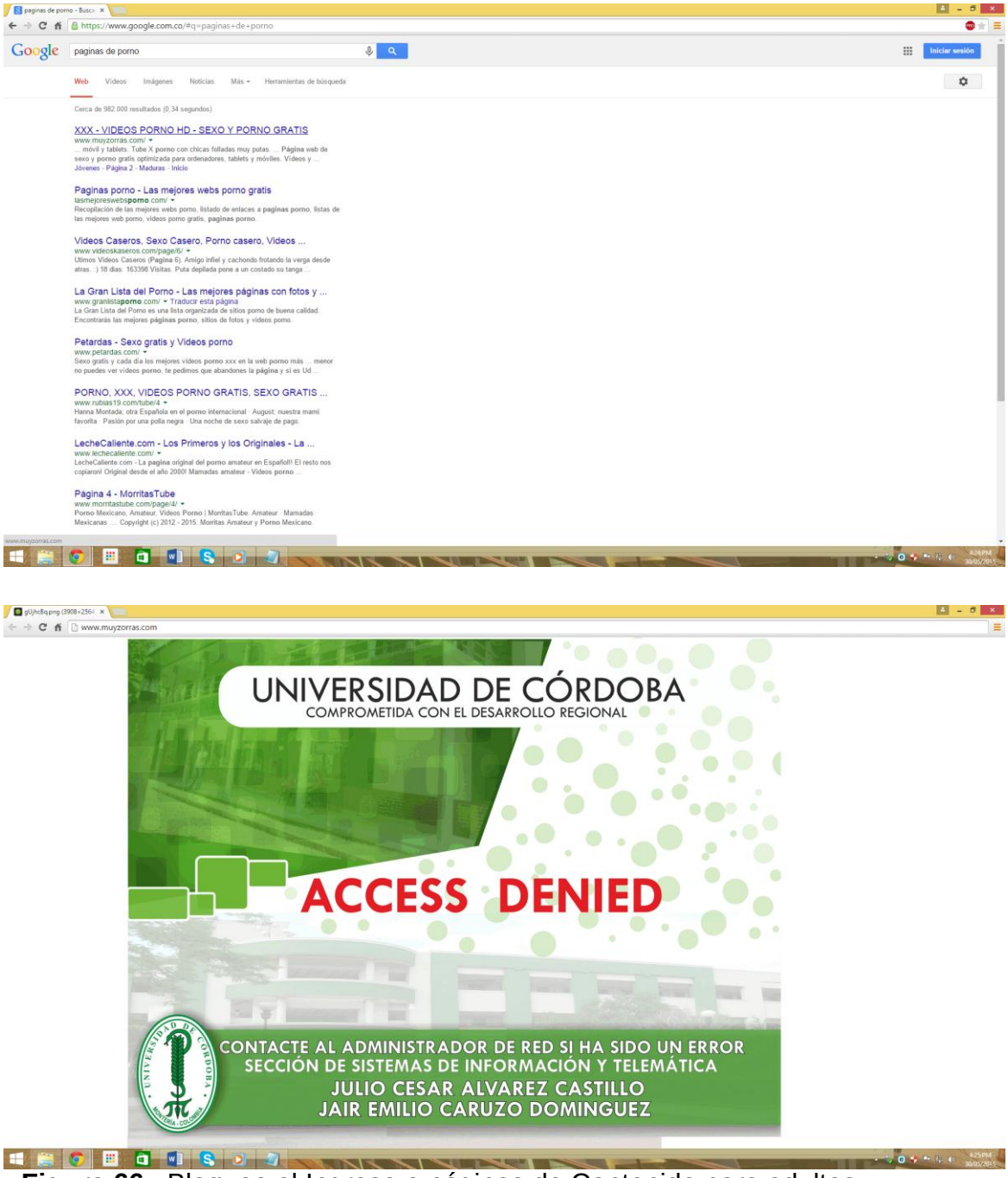


Figura 66. Bloqueo al Ingreso a páginas de Contenido para adultos.
Fuente: Elaboración Propia. 2015.

Figura 67. Bloqueo al Ingreso a redes sociales.
Fuente: Elaboración Propia. 2015.

Figura 68. Bloqueo al Ingreso a emisoras y tv online.
Fuente: Elaboración Propia. 2015.

Figura 69. Bloqueo al Ingreso a páginas de juegos online.
Fuente: Elaboración Propia. 2015.

Figura 70. Bloqueo al Ingreso a páginas de navegación anónima.
Fuente: Elaboración Propia. 2015.

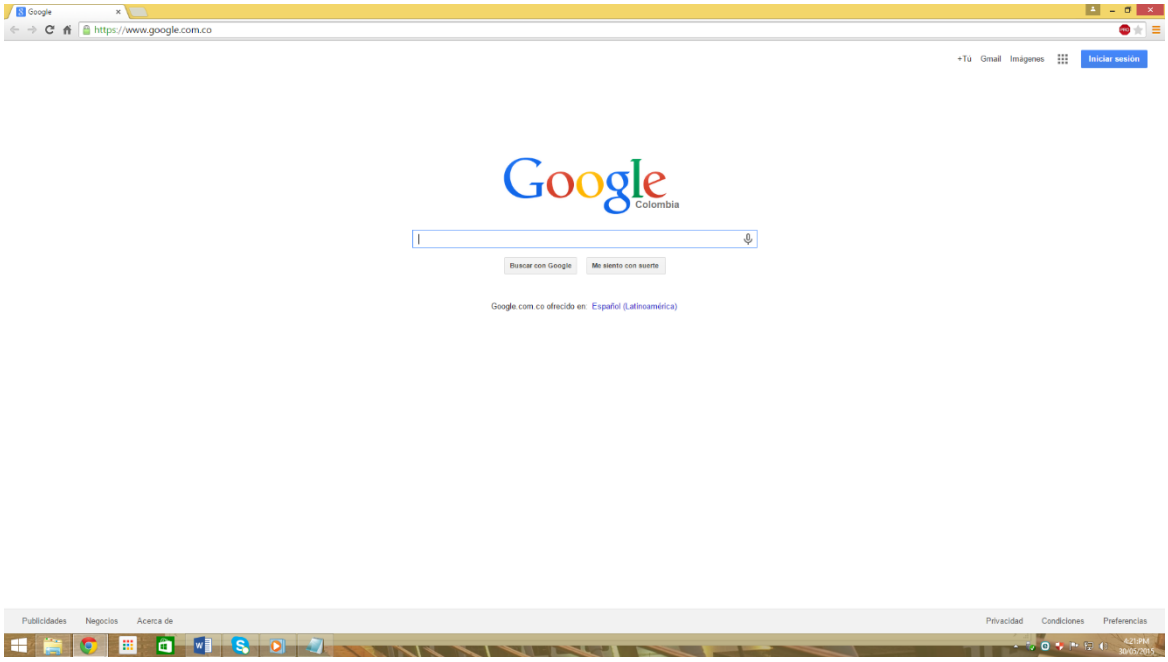


Figura 71. Navegación en páginas de consulta autorizadas
Fuente: Elaboración Propia. 2015.

Figura 72. Navegación en la página institucional
Fuente: Elaboración Propia. 2015.