UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Administración de proxy en Linux

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

David Martínez Quiroz

ASESOR DE INFORME

Ing. Carlos Alberto Román Zamitiz

Ciudad Universitaria, Cd. Mx., Ingresa 2016

Agradecimiento

Antes de comenzar quiero agradecer a mi familia y profesores por su valioso apoyo para concluir esta gran meta que no ha sido nada fácil, sin embargo ha sido muy motivadora tanto física como emocionalmente.

Mis padres que me han acompañado, apoyado y educado desde el comienzo de mi vida, gracias por el apoyo incondicional, los momentos buenos y malos que han tenido que superar para apoyarme en cada momento, y sobre todo su cariño incondicional que me brindan día a día.

A mi hermano que no solo ha sido mi amigo desde que tengo memoria, sino que además ha sido un compañero con el cual he aprendido y descubierto que los caminos que nos ofrece la vida no siempre son los más fáciles, sin embargo hay que disfrutar cada momento, ya que son únicos e irrepetibles.

A mi gran profesor el Ing. Carlos Alberto Román, Asesor de Trabajo Profesional, que sin su gran ayuda no hubiese sido posible culminar esta gran meta, y quien además, me apoyó en cada momento.

Gracias a todas aquellas personas que estuvieron compartiendo momentos especiales en mi vida, gracias a aquellos profesores que de verdad decidieron dar su mejor esfuerzo para transmitir sus conocimientos que han sido muy útiles, tanto laboral como personalmente.

Y por último, pero no menos importante gracias a la Empresa Mexicana del Petróleo y al Jefe de Sistemas el Ing. Benjamín Ortiz Durán, por dejarme laborar en sus instalaciones y me permitió poner mis conocimientos adquiridos a lo largo de la carrera en práctica, gracias a los trabajadores por enseñarme nuevas cosas las cuales podré que desarrollar a lo largo de mi vida profesional.

Facultad de Ingeniería

Nombre de la empresa: Empresa Mexicana del Petróleo

Índice

Introducción……1

Capítulo 1 Descripción de la empresa

Empresa Mexicana del Petróleo……..……3

Misión……...4

Visión……4

Propósito…….....4

Historia…….....5

Organigrama……9

Capítulo 2 Marco teórico

Seguridad Informática……10

Políticas de seguridad……..…12

Redes de Datos……..……..13

Red VPN……16

Sistema Operativo Linux……..17

Criptografía……17

Herramienta PuTTY……..20

Barracuda WebFilter……22

Capítulo 3 Descripción de puesto

Área de seguridad informática…….....24

Emplear la herramienta PuTTY……..…….……25

Monitoreo mediante Barracuda Web Filter…..……26

Implementación de redes VPN...……..27

Juntas dirigidas al tema de seguridad informática……28

Capítulo 4 Descripción de la participación del alumno en la empresa

Monitoreo de proxy mediante comandos de Linux….....29

Configuración de redes VPN…….……35

Administración de proxy de la Institución……...35

Aplicación de Barracuda Web Filter……..……36

Conclusiones…….....41

Bibliografía…….....42

Introducción

En este proyecto se explicará todo lo aprendido en la Institución, así como los conocimientos que fueron aplicados en el desarrollo de mi trabajo en la Empresa Mexicana del Petróleo.

Se dará a conocer las actividades diarias que se realizan en el Instituto, para demostrar la utilidad de la carrera de Ingeniería en Computación en el Área de Investigación Petrolera, que es la Institución de Investigación Petrolera más grande de la República Mexicana y que no sólo se localiza en la Ciudad de México sino que además tiene sedes en diversos sitios que conforman los Estados Unidos Mexicanos.

En el primer capítulo se hará referencia a los primeros años de la Empresa Mexicana del Petróleo, cómo surgió la idea de la construcción de esta gran Institución, los años en los cuales se comenzaron hacer sus primeros proyectos, básicamente su historia, misión y visión, las dificultades a las cuales se ha enfrentado a lo largo de su existencia y el por qué es tan importante para el país, se mostrará el organigrama de cómo está constituida la organización desde el Director General, hasta los empleados. Ya que cada uno es importante para el correcto funcionamiento de esta Empresa.

En el segundo capítulo se explicarán los conceptos básicos que se tienen que tener en cuenta para poder entender las situaciones con las que se trabajan en el Área de Tecnología de la Información que es parte esencial en la Institución. Se abarcarán temas desde seguridad informática, redes de computadoras, criptografía, sistemas operativos y los subtemas propios de cada uno de estos, además de ejemplos del porque es importante saber conceptos esenciales que se manejan y situaciones que pueden poner en riesgo la situación de la Empresa.

En el capítulo tres se mencionará una breve descripción de las actividades que deben realizar el personal que labora en el área de tecnologías de la información, específicamente en el área de seguridad informática, estas actividades abarcan

desde la revisión de temperatura y humedad de los Sites (ubicación de servidores) hasta el monitoreo, revisión de políticas de seguridad entre otras tareas.

Para finalizar en el capítulo cuatro describiré cada una de las actividades que realicé en la Institución, así como las herramientas utilizadas para la realización de mis actividades, mencionaré los problemas que llegan a surgir además de las medidas de seguridad que se aplican, por otro lado se notarán las medidas que se toman para de advertir a un usuario las búsquedas que se realizan y como se logra identificar a cada usuario que comete ciertas faltas que no se pueden pasar por alto.

Por motivos de seguridad de la institución, no se publicarán contraseñas de ningún tipo ni direcciones IP además de que los nombres de usuarios no serán visibles, sólo se publicarán imágenes de los resultados obtenidos en cuanto a la parte de monitoreo de Logs, para proteger la identidad de todos los trabajadores.

1 Descripción de la empresa

Empresa Mexicana del petróleo

La Empresa Mexicana del Petróleo es el Centro de Investigación de México dedicado al área petrolera. Por su calidad de centro de investigación, se mantiene a la vanguardia en el uso de nuevas tecnologías de información para soportar sus actividades sustantivas. Por esta razón, buena parte de su información se hospeda

en equipos de cómputo, dispositivo de almacenamiento y se mueve a través de redes de datos, en lo que se conoce como sistemas de información.

Estos sistemas de información están sujetos a riesgos y amenazas generadas, tanto en la misma empresa como fuera de ella, al interactuar e intercambiar información con otras Instituciones del Sector Energético, Universidades, socios, etc. Esta Empresa ha implementado desde tiempo atrás, controles para proteger su infraestructura informática y en general sus activos de información. El implantar su Sistema de Gestión de Seguridad de la Información (SGSI) permitirá una mejor gestión de los riesgos de seguridad a los cuales están expuestos sus activos. En dicha Institución apliqué los conocimientos adquiridos en la carrera de Ingeniería en Computación, con el módulo de redes y seguridad, ahí brindé apoyo en el área de tecnologías de la información, en el Departamento de Seguridad Informática.
En la Empresa Mexicana del Petróleo estuve realizando configuración del servicio Proxy a través de la consola Linux, con la finalidad de evitar ataques de negación de servicios, además de realizar monitoreo de los equipos pertenecientes a la Institución con la herramienta PuTTY que es utilizada mediante comandos de Linux.

Misión

Maximizar la generación de valor de los procesos de exploración, producción y transformación de hidrocarburos, mediante la aplicación de soluciones innovadoras y el desarrollo de capital humano especializado.

Visión

Somos la Institución Nacional productiva de excelencia que provee soluciones valiosas al sector de hidrocarburos, a través de investigación y desarrollo, servicios tecnológicos, formación de recursos humanos e innovación.

Propósito

Impulsar el desarrollo tecnológico del sector nacional de hidrocarburos público y privado.

La Empresa Mexicana del Petróleo, es el centro de investigación de México dedicado al área petrolera, cuyos objetivos principales son la investigación y desarrollo tecnológico, la ingeniería y servicios técnicos y la capacitación, así como el otorgamiento de grados académicos, la comercialización de los resultados de la investigación y desarrollo tecnológico y la suscripción de alianzas estratégicas y tecnológicas.

Como Centro Público de Investigación, la Empresa Mexicana del Petróleo tiene la Misión de transformar el conocimiento en tecnología y servicios de valor para la industria petrolera; y la Visión de ser un centro público de investigación de clase mundial con personal reconocido, con tecnologías y servicios que contribuyen al desarrollo de la industria petrolera.

Actualmente mediante un renovado esfuerzo, una mayor sinergia con Pemex y la apertura del mercado petrolero, la empresa busca integrarse a los objetivos y grandes proyectos de la industria petrolera al ofrecer investigación y desarrollo tecnológico, escalamiento, capacitación y comercialización de servicios de alto contenido tecnológico, que permitan aumentar la eficiencia, productividad y crecimiento del sector hidrocarburos.

Historia

Como consecuencia de la transformación industrial del país y de la necesidad de incrementar la tecnología relacionada con el desarrollo de las industrias petroleras, petroquímica básica, petroquímica derivada y química, el 23 de agosto de 1965 fue creada la Empresa Mexicana del Petróleo.

En el decreto que se publicó en el Diario Oficial el 26 de agosto de 1965, se establecen como objetivos de la empresa:

a. La investigación científica básica y aplicada;
b. El desarrollo de disciplinas de investigación básica y aplicada;
c. La formación de investigadores;
d. La difusión de los desarrollos científicos y su aplicación en la técnica petrolera.
e. La capacitación de personal obrero que pueda desempeñar labores en el nivel sub-profesional, dentro de la industria petrolera, petroquímica básica, petroquímica derivada y química. A más de cuatro décadas, la empresa sigue cumpliendo con los objetivos que le dieron vida.

La empresa nació por iniciativa del entonces Director General de Pemex, Jesús Reyes Heroles, quien reconoció que la planeación y el desarrollo de la industria petrolera deberían ser congruentes con las necesidades de una economía mixta. Por esta razón, consideró necesario fomentar la investigación petrolera y formar recursos humanos que impulsaran el desarrollo de tecnología propia.

En respuesta a esta exigencia, el Gobierno Federal decidió crear un "organismo descentralizado de interés público y preponderantemente científico, técnico, educativo y cultural, con personalidad jurídica y patrimonio propios, cuya función será buscar la independencia científica y tecnológica en el área petrolera".

De esta forma, desde 1965, la Empresa Mexicana del Petróleo ha contribuido al desarrollo del país, mediante la formación de recursos humanos y la creación de tecnología propia.

Una vez que se definieron los programas y se avanzó en la construcción de las instalaciones, se nombró como primer Director General al **Ing. Javier Barros Sierra**, quien tomó posesión el 31 de enero de 1966, fecha en la que se instaló también el Consejo Directivo, presidido por el Lic. Jesús Reyes Heroles.

En febrero de 2007, cuando asumió el cargo de Director General de la empresa, el doctor Héber Cinco Ley (2007-2010) refrendó el compromiso de la Institución para seguir siendo un centro público de investigación concebido para generar tecnología propia que le agregue valor a Pemex y le permita tener ventajas competitivas en los ámbitos nacional e internacional; así como capacitar y actualizar a los trabajadores de la industria más importante del país.

Para responder a los retos tecnológicos de la industria, la empresa focalizó sus actividades de investigación y desarrollo tecnológico en áreas estratégicas relacionadas con la exploración y explotación de yacimientos en aguas profundas, crudos pesados, explotación de aceite terciario del Golfo (Chicontepec) y la producción de combustibles limpios.

A la luz de los requerimientos de la industria más importante del país, el Dr. José Enrique Villa Rivera, en su calidad de Director General de la empresa (2010-2011), inició una transformación profunda de la Institución con el fin de fortalecer sus dos actividades sustantivas: la investigación y los servicios que proporciona a Petróleos Mexicanos, para así recuperar el liderazgo tecnológico y científico del Instituto.

Para ello, su gestión se regirá por los principios de transparencia, calidad, competitividad, rendición pública de los resultados del quehacer Institucional y un ejercicio austero de los recursos institucionales, en apego al marco normativo, con lo que está convencida la empresa, avanzará en su reposicionamiento y en la construcción de una organización más abierta, flexible y sensible a las necesidades de Pemex y del país.

Para marzo de 2011, el Instituto ya era dirigido por su décimo tercer Director General, el Dr. Efrén Parada Arias, quien se comprometió a enfrentar los retos de la Institución para apoyar y dar soluciones a la Industria Petrolera Nacional y dar continuidad y profundizar el proceso de cambio Institucional ya iniciado. Lo anterior conjuntamente con la comunidad, la cual ha acumulado un gran conocimiento acerca de las operaciones y procesos sustantivos de Pemex, además de que cuenta con el activo más importante en el país en infraestructura especializada.

Durante la administración del Dr. Efrén Parada, la Institución fue reconocida en diversos ámbitos, tal es el caso del Modelo de Administración por Procesos (MAP), distinguido por la Secretaría de la Función Pública como caso de éxito; así como del registró de calidad que expidió QMI SAI Global, mediante el cual este centro público de investigación se convirtió en la primera institución del sector público certificada en todos sus procesos, tanto los de investigación y operativos como los financieros y administrativos, al cumplir con los requisitos de la norma ISO 9001: 2008.

A partir de junio de 2012, se inició la gestión del Dr. Vinicio Suro Pérez como Director General de la empresa; a quien corresponde asumir el compromiso de reorganizar y adecuar al Instituto, con el fin de fortalecerlo, convertirlo en soporte técnico y tecnológico fundamental para Petróleos Mexicanos y el resto de la industria petrolera, que proporcione servicios tecnológicos orientados a optimizar los procesos de producción y transformación, tanto en exploración y extracción como en transformación industrial.

Lo anterior, derivado de la Reforma Energética del 2014 y de la reestructuración de Petróleos Mexicanos como una empresa productiva del Estado para aprovechar al máximo los recursos disponibles.

La reforma energética además de la reestructuración de Petróleos Mexicanos, también motivó la reforma del Decreto de Creación del Instituto, cuyo objeto predominante es:

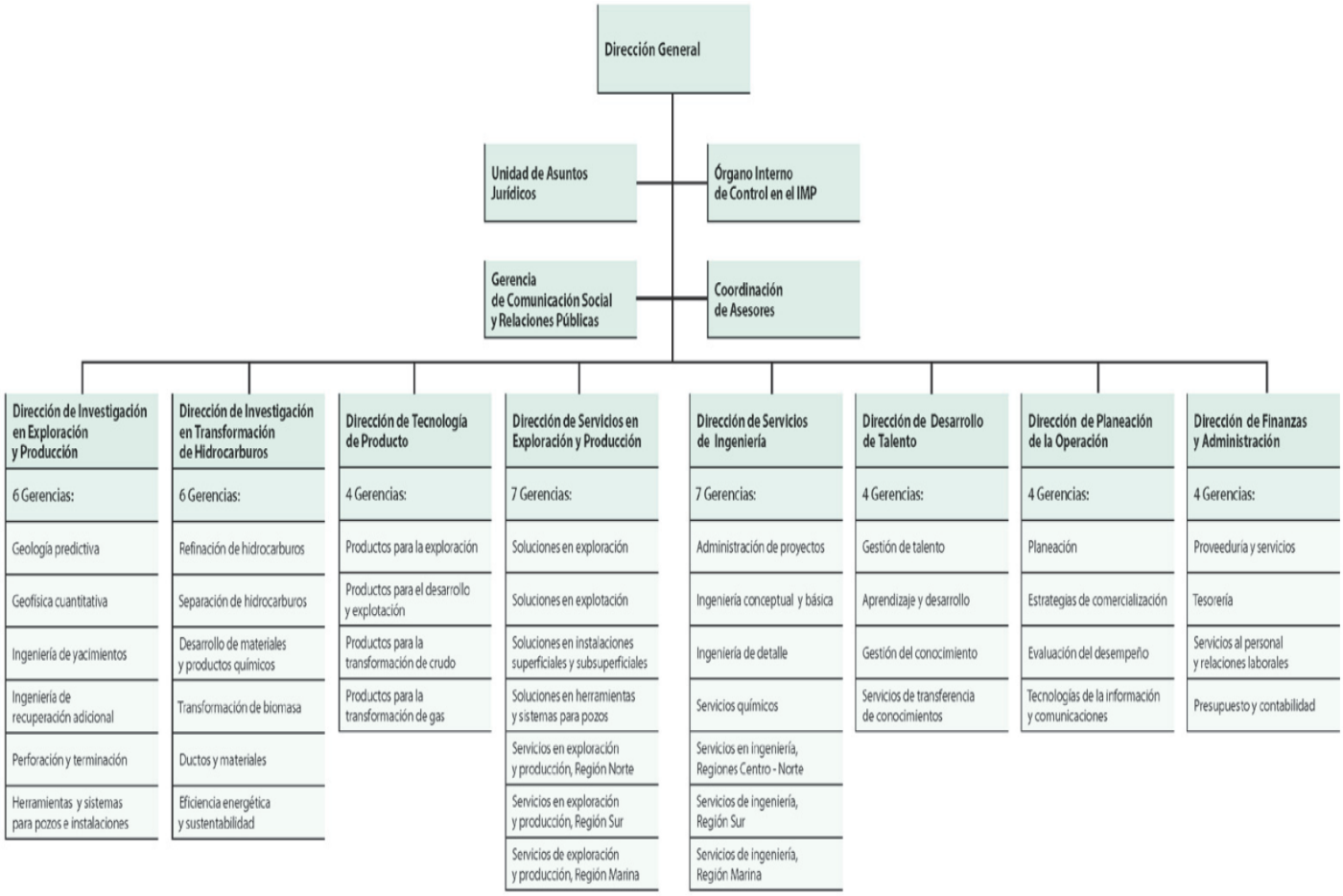
Realizar investigaciones, el desarrollo tecnológico, la innovación, el escalamiento de procesos y productos, la prestación de servicios tecnológicos orientados a optimizar los procesos de producción y transformación, tanto en exploración y extracción como en la transformación industrial y comercialización nacional e internacional de sus resultados en el sector hidrocarburos, así como la capacitación especializada en las áreas de su actividad.

El 3 de febrero de 2015, se notificó la designación por parte del Ejecutivo Federal al Dr. Ernesto Ríos Patrón como Director General de la empresa, en la sesión de

Instalación del nuevo Consejo de Administración de la Empresa Mexicana del Petróleo que presidió el Lic. Pedro Joaquín Coldwell, Secretario de Energía, quién aseveró que esta nueva etapa de la empresa debe ser fecunda y se deben dar pasos muy importantes para el desarrollo tecnológico de una industria de hidrocarburos, ahora pública y privada, con fuerte acento nacional.

El doctor Ernesto Ríos Patrón se comprometió no sólo a acelerar la transición de la empresa para que sea un participante destacado en el nuevo entorno de competencia abierta que marca la Reforma Energética, sino también para que el Instituto esté en condiciones competitivas para entregar productos y servicios que generen valor a la industria petrolera.

Organigrama



2 Marco teórico

Seguridad Informática

Como sabemos, la seguridad informática se enfoca en proteger la infraestructura computacional y todo lo relacionado con ésta (también incluye la información contenida). Para este fin existen una serie de herramientas, métodos, estándares, protocolos, reglas, y leyes concebidas para minimizar los posibles riesgos para la infraestructura o información.

La seguridad informática abarca software, bases de datos, metadatos, archivos y todo lo que tu organización valore como un activo y que signifique un riesgo si llegara a manos de otras personas; pues este tipo de información puede ser privilegiada o confidencial.

Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas).

Cualquier fallo en los mismos puede suponer una gran pérdida económica ocasionada por el patrón producido, bien por la pérdida de información o por el mal funcionamiento de los equipos informáticos, de modo que es muy importante asegurar un correcto funcionamiento de los sistemas y redes informáticas.
Uno de los principales problemas a los que se enfrenta la seguridad informática es la creencia de muchos usuarios de que a ellos nunca les va a pasar. Es impensable que nos vayamos de casa y no dejemos la puerta abierta. Lo mismo ocurre con la seguridad de la información.

Con unas buenas políticas de seguridad, tanto físicas como lógicas, conseguiremos que nuestros sistemas sean menos vulnerables a las distintas amenazas.

Bases de la Seguridad Informática

En general, un sistema será seguro o fiable si podemos garantizar tres aspectos:

- Confidencialidad: garantizar la confidencialidad de los datos significa asegurarse de que dichos datos son únicamente accesibles para las partes deseadas. Es decir, que si nuestra intención es compartir un archivo con cierta persona y mantenerlo en secreto entre ambos, nadie más debería ser capaz de acceder a ellos (salvo que una de las partes rompa dicha confidencialidad).
- Integridad: garantizar la integridad de los datos implica asegurar que dichos datos no han sido modificados por personas no autorizadas, ya sea de forma accidental o intencionada. Otra propiedad relacionada con la integridad de los datos es la autenticidad de los mismos, que generalmente implica asegurar que los datos provienen de quien dicen provenir y que por tanto no han sido modificados en tránsito.
- Disponibilidad: Consiste en la posibilidad de acceder a información o utilizar un servicio siempre que el usuario o usuarios autorizados lo necesiten; dentro de la disponibilidad también debemos considerar la recuperación del sistema frente a posibles incidentes de seguridad, así como frente a desastres naturales o intencionados (incendios, inundaciones, sabotajes, etc.).

Políticas de seguridad

Una política de seguridad es un conjunto de pautas establecidas para proteger a los recursos de la red de los ataques, ya sean desde el interior o desde el exterior de una empresa.

Para elaborar una política se debe comenzar por formular preguntas. ¿De qué manera la red ayuda a la organización a lograr su visión, su misión y su plan estratégico? ¿Cuáles son las implicaciones que tienen los requisitos de la empresa en la seguridad de la red y de qué manera esos requisitos se traducen en la compra de equipos especializados y en las configuraciones que se cargan en los dispositivos?

Una política de seguridad favorece a una organización de las siguientes maneras:

- Proporciona un medio para auditar la seguridad actual de la red y compara los requisitos con los que se encuentra instalado.
- Planifica mejoras de seguridad, incluidos equipos, software y procedimientos.
- Define las funciones y las responsabilidades de los ejecutivos, administradores y usuarios de la empresa.
- Define qué comportamientos están permitidos y cuáles no.
- Define un proceso para manejar los incidentes de seguridad de la red
- Permite la implementación y el cumplimiento de la seguridad global al funcionar como norma entre los sitios.
- Crea una base para fundar acciones legales, en caso de ser necesario.
- Funciones de una política de seguridad.

Redes de datos

Una red de datos es un grupo de computadoras que están interconectadas entre sí para comunicarse, además pueden compartir documentos y recursos. Cada una de estas redes ha sido diseñada específicamente para satisfacer sus objetivos, con una arquitectura determinada para facilitar el intercambio de los contenidos.

Por lo general, estas redes se basan en la conmutación de paquetes. Pueden clasificarse de distintas maneras de acuerdo a tu tipo o topología.

Topologías de redes

La topología de redes es la distribución física de los componentes que conforman una red, es decir la configuración espacial de la red, se denomina topología física. Los diferentes tipos de topología son:

- Topología de bus
- Topología de estrella
- Topología en anillo
- Topología de árbol
- Topología de malla

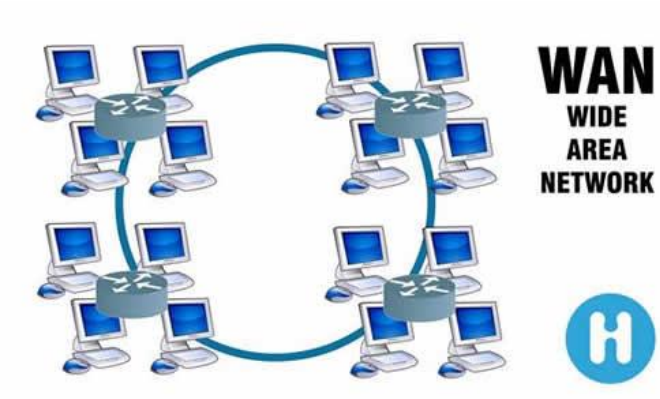
Sin embargo podemos realizar topologías híbridas, esto es fusionando dos o más topologías ya mencionadas.

Tipos de redes

Se distinguen diferentes tipos de redes (privadas) según su tamaño (en cuanto a la cantidad de equipos), su velocidad de transferencia de datos y su alcance. Las redes privadas pertenecen a una misma organización. Generalmente se dividen en tres tipos de redes:

LAN (local area network) o como su traducción lo dice Red de Área Local. Esta red conecta equipos en un área geográfica limitada, tal como una oficina o edificio. De esta manera se logra una conexión rápida, sin inconvenientes, donde todos tienen acceso a la misma información y dispositivos de manera sencilla.

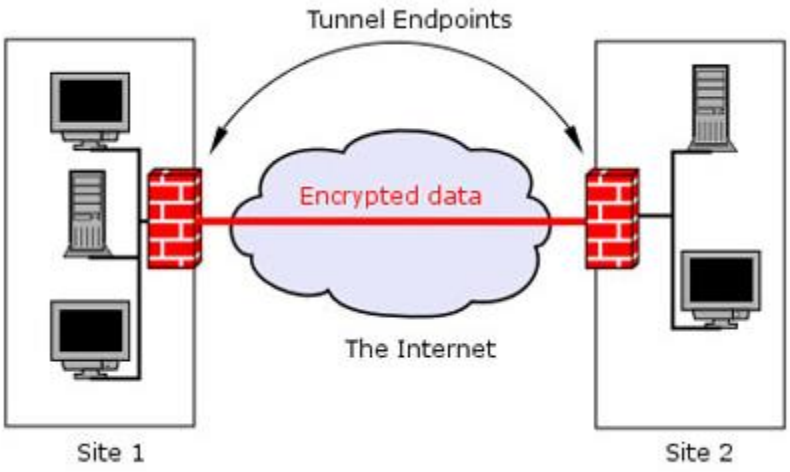
MAN (metropolitan area network) en español Red de Área Metropolitana. Ésta alcanza un área geográfica equivalente a un municipio. Se caracteriza por utilizar una tecnología análoga a las redes LAN, y se basa en la utilización de dos buses de carácter unidireccional, independientes entre sí en lo que se refiere a la transmisión de datos.



WAN (wide area network) o su traducción Red de Área Amplia. Estas redes se basan en la conexión de equipos informáticos ubicados en un área geográfica extensa, por ejemplo entre distintos continentes. Al comprender una distancia tan grande la transmisión de datos se realiza a una velocidad menor en relación con las redes anteriores. Sin embargo, tienen la ventaja de trasladar una cantidad de información mucho mayor. La conexión es realizada a través de fibra óptica o satélites.

Red VPN

Una red privada virtual se basa en un protocolo denominado **protocolo de túnel**, es decir, un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro.



El túnel simplemente hace uso de un protocolo especial (normalmente **SSH**) para crear un camino por el que circulan todos los datos desde un extremo a otro. Este "túnel" en realidad es la misma información que se manda pero cifrada por la acción del protocolo seguro de comunicación, lo cual hace que nuestros datos no puedan ser vistos por agentes externos.

Otro de los usos más extendidos de las VPN es para facilitar el acceso remoto a una red local. Un ejemplo clásico lo tenemos en los empleados que deben acceder a la red del trabajo desde su portátil cuando se encuentran desplazados. En su portátil, el empleado tiene instalado un programa cliente de VPN que, tras introducir siempre un usuario y un password, se conecta con un servidor VPN situado en las oficinas de la empresa y así tener acceso a toda la red de la misma.

VPN es prácticamente la tecnología más usada para permitir el acceso remoto y la conectividad entre distintos agentes y segmentos de una misma red local, cuya distancia entre si sea demasiado grande como para optar por una conexión física y real.

Sistema Operativo Linux

Linux es un sistema operativo, compatible Unix. Dos características muy peculiares lo diferencian del resto de sistemas que podemos encontrar en el mercado, la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente.

El sistema lo forman el núcleo del sistema (kernel) más un gran número de programas / bibliotecas que hacen posible su utilización. Muchos de estos programas y bibliotecas han sido posibles gracias al proyecto GNU, por esto mismo, muchos llaman a Linux, GNU/Linux, para resaltar que el sistema lo forman tanto el núcleo como gran parte del software producido por el proyecto GNU.

Linux se distribuye bajo la *GNU General Public License* por lo tanto, el código fuente tiene que estar siempre accesible y cualquier modificación o trabajo derivado, debe tener esta licencia.

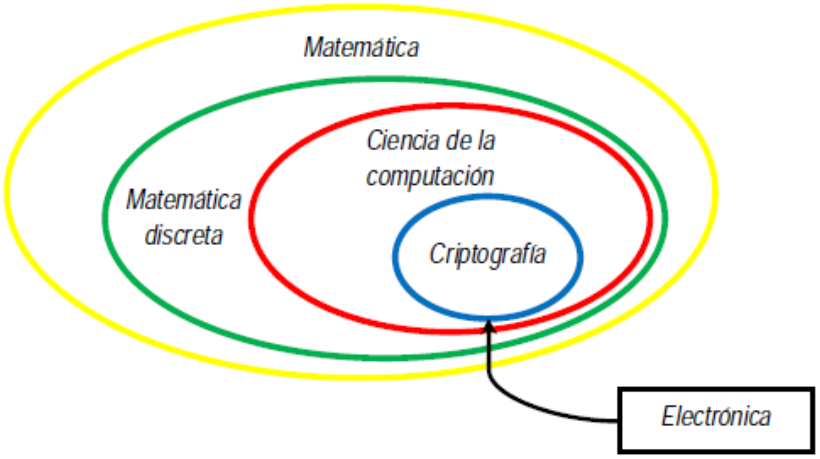
El sistema ha sido diseñado y programado por multitud de programadores alrededor del mundo. El núcleo del sistema sigue en continuo desarrollo bajo la coordinación de *Linus Torvalds*, la persona de la que partió la idea de este proyecto, a principios de la década de los noventa. Hoy en día, grandes compañías, como IBM, SUN, HP, Novell y RedHat, entre otras muchas, aportan a Linux grandes ayudas tanto económicas como de código.

Criptografía

Data aproximadamente de los años 500 a.C. Anteriormente la Criptografía era considerada como un arte pero en la actualidad se considera una ciencia gracias a su relación con la estadística, sin embargo, con el desarrollo de las ciencias de la computación y de la teoría de la información ha llegado a convertirse en una ciencia, para ser más exactos en una rama de las matemáticas, por otro lado con el auge

de la computación, la electrónica, la electrónica es una disciplina auxiliar de la criptografía.

La criptografía proviene del griego kryptos: "ocultar", y grafos: "escribir". Es decir, significa "escritura oculta". Como concepto son las técnicas utilizadas para cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes, de tal manera que sólo puedan ser leídos por las personas a quienes van dirigidos; sin embargo, el objetivo de la Criptografía no es sólo mantener los datos secretos, sino también protegerlos contra modificación y comprobar la fuente de los mismos.



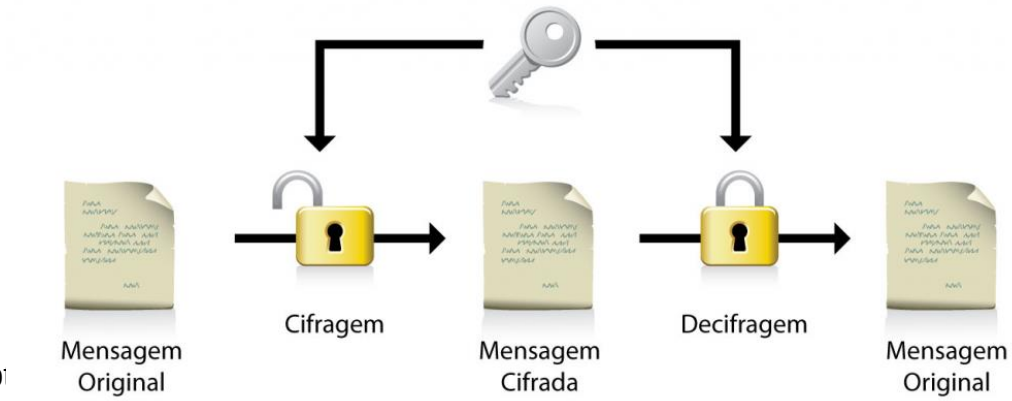
El Criptoanálisis es la ciencia que se ocupa del análisis de un texto cifrado para obtener la información original sin conocimiento de la clave secreta, ésto es, de forma ilícita, rompiendo así los procedimientos descifrados establecidos por la Criptografía, por lo que se dice que Criptoanálisis y Criptografía son ciencias complementarias, pero contrarias.

La Estenografía por su parte, estudia la forma de ocultar la existencia de un mensaje. Esta ciencia consiste en esconder en el interior de un mensaje, otro mensaje secreto, el cual sólo podrá ser entendido por el emisor y el receptor; y pasará inadvertido para todos los demás.

Criptografía simétrica.

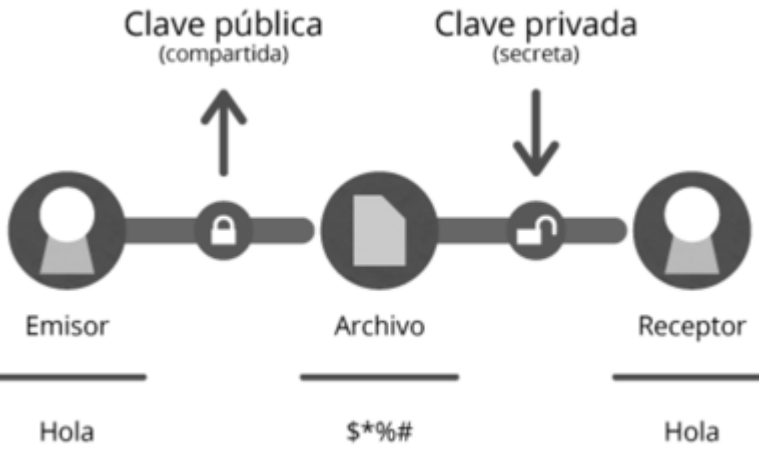
La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

La criptografía simétrica ha sido la más usada en toda la historia, ésta ha podido ser implementada en diferentes dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que sólo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.



Cript

La criptografía asimétrica es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas.



Sabiendo lo anterior, si queremos que tres compañeros de trabajo nos manden un archivo cifrado debemos de mandarle nuestra clave pública (que está vinculada a la privada) y nos podrán mandar de forma confidencial ese archivo que sólo nosotros podremos descifrar con la clave privada.

Otro propósito de este sistema es también el de poder firmar documentos, certificando que el emisor es quien dice ser, firmando con la clave privada y verificando la identidad con la pública.

Estos son los métodos criptográficos modernos que usamos comúnmente, aunque las aplicaciones nos abstraigan de todo esto, pero podemos hacerlo de forma manual si se diera el caso de que necesitamos mandar ciertos contenidos y queremos que tengan la confidencialidad adecuada.

Herramienta PuTTY

PuTTY es un cliente de red que soporta los protocolos SSH, Telnet y Rlogin y sirve principalmente para iniciar una sesión remota con otra máquina o servidor. Es de licencia libre y está diseñado y mantenido principalmente por Simon Tatham desde Gran Bretaña. A pesar de su sencillez es muy funcional y configurable.

Esta aplicación es como todas, tiene sus partes buenas y partes malas, pero si es cierto que mayormente tiene grandes ventajas como las siguientes:

- Es gratuito y de código abierto.
- Disponible para varias plataformas (Windows y Linux).
- Es una aplicación portable.
- Interfaz sencilla y manejable.
- Muy completo y ofrece una gran flexibilidad con multitud de opciones.
- Está en constante desarrollo.

Algunas características de PuTTY son:

- El almacenamiento de hosts y preferencias para uso posterior.
- Control sobre la clave de cifrado SSH y la versión de protocolo.
- Clientes de línea de comandos SCP y SFTP, llamados "pscp" y "psftp" respectivamente.
- Control sobre el redireccionamiento de puertos con SSH, incluyendo manejo empotrado de reenvío X11.
- Completos emuladores de terminal xterm, VT102, y ECMA-48.
- Soporte IPv6.
- Soporte 3DES, AES, RC4, Blowfish, DES.
- Soporte de autentificación de clave pública.
- Soporte para conexiones de puerto serie local.

El nombre PuTTY proviene de las siglas Pu: Port unique TTY: terminal type. Su traducción al castellano sería: Puerto único de tipo terminal.

Barracuda Web Filter

El Web Filter de Barracuda Networks permite a las organizaciones beneficiarse de las aplicaciones y herramientas que están en la web sin exponerse a malware y virus, a la pérdida de productividad de los usuarios ni al mal uso del ancho de banda. Como solución integral de administración de seguridad web, incorpora tecnología galardonada de protección contra spyware, malware y virus, con un potente motor de políticas y reportes. Las avanzadas opciones garantizan que las organizaciones se adapten a requisitos emergentes como la regulación de redes sociales, el filtrado remoto y la visibilidad del tráfico cifrado mediante SSL.

Además, el Web Filter de Barracuda Networks incluye licencias ilimitadas para usuarios remotos y dispositivos móviles que se encuentran fuera de la red

corporativa. Barracuda Web Filter también está disponible como virtual - appliance y en la versión cloud.

El Barracuda Web Filter ofrece a los administradores una visibilidad clara de la actividad en la Web para responder a esas preguntas importantes mientras que protege su red bloqueando amenazas latentes.

Integra diferentes tecnologías para hacer cumplir las políticas de filtrado de contenido destinadas a incrementar la productividad del usuario y evitar exponer tanto la infraestructura como a los usuarios a material inapropiado, reconocido por administradores de grandes corporativos, ya que permite la supervisión del tráfico web y tiene todo contemplado.

3 Descripción de puesto

Área de seguridad informática

Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de la Institución o constituir una amenaza para la Seguridad Nacional.

Las funciones del área de seguridad informática deberían ser:

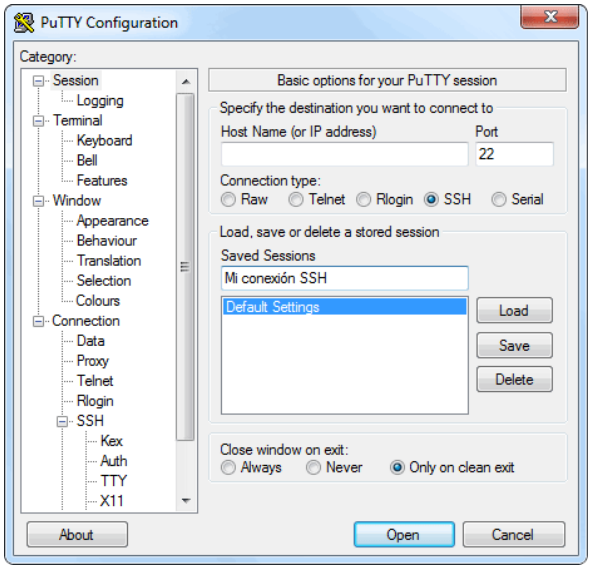
- Proteger los sistemas informáticos de la Empresa, ante posibles amenazas.
- Desarrollar, promocionar y actualizar las políticas y estándares de seguridad de la información.
- Mantener los usuarios, passwords y accesos a los sistemas por parte de los usuarios de la Empresa.
- Desarrollar e implementar el Plan de Seguridad.

- Asegurarse de que los aspectos relacionados con la seguridad sean considerados cuando se seleccionen los contratistas.
- Monitorear día a día la implementación y el uso de los mecanismos de seguridad de la información.
- Coordinar investigaciones de incidentes de seguridad informática.
- Revisar los logs de auditoría y sistemas de detección de intrusiones.
- Participar en los proyectos informáticos de la Empresa agregando todas las consideraciones de seguridad informática.

Emplear la herramienta PuTTY

Uno de las herramientas más utilizadas en la institución es PuTTY, que es utilizada solamente con comandos de Linux.

Al ejecutar PuTTY nos muestra la siguiente ventana de configuración.



En esta parte se coloca lo siguiente

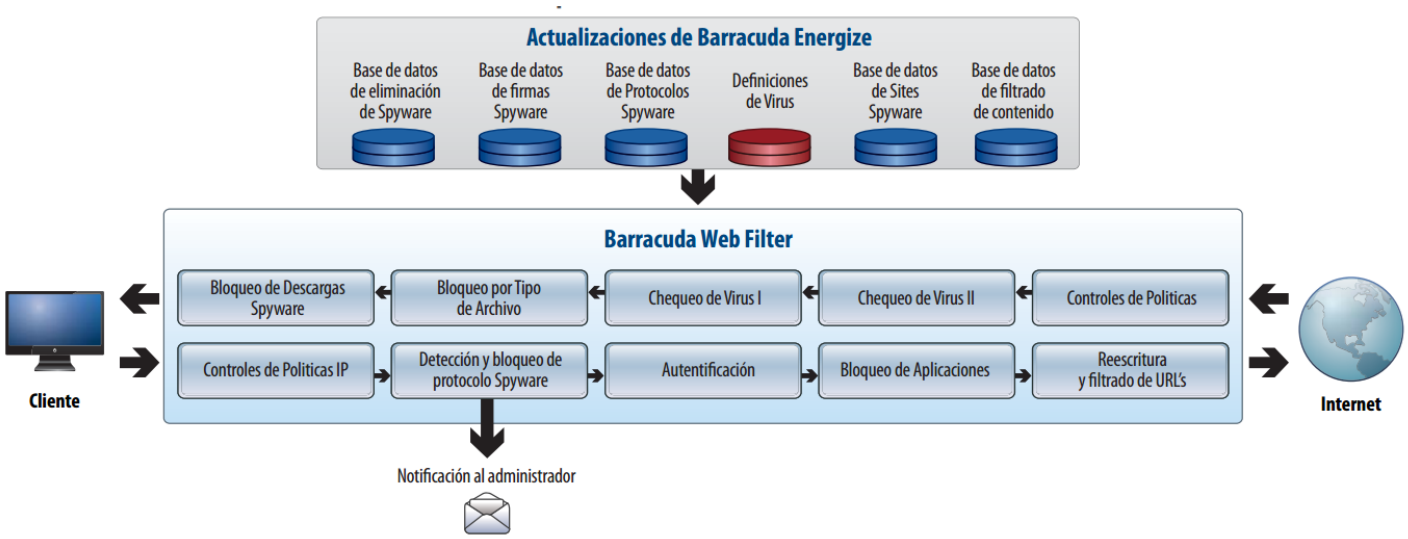
- ❖ Introducir la IP o Hostanme del servidor remoto.

- Seleccionar el puerto (normalmente para conectar a través de SSH es el 22 por defecto).
- Seleccionar en connection type la opción SSH (ya suele venir marcada por defecto).
- Hacemos click en el botón Open.
- Probablemente surja una advertencia, la cual no hay ningún problema es aceptada y posteriormente es solicitado el nombre de usuario y contraseña para iniciar sesión en el servidor remoto.

Con esos pasos se puede conectar con nuestro servidor remoto.

Monitoreo mediante Barracuda Web Filter

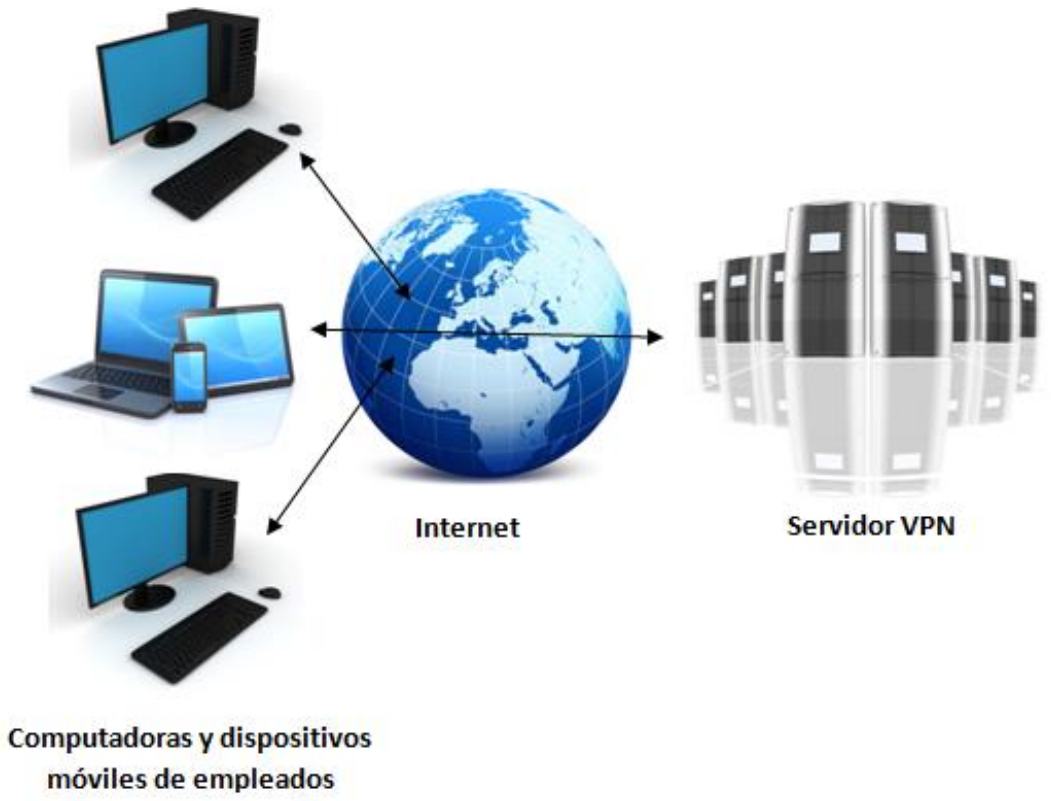
Barracuda permite a las organizaciones beneficiarse de aplicaciones y herramientas en línea sin exponerse a malware y virus que circulan por Internet, a la pérdida de productividad de los usuarios ni al mal uso del ancho de banda.



El Filtro Web de Barracuda ayuda de una forma muy eficiente a las organizaciones montar políticas personalizadas para usuarios particulares y grupos en múltiples zonas horarias.

Implementación de redes VPN

Es importante la tecnología VPN ya que permite configurar a distancia un equipo electrónico. Uno de los usos principales de la tecnología VPN es encapsular una IP privada de una red corporativa o de empresa dentro de una IP pública de Internet de forma que los empleados que trabajen desde casa puedan conectarse a la red de la oficina accediendo a los servicios, recursos, servidores, etc.



La tecnología que está detrás de este tipo de conexiones se denomina tunneling, ya que crea un "túnel" estableciendo comunicación entre dos puntos, por el que

circulan datos. La VPN como tal no almacena ningún tipo de datos, cualquier dato se almacena en los servidores o clientes que conforman la VPN.

Juntas dirigidas al tema de seguridad informática

Hoy en día, el tema de seguridad informática está presente día con día en la Empresa Mexicana del Petróleo, ya que en los últimos años hemos visto en diferentes empresas el riesgo creciente de robo, alteración o destrucción de datos por ciberataques.

Por esta razón el Instituto continuamente tiene que estar renovando sus políticas de seguridad, además del equipo con el que cuenta, se tienen que contratar a diversas empresas de seguridad para el apoyo y gestión de las diversas políticas que conforman a la Institución, las empresas contratadas deben garantizar cuatro puntos importantes los cuales son fiabilidad, confidencialidad, integridad y disponibilidad.

Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque, son los datos y la información los sujetos principales de protección de las técnicas de seguridad.

4 Descripción de la participación del alumno en la empresa.

Monitoreo de proxy´s mediante comandos de Linux

Como ya existía, se utiliza la Herramienta PuTTY para administrar los proxy`s del Instituto, y nos conectamos utilizando el protocolo SSH, el cual es uno de los canales más seguros de comunicación, ya que tiene la función de cifrar todos los datos que pasan por ese canal.

Por motivos de seguridad no se mostrarán las direcciones IP ni las contraseñas. En la captura de pantalla anterior estamos ingresando a los logs que es la parte donde podemos observar a cada usuario.

Los servidores proxy permiten proteger y mejorar el acceso a las páginas web, al conservarlas en la caché. De este modo, cuando un navegador envía una petición para acceder a una página web, que previamente ha sido almacenada en la caché, la respuesta y el tiempo de visualización es más rápido.
Los servidores proxy aumentan también la seguridad, ya que pueden filtrar cierto contenido web y programas maliciosos.

El Filtrado

El filtrado se aplica en función de la política de seguridad implementada en la red. Este permite bloquear sitios considerados maliciosos o sitios considerados inútiles en relación a la actividad de la empresa (pornografía, etc.).

Autenticación

A fin de limitar el acceso a la red exterior, y aumentar de este modo la seguridad de la red local, se puede implementar un sistema de autenticación para acceder a

recursos externos. Esto es bastante disuasivo para los usuarios que desean visitar sitios que estén en contra de las reglas de uso de Internet en la empresa.

Almacenamiento de 'logs'

```
-rw-------  1 root root     68512 Jun  5 03:28 secure-20160605
-rw-------  1 root root     68020 Jun 12 03:08 secure-20160612
-rw-------  1 root root     75411 Jun 20 11:28 secure-20160620
-rw-------  1 root root     95246 Jun 26 03:19 secure-20160626
-rw-r--r--  1 root root 785442558 Dec  9  2015 SoloUrl
-rw-------. 1 root root         0 Jan 14  2015 spice-vdagent.log
-rw-------  1 root root         0 Jun 26 03:28 spooler
-rw-------  1 root root         0 May 29 03:13 spooler-20160605
-rw-------  1 root root         0 Jun  5 03:33 spooler-20160612
-rw-------  1 root root         0 Jun 12 03:16 spooler-20160620
-rw-------  1 root root         0 Jun 20 11:36 spooler-20160626
-rwxr-xr-x  1 root root       668 Dec  1  2015 subtotal.pl
-rw-------. 1 root root         0 Jan 14  2015 tallylog
-rw-------  1 root root 332005159 Jun 28 08:29 WebFilters.log
-rw-------  1 root root  27256520 Jun 13 03:11 WebFilters.log-20160613.gz
-rw-------  1 root root 580673256 Jun 14 03:35 WebFilters.log-20160614.gz
-rw-------  1 root root 480093829 Jun 15 03:31 WebFilters.log-20160615.gz
-rw-------  1 root root 389114739 Jun 16 03:35 WebFilters.log-20160616.gz
-rw-------  1 root root 414807166 Jun 17 03:26 WebFilters.log-20160617.gz
-rw-------  1 root root 313836208 Jun 18 03:40 WebFilters.log-20160618.gz
-rw-------  1 root root 100563482 Jun 20 11:36 WebFilters.log-20160620.gz
-rw-------  1 root root 317116456 Jun 21 03:42 WebFilters.log-20160621.gz
-rw-------  1 root root 422467361 Jun 22 03:38 WebFilters.log-20160622.gz
-rw-------  1 root root 421927718 Jun 23 03:39 WebFilters.log-20160623.gz
-rw-------  1 root root 387452075 Jun 24 03:40 WebFilters.log-20160624.gz
-rw-------  1 root root 284560558 Jun 25 03:22 WebFilters.log-20160625.gz
-rw-------  1 root root  20108279 Jun 26 03:28 WebFilters.log-20160626.gz
-rw-------  1 root root  18552515 Jun 27 03:38 WebFilters.log-20160627.gz
-rw-------  1 root root 551937389 Jun 28 03:43 WebFilters.log-20160628.gz
-rw-r--r--. 1 root root         0 Jan 14  2015 wpa_supplicant.log
-rw-rw-r--. 1 root utmp    235008 Jun 28 08:27 wtmp
-rw-r--r--  1 root root  16978031 Jun 23 13:19 Xorg.0.log
-rw-r--r--  1 root root     73012 Jun 20 10:11 Xorg.0.log.old
-rw-r--r--  1 root root     47069 Jun 20 10:15 Xorg.1.log
-rw-r--r--  1 root root     73689 Apr 22  2015 Xorg.1.log.old
-rw-r--r--  1 root root     72832 Jun 16  2015 Xorg.2.log
-rw-r--r--. 1 root root     33054 Jan 14  2015 Xorg.9.log
```

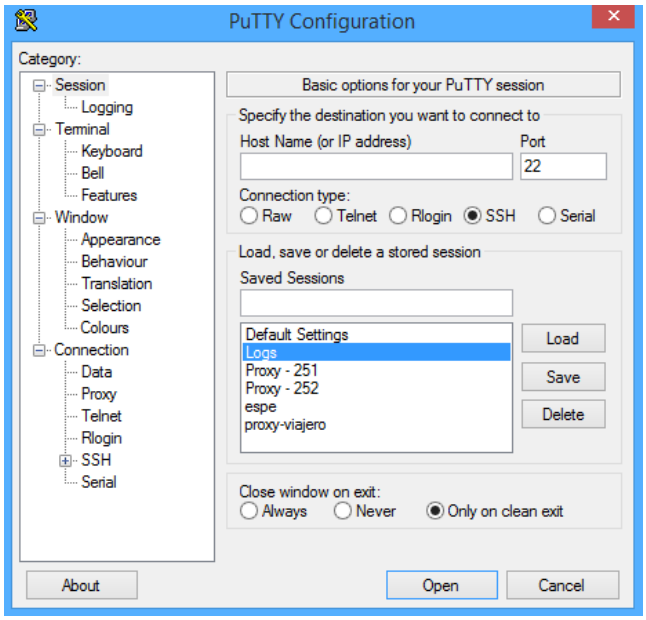
El almacenamiento de logs de los sitios visitados y páginas vistas, permite al administrador de la red, redefinir la política de seguridad de la red y/o detectar a un

usuario que visita frecuentemente sitios maliciosos o sin relación con la actividad de la empresa.

El uso común de proxy y VPN es muy similar. Sin embargo hay una diferencia importante que se debe subrayar: en una VPN se crea una conexión con criptografía, de tal forma que la información que transita por la conexión es ilegible sin las llaves correctas. Esto hace imposible que un ISP (o alguien con intenciones más oscuras) descifre el contenido que circula entre el cliente y la VPN.

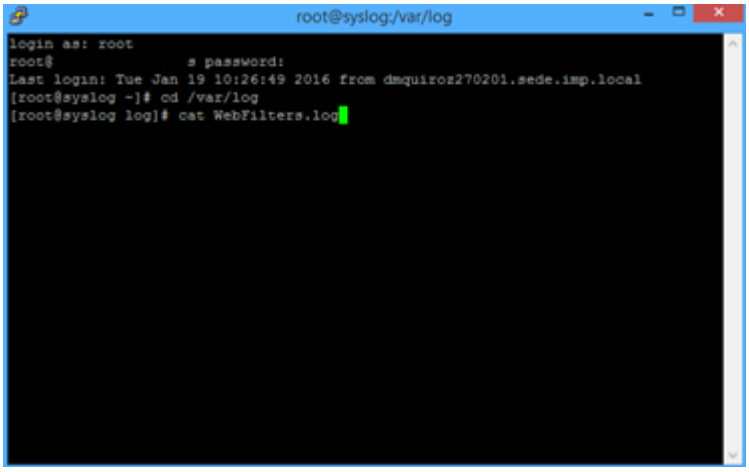
Para realizar el monitoreo de los proxy´s del Instituto, ejecuto el programa PuTTY el cual contiene las direcciones de los proxy´s y observamos que, la IP que contiene los registros diarios de los accesos de cada trabajador del Instituto, tiene el nombre de logs, una vez accedido en este sitio me coloco en la posición de Webfilter.log, como sabemos, para moverse entre los directorios de Linux utilizamos el comando:

`cd/ (carpeta la que se desea acceder).`

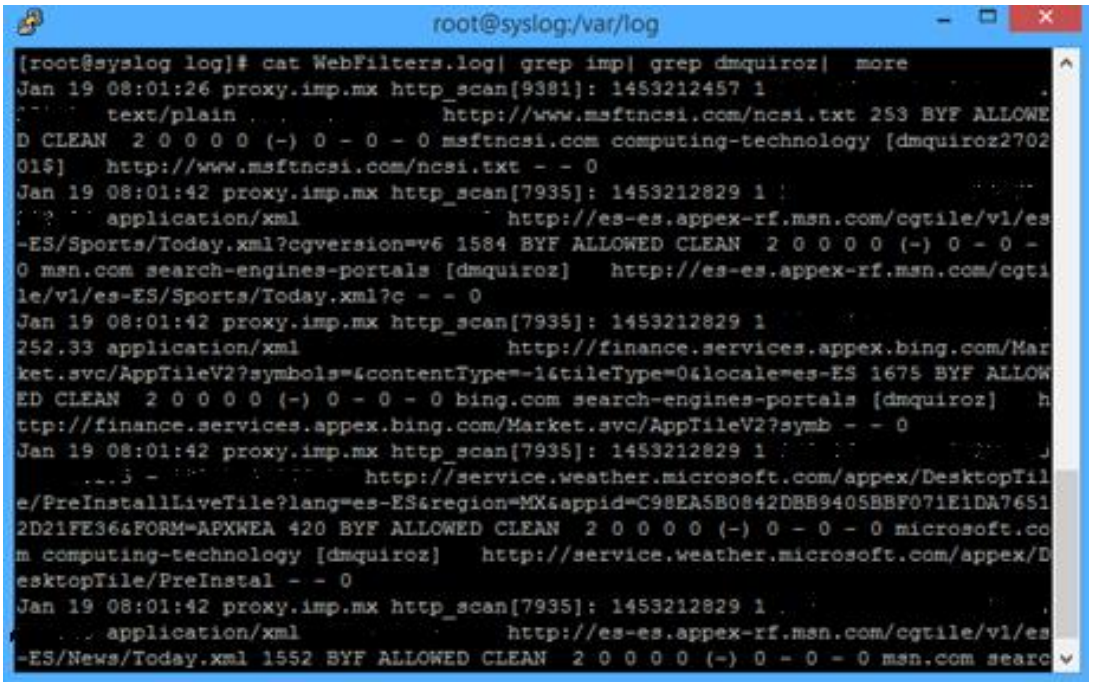


Ya que estoy en la ubicación destinada para monitorear utilizo el comando `catWebFilters.log` que es el que me va a mostrar el contenido de mi programa y archivo, sin embargo si sólo realizo ésto, el programa podría entrar y mostrarme

todas las búsquedas que realizan los trabajadores que laboran en la Institución, por lo que no encontraría resultados específicos.



Por lo que se necesita hacer una búsqueda más especializada, para esto se emplea el comando grep además de un more, ya que aún haciendo una búsqueda especializada son demasiados registros, así que gracias al comando more se despliegan poco a poco presionando tabulador.

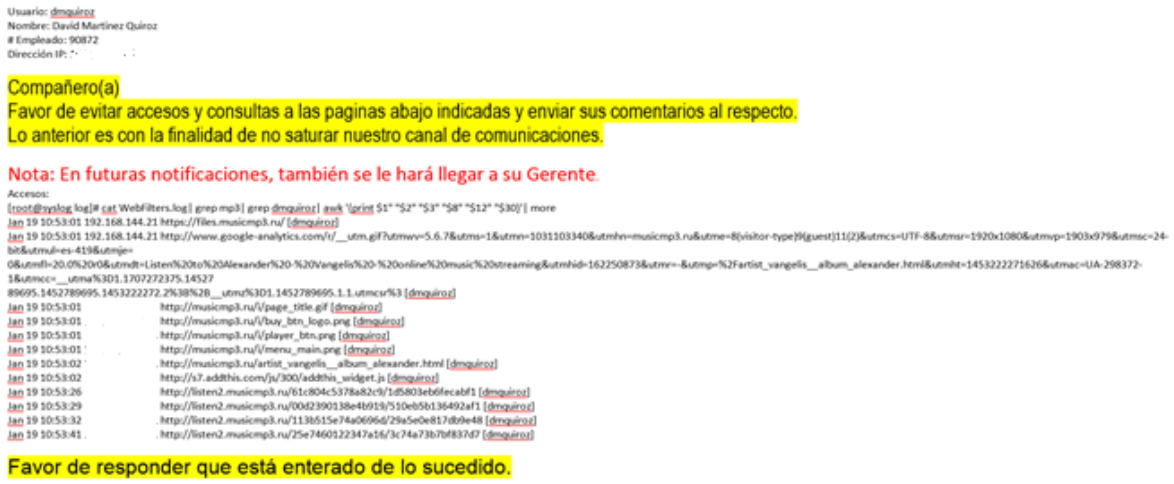


Como sabemos la Empresa Mexicana del Petróleo no permite acceder a páginas que interfieran con el desarrollo laboral, sin embargo en ocasiones los empleados

llegan a buscar páginas que los distraen de sus labores, por esta razón cuando se encuentra a un usuario en los logs, accediendo algún sitio restringido se procede a enviar una “alerta de seguridad”, en la cual advertimos al usuario que si vuelve a incurrir en esto se le enviará una copia a su Gerente y se procederá al bloqueo de su cuenta de usuario, y posteriormente se bloquea la página a la cual el usuario está accediendo.

En el mensaje que se le envía al usuario contiene su nombre, nombre de usuario, IP de la cual está accediendo, su número de empleado y por último los accesos a las páginas que ha realizado.

Por otro lado como ya sabemos la terminal de Linux trabaja por columnas, y éstas conforman una lista, al enviar un mensaje la evidencia no debe contener todas las columnas, ya que la evidencia debe ser clara para que el usuario vea de forma fácil la fecha, hora, IP, la página a la que está accediendo, y por último su usuario. Esta selección de columnas se logra con el uso del comando `awk'{print $#}'`.


Usuario: dmquiroz
Nombre: David Martínez Quiroz
Empleado: 90872
Dirección IP: [redacted]

Compañero(a)
Favor de evitar accesos y consultas a las paginas abajo indicadas y enviar sus comentarios al respecto.
Lo anterior es con la finalidad de no saturar nuestro canal de comunicaciones.

Nota: En futuras notificaciones, también se le hará llegar a su Gerente.

Accesos:
[root@syslog log]# cat WebFilters.log | grep mp3 | grep dmquiroz | awk '{print $1" "$2" "$3" "$8" "$12" "$30}' | more
Jan 19 10:53:01 192.168.144.21 https://files.musicmp3.ru/ [dmquiroz]
Jan 19 10:53:01 192.168.144.21 http://www.google-analytics.com/r/__utm.gif?utmwv=5.6.7&utms=1&utmn=1031103340&utmhn=musicmp3.ru&utme=8(visitor-type)9(guest)11(2)&utmcs=UTF-8&utmsr=1920x1080&utmvp=1903x979&utmsc=24-bit&utmul=es-419&utmje=
0&utmfl=20.0%20r0&utmdt=Listen%20to%20Alexander%20-%20Vangelis%20-%20online%20music%20streaming&utmhid=162250873&utmr=-&utmp=%2Fartist_vangelis__album_alexander.html&utmht=1453222271626&utmac=UA-298372-1&utmcc=__utma%3D1.1707272375.14527
89695.1452789695.1453222272.2%3B%2B__utmz%3D1.1452789695.1.1.utmcsr%3 [dmquiroz]
Jan 19 10:53:01 http://musicmp3.ru/i/page_title.gif [dmquiroz]
Jan 19 10:53:01 http://musicmp3.ru/i/buy_btn_logo.png [dmquiroz]
Jan 19 10:53:01 http://musicmp3.ru/i/player_btn.png [dmquiroz]
Jan 19 10:53:01 http://musicmp3.ru/i/menu_main.png [dmquiroz]
Jan 19 10:53:02 http://musicmp3.ru/artist_vangelis__album_alexander.html [dmquiroz]
Jan 19 10:53:02 http://s7.addthis.com/js/300/addthis_widget.js [dmquiroz]
Jan 19 10:53:26 http://listen2.musicmp3.ru/61c804c5378a82c9/1d5803eb6fecabf1 [dmquiroz]
Jan 19 10:53:29 http://listen2.musicmp3.ru/00d2390138e4b919/510eb5b136492af1 [dmquiroz]
Jan 19 10:53:32 http://listen2.musicmp3.ru/113b515e74a0696d/29a5e0e817db9e48 [dmquiroz]
Jan 19 10:53:41 http://listen2.musicmp3.ru/25e7460122347a16/3c74a73b7bf837d7 [dmquiroz]

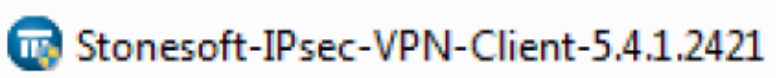
Favor de responder que está enterado de lo sucedido.

Configuración de redes VPN

Los empleados que conforman la empresa son demasiados, por lo cual no todos se encuentran dentro de la Institución, por lo que se realiza una conexión VPN, sin embargo debemos revisar las siguientes características:

- Procesador: Pentium 4 o superior
- Espacio libre en disco duro: 300 MB
- Memoria RAM: 512 MB o mayor

Posteriormente procedemos a instalar el software “Stonesoft-IPsec-VPN-Client-5.4.1.2421”



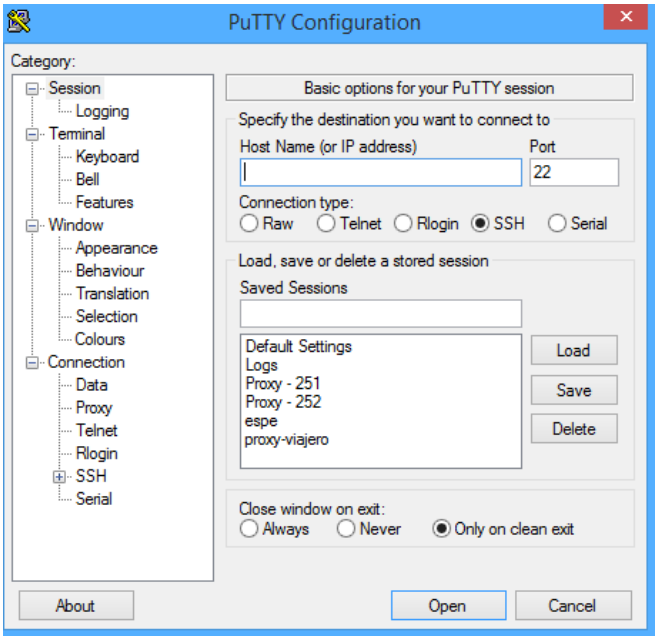
Una vez instalado el software procedemos a realizar la configuración para realizar la conexión VPN hacia la empresa, con lo cual se ingresa la dirección IP del host name a la cual acceder. Por último al establecer correctamente la conexión se podrá acceder a los servicios requeridos de la empresa, con esto los empleados se mantienen comunicados.

Administración de proxy´s de la empresa.

En la Empresa Mexicana del Petróleo se utilizan diferentes proxy´s para mantener comunicados a todos los empleados de la Institución, como en toda empresa, se manejan diferentes tipos de salidas, el proxy normal es utilizado para todos los empleados de la empresa, este proxy tiene restricciones a múltiples páginas como YouTube, Facebook, twitter, etc.

Sin embargo para los Gerentes y Directores, se les otorgan privilegios, el cual es el proxy especial, este tiene salidas a todo el contenido que se encuentra en internet. Además de estos dos proxy´s hay un tercero el cual se llama proxy viajero, este es parecido a la red VPN, sin embargo este es para usuarios que no solamente

trabajan fuera de la Institución sino que además se mueven por toda la República Mexicana y fuera de ella.



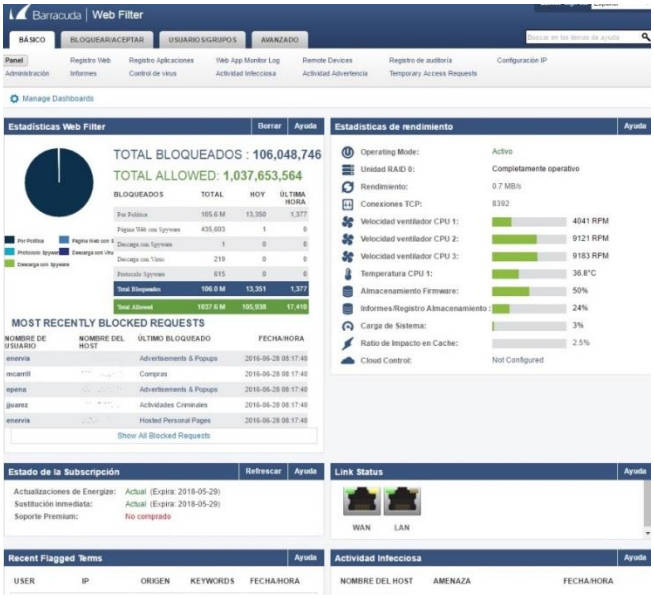
Al iniciar sesión en el proxy debo ingresar a los usuarios en una lista de permitidos y otra lista donde está la contraseña de cada usuario, se llaman `admitidos` y `PasswdViaja` respectivamente, al terminar de ingresar al usuario, debo reiniciar el servicio con los comandos `servicesquidreload`.

Aplicación de Barracuda Web Filter

Este programa es uno de los más importantes para la Institución ya que desde éste, se pueden ingresar a los usuarios, darles privilegios, o en su defecto bloquearles totalmente la salida de internet en su máquina, y solamente poder enviar correos, por otra parte desde este programa podemos quitar páginas que principalmente están causando pérdida de tiempo en los trabajadores.

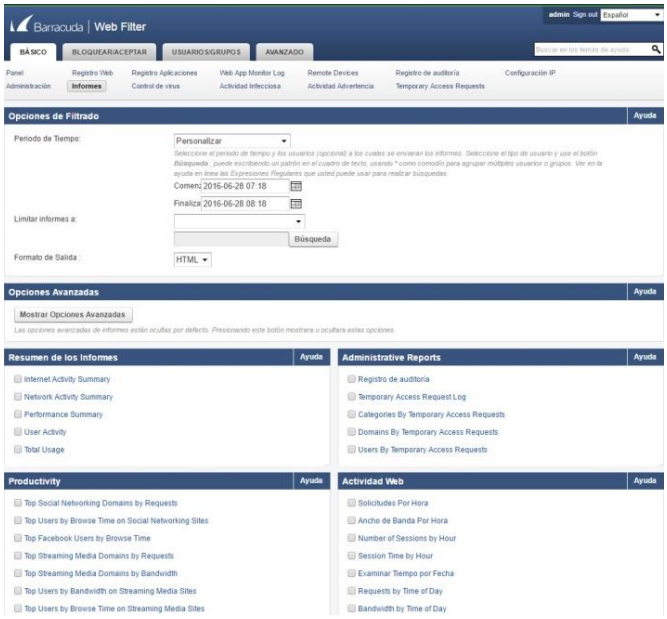
Claro que para poder bloquear usuarios además de saber a qué páginas ingresan se tiene que monitorear de primera instancia los logs, para poder ver que es lo que no se puede y a que si se puede tener acceso.

En la Institución era común el apoyo con el sistema barracuda ya que éste era esencial para informes de virus, altas de usuarios, bloqueos de páginas web entre otras actividades. Al ingresar podemos ver las estadísticas de rendimiento de los servidores, el total de infecciones y por supuesto qué usuarios han consumido más ancho de banda, y se ve de la siguiente forma.

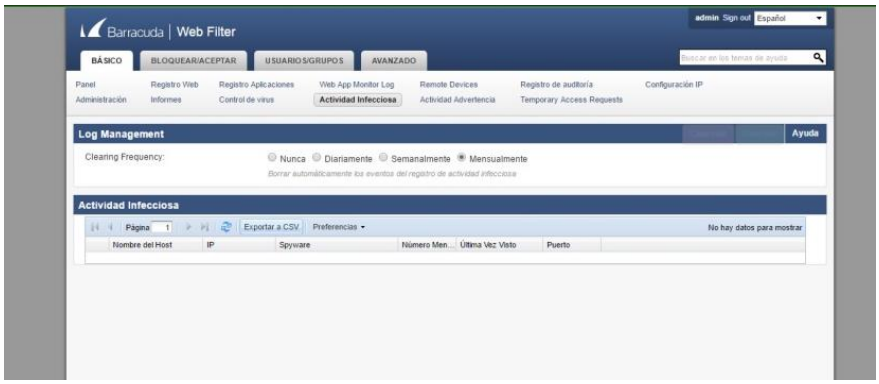


Los informes de infecciones eran realizados por las mañanas del día anterior al que se estaba revisando y los equipos que tuvieran infecciones eran atendidos lo antes

posible, por otro lado al sacar el informe se realizaba un documento en Exel donde se ubicaran a los usuarios afectados por los virus, por otro lado los usuarios que accedieran a páginas restringidas se procedía a bloquear la página, y posteriormente notificar al usuario como ya lo mencioné antes.

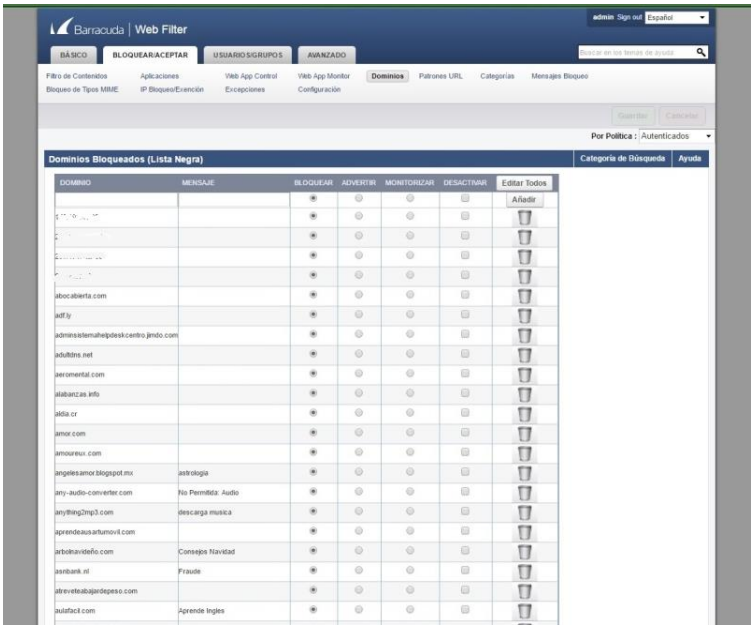


Al detectar que un Ransomware había ingresado a la Institución se tuvo que tomar decisiones más severas en cuanto a la desinfección de equipos, por lo cual se ingresa a la siguiente página.

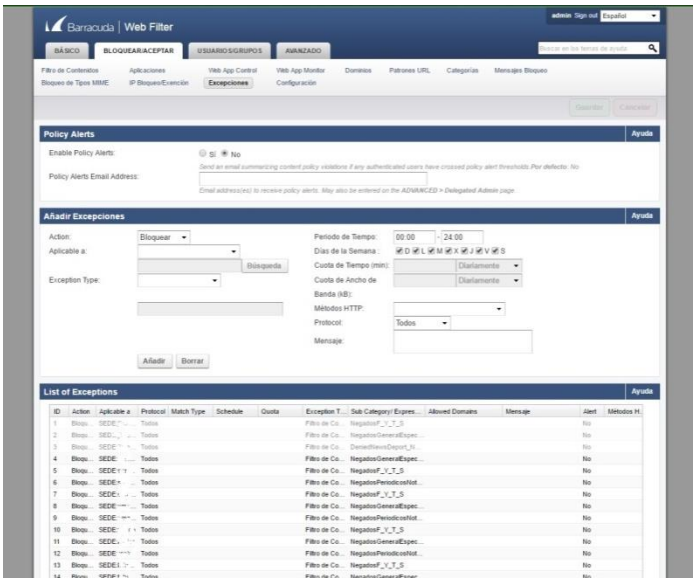


Aquí nos desplegaba una lista de los equipos que estuviesen infectados con el Ransomware que tenía la peculiaridad de cifrar todos los documentos, imágenes y videos, y les agregaba la extensión .mp3. Para detener esto utilizábamos el software barracuda antivirus y este eliminaba todas las amenazas que el antivirus Institucional no llegaba a detectar.

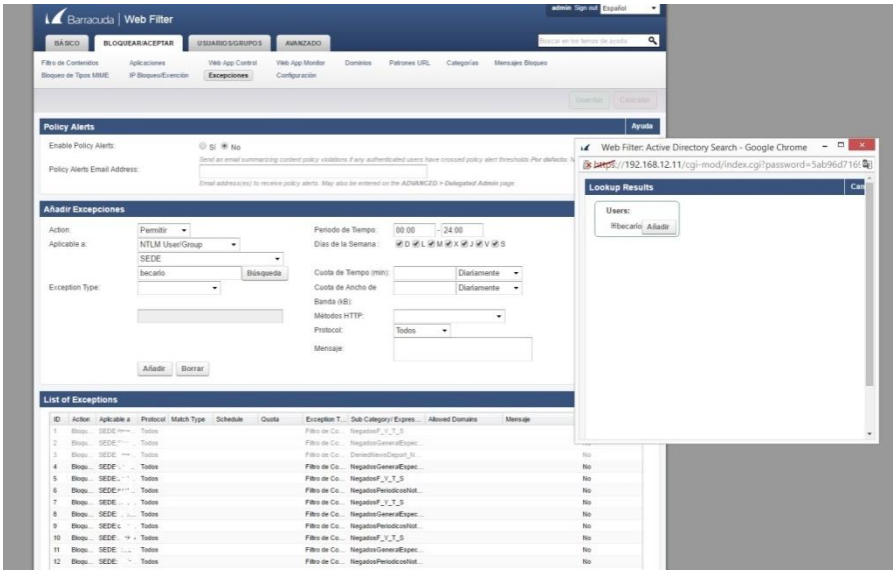
Hace un momento hable de que en esta herramienta de Barracuda Web Filter se podían bloquear las páginas, pues se bloquean en el apartado de dominio, donde se tiene una lista negra de los dominios a los cuales el Instituto tiene prohibido el acceso y una lista blanca que son los dominios permitidos para la Institución.



Mencione que a los nuevos empleados se les daba un nombre de usuario para ingresar a sus equipos e ingresar a internet, sin embargo no todos los usuarios gozan de los mismos privilegios, los directivos tienen todos los privilegios y a los empleados se les permite acceder sólo a los dominios de la lista blanca, a menos que sus superiores pidieran algunos acceso extra.



Para agregar a un usuario nuevo se tenían primero que negar los dominios restringidos, y posteriormente permitir el acceso a los dominios de la lista blanca.



Estas son algunas de las funciones que hay que llevar a cabo en la Empresa Mexicana del Petróleo con la herramienta Barracuda Web Filter.

Conclusiones

Las actividades laborales que realice en la empresa petrolera me sirvieron mucho, ya que comprendí de una manera adecuada el uso de los comandos de Linux, por otro lado me di cuenta que lo aprendido en la escuela me fue de gran utilidad ya que mis conocimientos teóricos fueron llevados a la práctica, no sólo en el ambiente de lenguajes de programación o arquitectura cliente servidor, que fueron las materias donde utilice este lenguaje, además materias como Seguridad Informática, Administración de Redes, Diseño de Sistemas Digitales, entre otras.

Además el servicio social es algo esencial para el desarrollo de las habilidades, ya que logré comprender que las actividades que se desarrollan te dan una idea más clara de los problemas, dificultades y trabajo diario a lo que nos enfrentaremos.

Algo que me agradó, fue que además de los conocimientos adquiridos en la escuela la Empresa Mexicana del Petróleo tiene grandes instalaciones, las cuales te dan un amplio conocimiento donde aplicas todos tus conocimientos como ya lo mencioné, pero además de tus conocimientos adquieres muchos otros más, de diferentes ramas de eléctrica con la que tiene que ver la ingeniería en computación, aprendí las redes de comunicaciones, en su central telefónica, vi como telecomunicaciones es un amplio campo el cual también se puede tener grandes aprendizajes.

Conocí lo que es un ambiente de trabajo y cuáles son los problemas a los que me tengo que enfrentar día con día.

Estoy agradecido con la Universidad y con la Institución por los conocimientos adquiridos, los cuales serán de gran utilidad para mi futuro y desarrollar con gran entusiasmo e interés mis actividades laborales.

Bibliografía, Referencias Electrónicas.

- PuTTY, (Marzo 2016). Obtenido de http://www.putty.org
- Álvaro Alea Fdz. (2003) Manual Linux Obtenido de http://www.ice.udl.es/
- Emilio CS (Diciembre 2014). Obtenido de http://www.aemilius.net/
- SimonTatham (2013). PuTTyUser ManualObtenidohttp://the.earth.li/
- Ben Meister (2007) PuTTYTutorial Obtenido http://www.cs.dartmouth.edu
- Javier Samaldone (2006)Tutorial GNU/Linux http://es.tldp.org/
- Seguridad Informática (2016). Obtenido de http://telmex.com
- Laboratorio de Redes y Seguridad (2012). Obtenido de http://redyseguridad.fi-p.unam.mx
- Cisco Security (2016). http://capacityacademy.com
- Cisco (2015). http://www.cisco.com
- EMP (2015) Instalacion de redes VPN.
- Comunicaciones y redes de computadores. 6ta edición, William stallings, Editorial Prentice all.
- Herramientas para elaborar tesis e investigaciones socioeducativas. Zapata, O. A. (2005), México, D.F.: Editorial Pax México.