MANUAL DE DIAGNOSTICO Y PREVENCION DE VULNERABILIDADES DE DATOS PARA PYMES

Estudiante Julián Hernán Barreto
Especialización Seguridad informática
UNAD 2018

Introducción

Este manual muestra algunas herramientas básicas de análisis de vulnerabilidades en una pyme con el fin de demostrar de una forma sencilla como evitar ataques de tipo informático y asegurar la infraestructura tecnológica para brindar una mejor seguridad tanto a la compañía como a los clientes, conservando las premisas de la seguridad informática (disponibilidad, integridad y confidencialidad de la información).

El manual está divido en dos fases, la primera fase contendrá el diagnostico, en esta fase se presentarán herramientas útiles para diagnosticar vulnerabilidades en los equipos de la pyme, la fase dos contendrá las pautas para asegurar los equipos con el fin de evitar a futuro ataques cibernéticos.

TABLA DE CONTENIDO

LISTA DE FIGURAS

Objetivo

Brindar apoyo y orientación a las pymes con respecto a la seguridad de la información mediante el manual de uso

Alcance

Esta buena práctica reunida en el manual de seguridad propuesto se deberá aplicar a todo el equipo en red del personal vinculado laboralmente con la pyme y los contratistas y terceros que tengan acceso a los recursos de información de la organización

Responsabilidades

El propietario de la pyme o en su defecto el encargado del área de informática deberá establecer unas directrices claras para dar soporte a la Seguridad de la Información, a través de la puesta en vigencia y mantenimiento del uso del manual de Seguridad informática para la pyme en la organización. Tendrá la responsabilidad primaria de documentar, actualizar e implantar Políticas y controles actualizados o que se evidencian en el uso diario de las tecnologías con el fin de estar siempre a la vanguardia de nuevos ataques informáticos, además deberá ser responsable de la actualización de los sistemas informáticos por un periodo no mayor a un mes

GLOSARIO

ATAQUE PASIVO: esta técnica solo se basa en obtener información del sistema, no altera ningún componente informático.

CÓDIGO MALICIOSO: programa instalado en el equipo sin previo conocimiento del usuario que tiene como objetivo perturbar el funcionamiento del sistema.

CONFIDENCIALIDAD: asegura que la información es utilizada solo por las personas autorizadas para ello.

DIRECTIVAS DE GRUPO: es un conjunto de reglas que controlan el entorno de trabajo de un usuario denegando funcionalidades del sistema que por perfil no debería ejecutar.

DISPONIBILIDAD: asegura que los usuarios autorizados tengan acceso a la información cuando ella es requerida.

ESCANEO DE RED: tiene por objetivo realizar una búsqueda de direcciones ip y puertos en una red de área local LAN.

FIREWALL: está diseñada para bloquear tráfico de datos tanto de entrada como de salida permitiendo así autorizar o denegar acceso a determinado servicio.

GUSANOS INFORMÁTICOS: tiene la propiedad de duplicarse en si, causando daños al sistema operativo.

INTEGRIDAD: Asegura que la información sea exacta y completa.

LAN: Red de Área Local, comúnmente utilizada para interconectar dispositivos de computo en un espacio geográfico determinado.

MITM: Hombre en el medio, es un tipo de ataque que tiene por objetivo escuchar o recepcionar los datos entre dos víctimas con el fin de ser capaz de manipular la información a conveniencia (leer, insertar y modificar).

PRIVILEGIOS DE ADMINISTRADOR: Rol en un sistema con capacidad de modificar cualquier componentes u objeto del sistema.

PROTOCOLO TCP: Protocolo de Control de Transmisión, este protocolo se compone de tres etapas, establecimiento de conexión, trasferencia de datos y fin de conexión.

PROTOCOLO UDP: Protocolo de nivel de trasporte, a diferencia de TCP el udp envía una petición y no espera respuesta es utilizado para servicio de DHCP y DNS.

PROXY: Parámetro de Windows que permite configurar el acceso a internet.

RIESGO: Posibilidad de que se explore una vulnerabilidad en un sistema y exponga la información o hardware a posible daño o perdía de información.

SISTEMA OPERATIVO: Agrupación de software que permite entregar al usuario una interfaz amigable, gestiona recursos de hardware y provee servicio a los programas de software, ejemplo sistema operativo Windows 7.

SNIFFER: Permite capturar todo el tráfico de red que cursa desde una interfaz de red.

SSH: interprete de ordenes seguro, sirve para acceder a maquinas remotas de forma segura, conserva la integridad de la conexión por medio de terminales cifradas en la comunicación entre el usuario y el equipo remoto

TERMINALES REMOTAS: Equipos conectados a la red de acceso remoto como ejemplo carpetas compartidas sitios ftp u acceso remoto a equipos en otra red de ordenadores.

TRAFICO DE RED: Trasmisión de datos en una red o grupo de trabajo.

TROYANOS INFORMÁTICOS: es otro tipo de código malicioso que tiene por objetivo tomar posesión del sistema operativo con fines delictivos.

VLAN: creación de redes lógicas dentro de una misma red física.

VULNERABILIDADES: Configuraciones incorrectas y malas prácticas de los sistemas que ponen en riesgo la confidencialidad de la información.

FASE 1 DIAGNOSTICO

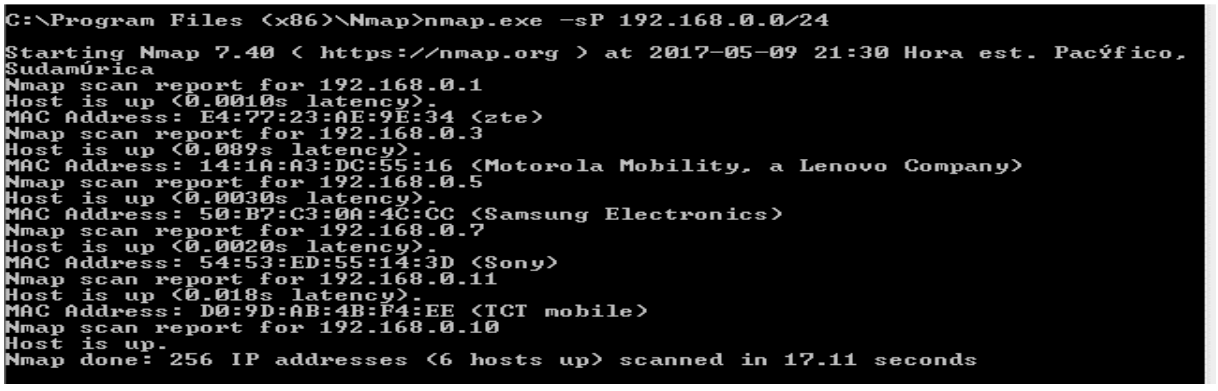
PUERTOS DE CONEXIÓN TCP

Esta fase evaluara el nivel de riesgos que tienen sus sistemas de información, para ello se debe utilizar una herramienta de prueba de penetración pasiva que busca como objetivos revisar que tal vulnerable están los equipos:

Como primera herramienta se utilizará nmap, esta herramienta realiza un ataque pasivo en busca de puertos abiertos y detección de sistema operativos, contiene múltiples comandos que permiten realizar un escaneo de red, esta herramienta es compatible con sistemas operativos Linux o Windows y se puede descargar de la siguiente URL https://nmap.org/ , en donde se podrá interactuar a modo de consola o grafico según la preferencia. el comando que se utilizara a continuación es -sP que significa **s** Sondeo **P** ping equipos que están presentes en la red.

Lo primero es realizar un escaneo a la red para determinar que equipos están disponibles o presentes, con el comando nmap -sP (sondeo Ping) más la red ejemplo: (192.168.0.1/24) se obtendrán las direcciones IP´S de los equipos que están encendidos y presentes en la red LAN

FIGURA 1 ESCANEO DE RED

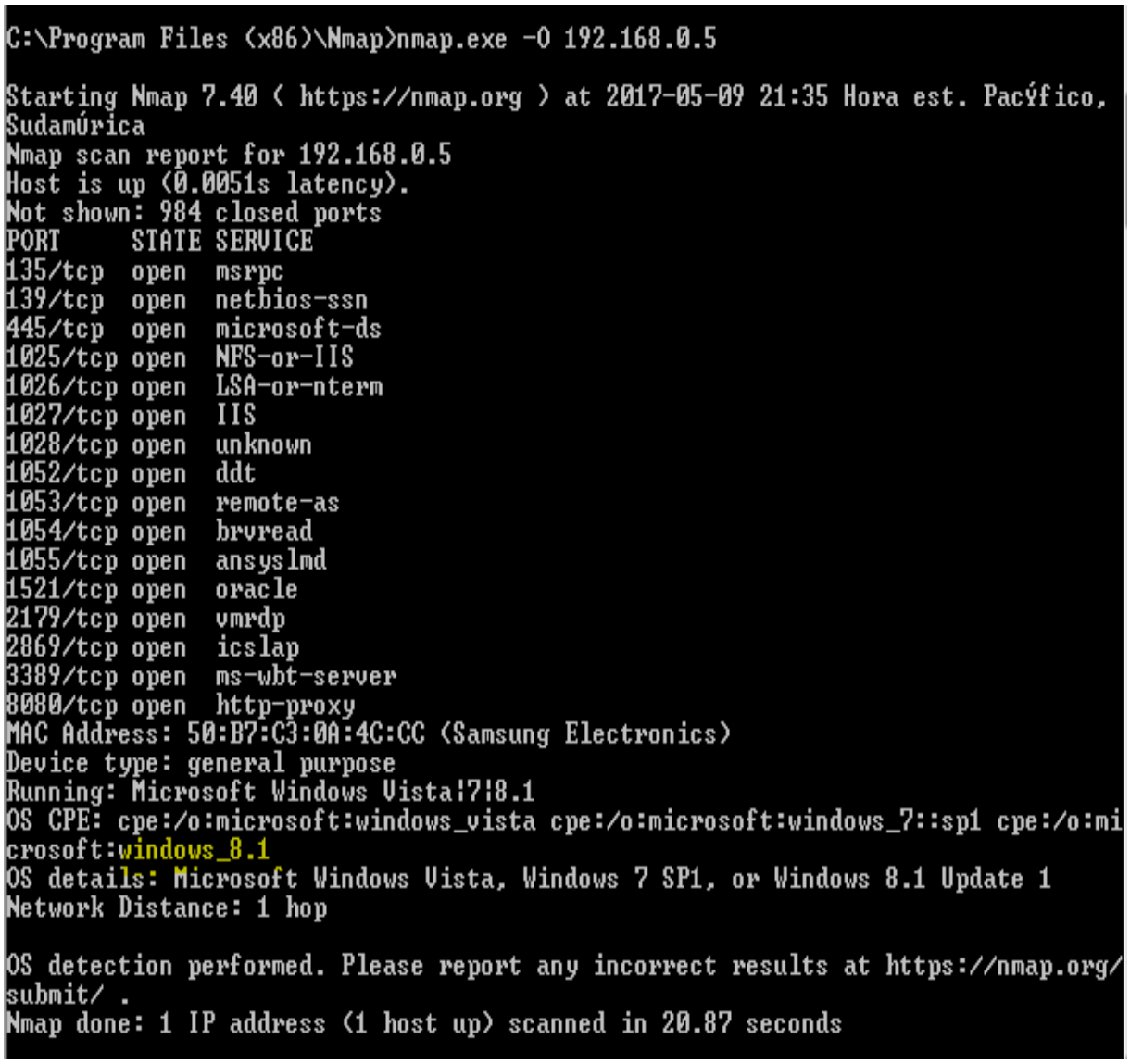


Fuente: Autor

Con el siguiente comando: nmap -O + la ip, se puede observar los puertos y el tipo de sistema operativo que tiene el equipo objetivo, se debe evaluar cada uno de los puertos, el rol que cumple el equipo (usuario o servidor) y finalmente revisar la

viabilidad técnica de cerrar los puertos que no son necesarios para la labor diaria del funcionario, esto ayudara a iniciar el control de seguridad en la red de trabajo.

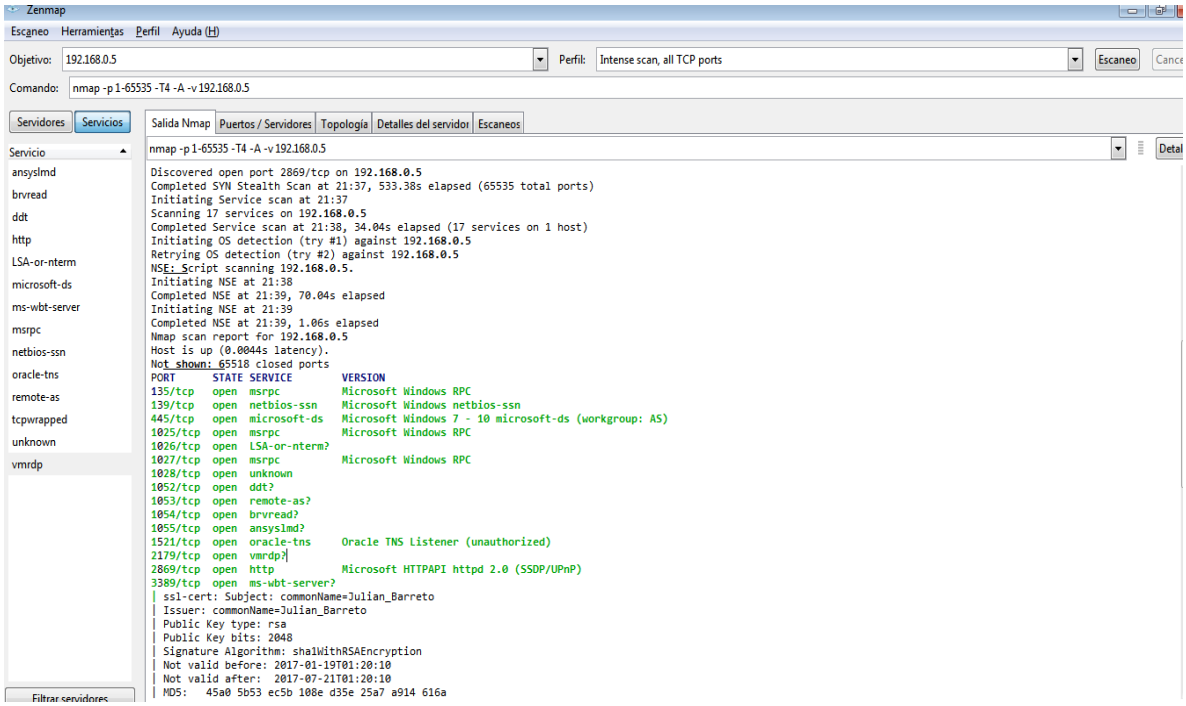
FIGURA 2 ESCANEO DE PUERTOS



Fuente: Autor

La siguiente imagen muestra la interfaz gráfica de nmap, instalada en un sistema Windows.

FIGURA 3 INTERFAZ GRAFICA ZENMAP



Fuente: Autor

PERMISOS DE USUARIO:

Es necesario que el usuario de acuerdo a su rol de trabajo en la compañía no tenga ningún privilegio especial sobre los equipos de cómputo que utiliza a diario ya que esto conlleva a que el usuario manipule a conveniencia el sistema, se deberá restringir de manera inicial y permanente los privilegios de instalación de software dado a que muchas veces los usuario instalan programas en los equipos que abren puertos innecesarios comprometiendo el sistema a adquirir virus y a iniciar ataques informáticos . Se debe tener en cuenta que ningún equipo de usuario debe tener puertos abiertos por seguridad a menos de que ejecute algún programa o servicio que requiera la apertura de algún puerto en especial, los siguientes puertos son necesarios en un equipo que tenga rol de servidor:

- 21 puerto de FTP. Permite subir servicio para compartir archivos en la red y acceder a sitios que se encuentran en servidores FTP.
- 25 SMTP Puerto de email. Se utiliza para conexión al servidor de correo electrónico.
- 80 puerto del HTTP. Permite publicar sitios web mediante un servidor web
- 110 POP3 Puerto de email. Uso del correo electrónico.

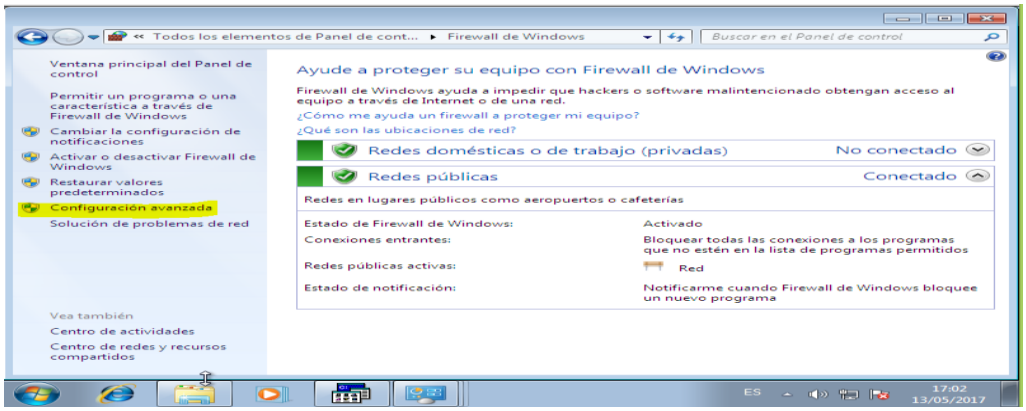
Como medida de prevención el usuario que no maneja ninguno de los servicios se puede optar por cerrarlos.

FIREWALL:

El firewall o cortafuegos, es un equipo de hardware o software que controla el tráfico de red permitiendo o denegando peticiones de comunicación mediante reglas o políticas configuradas por el administrador ,la ubicación de este equipo es en el punto de conexión interna de los equipos con la conexión externa (internet) ,teniendo en cuenta que la pyme no maneja en algunos casos un equipo dedicado para tal fin se aconseja utilizar el firewall de Windows, el cual se deberá configurar en cada uno de los equipos de cómputo asignados a los usuarios y de acuerdo a la justificación de cierre incensario de puertos , realizando los siguientes pasos:

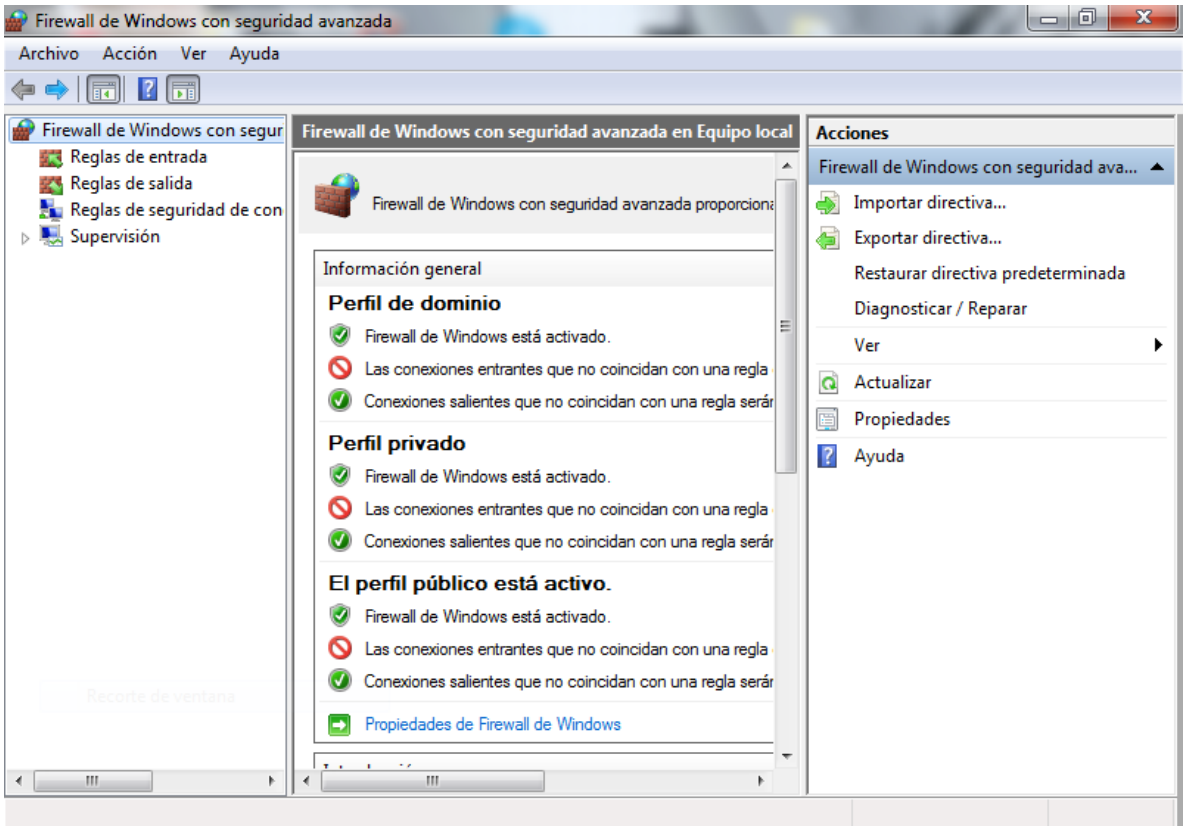
Inicio/Panel de control firewall de Windows

FIGURA 4 CONFIGURACION FIREWALL WINDOWS



Fuente: Autor

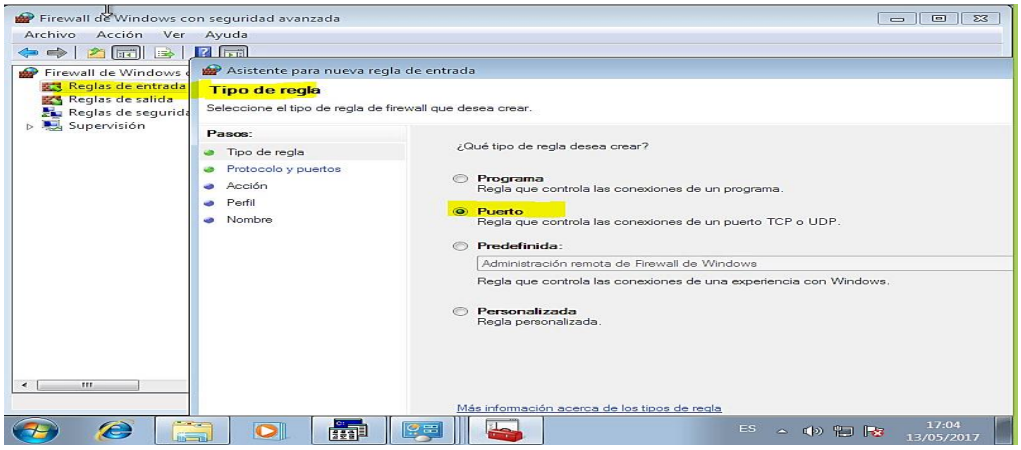
FIGURA 5 PANEL DE CONFIGURACION FIREWALL WINDOWS



Fuente: Autor

Clic derecho nueva regla.

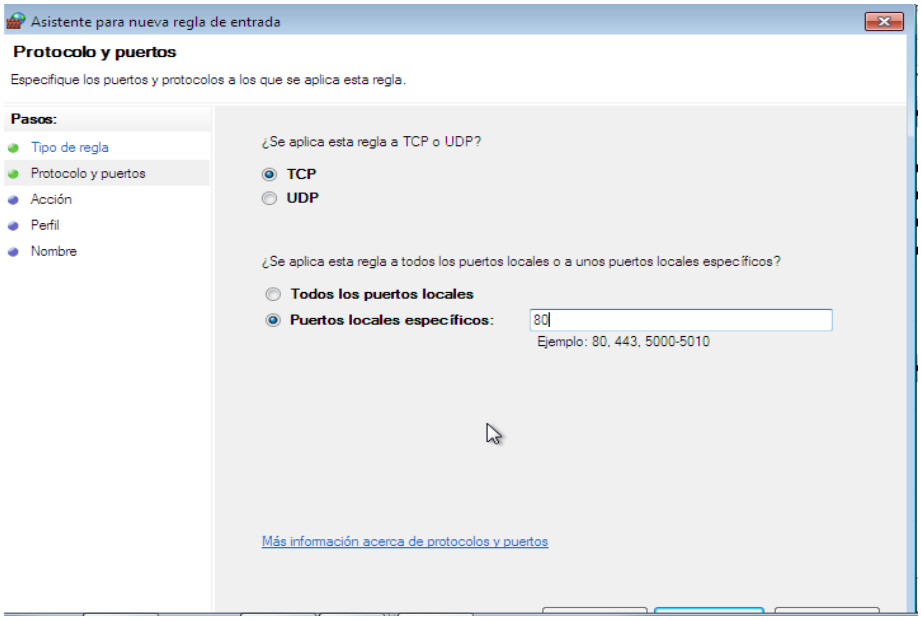
FIGURA 6 CONFIGURACIÓN FIREWALL WINDOWS



Fuente: Autor

Definir el tipo de protocolo sea UDP o TCP, normalmente los servicios web o de correo manejan puertos tcp los cuales manejan comunicación en los dos sentidos el puerto UDP maneja la comunicación en un solo sentido, para este ejemplo se bloqueará el puerto 80

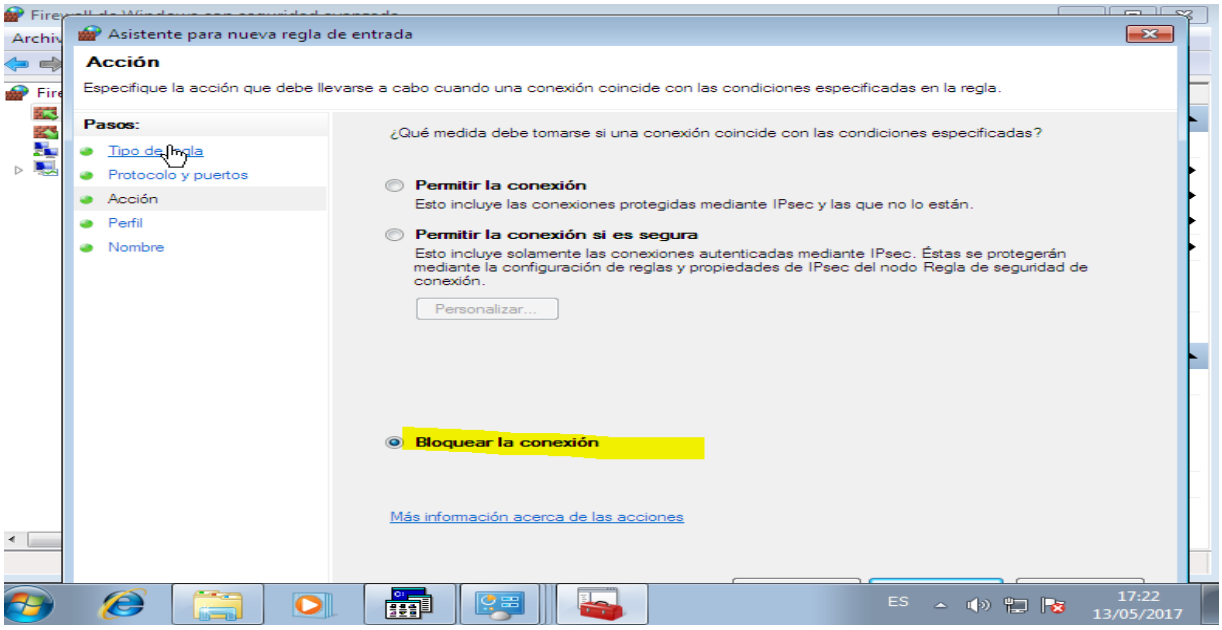
FIGURA 7 CONFIGURACIÓN FIREWALL WINDOWS



Fuente: Autor

Seleccionar la opción bloquear

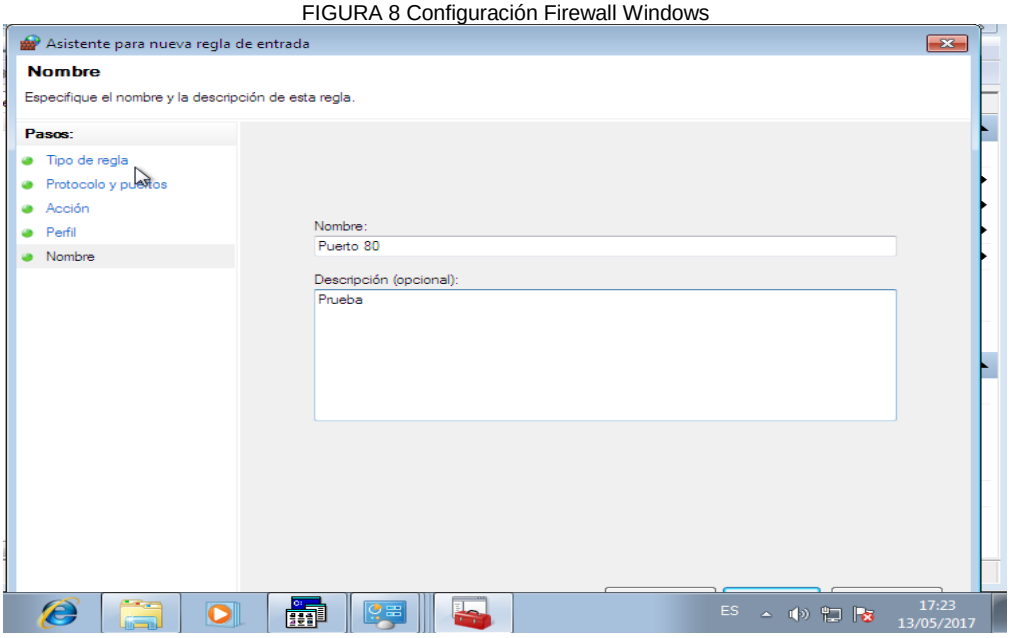
FIGURA 8 CONFIGURACIÓN FIREWALL WINDOWS



Fuente: Autor

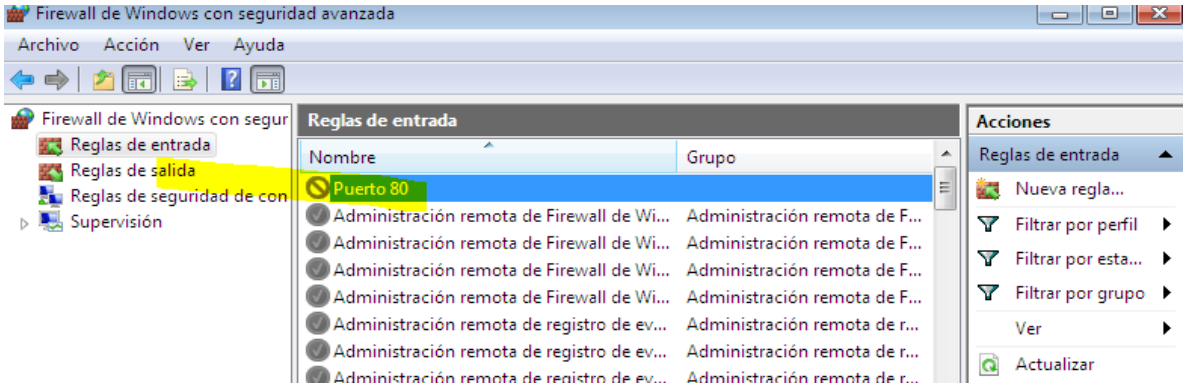
Nombre distintivo de la nueva regla.

FIGURA 8 Configuración Firewall Windows



Fuente: Autor

FIGURA 9 CONFIGURACIÓN FIREWALL WINDOWS



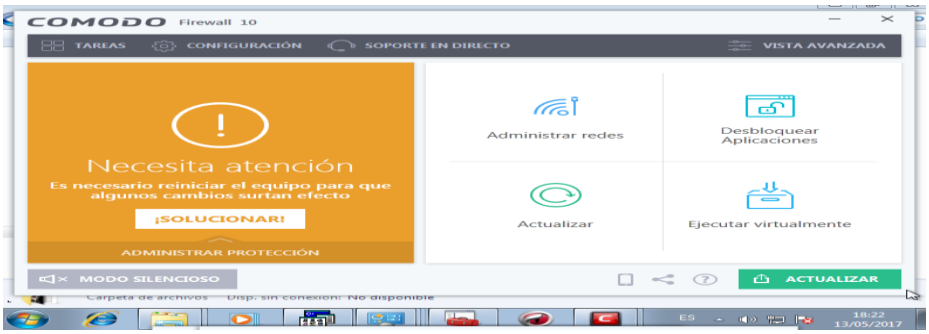
Fuente: Autor

Los antivirus son importantes para detectar y eliminar tráfico en los equipos de los usuarios finales, no obstante, hay varias herramientas gratuitas que ayudaran a garantizar el bloqueo de tráfico no deseable asegurando la conectividad de los equipos a la LAN de la Pymes.

Como un ejemplo esta la siguiente herramienta llamada, Comodo Firewall, esta herramienta permite controlar la ejecución de aplicaciones y el ingreso y salida a páginas web, además vigila puertos de escucha

Consola de la aplicación

FIGURA 10. FIREWALL



Fuente: Autor

Para las pymes que cuentan con un firewall perimetral ya sea a nivel de software o hardware, es necesario que se bloquee tráfico entrante innecesario, muchas veces las solicitudes de las áreas operativas no son específicas y esto causa que la apertura de puertos arbitrarios genere una vulnerabilidad inminente. Se sugiere tener presente los siguientes puntos:

- Asegurar que todos los equipos de la red pasen por el firewall
- Cerrar los puertos innecesarios de entrada con el fin de evitar posibles ataques informáticos.
- Las publicaciones de servicios (páginas Web, Servicios de correo, FTP) hacia internet deben estar en una zona desmilitarizada DMZ.
- Limitar en esta zona, solo tráfico necesario como http ftp etc., los demás puertos deben estar cerrados por seguridad.

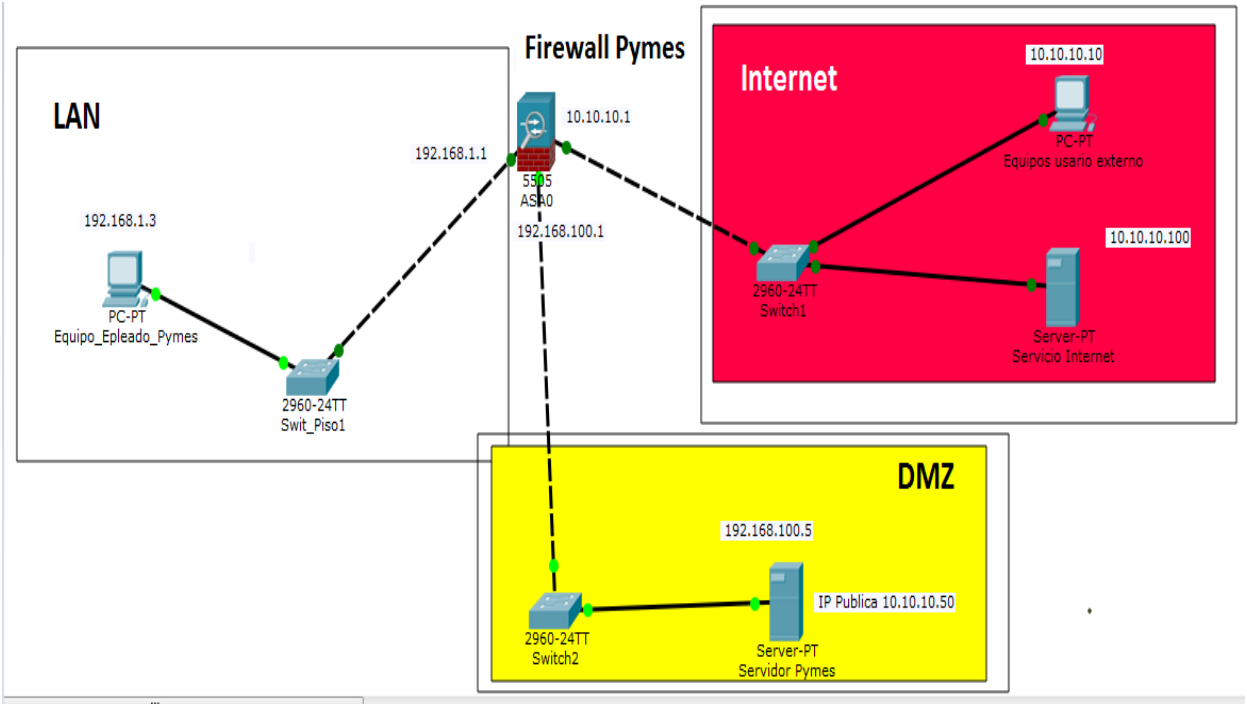
El siguiente diagrama demuestra un esquema de seguridad perimetral, donde se evidencian tres zonas de red (LAN, DMZ e internet) estas zonas manejan un nivel de seguridad diferente:

Zona LAN, esta zona debe tener mayor seguridad de entrada, debe tener acceso a la DMZ para poder compartir archivos, modificar publicaciones web, además debe tener acceso a internet todo el tráfico permitido es de salida para consultar servicios, el tráfico entrante es denegado para bridar mayor seguridad.

Zona DMZ, en esta zona están los servidores Web, FTP, DNS y demás recursos que comparta la pymes hacia internet, esta zona maneja un nivel de seguridad medio y solo se deberá permitir tráfico de entrada de acuerdo al servicio ofrecido por la pymes, se debe denegar acceso a la zona LAN, es necesario evaluar que puertos se deben cerrar para brindar una mayor seguridad, el tráfico ICMP como sugerencia debe ser denegado con el fin de no exponer el servicio a ataques de denegación de servicio.

Zona de internet, esta zona no maneja seguridad y esta todos los servicios que la pymes puede consultar hacia internet, deberá tener acceso a la zona DMZ para que los usuarios externos a la pymes puedan usar los servicios ofrecidos por la misma y no deberá tener acceso a la Zona LAN.

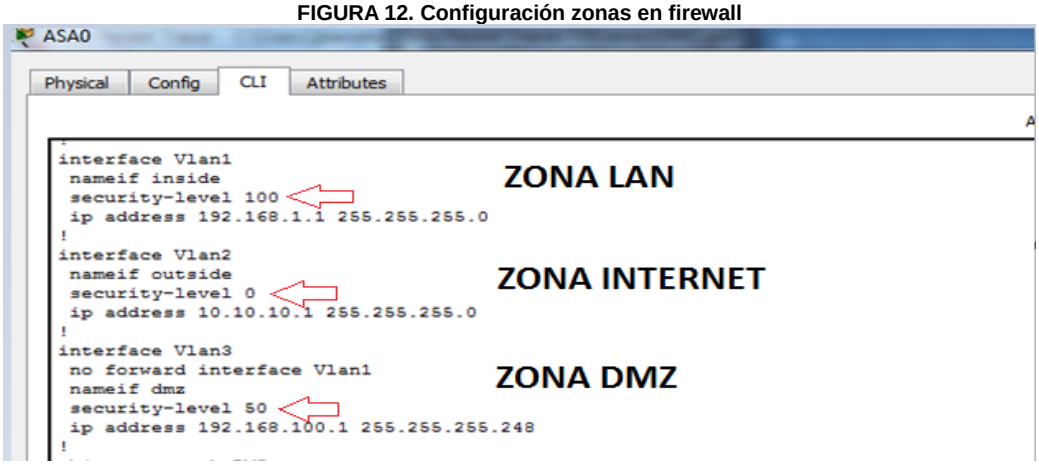
FIGURA 11. Zona dmz pymes



Fuente: Autor

La siguiente imagen muestra la configuración de nivel de seguridad en las zonas mencionadas.

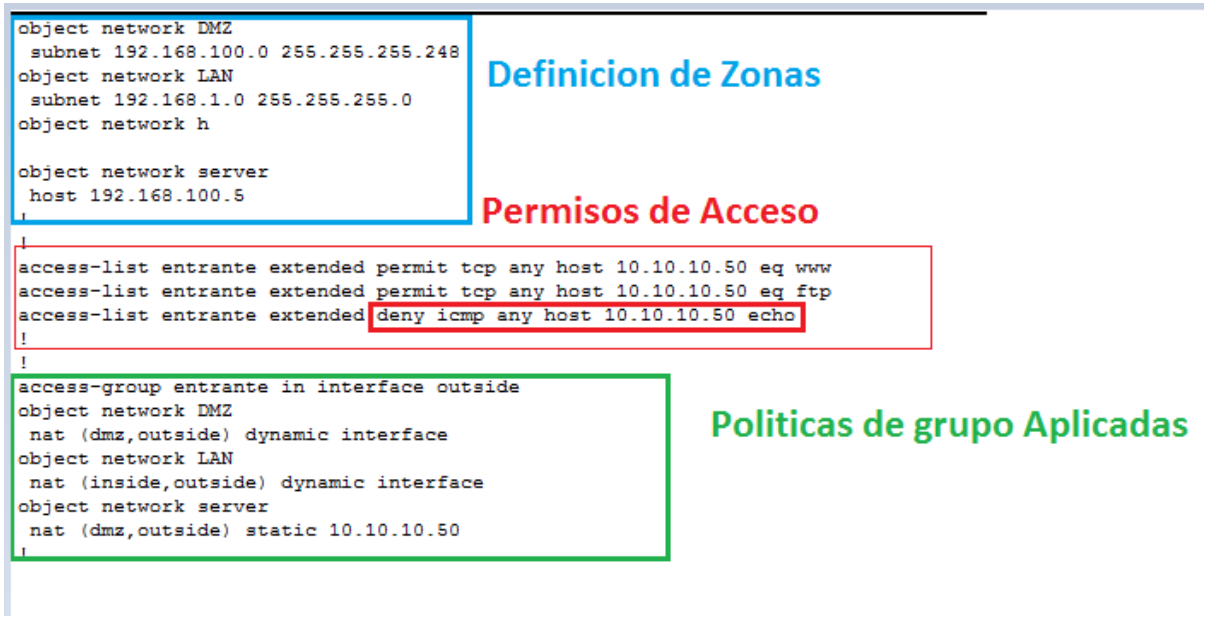
FIGURA 12. Configuración zonas en firewall



Fuente: Autor

Mediante la creación de objetos en el Firewall, se deberá definir los puertos permitidos de acuerdo a los servicios que ofrece la pyme, para este caso los servicio son (servicio web y servicio ftp), por seguridad se bloquea el tráfico ICMP.

FIGURA 13. configuracion firewall

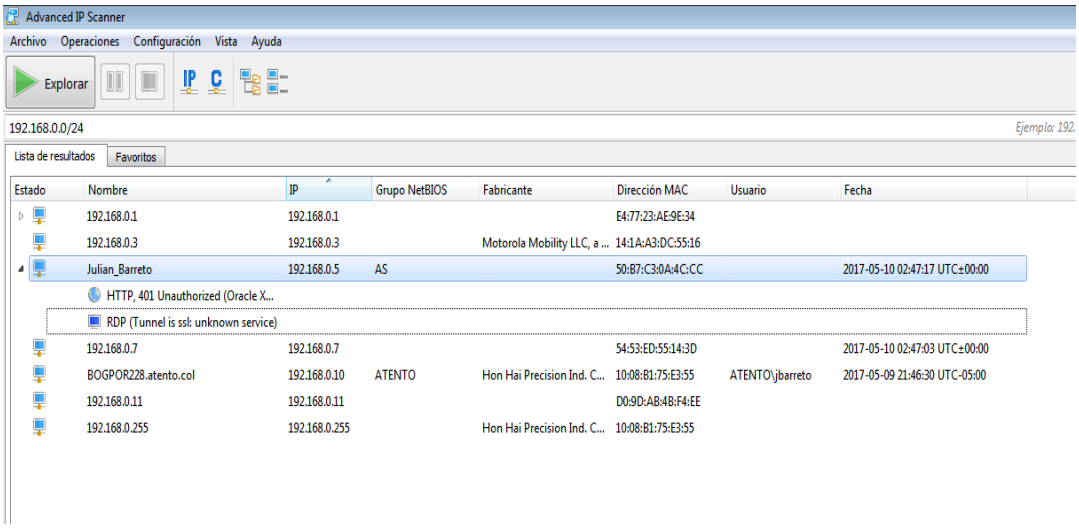


Fuente: Autor

HERRAMIENTA ÚTILES DE ESCANEO DE RED:

Otra herramienta útil para escaneo de equipos es Advanced IP Scanner la cual se puede descargar del sitio oficial https://www.advanced-ip-scanner.com/es/ , esta herramienta es gratis y realiza un escaneo profundo en la red e informa los equipos que tiene conexiones compartidas y termínales remotas activas, además con este software es posible verificar quien esta logueado en la máquina y muestra información de sistema operativo con la correspondiente dirección física MAC

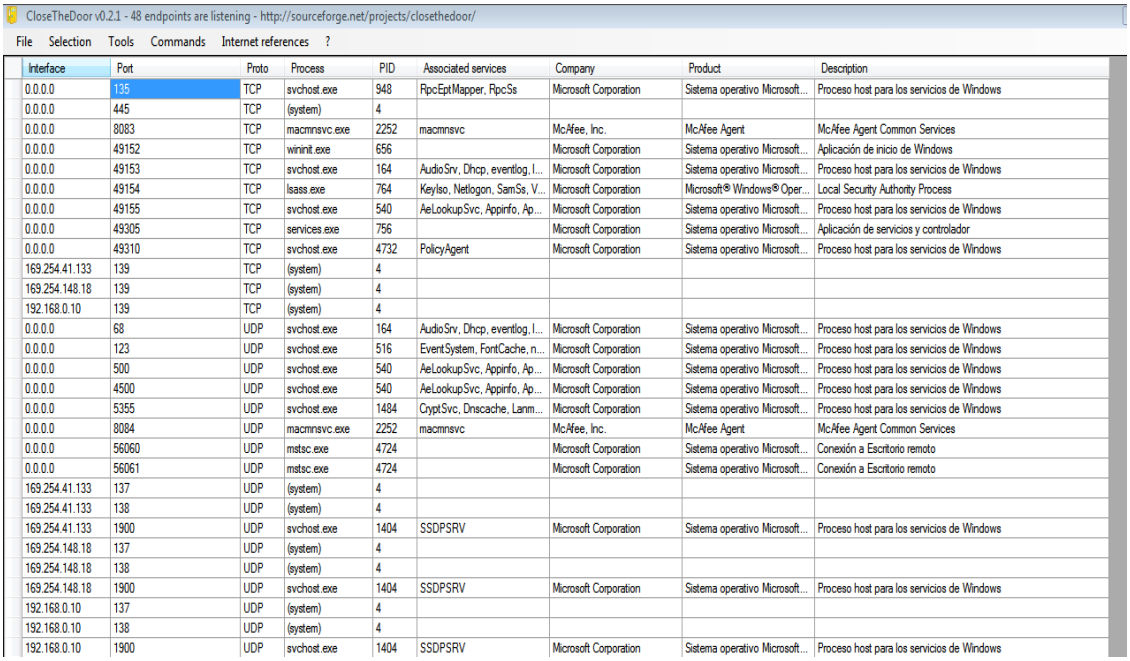
FIGURA 14 ESCANEO DE RED CON ADVANCED IP



Fuente: Autor

La herramienta CloseTheDoor es otra herramienta útil la cual ayudara a identificar los puertos desconocidos para tomarla decisión de cerrarlos según su uso

FIGURA 15 ESCANEO PUERTOS LOCALES

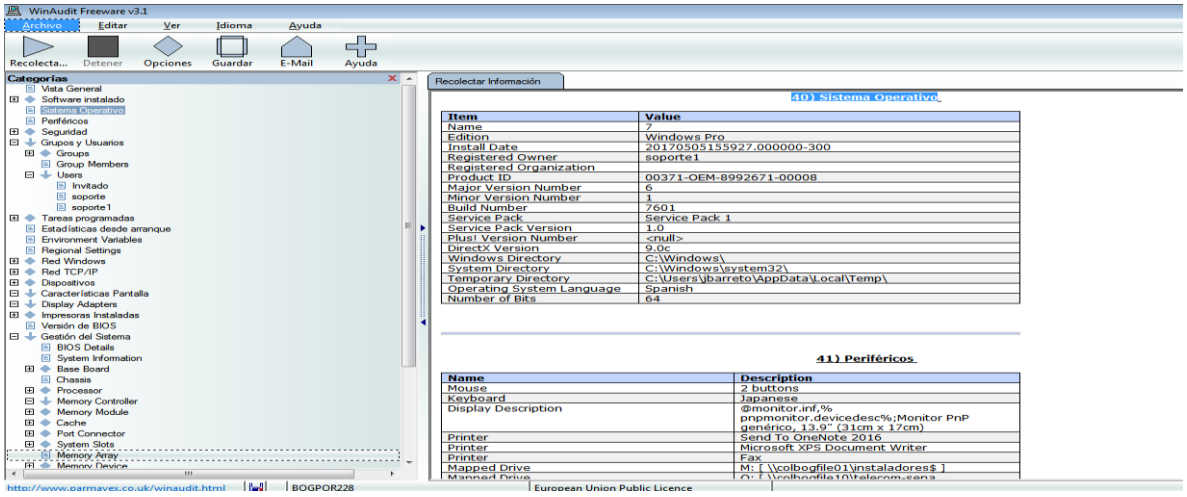


Fuente: Autor

La herramienta Winaud es gratis y básicamente realiza una inspección minuciosa al sistema operativo, el resultado es un informe detallado del software que se tiene instalado, los grupos creados en el sistema y los usuarios con privilegios, además

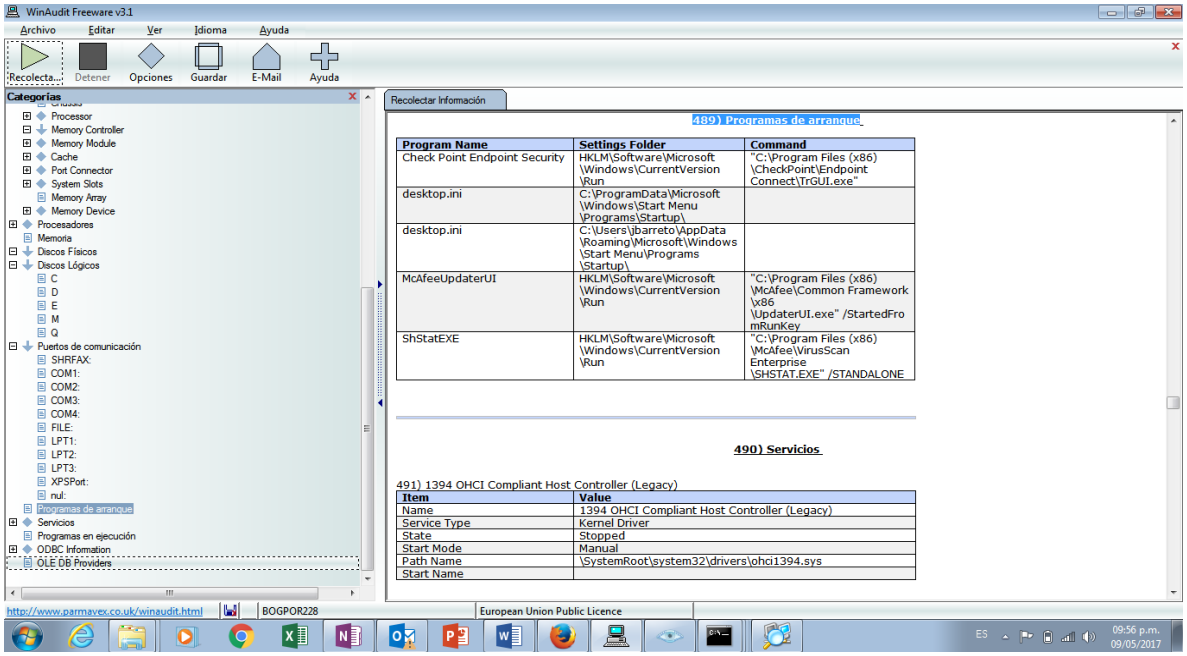
muestra un resumen del sistema operativo a nivel de hardware e información de la configuración de red.

FIGURA 16 AUDITORIA EQUIPO CON WINAUD



Fuente: Autor

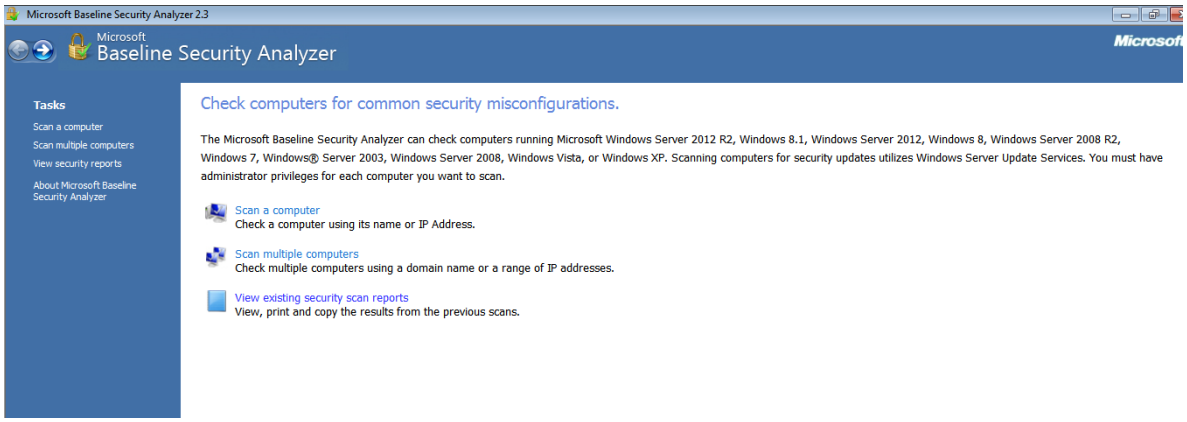
FIGURA 17 AUDITORIA EQUIPO CON WINAUD



Fuente: Autor

La herramienta de Microsoft Baseline security detecta las vulnerabilidades en los equipos de forma local o remota, esta herramienta se puede utilizar para determinar los riesgos que tienen los equipos de usuario y servidores

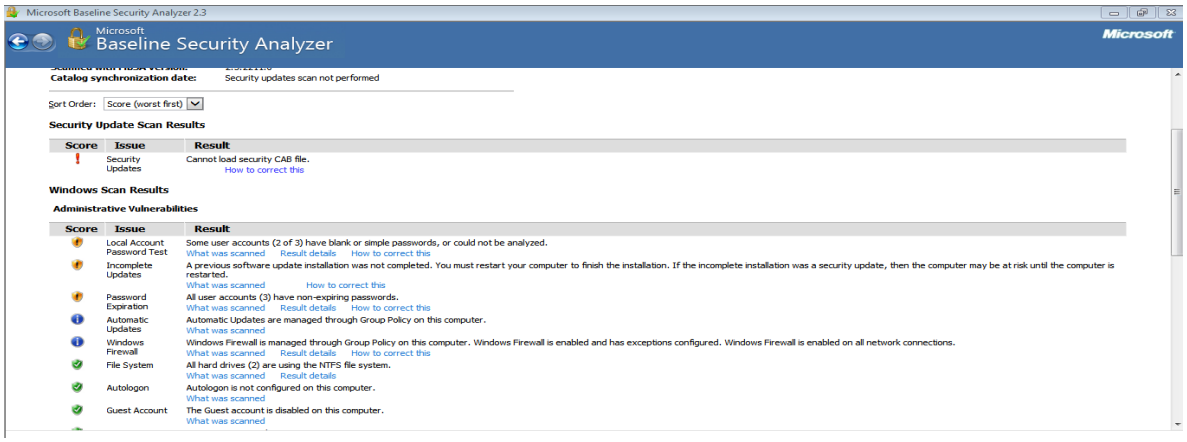
FIGURA 18 AUDITORIA EQUIPO CON MICROSOFT BASELINE SECURITY ANALYZER 2



Fuente: Autor

Para comprobar su funcionamiento se realiza una prueba de verificación de vulnerabilidades, se encuentra que el equipo de prueba no cuenta con actualizaciones de seguridad, además tiene un riesgo con los usuarios generados los cuales no cumple con la complejidad de contraseñas

FIGURA 19 PRUEBA AUDITORIA EQUIPO CON MICROSOFT BASELINE SECURITY ANALYZER 2



Fuente: Autor

FASE 2 PREVENCIÓN

ASEGURAMIENTO EQUIPOS DE USUARIOS:

Software malicioso

El software ataca principalmente a los equipos de usuarios ingenuos y redes LAN, que sin darse cuenta abren los sistemas a los delincuentes informáticos, los cuales tienen como objetivo robar la información o simplemente dañar el sistema de información, entre el software malicioso se tienen los virus informáticos, los gusanos, los troyanos entre otros. Este tipo de software malicioso tiene la capacidad de reproducirse y causar un grave daño no solo en un equipo, sino a una red completa de computadoras por consiguiente al ser detectado se le debe tratar con prioridad alta, para esto y como medida de prevención se deben asegurar los siguientes puntos en Cada uno de los equipos de usuario con el fin de evitar estos ataques.

Antivirus

El uso de un buen antivirus es importante para la compañía, los controles que se implementen en la organización no son suficiente para garantizar la seguridad de la información, las infinidades de ataques informáticos que surgen a diario, y las malas prácticas del usuario ponen en riesgo los sistemas de información, es necesario siempre estar a la vanguardia actualizando y verificando que antivirus protege de forma robusta la información.

En la actualidad los antivirus ofrecen muchos mecanismos de protección que van desde una la detección de malware hasta la protección de datos mediante backup en un sitio en internet ,la mayoría de antivirus ofrecen pruebas gratuitas para verificar el producto, no obstante en estas pruebas no ofrecen el producto por completo ,es aconsejable comprar el paquete de seguridad completo con el fin de proteger la información, la mayoría de estos productos oscilan entre $85.000 a $200.000 por cada PC , a continuación se relacionan tres tipos de antivirus en el mercado describiendo sus correspondientes características.

Karpesky:

Es una compañía de origen ruso dedicada a la seguridad informática garantiza la protección a más de 300 millones de usuarios. Maneja tres productos en el mercado:

Antivirus, cuenta con las protecciones necesarias para evitar spyware, phishing y sitios web peligrosos tiene un costo anual por cada PC de $69.000 al año.

Internet Security: este paquete incluye protección para equipo móviles con la misma licencia, ofrece seguridad en las transacciones en internet, ofrece filtro de contenidos en internet para niños. tiene un costo anual de $117.000 al año.

Total, Security: este paquete incluye todas las características anteriores, además incluye cifrado de contraseñas y copias de seguridad en internet tiene un costo por cada PC de $165.000 al año

ESET Internet Security:
Es una compañía de origen eslovaco, fundada en 1992 y fusionada con dos compañías privadas con presencia en más de 161 países, maneja un producto completo que tiene las siguientes características:

Sistema de prevención de intrusiones basado en el host (HIPS) - Permite personalizar la conducta del sistema con mayor detalle. Ofrece la opción de especificar reglas para el registro del sistema y los procesos y programas activos, de modo que permite ajustar la postura con respecto a la seguridad.

Protección contra ataques basados en scripts - Detecta ataques causados por scripts maliciosos que intentan aprovechar vulnerabilidades de Windows PowerShell. También detecta scripts maliciosos de JavaScript que pueden atacar a través de su navegador. Protege los navegadores Mozilla Firefox, Google Chrome, Microsoft Internet Explorer y Microsoft Edge.

Control de Webcam y Router - muestra un mensaje de alerta si alguien intenta acceder a tu cámara Web. Te permite revisar la seguridad de tu router y controlar quién está conectado.

Protección contra ataques de red - Protege todas las comunicaciones, ya que bloquea los ataques que intentan aprovechar las vulnerabilidades de la red.

Protección para Banca y Pagos en línea - Esta funcionalidad permite asegurar transacciones y pagos en línea en sitios bancarios y ayuda a estar protegido en cada una de las compras en línea. Viene con una nueva interfaz de usuario y es totalmente compatible con Windows®10.

Protección contra Botnets - Se trata de una novedosa tecnología que te protege de las infiltraciones por malware de tipo botnet: no solo previene el envío de spam sino que también evita que se lleven a cabo ataques de red desde el equipo.

Bloqueo de Exploits - Bloquea los ataques diseñados específicamente para evadir la detección antivirus. Detiene amenazas dirigidas y te protege ante ataques en navegadores Web, lectores de PDF y otros programas, inclusive software basado en Java.

Exploración Avanzada de Memoria - Mejora la detección de códigos maliciosos persistentes que utilizan varias capas de cifrado para ocultar su actividad.

Control Parental - Permite definir qué contenidos podrán ser accedidos en Internet. Elige entre más de 20 categorías o define accesos a sitios específicos.

Anti–Phishing - Realiza transacciones en línea de manera segura y evita que sitios fraudulentos obtengan información personal.

Firewall Personal - Evita que intercepten información y que el equipo este en un estado invisible mientras están conectados en redes WI-FI públicas. Define distintos perfiles para la conexión que se utiliza.

Antispam - ESET Internet Security se encarga de los molestos mensajes de correo no deseados con un filtro para spam más pequeño, veloz y eficaz. Se integra con los clientes de correo electrónico más populares, Windows Mail, Windows Live Mail y Mozilla Thunderbird.
Control Avanzado de Medios Removibles - Permite definir qué tipos de dispositivos pueden ser utilizados o no dentro del equipo, se podrá crear reglas para unidades USB, CD o Firewire entre otros. Además, al momento de conectar uno de estos dispositivos se podrá explorar en busca de amenazas.[1] ,tiene un costo por cada pc de $144.000 por año.

Gdatasoftware:

Es una compañía de origen alemán la cual ofrece como las demás compañías de antivirus soluciones de seguridad informática, fue fundado en el año 1985.Sus principales características son:

protección contra malware aún desconocido. G DATA Antivirus lo detecta debido a su comportamiento notable.

[1]Antivirus eset ,{en línea} {diciembre de 2017} Disponible en: https://co.tienda.eset-la.com/eset-internet-security?gclid=CjwKCAiAu4nRBRBKEiwANms5W6N_2THh92LGXEN0xcVAwF_oFGyCjGdc6DO0VQBwmpr5wbYolFrZeBoCQSEQAvD_BwE

Escanea el correo electrónico entrante y los archivos adjuntos en busca de contenido sospechoso. Los peligros se detectan antes de que algo haya sucedido.
Protección de explotación.

Protege los equipos contra delincuentes que explotan agujeros de seguridad en aplicaciones de Office y lectores de PDF, por ejemplo.

Anti-Ransomwareoptimized
No hay oportunidad para extorsionar troyanos: se impide que los delincuentes encripten los archivos.

Protección contra dispositivos USB manipulados que pretenden ser teclados, aunque parezcan memorias USB o discos duros externos.

Gestión de actualizaciones
Especifique cuándo y dónde su PC carga las actualizaciones. Esto le ayuda a evitar costos adicionales al iniciar sesión en una WLAN de un tercero[2]
El costo del único paquete por cada PC es de $90.000 por año.

Creación de cuentas de Red:

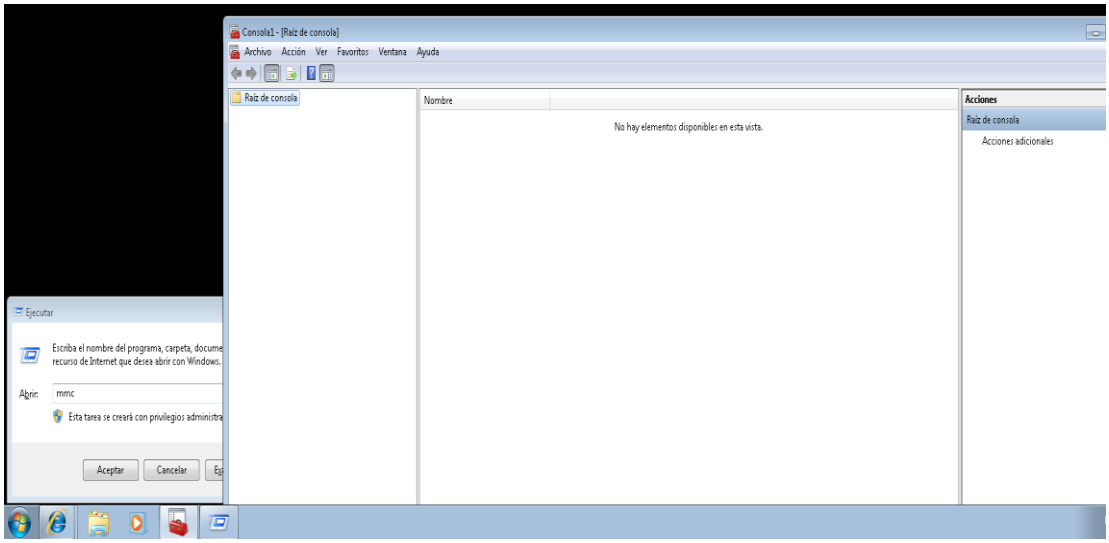
Usualmente la pyme no tiene un controlador de dominio y sus cuentas de acceso al sistema normalmente son locales de cada equipo teniendo en cuanta esta premisa, se deben crear en los equipos de usuarios dos cuentas, una cuenta deberá tener perfil de administrador y la otra cuenta con privilegios limitados será la del usuario o empleado con el objetivo de controlar el uso del sistema.

La cuenta de administrador de sistema operativo Windows por defecto se debe deshabilitar, esta cuenta normalmente esta creada en sistemas Windows y no tiene contraseña por consiguiente se debe deshabilitar y crear una nueva cuenta con nombre alusivo a tecnología o con otro nombre relevante para la compañía, esto evitará que el atacante o personal ajeno a la compañía tenga conocimiento del usuario de acceso, este nuevo usuario se deberá agregar al grupo de usuario administradores del sistema.

En las siguientes imágenes se demuestran los pasos para realizar la creación y des habilitación de la cuenta de administrador.
Es necesario ejecutar la consola de Windows mmc , para sacar esta opción pulsar las teclas “Windows+R” y en la ventana ejecutar escribir mmc y finalmente la tecla enter.

[2] Antivirus gdatasoftware ,{en línea} {diciembre de 2017} Disponible en: https://www.gdatasoftware.com/antivirus-for-windows

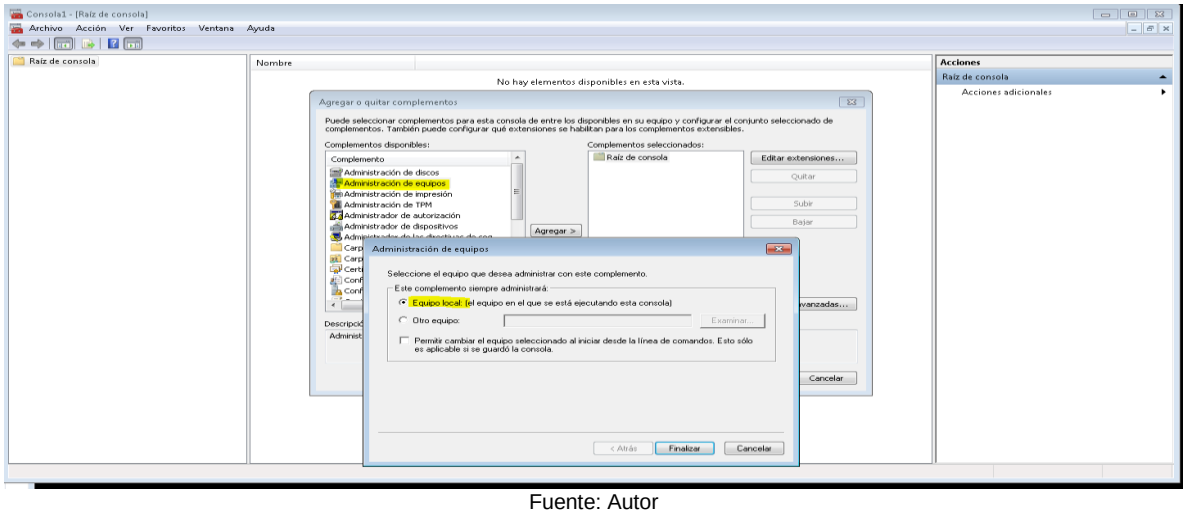
FIGURA 20 CONSOLA MMC



Fuente: Autor

Posterior a ejecutar el comando se abrirá una nueva ventana de nombre consola, se debe ir a Archivo y dar clic en agregar o quitar complementos allí se debe agregar administración de equipos seguido Equipo local como se muestra en la siguiente figura

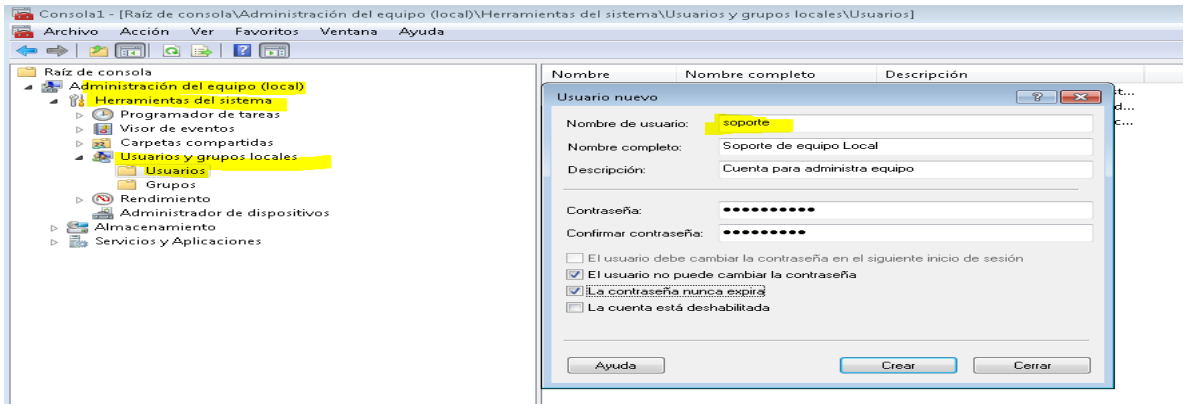
FIGURA 21 ADMINISTRACIÓN DE EQUIPO



Fuente: Autor

Una vez agregado el equipo local, se debe ir A Administrador del equipo Local/Herramientas del sistema/Usuario y grupos locales/usuarios y allí crear un nuevo usuario de red para la administración del equipo local.

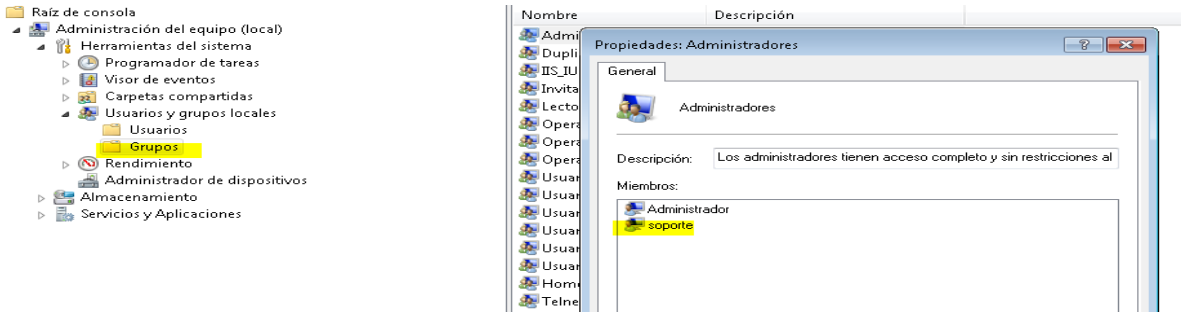
FIGURA 22 ADMINISTRACIÓN DE EQUIPO



Fuente: Autor

Una vez creado y teniendo en cuanta que este mismo usuario deberá ser replicado en los demás equipos, se deberá generar una contraseña segura y robusta ,solo el encargado de dar soporte a los equipos tendrá conocimiento y no se deberá compartir con los usuarios de los equipos, esta debe contener letras mayúsculas y minúsculas y deberá contener caracteres especiales ,un ejemplo de contraseña robusta seria :S0p0rt3pym3s:2017*- :luego de crear y generar la clave de acceso para el nuevo usuario administrador se deberá agregar al grupo de administradores locales para que tenga todos los privilegios de administrador de equipo tales como instalaciones, configuración y demás parámetros .

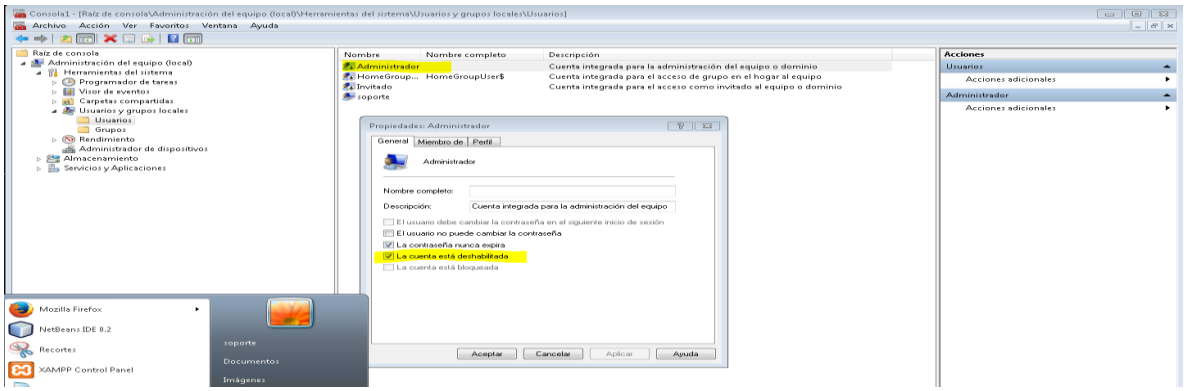
FIGURA 23 ADMINISTRACIÓN DE EQUIPO



Fuente: Autor

Ya agregado el usuario soporte en el grupo administradores se debe proceder a iniciar sesión con este nuevo usuario para posteriormente dar de baja o deshabilitar el usuario administrador y demás cuentas que se hayan creado por defecto en el sistema operativo.

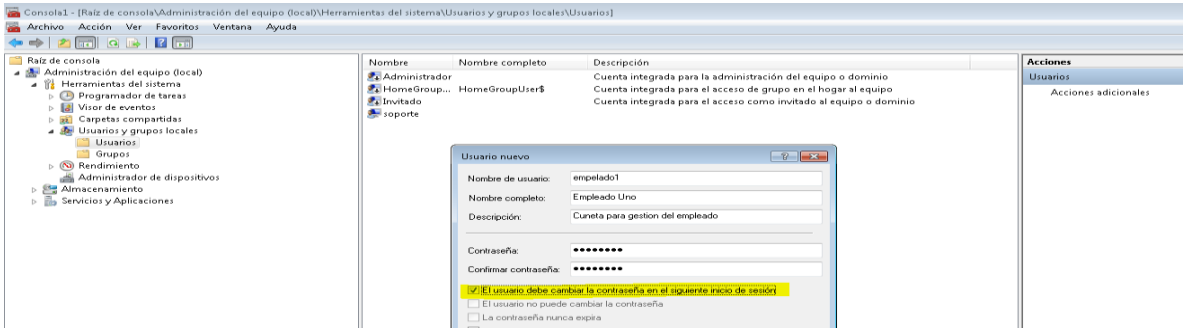
FIGURA 24 ADMINISTRACIÓN DE EQUIPO



Fuente: Autor

La creación del usuario de escritorio o de empleado debe tener las correspondientes restricciones y deberá ser creado en el grupo de usuarios de Windows el cual ya viene parametrizado con las restricciones necesario a la no modificación del sistema.
Los pasos son similares a la creación del usuario administrador, pero esto debe permitir al usuario poner su contraseña de red, aconsejando al mismo generar una contraseña robusta con caracteres especiales

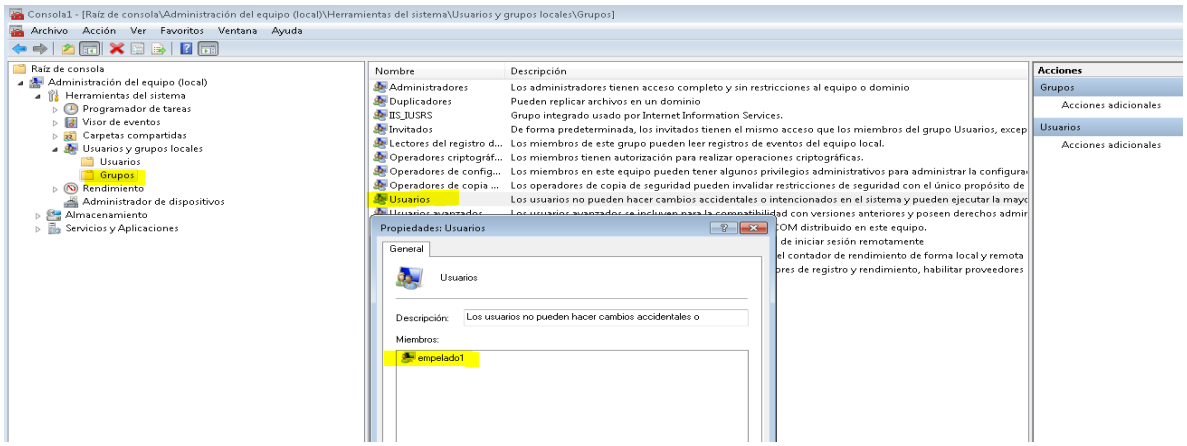
FIGURA 25 ADMINISTRACIÓN DE EQUIPO



Fuente: Autor

Incluirlo en el grupo de usuarios.

FIGURA 26 ADMINISTRACIÓN DE EQUIPO



Fuente: Autor

CONFIGURACIÓN DE POLÍTICAS LOCALES DE EQUIPO:

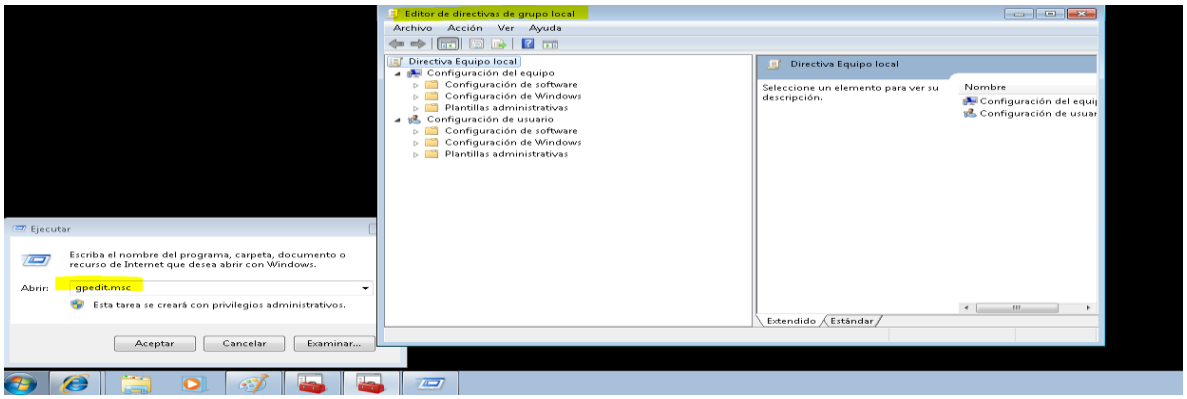
Hay una serie de políticas que se pueden adaptar al uso diario del sistema en equipos de usuario final, con el fin de evitar mal uso de los recursos informáticos y evitar ataques de malware o robo de información por su desconocimiento, para ello se exponen las siguientes reglas a nivel local de cada equipo:

Configuración de directivas de grupo para medios extraíbles USB CD,

Esta directiva busca que el usuario no utilice USB u otro tipo de medios extraíbles. Cuando el usuario intente conectar medios extraíbles a su equipo esta política denegara el acceso y no permitirá reproducir este medio de almacenamiento, esta política evitara paso de información confidencial a medios extraíbles y evitara la propagación de virus externos a la maquina local, en la siguiente figura se muestra la configuración de esta política.

Mediante las teclas Windows +R escribir el siguiente comando: gpedit.msc

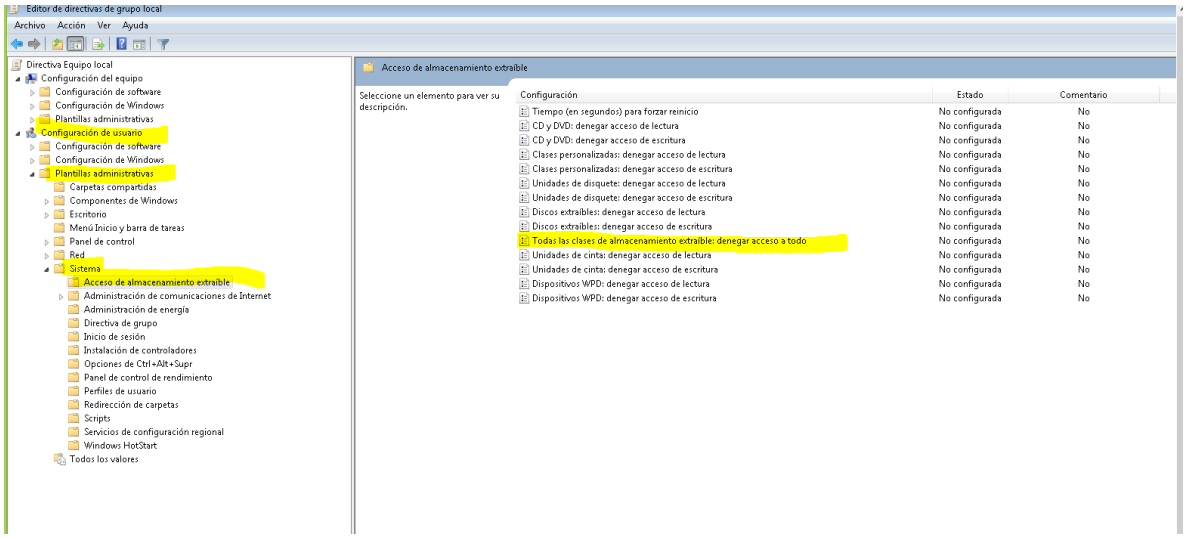
FIGURA 27 EJECUCIÓN DE CONSOLA DIRECTIVAS DE GRUPO



Fuente: Autor

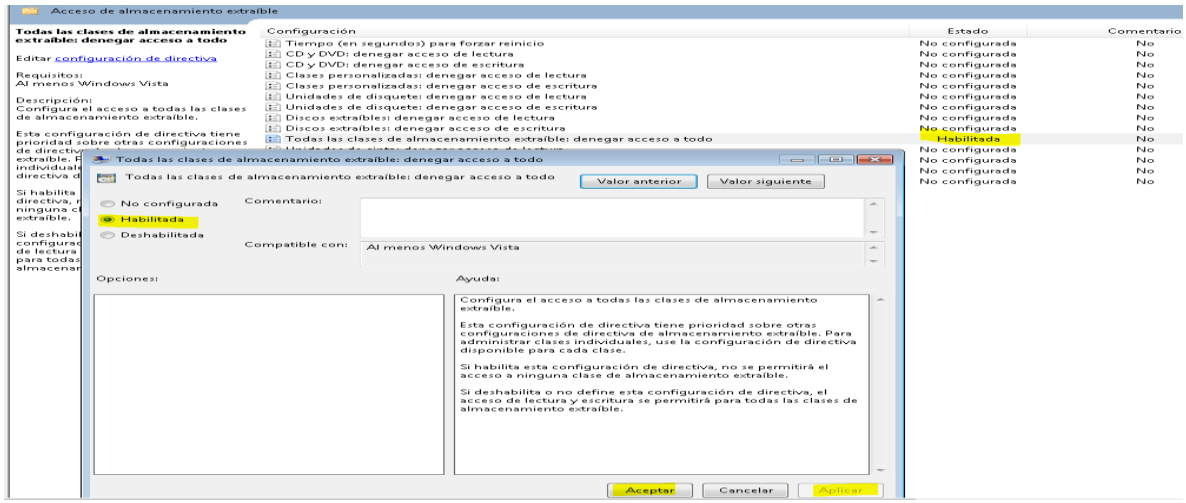
Posterior a abrir la ventana de editor de directivas de grupo local, navegar a: configuración de usuario/Plantillas administrativas/Sistema/Acceso de almacenamiento extraíble y editar la directiva de “Todas las clases de almacenamiento extraíble: denegar acceso a todo” aplicar y aceptar

FIGURA 28 ADMINISTRACIÓN DE DIRECTIVAS DE GRUPO



Fuente: Autor

FIGURA 29 ADMINISTRACIÓN DE DIRECTIVAS DE GRUPO

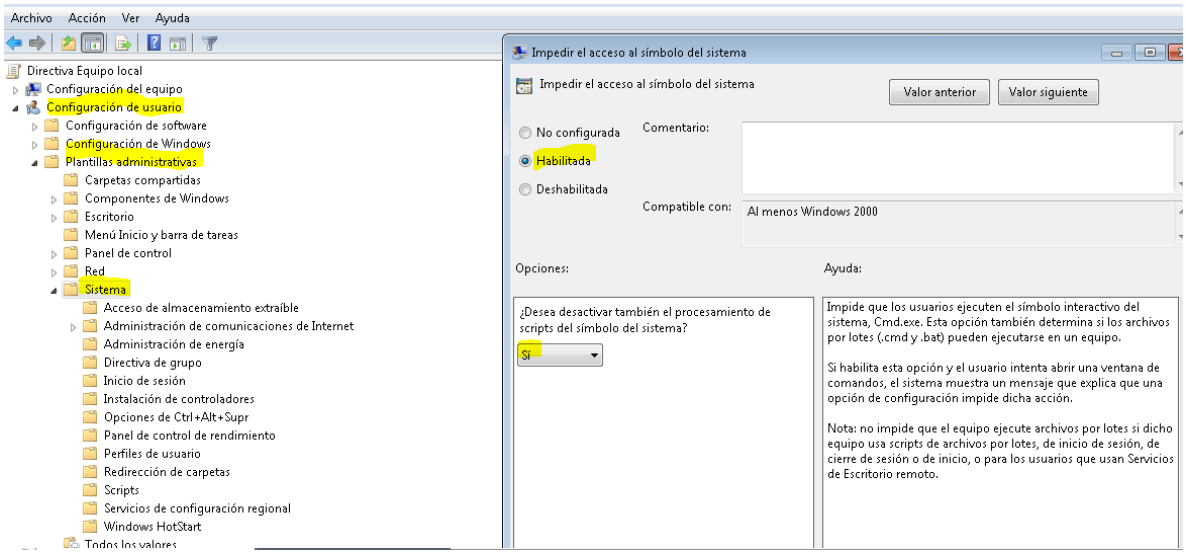


Fuente: Autor

Manipulación de Consola CMD

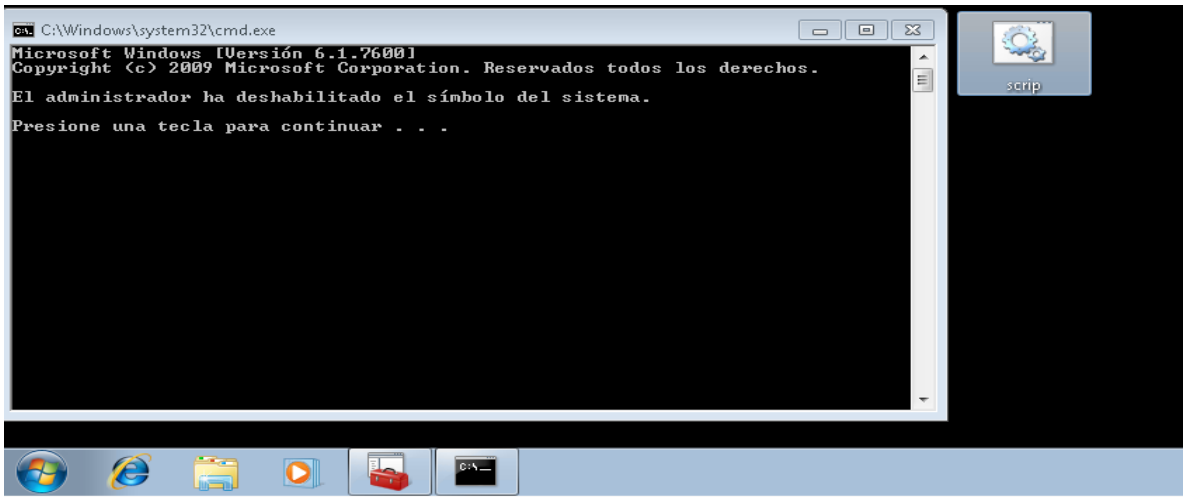
La siguiente directiva impide que los usuarios del equipo local manipulen la consola del sistema CMD además impedirá la ejecución de archivos .bat y scripts los cuales son los más utilizados para ataques cibernéticos

FIGURA 30 ADMINISTRACIÓN DE DIRECTIVAS DE GRUPO



Fuente: Autor

FIGURA 31 PRUEBA POLÍTICA DE GRUPO

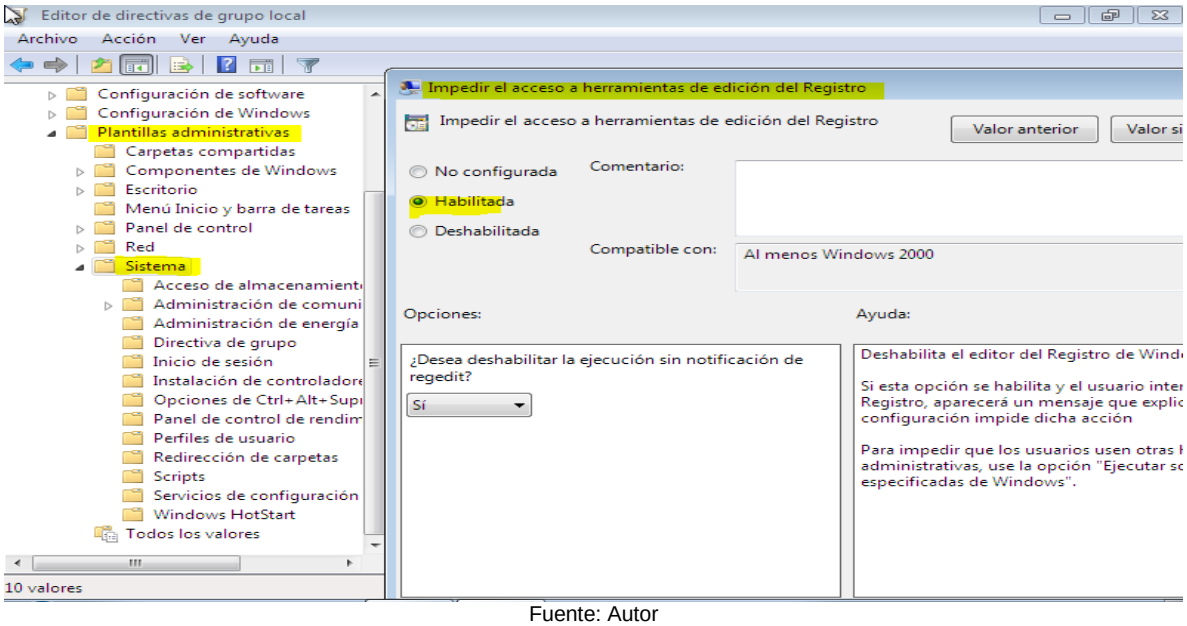


Fuente: Autor

Manipulación de registro de Windows

La directiva de editor de registro impedirá que cualquier tipo de ataque se instale o modifique entradas en el registro del sistema, además evitará que se configure procesos al inicio de sesión del usuario

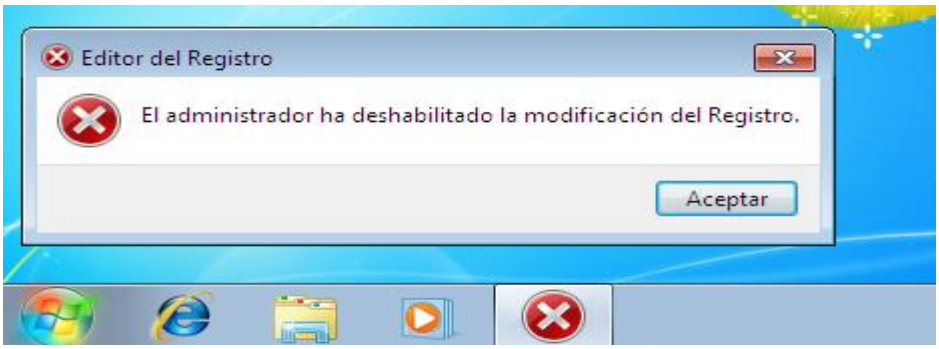
FIGURA 32 EDITOR POLÍTICA DE GRUPO



Fuente: Autor

Luego de aplicar la directiva, cualquier ejecución en el registro del sistema será impedido

FIGURA 33 PRUEBA POLÍTICA DE GRUPO



Fuente: Autor

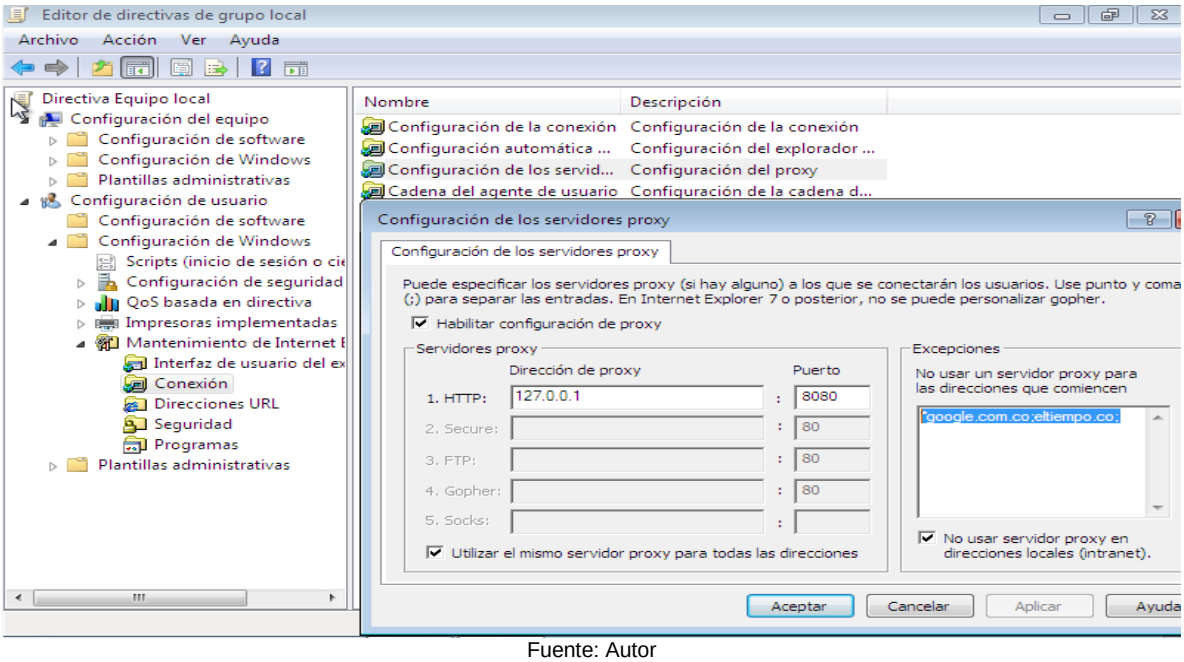
Navegación en internet

Navegación a páginas no autorizadas, todas las pymes en su mayoría utilizan navegación a internet, esto es un riesgo informático si los empleados no lo saben manejar de una forma adecuada, la siguiente directiva restringirá el uso de navegación web contando que el grupo de equipo tiene navegación libre.

Se debe editar la directiva configuración de usuario/configuración de Windows/mantenimiento de internet Explorer/conexión

En la siguiente ventana se deberá poner la dirección local del equipo que en este caso para todos los equipos es 127.0.0.1 con puerto por defecto 8080, las páginas que se requieren para navegar por el perfil del usuario se deben colocar como excepciones con el fin de tener únicamente navegación a las paginas utilizadas para fines laborales

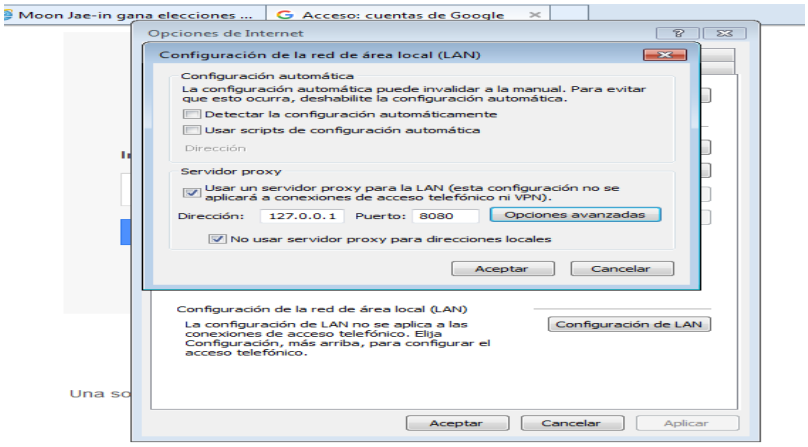
FIGURA 34 EDITOR POLÍTICA DE GRUPO



Fuente: Autor

Luego de configurar la directiva y verificar en las opciones de internet debe aparecer la modificación de proxy realizada tal y como se muestra en la siguiente imagen

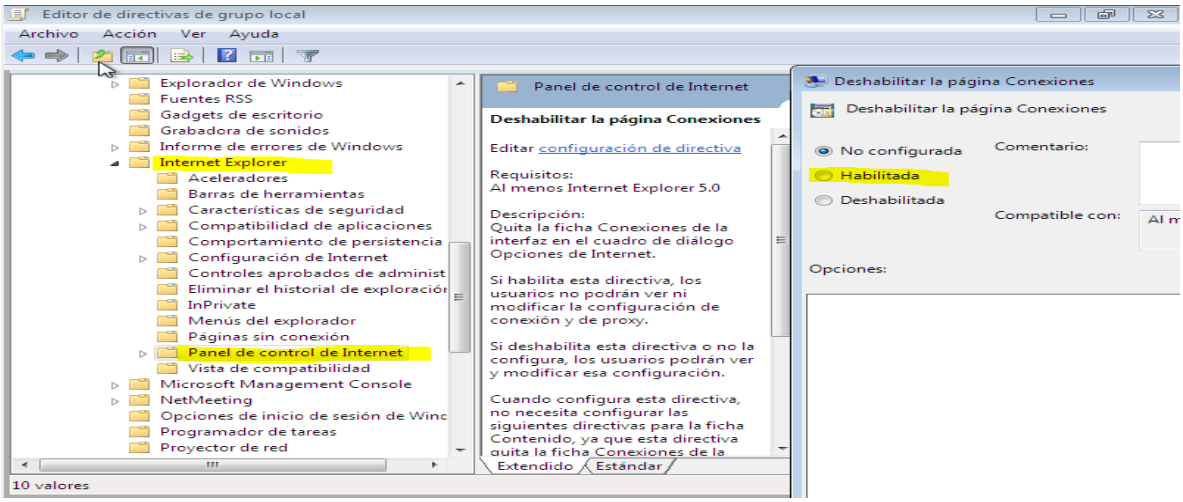
FIGURA 35 PRUEBA POLÍTICA DE GRUPO



Fuente: Autor

Para evitar que el usuario pueda manipular estas configuraciones se debe editar la siguiente directiva que busca ocultar el botón de conexiones en el panel de configuración de opciones de internet, con esta configuración se asegura que el usuario no logrará modificar los parámetros del proxy

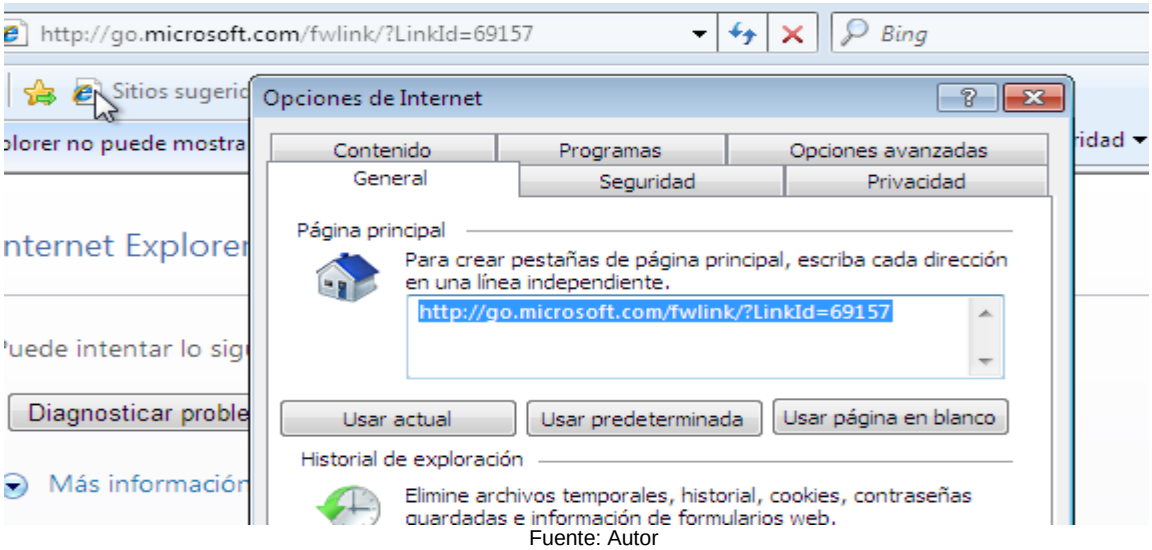
FIGURA 36 EDITOR POLÍTICA DE GRUPO



Fuente: Autor

La siguiente imagen muestra la cinta de opciones sin la pestaña de conexiones

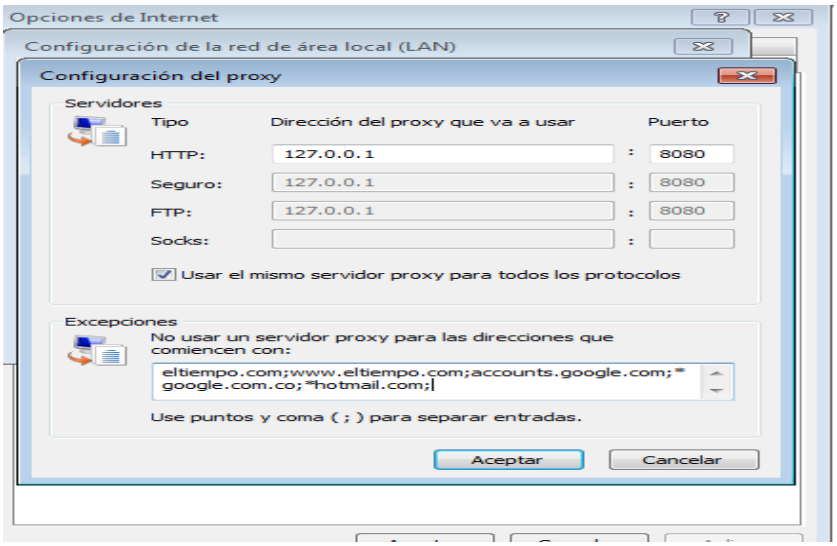
FIGURA 37 PRUEBA POLÍTICA DE GRUPO



Fuente: Autor

A continuación, se realiza una prueba simulando que el usuario debe ingresar a la página el tiempo.com y a la página de Google, como se evidencia en las excepciones, solo debe contener los dominios permitidos

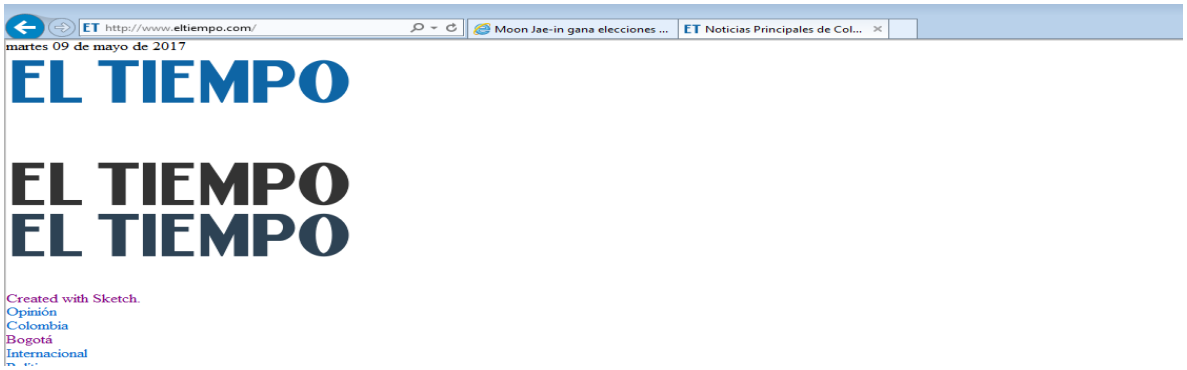
FIGURA 38 PRUEBA POLÍTICA DE GRUPO



Fuente: Autor

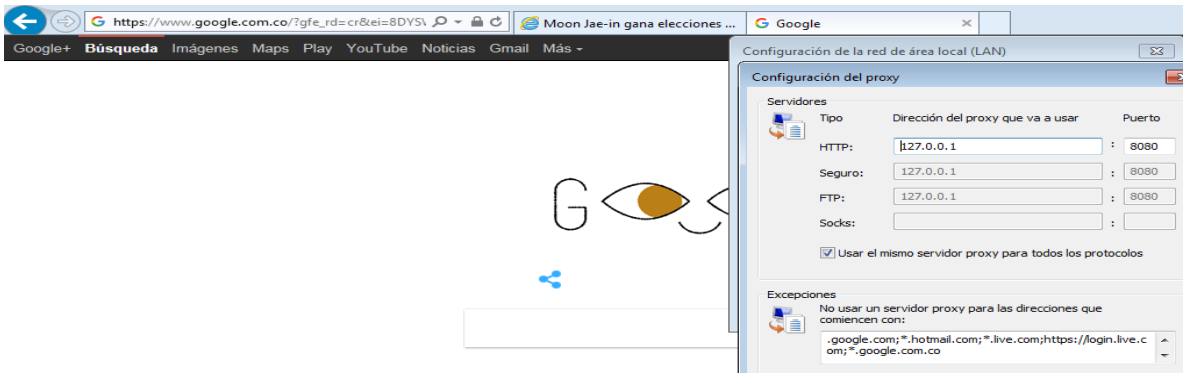
Acceso a páginas permitidas

FIGURA 39 PRUEBA POLÍTICA DE GRUPO



Fuente: Autor

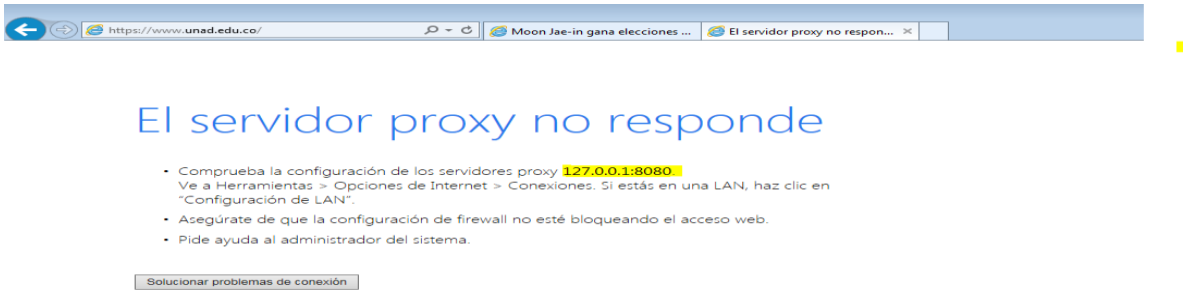
FIGURA 40 PRUEBA POLÍTICA DE GRUPO



Fuente: Autor

El usuario al acceder a una página no permitida, el navegador le mostrara el siguiente mensaje.

FIGURA 41 PRUEBA POLÍTICA DE GRUPO

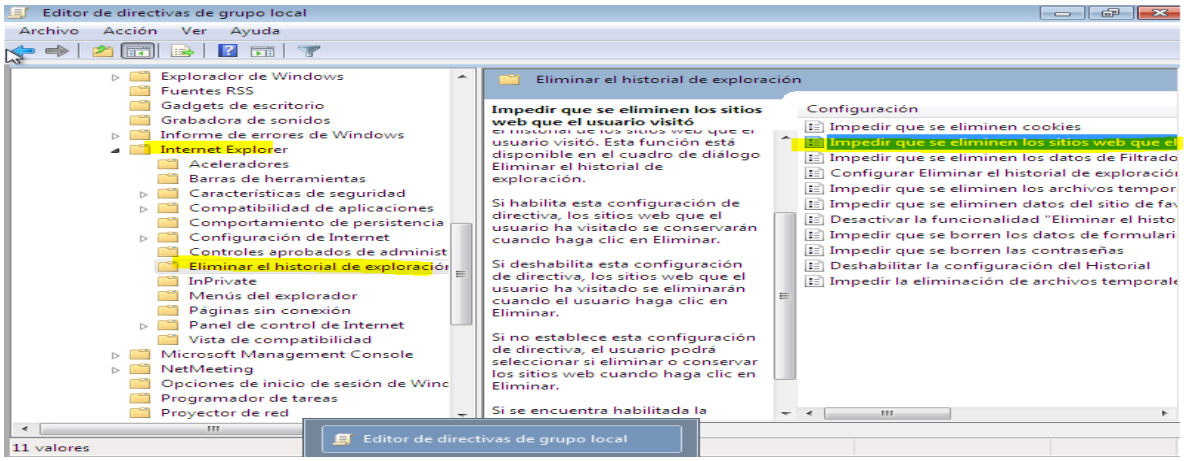


Fuente: Autor

Configuración de Auditoria

Como plan de mejora y monitoreo de acceso web en los equipos de usuarios, se debe editar la directiva de impedir el borrado de historial de navegación, con el fin de realizar revisiones de rutina quincenales o mensuales para detectar si el usuario ha navegado a paginas no autorizadas.

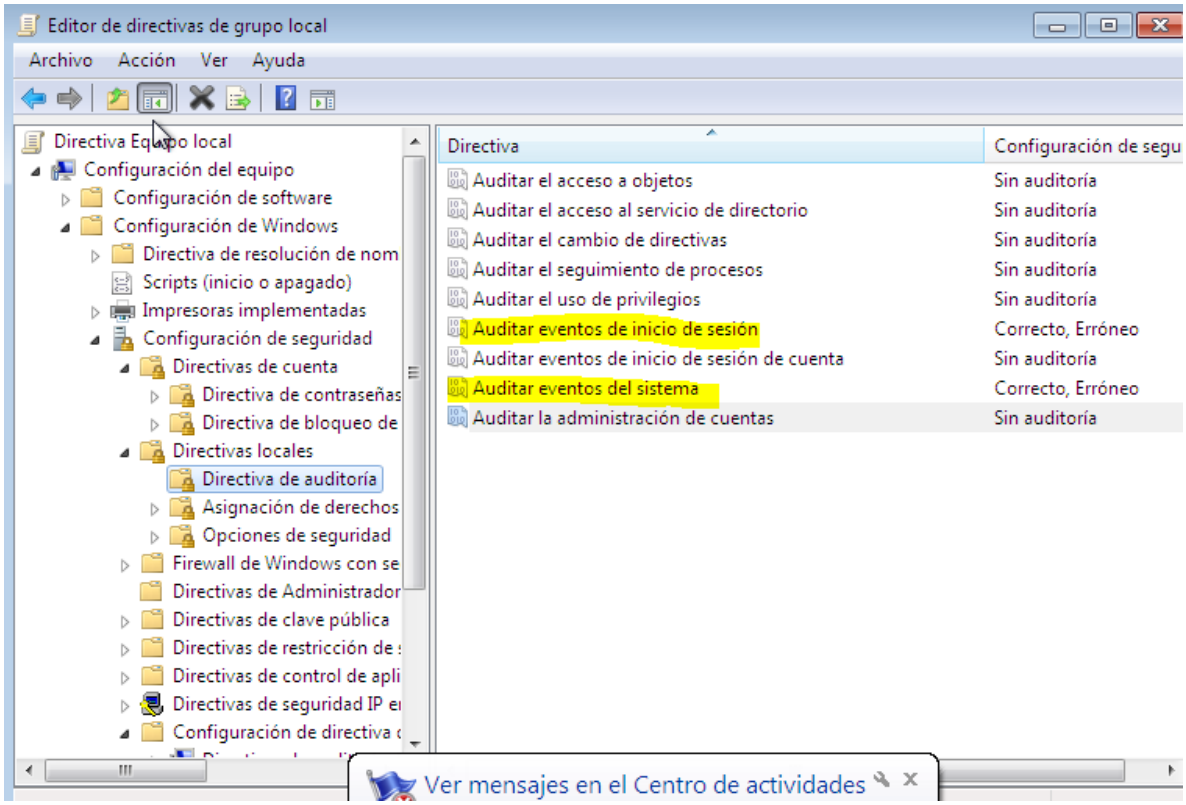
FIGURA 42 EDITOR POLÍTICA DE GRUPO



Fuente: Autor

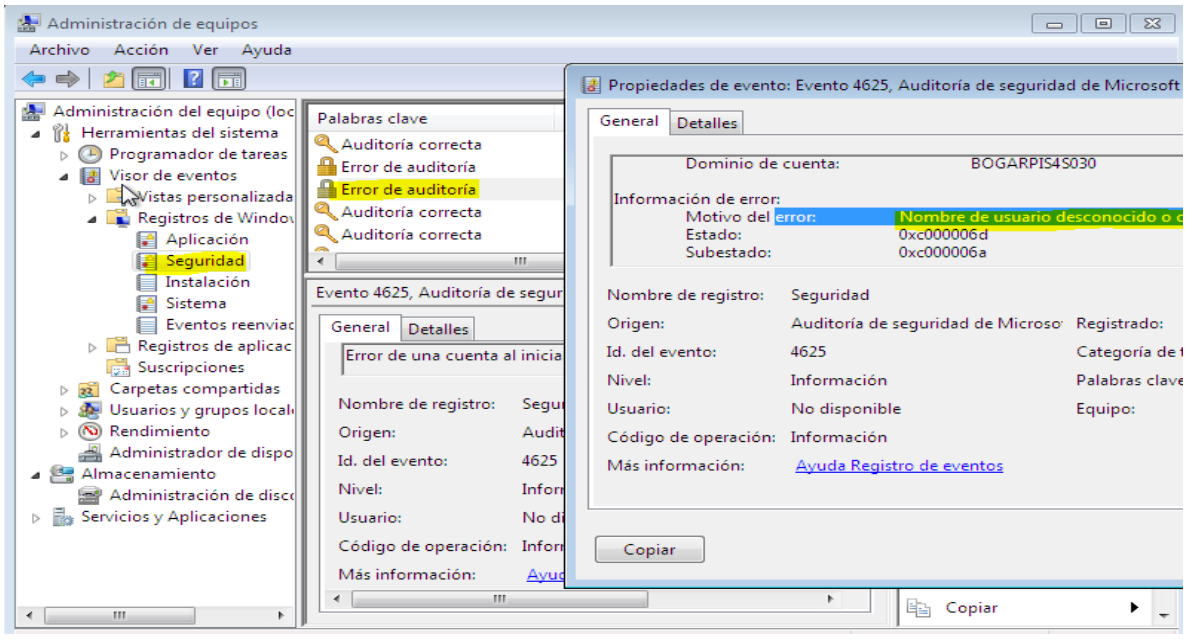
La directiva de auditoria permite visualizar la recurrencia de Accesos erróneos por el usuario o por persona ajenas a la empresa o dependencia, esto nos dará una alerta para evitar posibles robos de información

FIGURA 43 EDITOR POLÍTICA DE GRUPO



Fuente: Autor

FIGURA 44 EDITOR POLÍTICA DE GRUPO

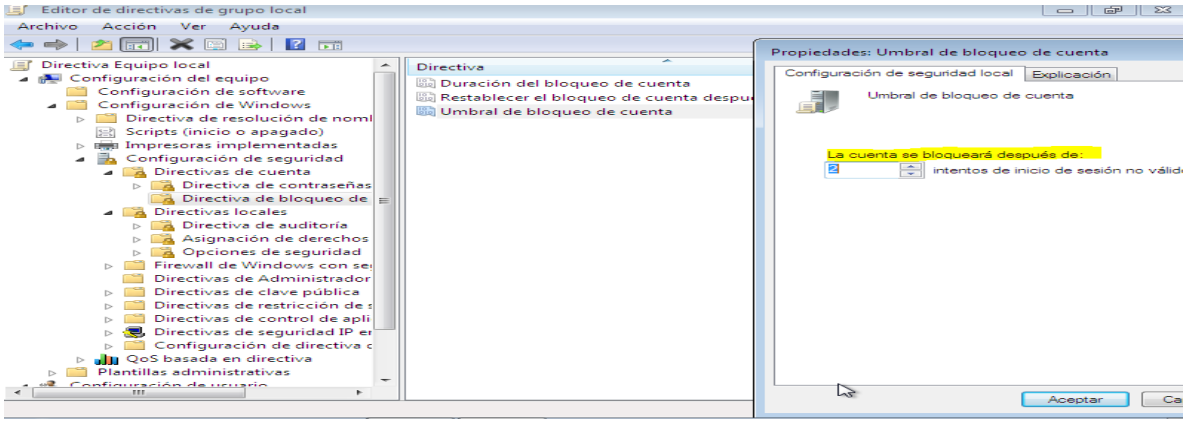


Fuente: Autor

Configuración de contraseñas de acceso

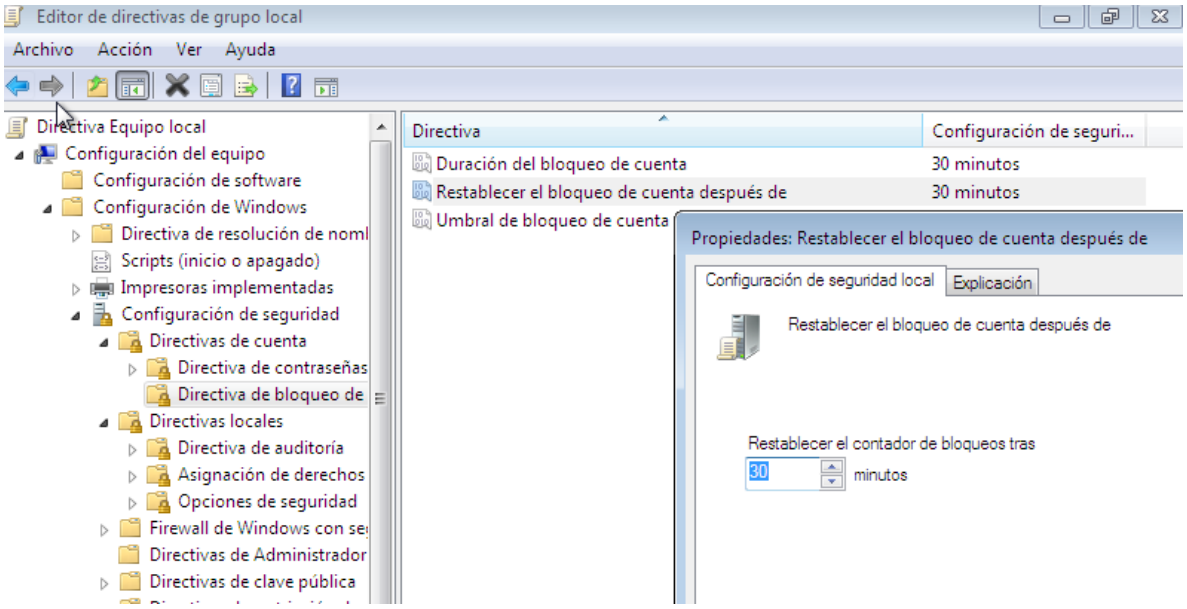
Directiva de bloqueo de contraseña, esta directiva tiene por objetivo permitir dos intentos de acceso a la sesión del sistema operativo, si el usuario accede de forma errónea la contraseña se deberá bloquear y se restablecerá en los próximos 30 minutos, esta directiva protege el acceso a los datos de personal no autorizado.

FIGURA 45 EDITOR POLÍTICA DE GRUPO



Fuente: Autor

FIGURA 46 EDITOR POLÍTICA DE GRUPO



Fuente: Autor

ASEGURAMIENTO REDES LAN

Teniendo en cuenta un ambiente de trabajo en donde algunas pymes utilicen equipos sofisticados para conectar más de 10 equipos de cómputo, se debe tener en cuenta la siguiente configuración con el fin de agrupar y tener una mejor administración a nivel de red:

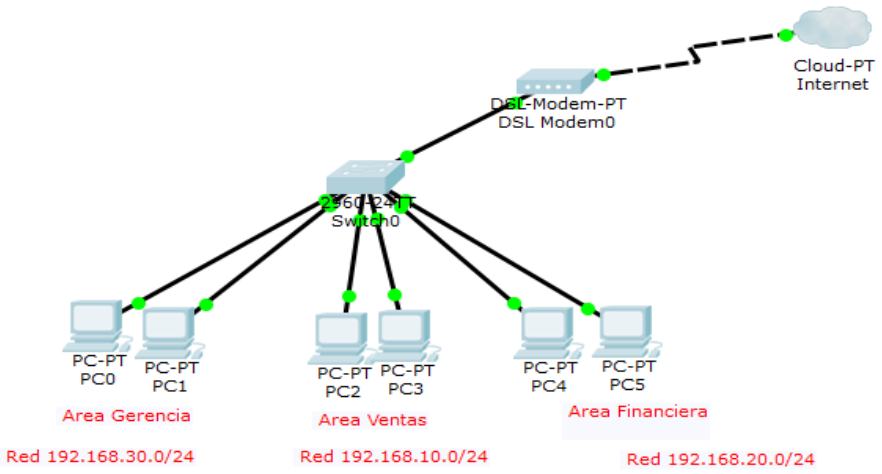
Red de 10 o más equipos:

La configuración de la red LAN debe ser segmentada por dependencias con el fin de lograr impedir que un usuario con experticia en sistemas ajeno al área ingrese de forma fraudulenta por consola de red sin que el otro usuario se percate de este acceso.

Lo primero es dividir los equipos por dependencias siendo como ejemplo, área de producción, área financiera, área de marketing etc. Para esto, se hace uso de redes LAN virtuales o VLAN que permiten dividir el tráfico que pasa por un mismo switch

El siguiente ejemplo es tomado de la herramienta Packet Tracer de cisco como simulación de una red LAN

FIGURA 47 SIMULACIÓN LAN

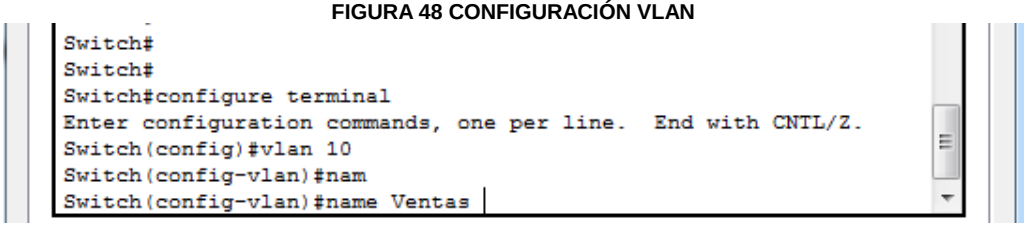


Fuente: Autor

La creación de la vlan en cualquier equipo de comunicación se realiza de la siguiente manera:

sobre la consola global de configuración enviar el comando vlan seguido del número de identificación, este número lo puede escoger a su selección, en este caso se toma el numero 10 como identificación seguido de la tecla enter ,luego se debe asignar el nombre a la vlan creada, este nombre se crea con el comando name, este nombre también se puede seleccionar el que mejor convenga para diferenciar el área o el grupo de trabajo, en este caso se utiliza “ventas”; el comando queda finalmente name ventas seguido de la tecla enter ,como se muestra en la figura 46

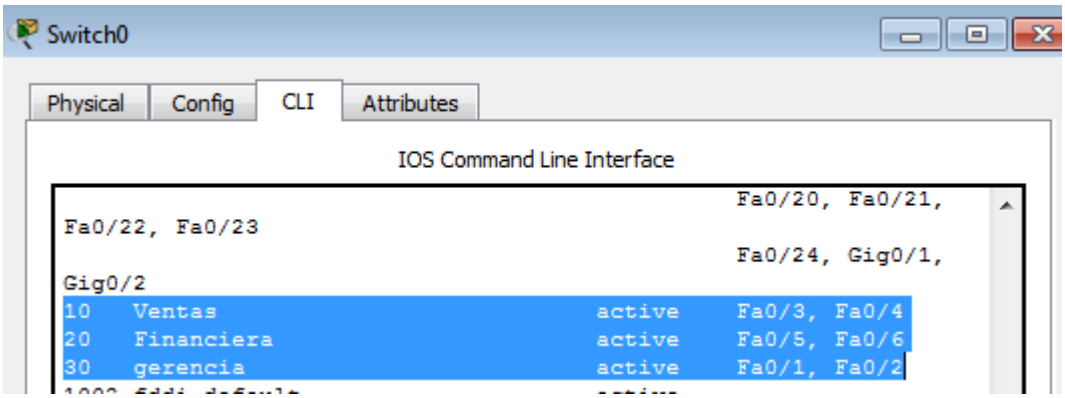
FIGURA 48 CONFIGURACIÓN VLAN



Fuente: Autor

Teniendo activas las vlan el siguiente paso, es identificar los puntos de red que conectan los equipos para así una vez identificados asignar la vlan correspondiente.

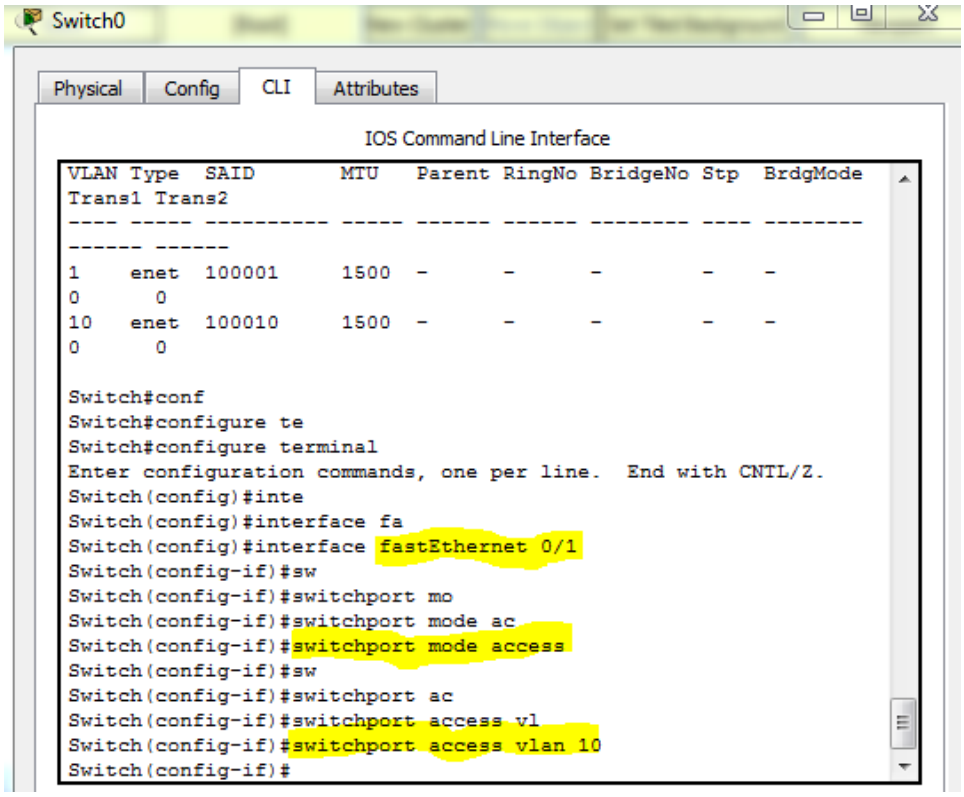
FIGURA 49 CONFIGURACIÓN VLAN



Fuente: Autor

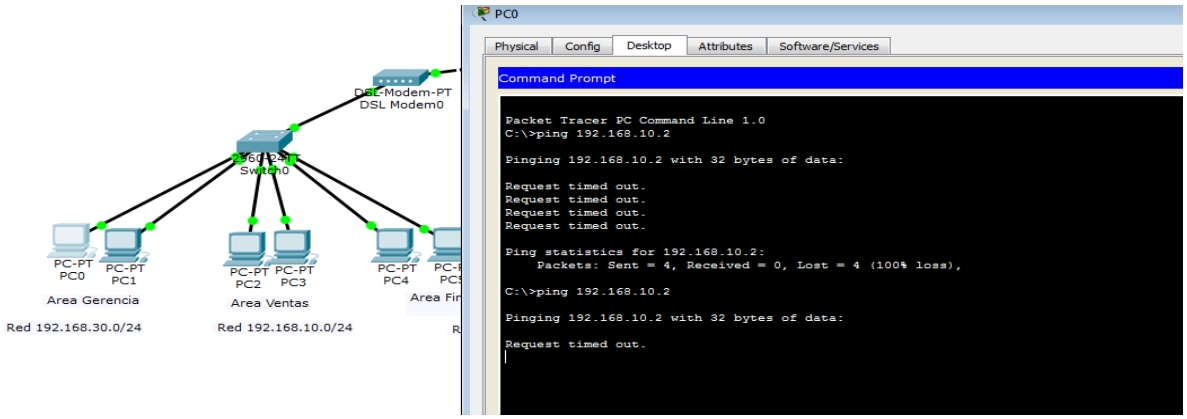
En la siguiente figura se muestra como configurar el punto de red donde se encuentra directamente conectados un equipo del grupo de ventas ,una vez ubicado en la consola del swich en modo de configuración global se debe seleccionar la interfaz de red a configurar ,seguido se debe asignar la vlan ,la cual para este ejemplo es la vlan 10 una vez asignada se debe ejecutar el comando switchport mode Access seguido de la tecla enter ,este comando pone el punto en modo acceso solo para recibir la vlan correspondiente ,luego se debe ejecutar el comando switchport access vlan 10 el cual asigna la vlan correspondiente a ventas.

FIGURA 50 PRUEBAS DE CONECTIVIDAD EN SEGMENTOS DE RED



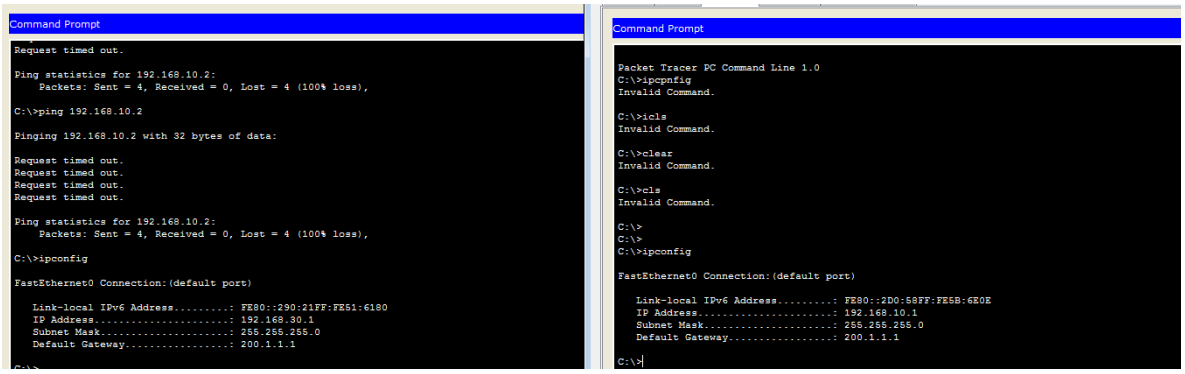
Fuente: Autor

FIGURA 51 PRUEBAS DE CONECTIVIDAD EN SEGMENTOS DE RED



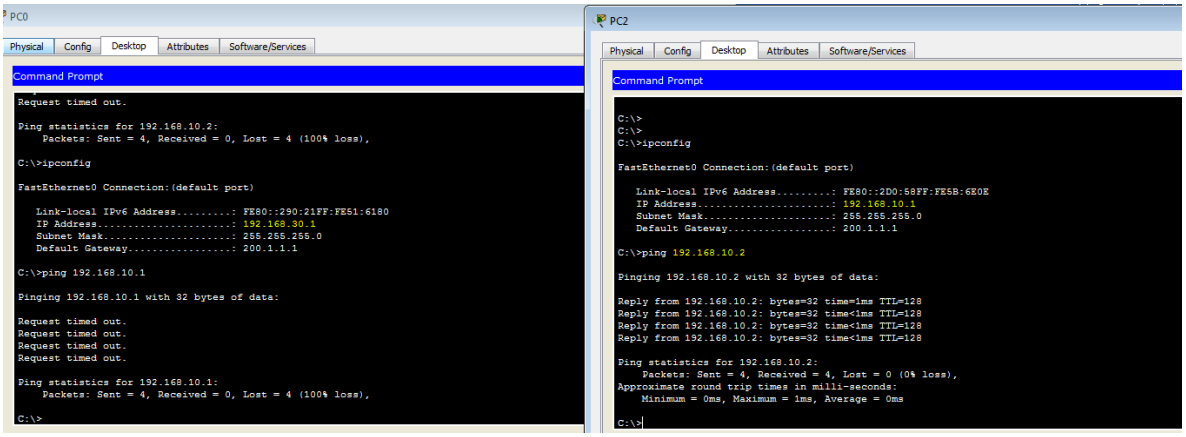
Fuente: Autor

FIGURA 52 PRUEBAS DE CONECTIVIDAD EN SEGMENTOS DE RED



Fuente: Autor

FIGURA 53 PRUEBAS DE CONECTIVIDAD EN SEGMENTOS DE RED



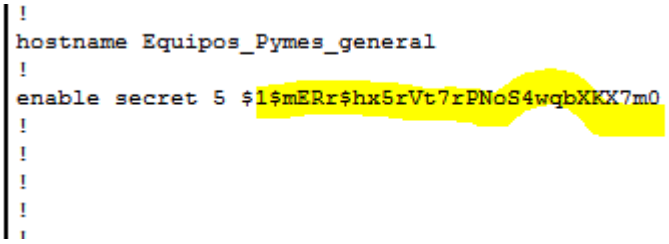
Fuente: Autor

CONFIGURACIÓN DE CREDENCIALES PARA EQUIPOS DE COMUNICACIÓN:

Configurar contraseña de acceso remoto y consola mediante protocolo seguro SSH con el fin de evitar ataques de MITM (Man in the middle)

Configuración de contraseña de acceso, al igual que en la sesión de equipos de escritorio el acceso a la administración de equipos de comunicación debe ser cifrada con el fin de evitar a ataque de sniffin en la red, basado en un equipo cisco la siguiente imagen demuestra los parámetros de configuración que se deben tener en cuenta al momento del montaje de la red de datos

FIGURA 54 CONFIGURACIÓN SSH EQUIPOS DE COMUNICACIÓN

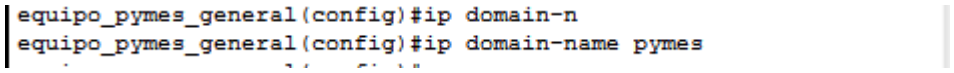


Fuente: Autor

El comando para cifrar contraseñas en Cisco es enable secret + la contraseña, ahora para generar un protocolo seguro de conexión diferente a el protocolo inseguro telnet se debe realizar de la siguiente forma

Lo primero es generar un dominio en el equipo cisco, con el comando ip domain-name

FIGURA 55 CONFIGURACIÓN SSH EQUIPOS DE COMUNICACIÓN



Fuente: Autor

Seguido se debe general la clave rsa con el comando crypto key generate rsa

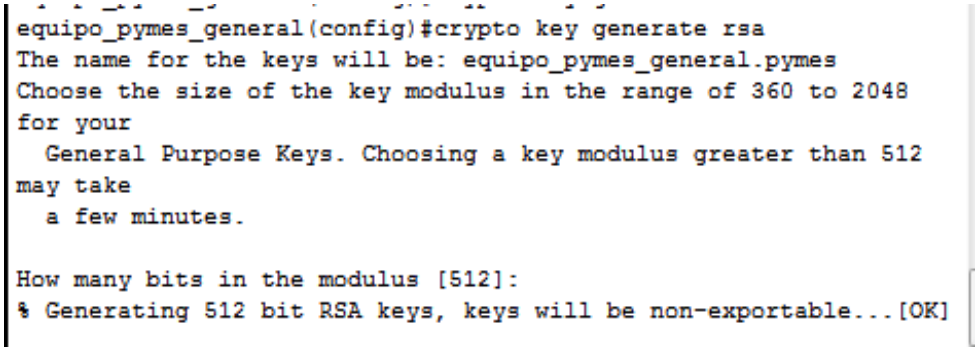


FIGURA 56 CONFIGURACIÓN SSH EQUIPOS DE COMUNICACIÓN

FUENTE: AUTOR

Una vez generado la llave de conexión se procede a configurar la interface de conexión remota mediante el comando line vty 0 4

FIGURA 57 CONFIGURACIÓN SSH EQUIPOS DE COMUNICACIÓN

```
equipo_pymes_general(config)#line vty 0 4
```

Fuente: Autor

Y los comandos transport input ssh

FIGURA 58 CONFIGURACIÓN SSH EQUIPOS DE COMUNICACIÓN

```
equipo_pymes_general(config-line)#transport input ssh
```

Fuente: Autor

Posterior a esta configuración se debe definir los privilegios de conexión y el usuario y contraseña

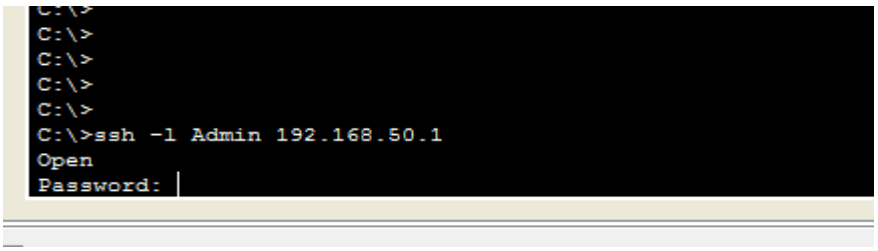
FIGURA 59 CONFIGURACIÓN SSH EQUIPOS DE COMUNICACIÓN

```
equipo_pymes_general(config-line)#login local
equipo_pymes_general(config-line)#exit
equipo_pymes_general(config)#use
equipo_pymes_general(config)#username admin pa
equipo_pymes_general(config)#username admin pri
equipo_pymes_general(config)#username admin privilege 15 pas
equipo_pymes_general(config)#username admin privilege 15 password cisco
```

Fuente: Autor

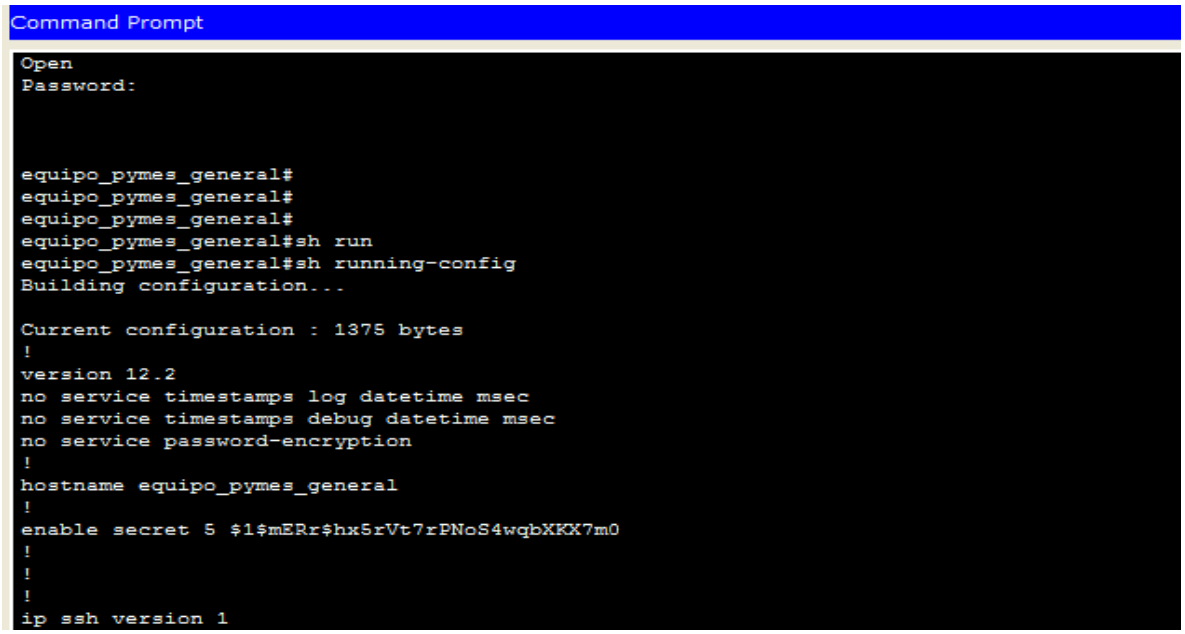
Luego de configurar la conexión se comprueba desde un equipo externo la conexión remota

FIGURA 60 PRUEBA SSH EQUIPOS DE COMUNICACIÓN



Fuente: Autor

FIGURA 61 PRUEBA SSH EQUIPOS DE COMUNICACIÓN



Fuente: Autor

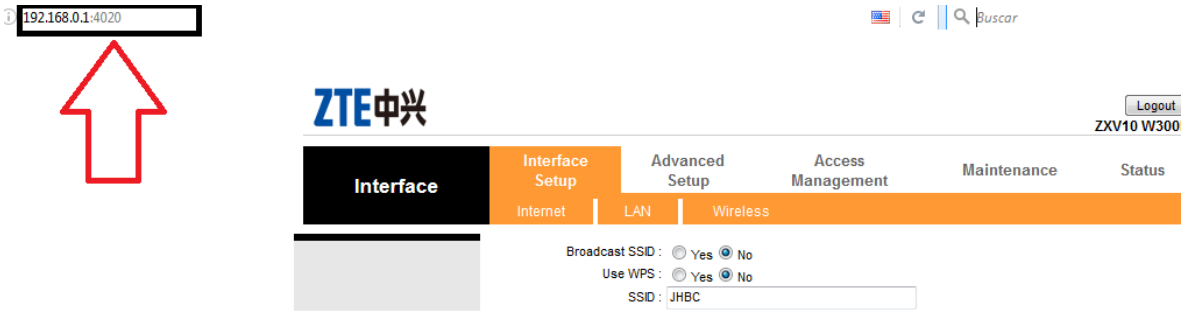
RED DE MENOS DE 10 EQUIPOS EN UN ENTORNO DE CONEXIÓN POR SWITCH Y MODEM

Para las pymes que no utilicen enrutadores especiales, se debe tener las siguientes configuraciones para asegurar el correcto uso del servicio en red.

El proveedor se servicio debe asegurar que la contraseña de acceso al modem cumple con los estándares de complejidad de acceso, para esto y una vez instalado o soportado el servicio se debe exigir esta configuración.

Exigir al proveedor de servicio que la conexión a la administración del modem se haga por un puerto especifico, no utilizar el puerto por defecto 80, este lo pueden cambiar por un puerto diferente, con el fin de que ningún usuario ajeno a este tipo de conexión intente acceder.

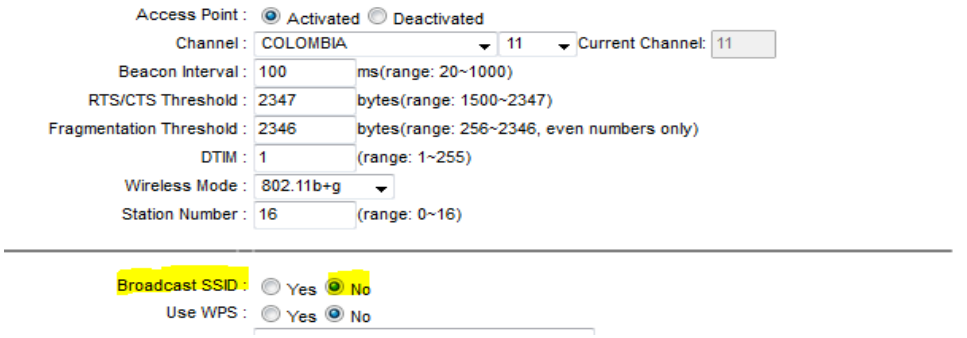
FIGURA 62 CONFIGURACIÓN RED INALÁMBRICA



Fuente: Autor

Para el uso del servicio WIFI se puede configurar de la siguiente forma:
En la difusión del SSID chequear la casilla de No, con el fin de que nadie pueda ver el nombre de la red inalámbrica, esto permite que ningún desconocido se pueda conectar a la red.

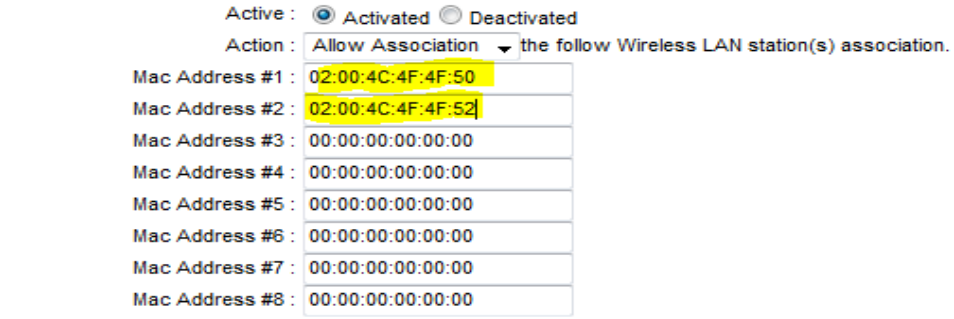
FIGURA 63 CONFIGURACIÓN RED INALÁMBRICA



Fuente: Autor

Para permitir conexión a la red inalámbrica es aconsejase configurar el modem para que acepte solo direcciones físicas permitidas MAC esto genera seguridad que los usuarios que se conecten son los autorizados por la empresa.

FIGURA 64 CONFIGURACIÓN DE ACCESO A RED INALÁMBRICA



Fuente: Autor

Ejecución de las pruebas

Acceso a equipo en modo administrador o invitado, combinando contraseñas comunes, este punto es uno de los más vulnerables porque desde la instalación del sistema operativo muchas veces no se presta atención al usuario administrador generado por defecto y no se asegura que el mismo lleve una contraseña o sea renombrado por un nombre diferente.

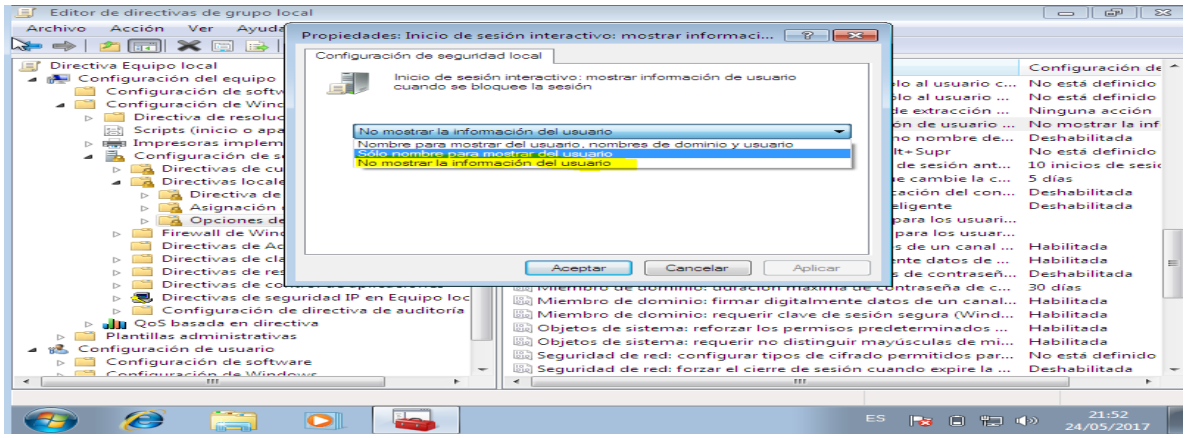
La presentación del sistema se puede observar de la siguiente forma, como se evidencia en la figura 1 la cuenta admin esta activada y mostrada al inicio del sistema lo que pone en riesgo que algún intruso pueda acceder a la cuenta y administrar el equipo o robar información. Para este caso se debe seguir el manual de la página 31 donde se indica que el usuario administrador debe ser renombrado con otro nombre y que la cuenta deberá tener una contraseña robusta.

FIGURA 65 ACCESO A SISTEMA

Fuente: Autor

Además, se hace necesario ocultar los usuarios de logon con el fin de que el atacante desconozca el usuario de inicio de sesión, con la herramienta de directivas de grupo se deberá aplicar la siguiente opción

FIGURA 66 EJECUCIÓN POLÍTICA



Fuente: Autor

De esta forma una vez el equipo se bloquee o solo se encienda la presentación del sistema quedara de la siguiente forma

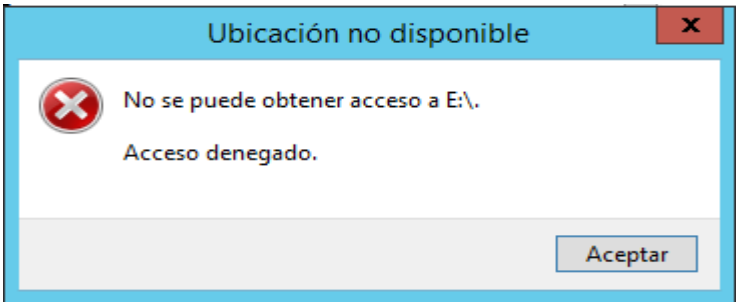
FIGURA 67 ACCESO A SISTEMA

Fuente: Autor

Uso de medios extraíbles en cualquier equipo, esta práctica es común en los usuarios, llevan permanentemente medios extraíbles comúnmente USB para extraer información de los equipos, esto genera un grave riego a la organización dado que pueden contaminar el equipo con virus o pueden llevarse información importante de la empresa, para el bloqueo de los puertos se debe seguir el manual.

Luego de aplicar la política descrita en el manual el sistema emitirá el siguiente mensaje de error una vez se conecte el dispositivo extraíble al equipo

FIGURA 68 DENEGAR CONEXIONES DE MEDIOS EXTRAÍBLE



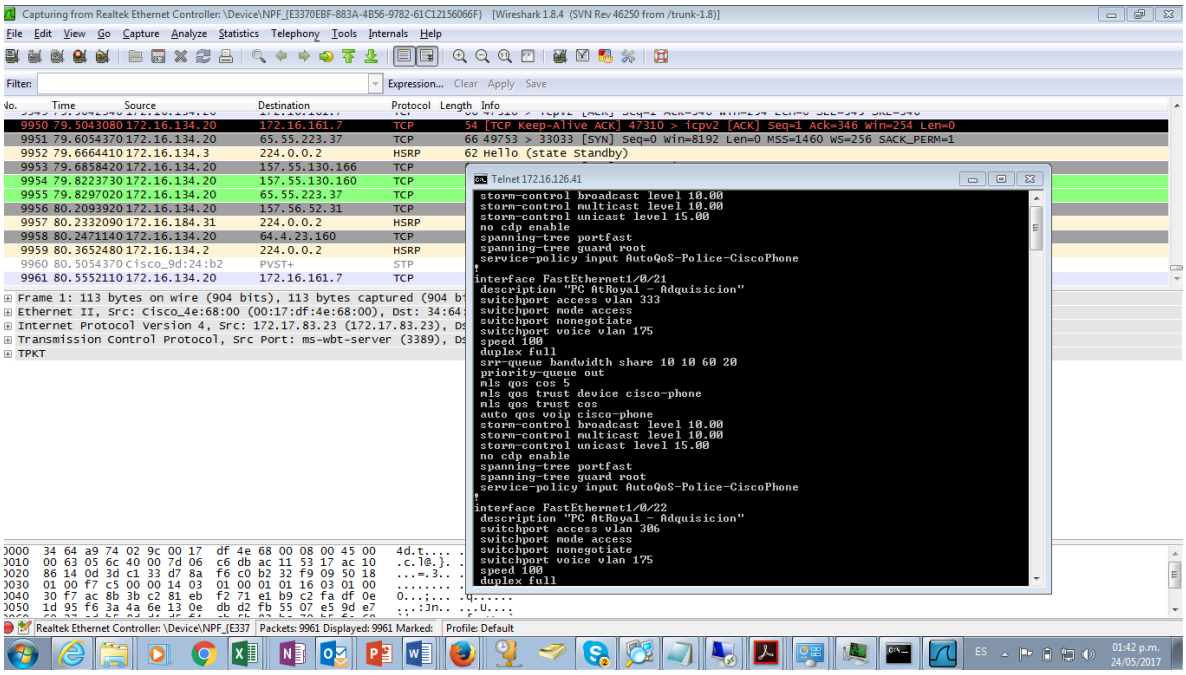
Fuente: Autor

Navegación a sitios con alto riesgo de virus, el error más común de los administradores o encargados del área de sistemas es dejar los equipos con navegación libre a internet, los usuarios en tiempo de ocio pueden consultar páginas con alta probabilidad de virus o descargar, malware de los correos electrónicos para esto es necesario restringir el uso de navegación web para evitar riesgos de ataques informáticos; en parte del manual se especifica la forma de bloqueo de navegación con el fin de permitir solo páginas de uso diario laboral .una vez configurada la política el usuario al intentar acceder a un sitio web bloqueado el navegador le mostrara un mensaje de error impidiendo así la navegación en páginas de internet

Acceso a equipos de comunicación por Telnet ,normalmente cuando se configura un equipo de comunicación , Swich o router el mismo se configura para obtener acceso remoto mediante la consola de comando, para así acceder desde cualquier equipo de la red de la pymes ,este protocolo es inseguro dado que el trasporte de datos se envía en texto plano y genera un alto riesgo de escucha de tráfico desde cualquier equipo, obteniendo así las credenciales de acceso y vulnerando la administración de los equipos en red .

En la siguiente figura se demuestra la captura de usuario y contraseña escuchando el tráfico con wireshark, el usuario accedió al equipo switch mediante la consola cmd de Windows ejecutando un telnet a la IP del equipo como se puede observar, en este mismo equipo a modo de ejemplo se inició la captura de tráfico.

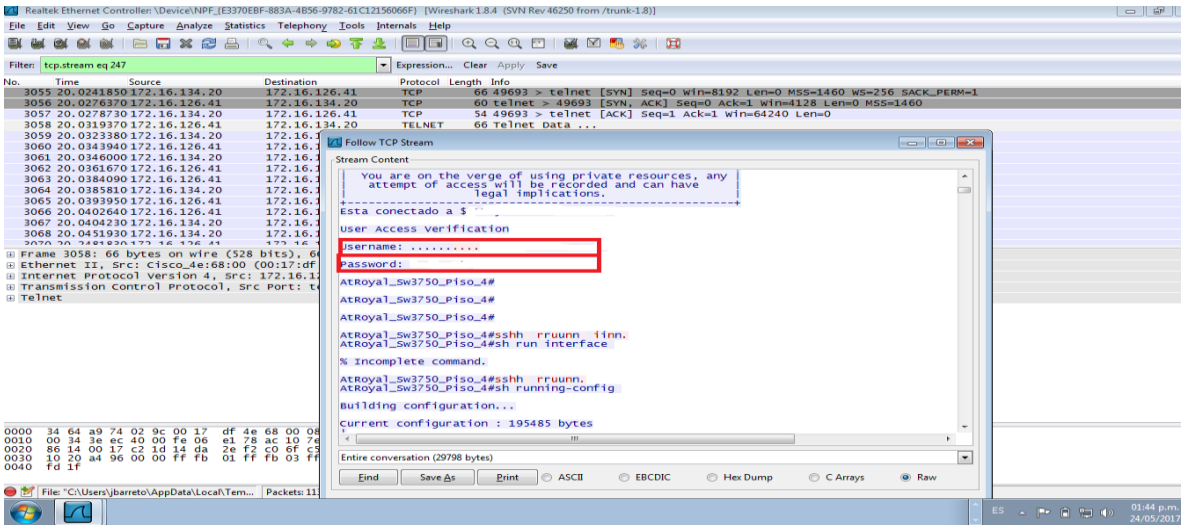
FIGURA 69 ANÁLISIS DE TRAFICO WIRESHARK



Fuente: Autor

Luego de realizar el filtro en la herramienta Wiresahrk filtrando el tráfico interesante, en este caso protocolo telnet y analizando la trama se evidencia claramente el usuario y contraseña obtenido del equipo

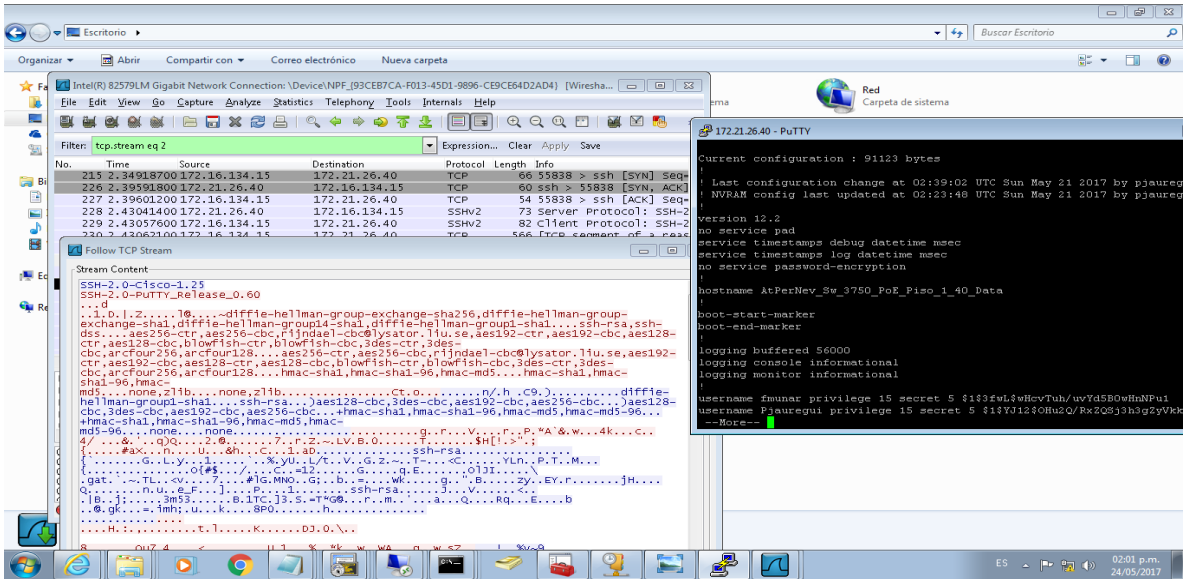
FIGURA 70 ANÁLISIS DE TRÁFICO WIRESHARK



Fuente: Autor

Como se especifica en el manual, se debe realizar la configuración segura con el protocolo SSH el cual cifra la información impidiendo que el atacante pueda obtener la contraseña, como se puede ver en la siguiente figura un equipo correctamente configurado, el usuario se conecta por el protocolo SSH, se evidencia según la trama de wireshark el cifrado de información impidiendo obtener los datos de acceso al equipo de comunicación

FIGURA 71 ANÁLISIS DE TRÁFICO WIRESHARK



Fuente: Autor

Conclusiones:

Luego de realizar cada una de las revisiones propuestas por el manual y ejecutar los controles enunciados en la fase se prevención, se evidencia que es necesario restringir cualquier acceso no permitido al usuario, con el fin de garantizar y controlar cualquiera ataque informático que se pueda presentar, esto garantizad además que cada empleado concentre su atención en función de su rol de trabajo.

Los resultados fueron obtenidos en cada una de la GPO (Group Policy Object) expuesta en el manual, las mismas se realizarán en entorno real para comprobar su funcionalidad.

Es necesario que la pyme cuente con un antivirus licenciado para brindar una mejor seguridad de la información.

Es necesario que la pyme realice periódicamente Backus de la información este proceso lo puede realizar con el mismo paquete de antivirus que adquiere los cuales ofrecen almacenamiento en internet

La pyme es responsable de que todos sus sistemas se encuentren actualizados de acuerdo a las sugerencias de los fabricantes