Universidad Autónoma Metropolitana Unidad Azcapotzalco

División de Ciencias Básicas e Ingeniería

Licenciatura en Ingeniería en Computación

Estancia Profesional

Diseño e implementación de un sistema de seguridad para redes corporativas

Alumna: Yesenia Díaz Hernández
Matricula: 210329432

Asesores:

Interno: M. en C. José Alfredo Estrada Soto

Externo: Ing. Mario Ernesto Gómez Romero

Trimestre 2018 Invierno

Fecha de entrega: 02 de abril de 2018

Declaratoria

Yo, José Alfredo Estrada Soto, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

M. en C. José Alfredo Estrada Soto

Yo, Mario Ernesto Gómez Romero, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

Ing. Mario Ernesto Gómez Romero

Yo, Yesenia Díaz Hernández, doy mi autorización a la Coordinación de Servicios de Información de la Universidad Autónoma Metropolitana, Unidad Azcapotzalco, para publicar el presente documento en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

Yesenia Díaz Hernández

Tabla de contenido

Índice de figuras

Diagramas

Resumen

En el presente proyecto se implementa un sistema de seguridad para la empresa ABC Uniformes S.A. de C.V. en donde se hace uso del dispositivo FortiGate 90D en el que recae la mayor parte del sistema, ya que en él se implementan las políticas de seguridad de acuerdo a las necesidades de la empresa.

Con el sistema de seguridad se pretende qué ninguna persona ajena a la empresa pueda acceder a la información que se maneja, ya que cuenta con una red interna en la cual no se podrá acceder si no se tienen los permisos correspondientes en el FortiGate 90D y en el Synology. Además de que el personal podrá consultar la información sin la necesidad de encontrarse físicamente en el establecimiento por medio de una VPN SSL, con la cual podrán conectarse de manera segura.

También se implementa un mecanismo en el que el personal de la empresa pueda trabajar con carpetas compartidas, y si el equipo llegara a presentar algún fallo, la información no se pierde, ya que se alojará en un NAS Synology[1].

Introducción

En la actualidad el manejo de información a través de internet se ha vuelto indispensable, por lo que las "amenazas informáticas"[2] van en aumento; debido a esto, la información debe estar protegida de cualquier acceso no autorizado y evitar cualquier filtrado o mal uso que se le pudiera dar.

Para ello, existen sistemas de seguridad en redes que pueden ser adaptados de acuerdo con las necesidades que una corporación pueda tener. Algunos de estos sistemas pueden contemplar cuestiones tan básicas, como el que únicamente el personal externo a la corporación no pueda entrar en contacto con información clasificada; otros, pueden ser más robustos e incorporar una variedad de situaciones consideradas como "de riesgo" por la empresa.

T&B Talent S.A. de C.V. (TBT) es una empresa mexicana con más de 17 años de experiencia con soluciones de seguridad informática para todo tipo de negocio. Está integrada por profesionales especializados con formación en tecnologías de la información, seguridad, redes e infraestructura, con amplia experiencia en el diseño, implementación y soporte.

En el presente reporte se ve el desarrollo de un sistema de seguridad para redes corporativas, el cual se implementó en la empresa ABC Uniformes S.A. de C.V. uno de los clientes de la empresa T&B Talent.

---

[1] NAS (*Network Attac*hed Storage) son un arreglo de varios discos duros que se conecta mediante un cable de red o un *router*.

[2] Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Figura 1. Logotipo de la empresa

Figura 2. Logotipo de la empresa cliente

Antecedentes

Proyectos de integración o terminales

Implementar niveles de seguridad que fortalezcan la seguridad informática de una empresa [1]

En lo que se enfoca el proyecto terminal es en tomar medidas para que solo personal autorizado pueda acceder a información confidencial y protegerla de posibles riesgos, la similitud con este proyecto es que se crean políticas de seguridad para restringir el acceso a información importante, la diferencia es que se emplearía un fortigate 90D y no un fortigate 80CM, como lo hicieron ellos, el cual ya se considera obsoleto para ciertas funciones.

Configuración e implementación de políticas de seguridad para la protección de una red corporativa [2]

Lo que se realizó en el proyecto terminal fueron políticas para limitar el acceso a la red interna y crear permisos para el acceso a la información con un fortigate 200B. En lo que se parece la presente propuesta es en la creación de políticas para el acceso adecuado a la información, en lo que difiere es que en este proyecto solo hace énfasis a la red interna en cambio en la presente propuesta se hace referencia a la red interna y externa haciendo uso de un fortigate 90D y el uso de VPN para la conexión externa.

Administración y seguridad de una red corporativa mediante un firewall fortigate 90D [3]

El proyecto se especializa en la creación e implementación de políticas de seguridad, es decir, limita el tráfico de información hacia la red externa (como páginas con malware) para poder proteger la integridad de los datos. La similitud es la utilización del fortigate 90D para la creación de políticas, en lo que difiere es en la creación de políticas para el acceso remoto por medio de VPN, y el monitoreo del tráfico en la red.

Tesis

Control de Acceso a Redes [4]

En la tesis se habla de controlar el acceso a la información de una corporación haciendo uso de un NAC Cisco, hace uso de VPN para el acceso remoto a la red interna, la tesis se parece en que hace uso de un dispositivo para controlar el acceso a la información así como también la implementación de VPN, la diferencia con la tesis es que el utiliza NAC Cisco y en la propuesta se va a utilizar un firewall fortigate 90D y un NAS para controlar el acceso a la información.

Estudio e Implementación de una Metodología de prevención de intrusos para redes LAN [5]

En la tesis se realiza una implementación de un sistema de seguridad el cual indica quien está tratando de entrar en la red sin autorización, la similitud que tiene con la propuesta es la implementación del sistema para controlar quien puede hacer uso de cierta información y quien no, la diferencia es que utiliza el software Snort para la implementación del sistema en Linux, mientras que en la propuesta se hace uso de un firewall fortigate 90D en Windows.

Diseño e Implementación de un prototipo de DMZ y la Interconexión segura mediante VPN utilizando el firewall fortigate 60 [6]

En la tesis se realiza la implementación de una zona desmilitarizada (DMZ) y la creación de VPN para la conexión a la red interna pasando por la DMZ de manera segura. La similitud es que para realizar la conexión a la red interna mediante VPN hace uso de un fortigate, en lo que difiere es que utiliza un fortigate 60 y en la presente propuesta se utiliza un fortigate 90D el cual tiene otras características y funciones para poder acceder a la red por medio de VPN.

Justificación

Hoy en día, la información ha tomado mucha importancia por lo cual se debe restringir el acceso a ella, y solo usuarios con autorización podrán acceder a la información. La seguridad informática es importante cuando se habla de proteger información de cualquier establecimiento ya sea una empresa pública como el INE (Instituto Nacional Electoral) o privada en donde afectaría en demasía si se llegara a tener acceso a información clasificada como, por ejemplo, para poder ganar alguna licitación.

La creación de políticas de seguridad es una labor fundamental que involucra al personal, los procesos y los recursos de la corporación. “Cada vez más las redes están expuestas a virus informáticos, *spam*, código malicioso, *hackers y crackers* que penetran los sistemas de seguridad” [7].

Por este motivo se diseño e implementó un sistema de seguridad para la empresa ABC Uniformes S.A. de C.V. en donde la información de cualquier índole, ya sea

administrativa, comercial, privilegiada, entre otras, se garantice que solo personal autorizado podrá acceder a ella.

Objetivos

Objetivo general

Diseñar e implementar un sistema de seguridad para una red corporativa con base en políticas de seguridad.

Objetivos específicos

- Analizar la topología de red de la empresa para identificar los elementos críticos de seguridad.
- Diseñar y elaborar las políticas de seguridad con respecto al acceso a la información, tanto de manera local como remota.
- Diseñar e implementar un sistema de monitorización para extraer información relacionada al tráfico de la red.
- Construir el sistema de seguridad de red.

Marco teórico

Fortinet

Fortinet es una empresa multinacional de Estados Unidos con sede en Sunnyvale, California. Se dedica al desarrollo y la comercialización de software, dispositivos y servicios de ciberseguridad, como firewalls, antivirus, prevención de intrusiones y seguridad en dispositivos de usuario, entre otros.

Fortinet desarrolla y comercializa hardware y software de seguridad y redes informáticas. Es conocida sobre todo por su gama de dispositivos de seguridad FortiGate, que combinan numerosas funciones de ciberseguridad.

Los dispositivos de la serie FortiGate 90 - 60 ofrecen hasta 4 Gbps de rendimiento de cortafuegos, además de múltiples puertos integrados de 1 GE. Esta combinación de rendimiento, densidad de puertos y características de seguridad consolidadas ofrece una plataforma ideal para pequeñas y medianas empresas, así como para empresas distribuidas. En la implementación del sistema de seguridad se cuenta con un FortiGate 90D.

VPN

Una VPN (*Virtual Private Network*) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. La utilización de esta tecnología permite que personal de una corporación pueda entrar a la red privada por medio de un canal seguro en el que se siguen manteniendo las políticas de seguridad y restricciones que maneje la empresa y en donde no haya intrusos que pongan en riesgo la información de la corporación.

Tipos de VPN:

VPN site to site

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El equipo central VPN, que posee un vinculo a Internet permanente, acepta las conexiones vía Internet provenientes de los sitios y establece el "túnel" VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha.

VPN de acceso remoto

Son comunicaciones donde los usuarios se conectan con la empresa desde sitios remotos (oficinas comerciales, casas, hoteles, etc.) utilizando Internet como medio de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa, con sus respectivos permisos.

VPN SSL

Una VPN SSL (*Virtual Private Network – Secure Sockets Layer*) es una forma de red privada virtual (VPN) que se puede usar con un navegador web estándar, no requiere la instalación de software cliente especializado en la computadora del usuario final.

Un servidor SSL VPN funciona mediante la creación de un canal virtual a través de Internet público utilizando el cifrado simétrico. Ambos lados del canal tienen las llaves que se utilizan para cifrar y descifrar el tráfico.

Existen dos tipos de VPN SSL:

SSL Portal VPN: este tipo de VPN SSL permite una sola conexión SSL a un sitio Web para que el usuario final pueda acceder de forma segura a varios servicios de red. El usuario remoto accede al gateway SSL VPN utilizando cualquier navegador web moderno, se identifica con el gateway mediante un método de autenticación soportado por este gateway y, a continuación, se le presenta una página Web que actúa como el portal hacia otros servicios.

VPN de túnel SSL: este tipo de VPN SSL permite a un navegador Web acceder de forma segura a varios servicios de red, incluidas aplicaciones y protocolos que no están basados en Web, a través de un túnel que se ejecuta bajo SSL. Las VPN de túnel SSL requieren que el navegador Web pueda manejar contenido activo, lo que les permite proporcionar funcionalidad que no es accesible a las VPNs de portal SSL. Ejemplos de contenido activo incluyen Java, JavaScript, Active X o aplicaciones o plug-ins de Flash.

En el sistema de seguridad se implementó una VPN SSL para realizar la conexión, la cual se describe más adelante.

Políticas de seguridad

En importante que en una empresa exista “seguridad informática: la cual se define como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema” [8].

Por ello en la empresa ABC Uniformes S.A de C.V. se implementaron políticas de seguridad de acuerdo a las vulnerabilidades que se detectaron y las que la empresa indico que se aplicaran, como es el caso de que solo cierto personal pudiera accesar a ciertos sitios web, entre otras que se mostraran más adelante.

Panda Cloud Security

Panda Security es una empresa española especializada en la creación de soluciones de seguridad informática. Centrada inicialmente en la creación de un programa antivirus y que permite el escaneo automático de amenazas.

Endpoint Protection protege de forma centralizada todas las estaciones de trabajo y servidores Windows, Mac, Linux, incluyendo equipos portátiles, teléfonos móviles y los principales sistemas de virtualización. Se utiliza para proteger la red informática de manera sencilla y en modo on line. La protección que proporciona neutraliza spyware, troyanos, virus y cualquier otra amenaza dirigida contra los equipos.

Se hizo uso del software Panda Cloud Security para poder monitorizar los equipos que estén conectados a la red de la empresa y así poder ver en tiempo real lo que esté haciendo el personal o en su caso poder ayudar remotamente al personal que no se encuentre físicamente en la empresa.

Desarrollo del proyecto

A continuación se muestra el desarrollo del proyecto “Diseño e implementación de un sistema de seguridad para redes corporativas” implementado en la empresa ABC Uniformes S.A de C.V.

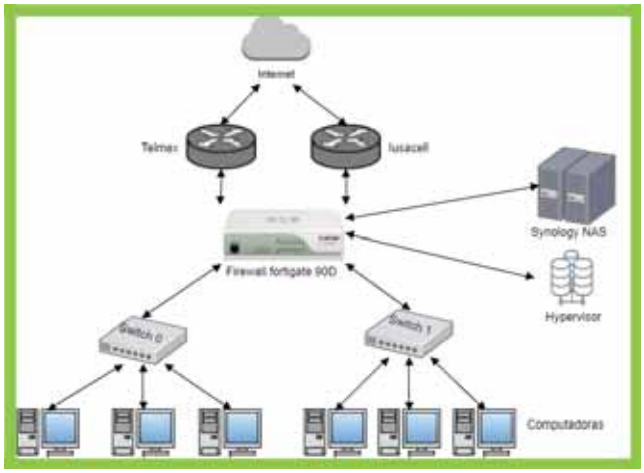

Diagrama 1. Mapa de red

Para la realización del proyecto se hizo un mapa de red de la empresa, para poder visualizar y saber cómo está organizada.

NAS Synology ds416

Es un servidor en donde se encuentra almacenada (en carpetas) toda la información de la empresa, para poder consultarla se necesita la creación de usuarios en el sistema, con permisos específicos.

Creación de usuarios

Para la creación de usuarios en el NAS Synology es necesario ingresar la ruta http://10.1.1.119:5000 en donde se pondrá el usuario y contraseña, para poder acceder al Synology.

Figura 3. Usuario y contraseña en el Synology.

Se selecciona el ícono de Panel de Control y posteriormente se elige Usuario.

Figura 4. Creación de usuario 1.

Al seleccionar el icono de Usuario se ingresa a un menú, en donde se encuentran todos los usuarios creados en el sistema, en donde se selecciona crear de las pestañas que se muestran.

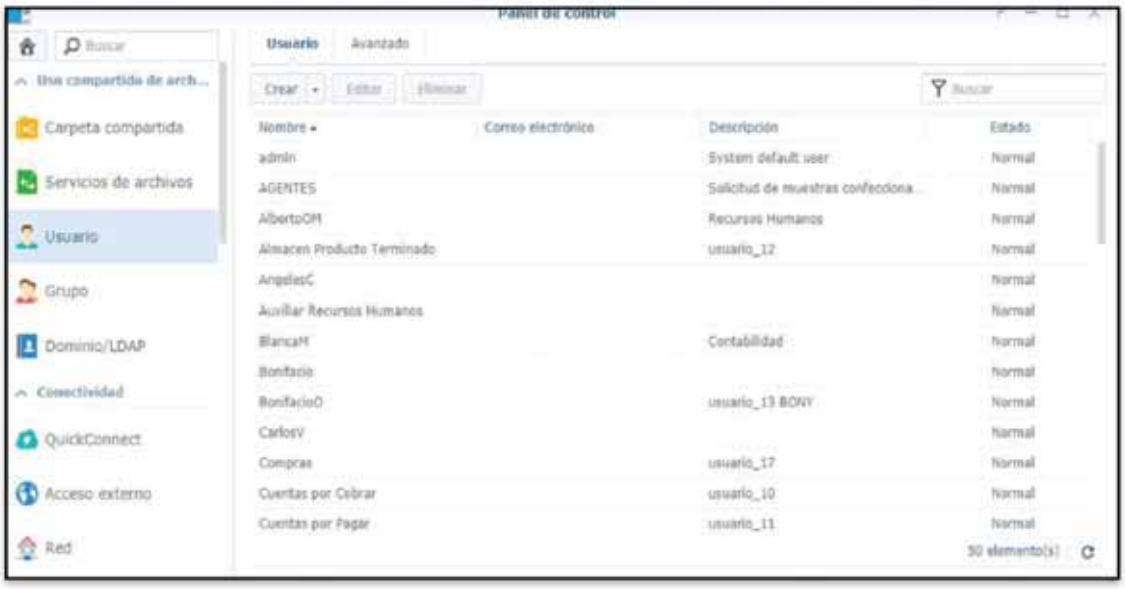

Figura 5. Creación de usuario 2

A continuación, es necesario ingresar los datos del nuevo usuario como son: nombre en este caso Ejemplo, descripción (el área en donde se desempeña) y una contraseña que vaya de acuerdo a la nomenclatura utilizada. Para que se tenga una mayor seguridad se activa la casilla No permitir que el usuario cambie la contraseña de la cuenta.

Figura 6. Configuración de nombre y contraseña de usuario.

Se configura la capacidad de almacenamiento que va tener el usuario en el synology, lo más adecuado es no limitarlo al menos que sea necesario hacerlo.

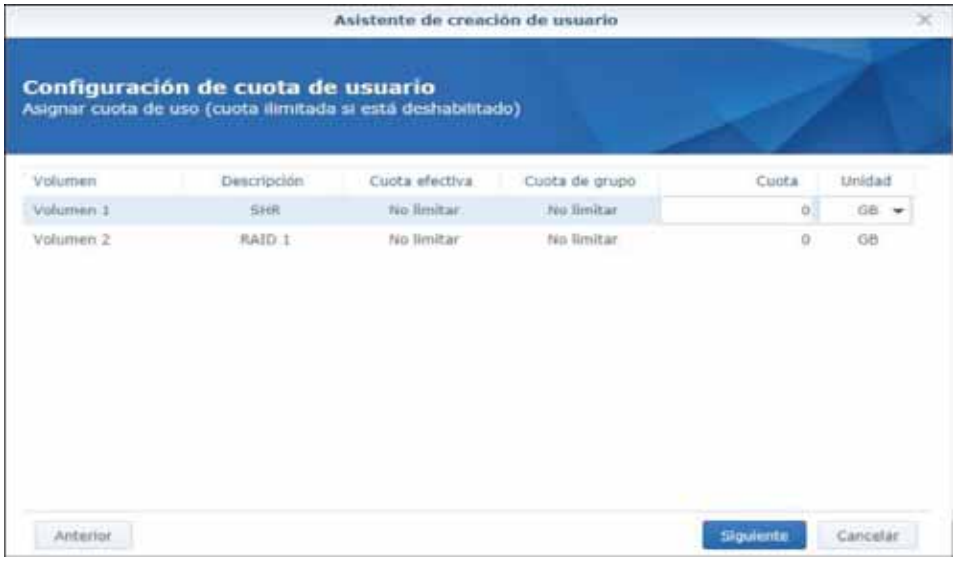

Figura 7. Configuración de almacenamiento del usuario.

Se asigna permisos al usuario para que pueda acceder a las aplicaciones necesarias, estas se establecen de acuerdo a los requerimientos de la empresa.

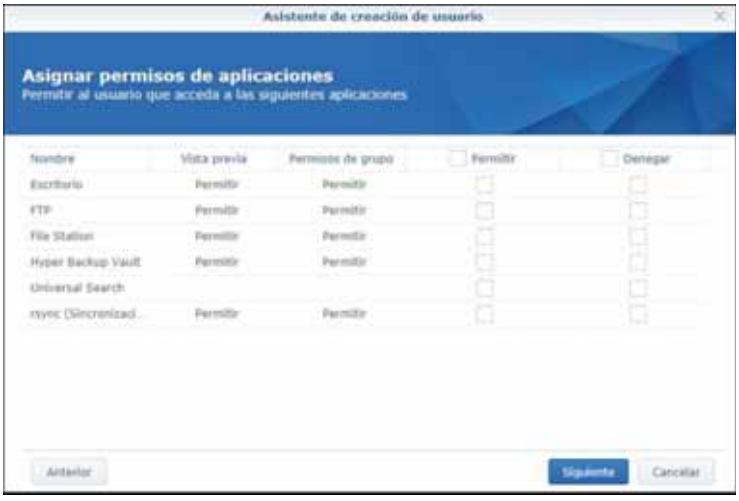

Figura 8. Configuración de permisos de aplicaciones.

Al término de todas las configuraciones anteriormente descritas se crea el nuevo usuario, el cual se puede ver en el panel de control.

Figura 9. Comprobación del usuario creado.

Creación de carpetas

Para crear una carpeta se dirige al icono File Station al entrar se muestra un submenu en donde se selecciona *crear → crear nueva carpeta compartida*

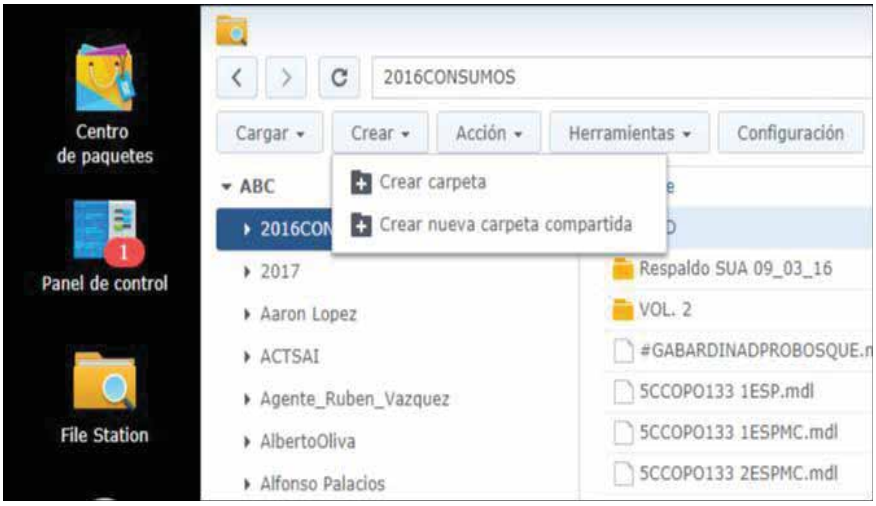

Figura 10. Creación de carpeta.

A continuación se configura los datos de la carpeta como son: nombre y descripcion. Se tienen que activar las casillas Ocultar subcarpetas y archivos de usuarios sin permisos para que la carpeta no la puedan ver personas que no tengan autorizacion, Habilitar papeleria de reciclaje en donde se van todos los archivos eliminados de la carpeta, Acceso restringido unicamente a administradores donde solo los administradores puedan entrar a la papeleria de reciclaje para poder recuperar archivos elimininados por error.

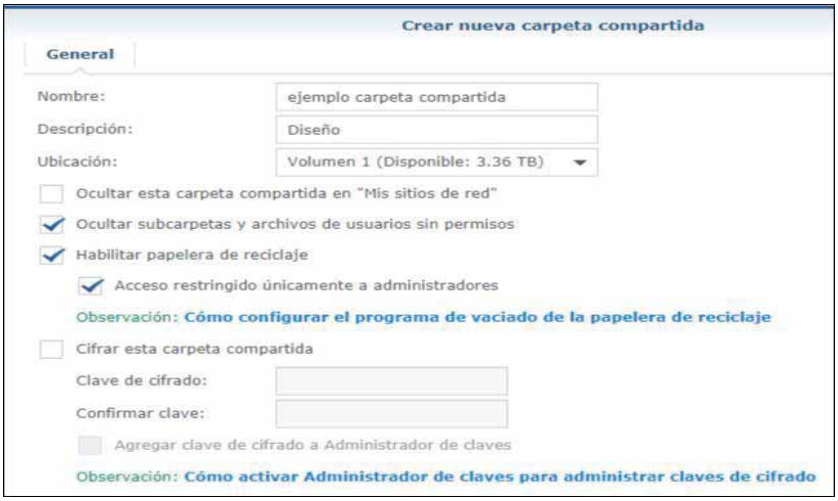

Figura 11. Configuración de la nueva carpeta.

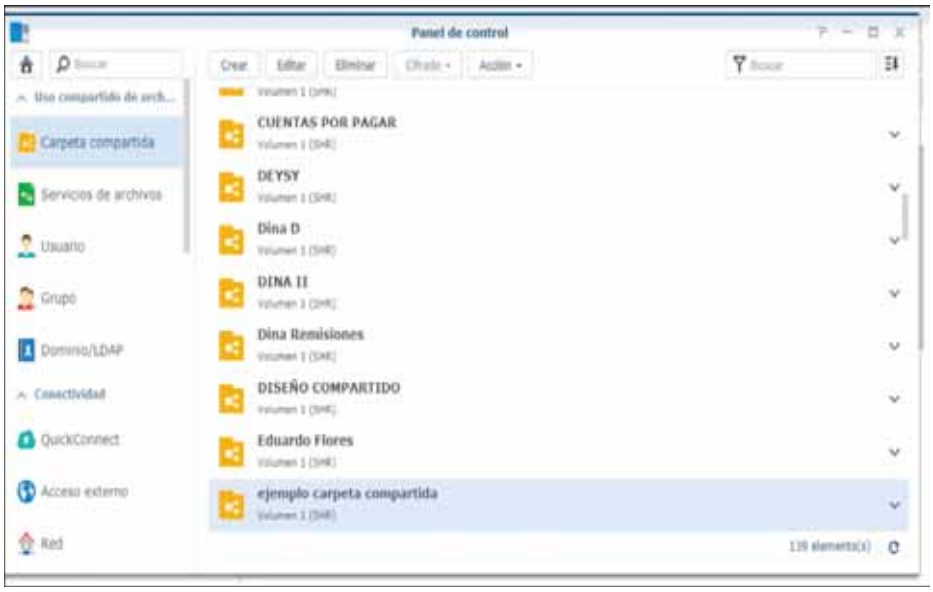

Figura 12. Comprobación de la nueva carpeta.

Configuración de accesos restringidos a la información

Al crear el usuario, se le tiene que dar permisos específicos para que pueda hacer uso de las carpetas que necesite, de acuerdo a las especificaciones dadas por la empresa, los permisos pueden ser de solo lectura o de lectura y escritura.

Para dar los permisos se realizan los siguientes pasos:

Se selecciona la carpeta a la cual se le va a dar permiso, con botón izquierdo del raton se selecciona propiedades (ver Figura 13) en donde aparece una ventana (ver Figura 14) en la cual se elige el usuario que va poder entrar a la carpeta.

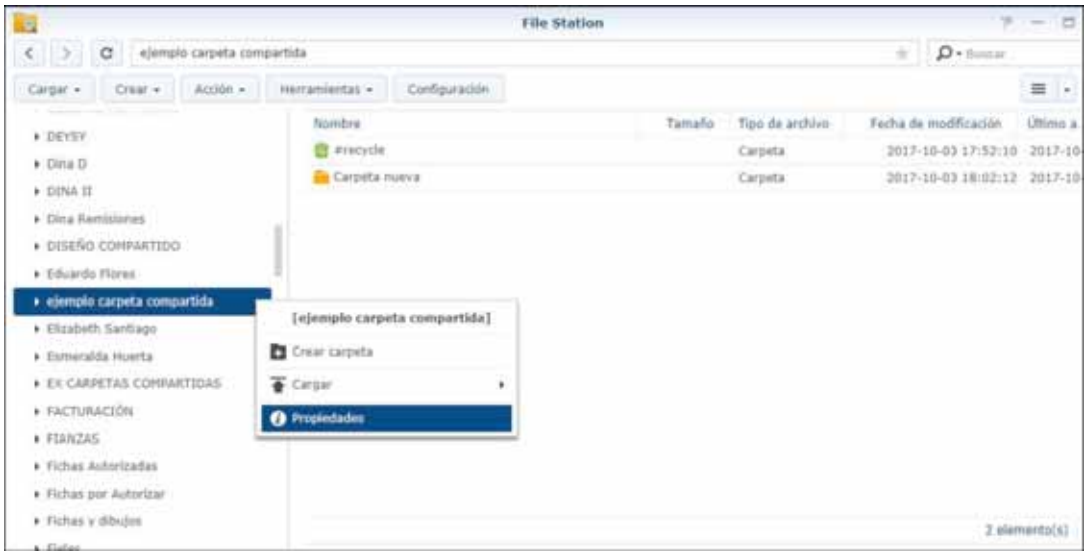

Figura 13. Carpeta a la que se le dará permiso.

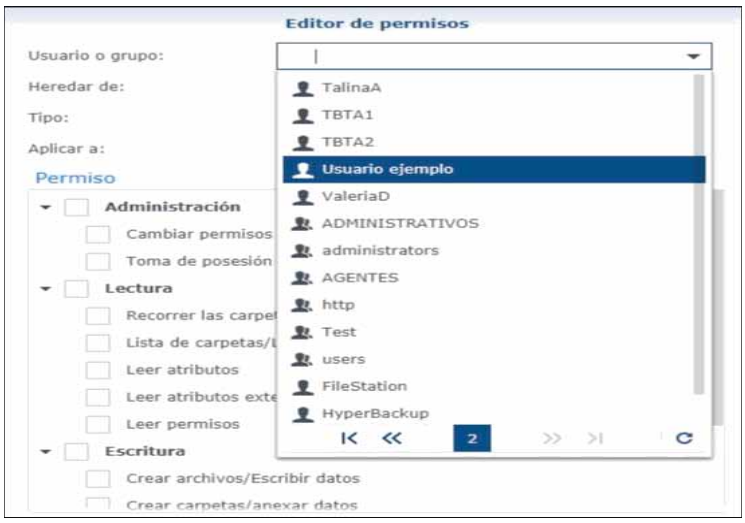

Figura 14. Selección de usuario

En la misma ventana se realiza la configuración de permisos, en usuario o grupo se elige el usuario al cual se le va a dar el permiso; en heredar de se pone ninguno; en tipo se puede elegir dos cosas: denegar o permitir, que en este caso se elige permitir; en aplicar a se elige todo, lo cual indica que el usuario va poder ver todo lo que hay en la carpeta incluyendo las subcarpetas.

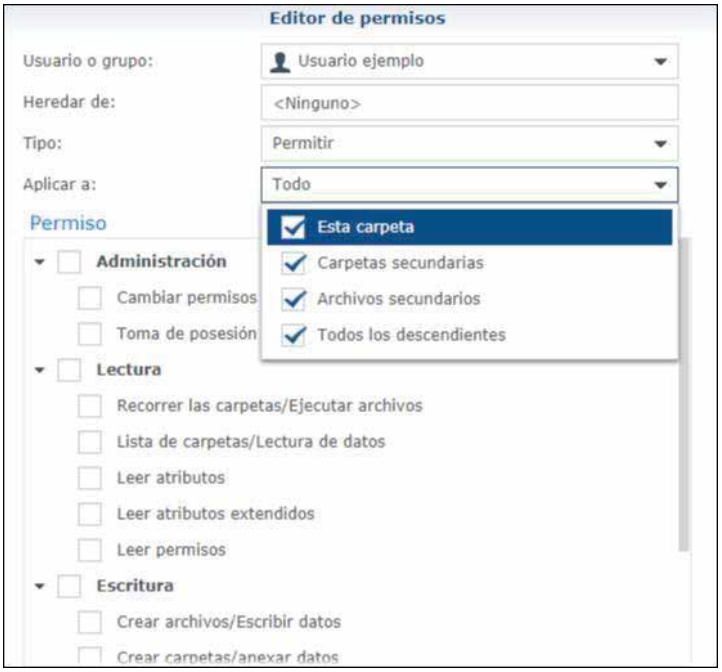

Figura 15. Elección de permisos sobre la carpeta.

Sin salirnos de la ventana activamos la casilla de lectura si se quiere que el usuario pueda solo consultar la información sin poder modificarla, si se requiere que el usuario pueda consultar y modificar la información se activan las casillas lectura y escritura, a ningún usuario se le va dar permisos de administrador.

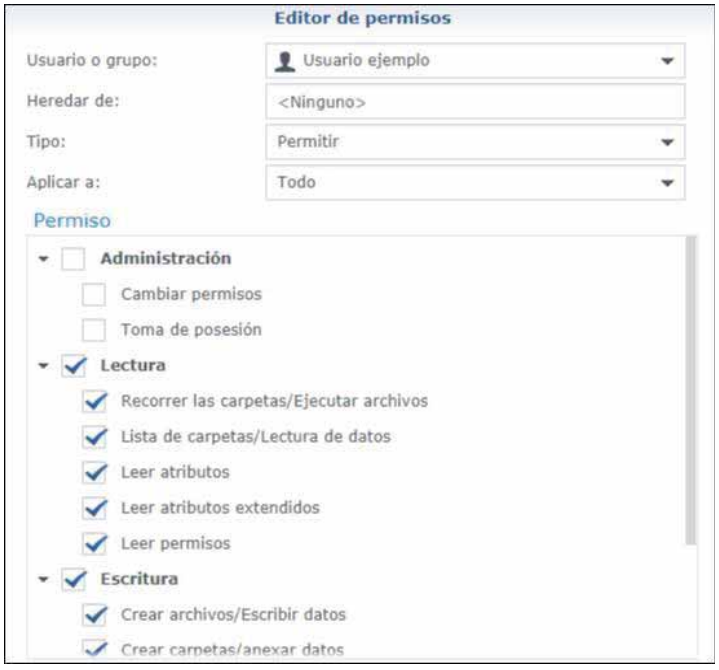

Figura 16. Permisos de lectura y escritura.

Dado los permisos correspondientes se guarda la configuración, y enseguida nos muestra una ventana, en donde se puede ver el usuario con los permisos correspondientes.

Figura 17. Verificación de que el usuario tiene los permisos dados.

A veces es necesario dar permisos para que se pueda consultar una carpeta específica la cual se puede encontrar dentro de otra carpeta, pero se requiere que el usuario solo pueda entrar a esa y no a las demás carpetas. Para ello se siguen los siguientes pasos:

Para poder dar permiso a una subcarpeta primero es necesario darle permiso a toda la carpeta, por lo cual se selecciona la carpeta raíz, en este caso es: ejemplo carpeta compartida, con botón izquierdo del raton elegimos propiedades.

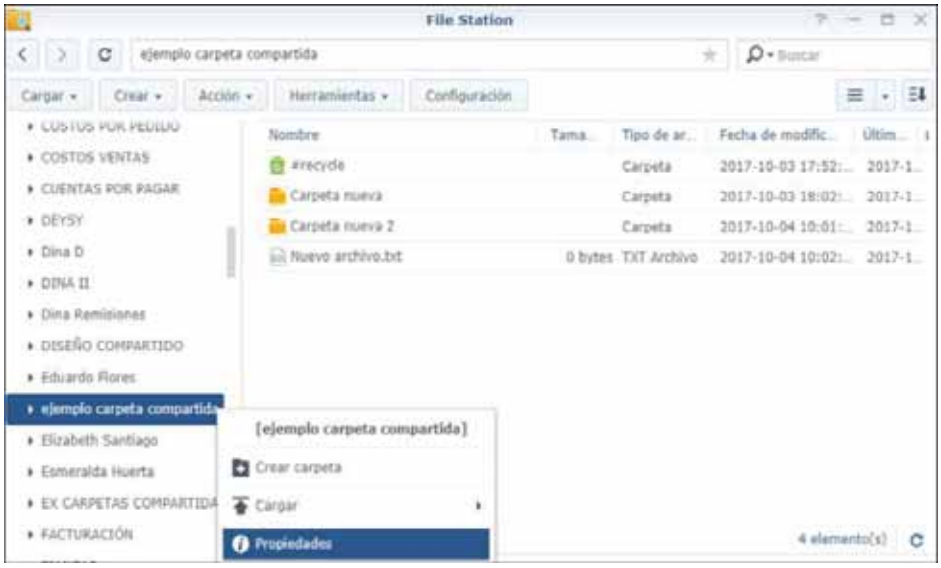

Figura 18. Entrar a las propiedades de la carpeta raíz.

Al entrar en las propiedades de la carpeta se ve una ventana en donde se puede ver los usuarios que tienen permiso de entrar a esa carpeta, en la cual se selecciona crear.

Figura 19. Usuarios que tienen permisos.

Enseguida se selecciona el usuario al cual se le dará permiso (ver Figura 20), en tipo se pone permitir y en aplicar a se activa la casilla esta carpeta para que solo pueda consultar la carpeta seleccionada y no pueda ver las demás carpetas que se encuentran en ella (ver Figura 21).

Figura 20. Selección de usuario

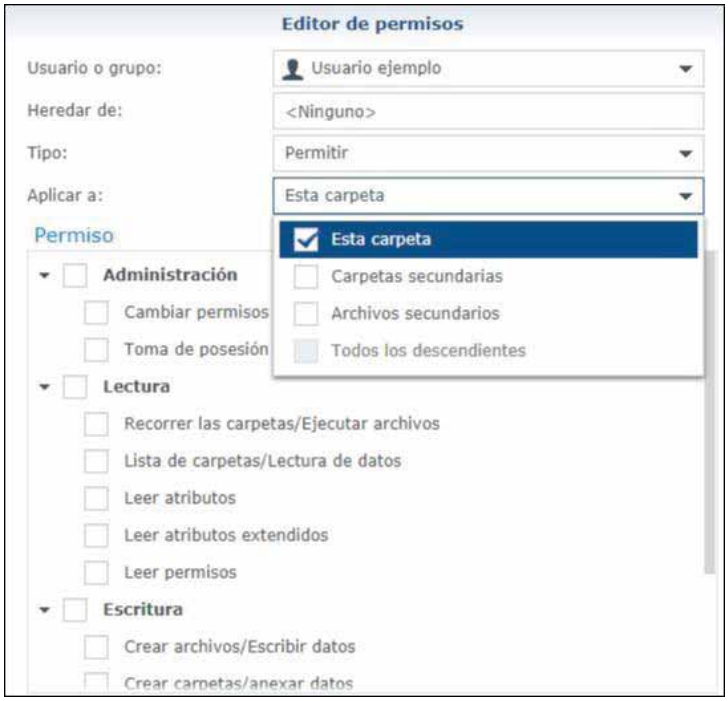

Figura 21. Selección de consulta a una carpeta.

También se le dan permisos de lectura y escritura activando la casilla que en este caso, solo es permiso de lectura.

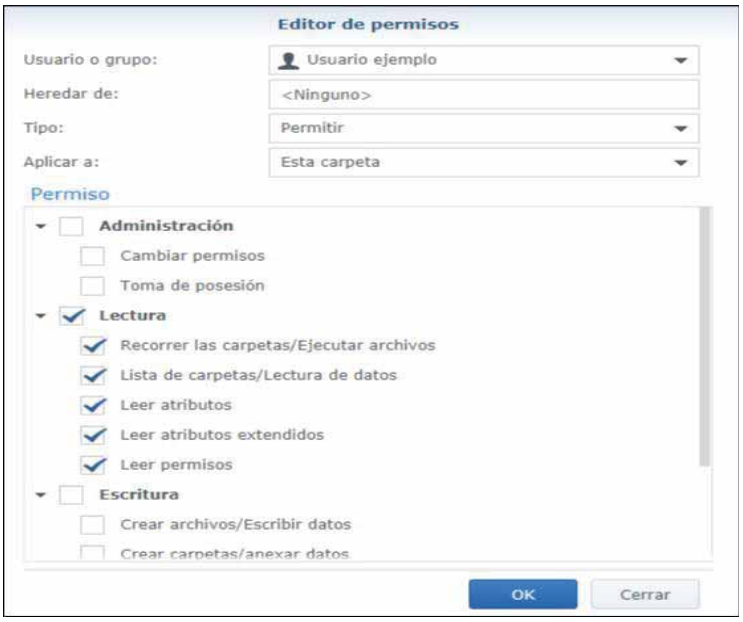

Figura 22. Permiso de lectura.

Al guardar la configuración se muestra el usuario al que se le dio permiso.

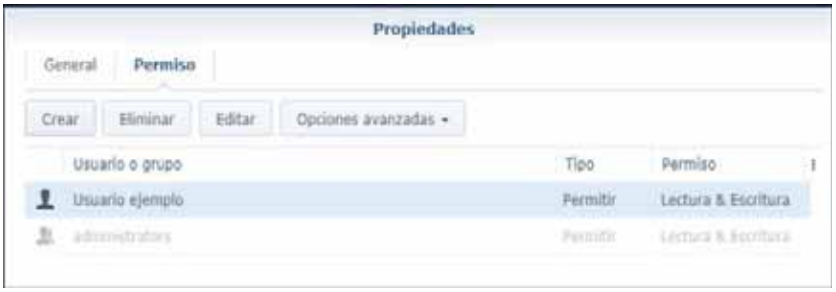

Figura 23. Comprobación de que el usuario tiene los permisos.

Colocación de permisos a los usuarios

Cuando la carpeta es creada se queda almacenada en el synology y el usuario al que se le dio el permiso no puede entrar a ella, debido a que no la tiene activada, por lo cual se necesita colocar la carpeta en el equipo del usuario para que pueda tener acceso a ella con los permisos correspondientes.

Para realizar esto se pone un acceso directo en el equipo del usuario de la siguiente manera:

En el escritorio del equipo con el botón izquierdo se selecciona *nuevo* → *acceso directo.*

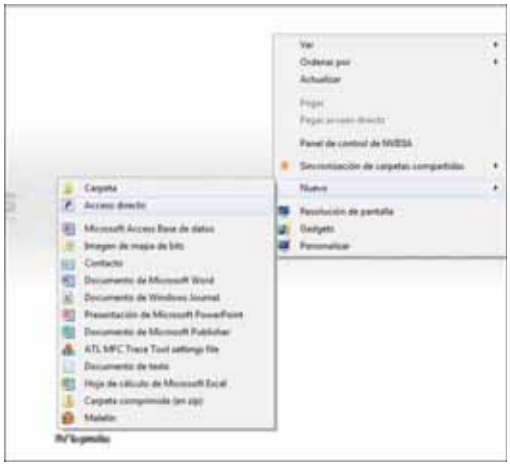

Figura 24. Creación de acceso directo.

Enseguida nos aparece una ventana en donde se pone la ruta de la carpeta creada, la cual se encuentra en el synology (ver Figura 25), al dar siguiente se abre una ventana en donde se pone el nombre del acceso directo(ver Figura 26). Al tener el acceso directo en el equipo del usuario, este puede entrar y consultar la información.

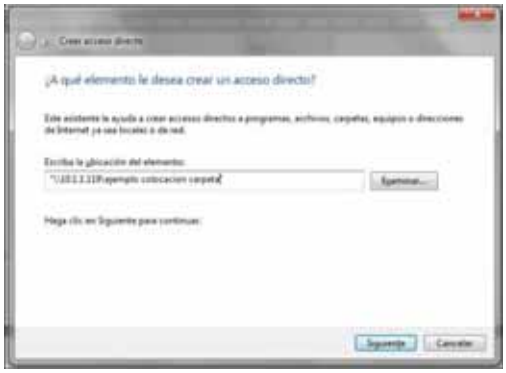

Figura 25. Ruta de la carpeta.

Figura 26. Nombre del acceso.

Configuración de Políticas de Seguridad

Las políticas de seguridad son importantes ya que se tiene un mejor control del sistema informático de la empresa, cada empresa tiene sus propias políticas de seguridad según sus necesidades. En la empresa ABC Uniformes S.A de C.V. se emplearon dos políticas: política de filtrado web y la política de control de aplicaciones.

Política de filtrado web

La política de filtrado web es para evitar que los usuarios de la empresa puedan entrar a páginas web altamente peligrosas, a páginas web para adultos o a páginas web de redes sociales que pudieran poner en riesgo a la empresa o su desempeño en el trabajo. Para llegar a la configuración se va a *Security Profiles→ web filter.*

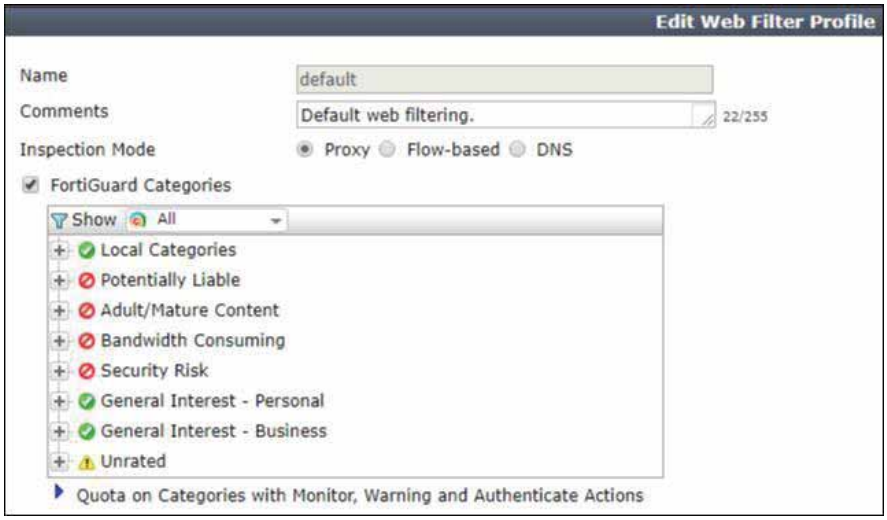

Figura 27. Filtrado web.

Política de control de aplicaciones.

Se emplea para controlar lo que los usuarios realizan al usar el internet. Las aplicaciones están clasificadas por categorías: de juego, acceso remoto, social media (redes sociales como son Facebook, twitter, instagram), video y audio (como es youtube, dailymotion) entre otras, en donde se tiene la alternativa de autorizar, de autoriza pero se está monitoreando o de prohibir. Para llegar a la configuración se va a *Security Profiles→Application Control.*

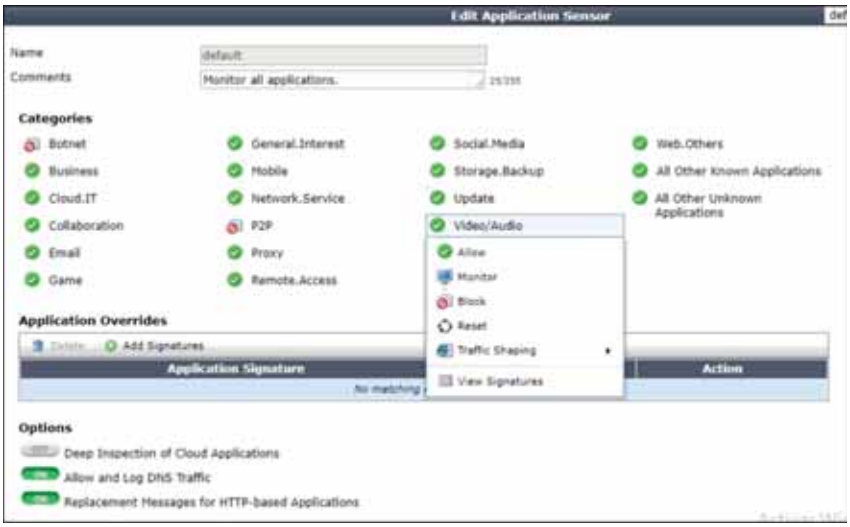

Figura 28. Control de aplicaciones.

Las Políticas de seguridad están clasificadas en tres grupos: el vip, el intermedio y el general. Cada grupo tiene permisos establecidos, para el uso del internet por ejemplo: el vip y el intermedio tiene permiso para acceder a YouTube pero el general no tiene permiso, el vip tiene permiso para consultar cualquier página web pero el intermedio y el general no, el grupo intermedio puede consultar más páginas web que el general. Para llegar a la configuración se va a *Police & Objects→IPv4.*

Figura 29. Grupos de políticas de seguridad.

Creación de usuarios

Se tienen que crear usuarios para que puedan entrar a la red interna de la empresa para ello es necesario acceder al Fortinet FortiGate 90D, se utiliza la dirección 10.1.1.1:9447 en el navegador, que llevará a la siguiente página, en la cual se ingresa el usuario y contraseña.

Figura 30. Autentificarse en el fortinet.

Al entrar en el fortinet se ve el estatus del dispositivo como: el nombre del host, su número serial, la versión y el tiempo en el que ha estado funcionando.

Figura 31. Estatus del dispositivo.

Se selecciona Policy & Objects del menú, el cual abre un submenú en donde se va a *Objects→Addresses*. Ahí se podrá ver una lista con todas las direcciones IP que ya estén ocupadas. Para crear la nueva dirección IP que va ocupar el usuario se selecciona créate new.

Figura 32. Creación de nueva dirección.

El cual lleva a un submenú en el cual se configura la dirección del nuevo usuario de la siguiente manera:

- Category: Address
- Name: SISTEMAS/EjemploUsuario (para este caso).
- Type: va tener un submenú en donde se selecciona “IP/Netmask”.

Figura 33. Configuración de la dirección IP.

- Subnet/IP Range: Se pondrá una dirección que esté en el rango de la empresa y que se haya verificado que no se esté utilizando. El rango se comprende desde la 10.1.1.1 hasta la 10.1.1.255.
- Interface: Será la interface con el nombre “Internal”.
- La casilla de Show in address list siempre será activada.
- Los comentarios son opcionales en caso de haberlos.

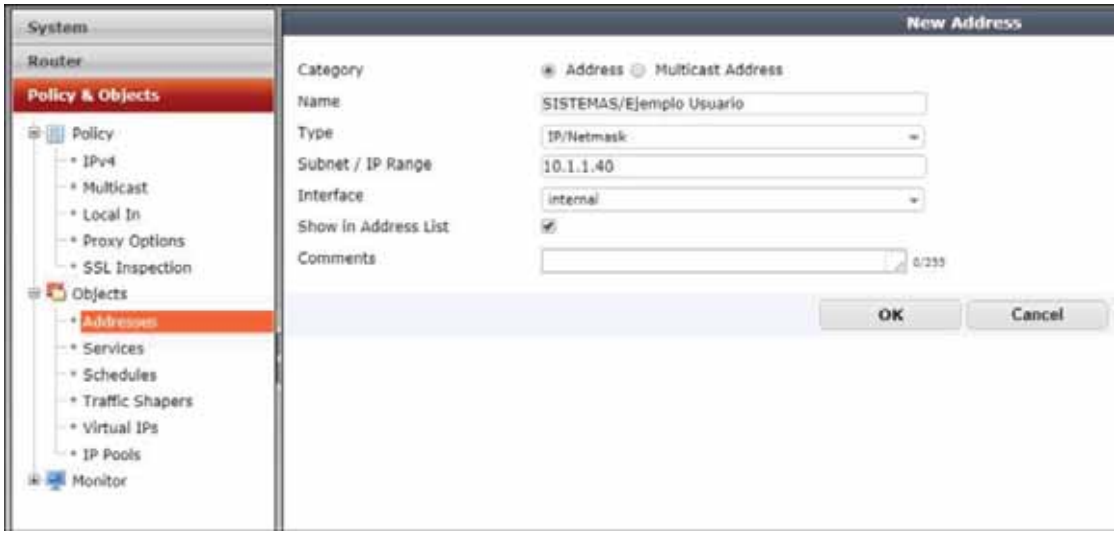

Figura 34. Configuración de la IP 2.

Al guardar el usuario se podrá ver en la lista de direcciones. En el caso en que se llegara a duplicar la dirección IP la segunda dirección que se ponga no podrá tener salida a internet.

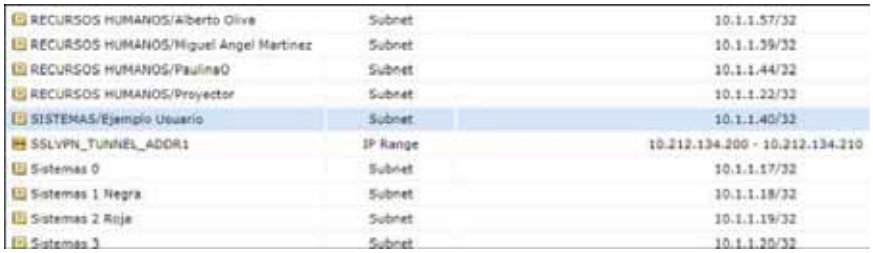

Figura 35. Verificación de la dirección IP creada.

Al tener la dirección IP creada se tiene que agregar a un grupo nuevo para que se cumplan las políticas de seguridad creadas anteriormente, de lo contrario no se tendrá salida a internet.

En el mismo menú, *Policy & objects → objects → addresses,* se desliza la ventana hacia abajo donde se encuentran los grupos existentes, en los cuales se agrega la nueva dirección IP, dependiendo de los permisos que se le tengan que dar.

Figura 36. Grupos de políticas de seguridad.

En este caso se agrega al grupo general. Se da clic derecho sobre el grupo al que se va agregar, y se selecciona la opción editar.

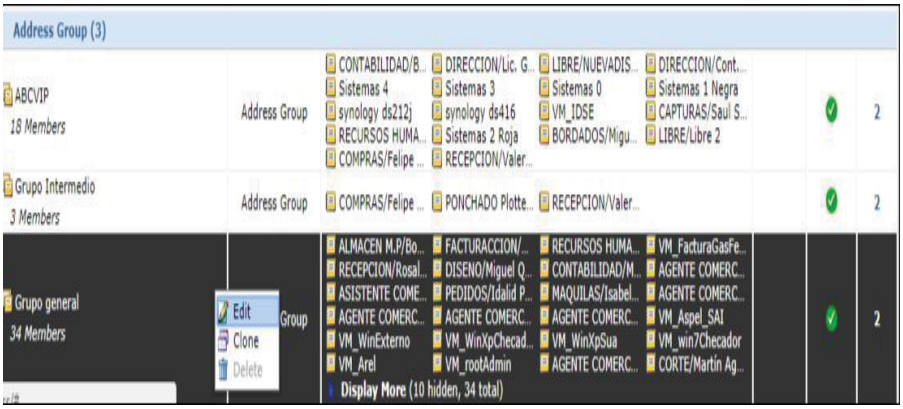

Figura 37. Elección de grupo.

Esto hace que se muestren los objetos agregados a este grupo, y dando clic en el ícono "+" se tiene la opción de agregar.

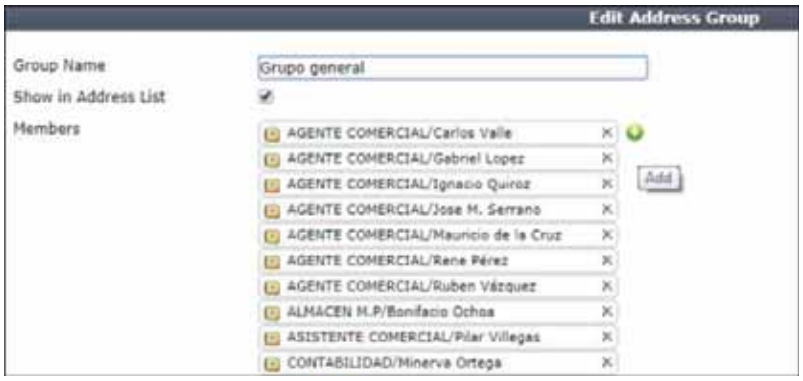

Figura 38. Agregar nuevo usuario.

Al seleccionar el símbolo "+" se desplegara un submenú con todas las direcciones IP creadas, en donde se busca la dirección que se creó, que es *SISTEMAS/Ejemplo Usuario*, al guardarlo se mostrara en el grupo al que fue agregado.

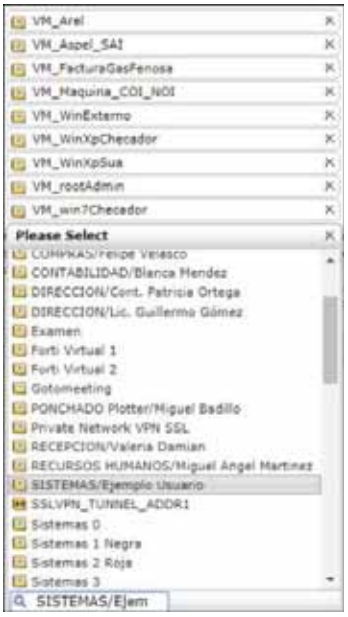

Figura 39. Selección de usuario.

Creación de usuarios VPN

En la empresa se requiere que los usuarios puedan consultar la información desde una red externa, lo cual se puede llevar a cabo con la implementación de una VPN SSL, el cual es un medio seguro para que se puedan conectar los usuarios desde una red externa a la red interna de la empresa, y poder trabajar sin necesidad de encontrarse físicamente en el establecimiento.

Para la creación de usuarios VPN es necesario ingresar al fortinet de la misma manera en la cual se entró en la creación de usuarios anteriormente descrita, también se utiliza la dirección 10.1.1.1:9447 en donde se tiene que autentificar.

Figura 40. Autentificación

Dentro del fortinet se dirige a *User & Device → User Definition* en donde se visualiza la lista de usuarios que cuentan con VPN. Para crear un nuevo usuario se selecciona Create New.

Figura 41. Creación de usuario VPN.

Al seleccionar Create New se muestra un submenú en donde se configura el usuario de la siguiente manera:

- User Type: se activa la casilla Local User (ver Figura 42).
- Login Credentials: se ingresa el nombre del usuario que en este caso es *usuario prueba* (ver Figura 43).
- Contact Info: se ingresa el correo electrónico esto es opcional (ver Figura 44).
- Extra Info: se selecciona el grupo de políticas de seguridad al que va a pertenecer el usuario que en este caso es *Prevención* y se activan las casillas enable y user group (ver Figura 45).

Figura 42. Tipo de usuario.

Figura 43. Ingreso de nombre y usuario.

Figura 44. Ingreso de correo electrónico.

Figura 45. Elección de grupo de políticas de seguridad.

Al guardar la configuración del nuevo usuario se podrá ver en la lista de usuarios.

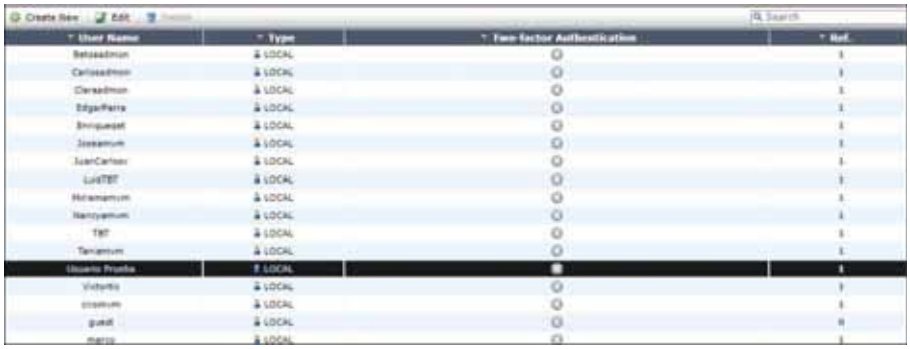

Figura 46. Comprobación de usuario VPN creado.

Eliminación de usuarios de VPN

Con el cambio de personal que se presenta en la empresa es necesario depurar a los usuarios que ya no laboran, como medida de seguridad para evitar cualquier filtración de información.

Para eliminar un usuario de VPN se siguen los siguientes pasos:

- Como todos los usuarios están en un grupo determinado, en donde se rigen las políticas de seguridad, primero se tiene que quitar de ese grupo para su posterior eliminación, de lo contrario no se puede eliminar el usuario. Para realizar esto se dirige a *User & Device -> User Groups*.

Figura 47. Grupos con las políticas de seguridad.

- Se selecciona el grupo en el cual se encuentra el usuario y con botón derecho del raton se elige Edit.

Figura 48. Elección del grupo en donde se encuentra el usuario.

- En donde se busca el usuario que se desea eliminar que en este caso es *usuario prueba*, ya encontrado se le da en el símbolo “x” para eliminarlo y se guarda la operación realizada.

Figura 49. Eliminación del usuario del grupo.

- Al haberlo eliminado del grupo se procede a eliminar el usuario, para ello en la misma ruta *User & Device -> User Groups* se selecciona el usuario que se desea eliminar y se le da Delete con esto el usuario ya está eliminado.

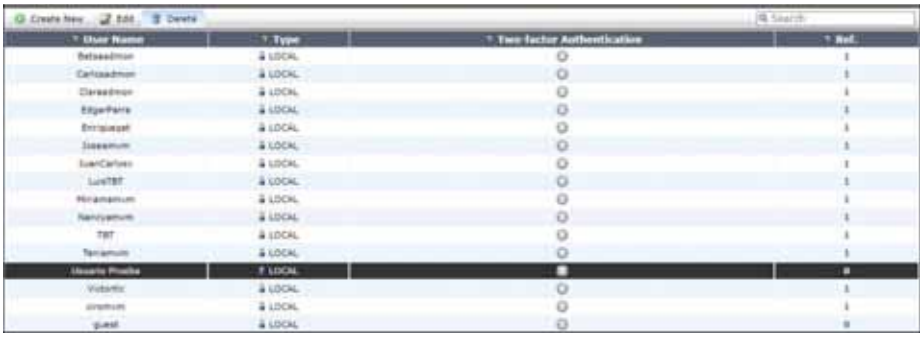

Figura 50. Eliminación del usuario en el sistema.

Configuración para poder conectarse a la VPN SSL

Al estar creado el usuario de VPN, es necesario darle acceso al usuario para que pueda entrar a la red interna desde una red externa de manera segura, para ello es necesario configurar el equipo del usuario haciendo uso del software FortiClient de la siguiente manera:

- Se ejecuta el programa FortiClient y se selecciona Remote Access.

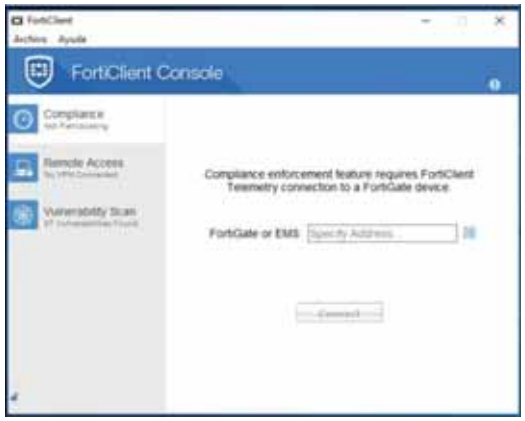

Figura 51. Ejecución del programa.

- En donde se ingresa la información para llevar a cabo la conexión, la cual es: Nombre de la conexión este puede ser cualquier nombre; Descripción esta es optativa solo si se requiere poner algún comentario; Remote Gateway es la dirección IP del fortinet con el formato 10.1.1.x; Autenticación se activa Save login para que se guarde la configuración del usuario.

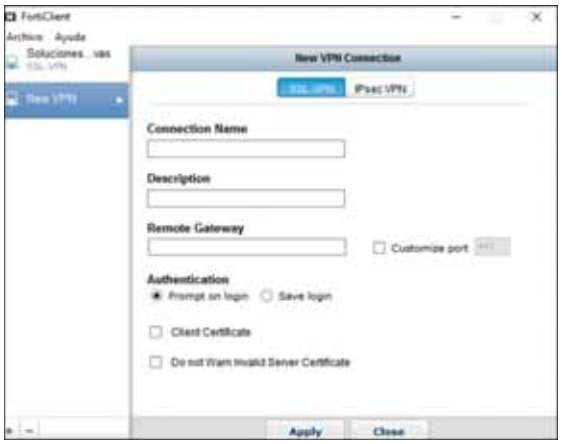

Figura 52. Configuración de la conexión.

Realizada la configuración se procede a conectarse para verificar que la conexión se realice de manera segura. Se utiliza el mismo programa, como la configuración fue guardada, al ejecutar nuevamente el programa solo pedirá la contraseña del usuario, esta es la que se puso en la creación del usuario VPN.

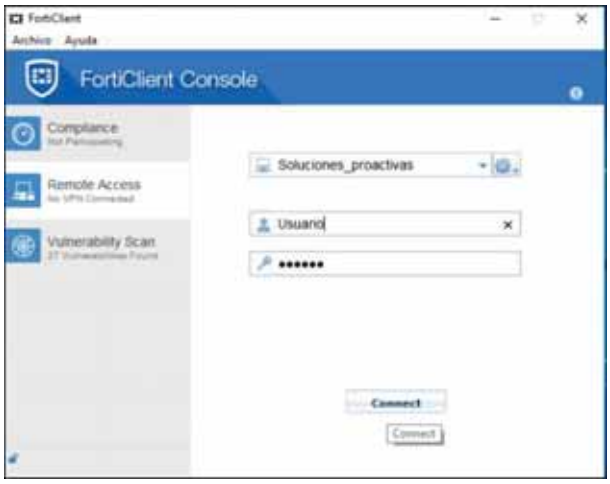

Figura 53. Autenticación.

Al realizar la conexión, aparece una ventana de alerta de seguridad en donde se le da "si".

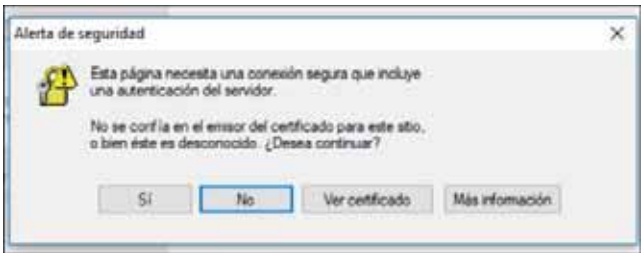

Figura 54. Alerta de seguridad.

Si la conexión se realizó bien, la ventana mostrara el tiempo que lleva conectado y los bytes de transmisión utilizados, con esto ya se está conectado a la red interna de la empresa pero falta el poder conectarse al synology para poder ver la información que se necesita.

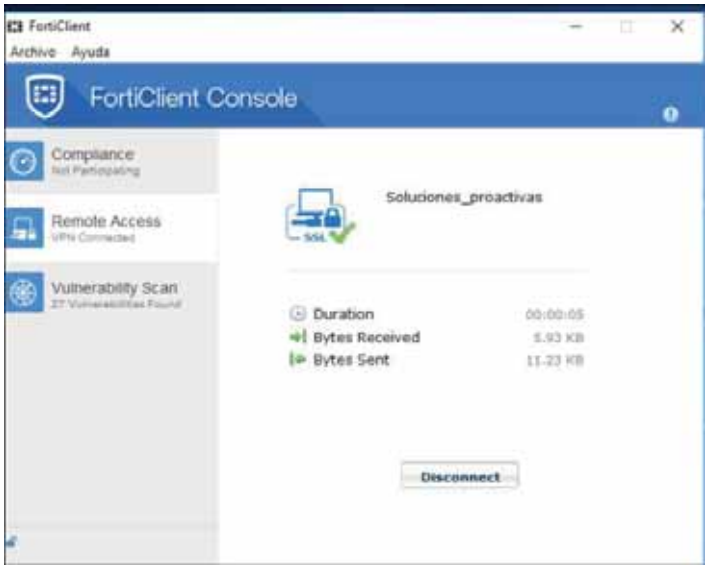

Figura 55. Conexión establecida.

La conexión al synology es sencilla, como cada usuario ya tiene configurado las credenciales necesarias en su equipo, solo tiene que introducir su usuario y contraseña para poder hacer uso de la información.

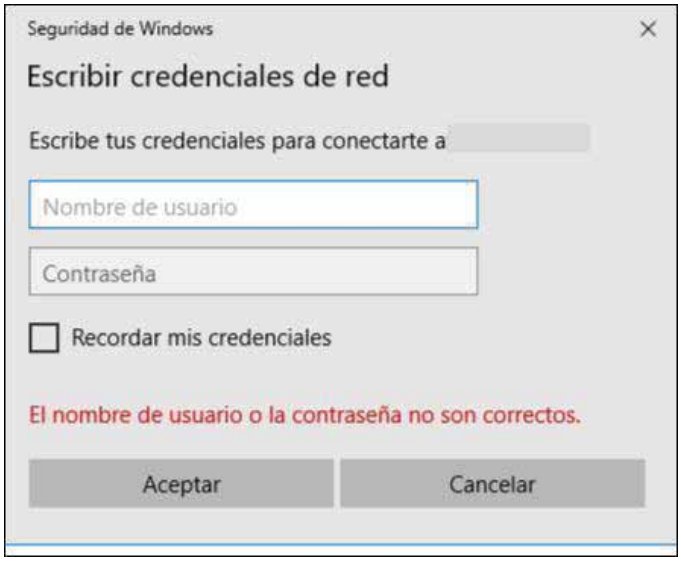

Figura 56. Credenciales de red.

Panda Cloud Security

El programa Panda Cloud Security se puede utilizar de muchas maneras, en este caso se emplea en el sistema de seguridad para la monitorización de los usuarios de la empresa, así como en el bloqueo de puertos de los equipos, ya que la seguridad esta implementada en el fortinet. Para ello es necesario que el programa este instalado en todos los equipos de la empresa.

Bloqueo de puertos en los equipos de los usuarios

Para mantener la seguridad de la información de la empresa es necesario bloquear los puertos de los equipos de los usuarios ya que se puede filtrar información de manera intencional o accidental. El bloqueo de USB es una medida para evitar que entre algún *malware* al sistema y prevenir que los usuarios saquen información confidencial de la empresa.

Para realizar el bloqueo de puertos se tiene que entrar al sistema por medio de la página web **https://www.pandacloudsecurity.com/** en donde se tiene que ingresar el correo electrónico con el que se dio de alta el programa que lleva el siguiente formato: nombre@dominio de la empresa y la contraseña.

Figura 57.Autentificacion en el panda.

Para realizar el bloqueo de USB con el Panda Cloud se realiza lo siguiente:

Ya dentro del sistema se ingresa a Endpoint Protection Plus en donde se selecciona la pestaña de configuración en el cual se crea un grupo, que en este caso lo llamare "pruebas" para ello en la sección de la izquierda doy clic en el icono "+".

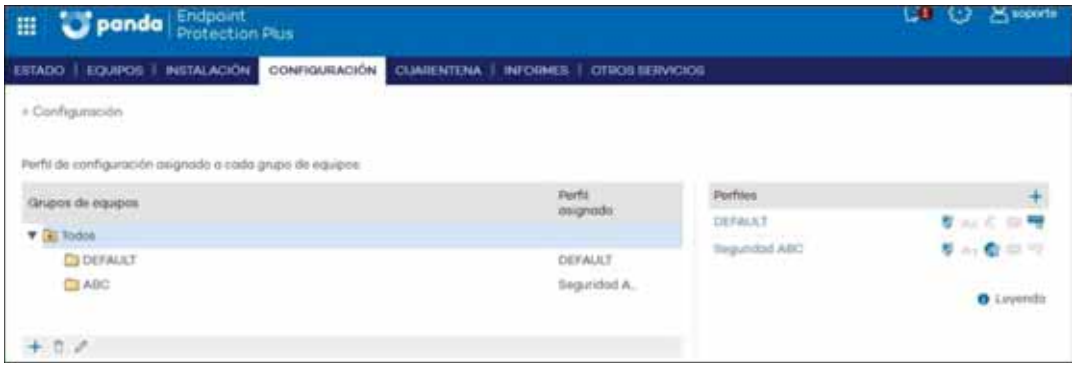

Figura 58.Creacion de grupo.

Dónde se configura un perfil para el grupo, en el cual van a estar los equipos, es más factible crear un grupo en donde se vayan agregando los usuarios nuevos, en vez de configurarlo cada vez que entre un nuevo usuario.

Figura 59.Perfil del grupo.

Como se quiere bloquear los puertos USB nos vamos a la sección Control de dispositivos en donde se visualizan diferentes dispositivos. Se tiene que activar la casilla Activar el control de dispositivos para que se pueda modificar, enseguida se elige en la sección de Comportamiento la opción de Unidades de almacenamiento extraíbles y se selecciona del submenú la propiedad de Bloquear.

Figura 60.Bloqueo de USB.

En caso de querer generar alguna excepción sobre algún dispositivo se agregaran en este apartado.

Figura 61.Excepción de dispositivo.

De regreso con la configuración del grupo creado se le asigna el perfil que se ha creado que es pruebas.

Figura 62.Eleccion de grupo.

Quedando el nuevo grupo “pruebas” en el sistema del Panda Cloud.

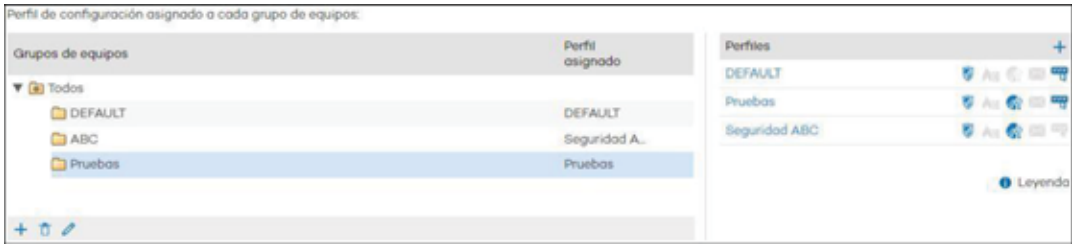

Figura 63.Grupo pruebas creado.

Como el grupo ya está creado, ahora se tiene que mover a los usuarios, a los cuales se quiere aplicar el perfil (bloqueo de USB). Para ello se va a la sección de equipos.

Se seleccionan los equipos y se da clic en mover, en donde el sistema pedirá seleccionar el grupo al que se quiere mover que en este caso es “pruebas”.

Figura 64. Movimiento de equipos.

Con esto se bloquea el USB en los equipos que están en el grupo.

Acceso remoto

A veces es necesario entrar al equipo de un usuario que no se encuentra en la empresa por lo cual se tiene que acceder remotamente al equipo. En la lista de usuarios que se tiene en el panda hay un apartado en donde señala si se tiene activado el acceso remoto, si está activado se podrá ver un icono color azul de lo contrario va estar gris, esto quiere decir, que se va poder acceder solo a los equipos que estén activados, los que están activados son los equipos que se encuentran prendidos.

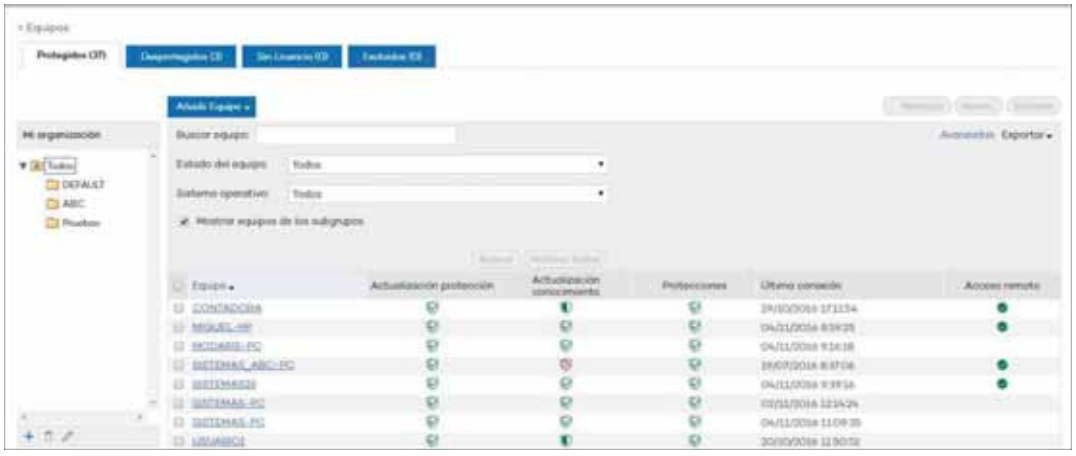

Figura 65. Equipos con acceso remoto activado.

En la pestaña Devices se puede ver el hostname de los equipos, al igual se puede saber si es un equipo de escritorio o portátil y la dirección IP que tiene. En cada uno de los equipos hay un icono en forma de ojo que al seleccionarlo se puede acceder remotamente al equipo.

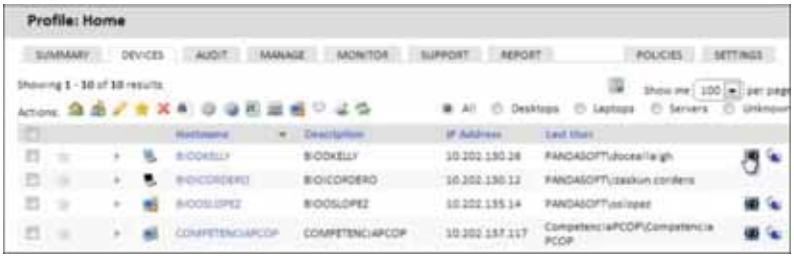

Figura 66. Propiedades de los equipos.

Al entrar se podrá ver el escritorio del equipo o en su caso lo que esté realizando el usuario, en la ventana del panda también se podrá realizar una conversación en tiempo real con el usuario. Con esto se puede dar apoyo al usuario o en su caso poder monitorearlo, ya que con este programa no se necesita de la autorización del usuario para poder entrar al equipo. Existen una variedad de programas que te permiten acceder remotamente a un equipo como por ejemplo: TeamViewer, NoMachine, y AnyDesk pero estos te piden autorización de parte del usuario.

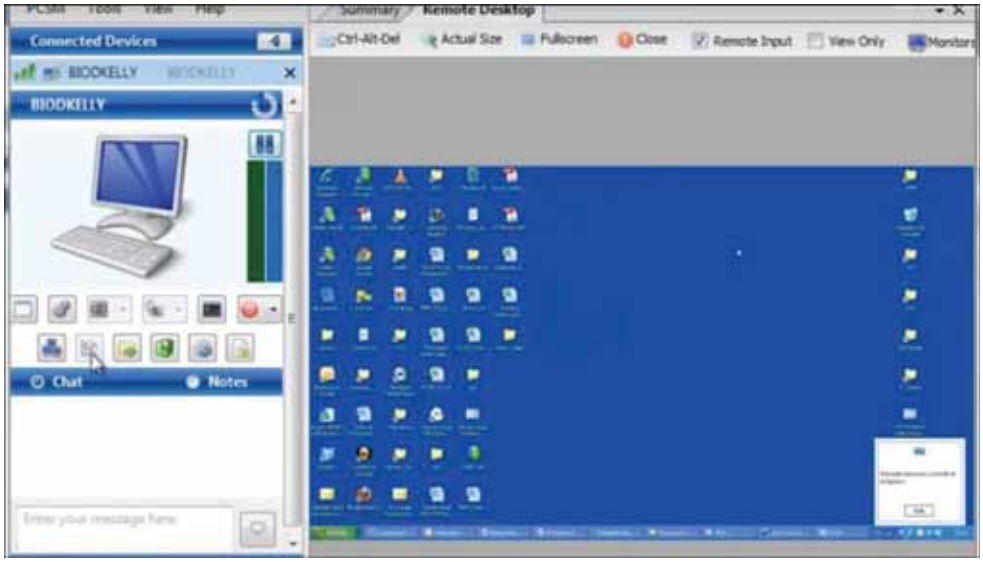

Figura 67. Dentro del equipo.

Resultados

El sistema de seguridad fue realizado de acuerdo a lo descrito en la propuesta, ya que se implementaron las políticas de seguridad de acuerdo a las necesidades de la empresa, se creó un canal de comunicación seguro para que el personal pudiera acceder a la red de la empresa sin necesidad de estar físicamente en ella. Se crearon carpetas en el NAS con la información de la empresa, estas se hicieron compartidas debido a que más de un usuario necesita la misma información y al utilizar este mecanismo los usuarios que tengan permiso de entrar a la carpeta podrán ver los cambios realizados en el documento, sin necesidad de que el usuario que modificó el documento se lo tenga que enviar a todos los usuarios que lo utilizan. En pocas palabras la información está en red.

También se implementó un sistema de monitorización en donde se puede ver lo que están haciendo los usuarios, con este sistema también se puede apoyar a los usuarios que no se encuentre en la empresa.

Análisis y discusión de resultados

Que los usuarios trabajen en carpetas compartidas (que se encuentran almacenadas en el sinology) es un mecanismo de seguridad, ya que se garantiza que el trabajo realizado va estar respaldado en el servidor y cualquier problema que pudiera tener el equipo, la información no se pierde. Además, al perderse la conexión del internet no afecta la utilización de las carpetas ya que están en la red interna de la empresa. Sin embargo, si le llegara a pasar algo al synology sí habría problemas ya que ahí está concentrada toda la información.

Lo mismo pasa con el fortinet, su utilización es cómoda y útil, pero toda la protección del sistema se concentra en el dispositivo y al haber un problema con él afectaría a los usuarios directamente.

Se debe tener mucho cuidado con la implementación de las políticas de seguridad, ya que si no se aplican de la manera correcta, se puede tener problemas con la efectividad de los equipos ya que estas tienen un nivel de prioridad y si no se llegara a cumplir la primera política toma la segunda y así sucesivamente, causando un problema de seguridad en el sistema, ya que los usuarios podrían entrar a páginas web con malware, o simplemente que las políticas entren en conflicto entre sí, por ello se tienen que diseñar e implementar de la mejor manera posible.

Conclusiones

Se puede concluir que en la estancia realizada en la empresa T&B Talent, me dejó mucho aprendizaje, ya que conocí nuevos dispositivos y aprendí para qué se emplean y cómo se utilizan cada uno de ellos.

La utilización del fortinet es un reto por lo cual uno se tiene que documentar sobre él, para poder utilizarlo. A lo largo del documento se describen los pasos para la creación del sistema, a simple vista uno pensaría que es fácil su implementación pero no es así ya que hay que saber qué tipo de configuraciones se tienen que realizar, por ejemplo en la VPN SSL se realizó un tunnel encriptado para hacer un canal de transmisión seguro, en donde la conexión no fuera de riesgo.

Al realizar el proyecto en la modalidad de estancia profesional fue benéfico ya que me pude dar una idea de cómo es el campo laboral y de los problemas que pueden surgir.

Referencias bibliográficas

[1] L. Moran Camero, "Implementar niveles de seguridad que fortalezcan la seguridad informática de un empresa," proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2016.

[2] M. A. Ruiz Mompala, "Configuración e implementación de políticas de seguridad para la protección de una red corporativa," proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2014.

[3] G. Donaciano Escobar, "Administración y seguridad de una red corporativa mediante un firewall fortigate 90D," proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2016.

[4] D. O. Esmoris, "Control de Acceso a Redes", tesis, Universidad Nacional de La Plata, Ciudad de La Plata, Buenos Aires, 2010.

[5] G. C. Torres Anda gana, "Estudio e Implementación de una Metodología de prevención de intrusos para redes LAN", tesis, Escuela Superior Politécnica de Chimborazo, Ecuador, 2010.

[6] A. E. Conza González, "Diseño e Implementación de un prototipo de DMZ y la Interconexión segura mediante VPN utilizando el firewall fortigate 60", tesis, Escuela Politécnica Nacional, Ecuador, 2006.

[7] C. A. Dussan Clavijo, "Políticas de Seguridad Informática," Red de Revistas Científicas de América Latina y el Caribe, España y Portugal, Vol.2, No. 1, 2006.

[8] A. Gomez Vieites, “Enciclopedia de la Seguridad Informática,” Segunda Edición, editorial Ra-Ma.

Información sobre el Fortinet: **https://www.fortinet.com/** consultada por última vez el 25 de febrero del 2018.

Información sobre VPN SSL**:** **http://searchdatacenter.techtarget.com/es/definicion/VPN-SSL** **consultada por** última vez el 25 de febrero del 2018.

Información sobre el Panda Cloud Security: **https://www.pandasecurity.com/mexico/** Consultada por última vez el 25 de febrero