

Universidad Autónoma Metropolitana  
Unidad Azcapotzalco  
División de Ciencias Básicas e Ingeniería  
  
Licenciatura en Ingeniería en Computación

Proyecto de integración:

Estancia Profesional

**Seguridad perimetral en una red de computadoras empresarial.**

Empresa: T&B Talent S.A. de C.V.


Alumno: Saúl Amado Ramírez  
Matricula: 210335140

Asesor interno: José Alfredo Estrada Soto


Asesor externo: Mario Ernesto Gómez Romero

Trimestre 2017 Primavera.  
30 de agosto de 2017

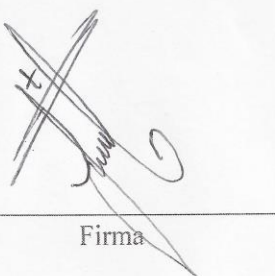
Yo, José Alfredo Estrada Soto, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

  
Firma

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.

  
Firma

Yo, Saúl Amado Ramírez, 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.

  
Firma

**Resumen:**

La seguridad informática es cada vez más compleja ya que se necesitan implementar tecnologías y procedimientos robustos para autenticar y resguardar los datos que viajan a través de las redes computacionales. En dicha seguridad, se deben de adoptar medidas tales como: autenticidad, confidencialidad, disponibilidad, integridad, privacidad y auditoria de los datos, que constantemente se desplazan a través de la red dentro de la empresa.

Dichas tecnologías son creadas para proteger los datos que pueden ser modificados y alterados por terceras personas, usuarios o software ajenos a la empresa, el problema es mitigado cifrando los datos que se envían y reciben en la red e implementando medidas de seguridad acorde a las vulnerabilidades de la red. El propósito es proporcionar la comunicación segura entre el emisor y receptor, esto se logra dotando sólo a personal capacitado con derechos de acceso, aumentando así la productividad y flexibilidad de la red y aplicaciones empresariales, alcanzando una mejora en la red empresarial, ya que el objetivo principal es implementar medidas que permitan establecer una seguridad perimetral mejorando la eficacia y nivel de seguridad de la red dentro de la empresa, para la integridad y confidencialidad de los datos y por ende, dar un servicio seguro y garantizado a la empresa.

Este escrito está dirigido a la implementación de estrategias y políticas de seguridad con base a las necesidades del cliente de la empresa T&B Talent S.A. de C.V.: Artículos Básicos de Calidad en Uniformes y Equipos S.A. de C.V., con el objetivo de minimizar las vulnerabilidades de los bienes y recursos, aumentando la seguridad y confidencialidad de los datos.

# Tabla de contenido

	Pág.
1. Índice de imágenes .....	5
2. Índice de diagramas.....	7
3. Introducción .....	8
4. Antecedentes .....	9
5. Justificación.....	12
6. Objetivos .....	13
6.1. General.....	13
6.2. Específicos.....	13
7. Marco teórico .....	13
8. Desarrollo del proyecto.....	16
8.1. Virtualización de un servidor con VMware vSphere ESXi 5.0 .....	18
8.2. Administrar y gestionar un servidor ESXi usando VMware vSphere Client.....	23
8.3. Configuración del equipo FortiGate 90D .....	25
8.3.1. Configuración de Interfaces.....	25
8.3.2. Configuración de Políticas.....	27
8.3.3. Configuración de Objetos y Grupos.....	29
8.3.4. Configuración de Perfiles de seguridad .....	31
8.4. Administración y gestión de tareas avanzadas del servidor Synology NAS .....	33
8.4.1. Comprobar la información del sistema .....	34
8.4.2. Verificar registros del sistema.....	34
8.4.3. Supervisar recursos del sistema .....	34
8.4.4. Analizar el uso del sistema.....	34
8.4.5. Automatizar tareas .....	35
8.4.6. Actualizar DSM o restaurar los valores predeterminados.....	35
9. Resultados .....	36
10. Análisis y discusión de resultados.....	37
11. Conclusiones .....	37
12. Referencias bibliográficas.....	39
13. Anexos .....	39
13.1. Inventario de equipos .....	39
13.2. Manual para dar de alta un correo electrónico en cPanel .....	40

# 1. Índice de imágenes.

	Pág.
Imagen 1: Instalación de ESXi 5.0.....	18
Imagen 2: Descarga de los módulos de instalación.....	18
Imagen 3: Aceptar términos de la licencia.....	19
Imagen 4: Continuar con la instalación.....	19
Imagen 5: Detección de discos duros.....	20
Imagen 6: Selección del idioma.....	20
Imagen 7: Ingresar una contraseña.....	21
Imagen 8: Confirmar la instalación.....	21
Imagen 9: Estatus del porcentaje de instalación.....	21
Imagen 10: Reiniciar para terminar la instalación.....	22
Imagen 11: Inicio de VMware ESXi 5.0.....	22
Imagen 12: Inicio de instalación de VMware vSphere Client.....	23
Imagen 13: Finalizamos el proceso de instalación.....	23
Imagen 14: Iniciar VMware vSphere Client.....	24
Imagen 15: Interfaz de VMware vSphere Client.....	24
Imagen 16: Información del FortiGate 90D.....	25
Imagen 17: Configuración de la Interface Internal.....	26
Imagen 18: Lista de interfaces configuradas.....	26
Imagen 19: Configuración de una nueva política de seguridad.....	27
Imagen 20: Políticas de seguridad aplicadas en la red.....	28
Imagen 21: Monitoreo de políticas de seguridad.....	28
Imagen 22: Creación de un nuevo objeto.....	29
Imagen 23: Crear un objeto de dirección.....	29
Imagen 24: Llenado de campos para crear el objeto.....	29
Imagen 25: Creación de un grupo en el FortiGate.....	30
Imagen 26: Configuración del tráfico de transmisión.....	30
Imagen 27: Configuración de equipos con NAT.....	30
Imagen 28: Configuración del Web Filter.....	31
Imagen 29: Monitoreo de aplicaciones y servicios.....	31
Imagen 30: Bloqueo de aplicaciones y servicios.....	32

Imagen 31: Agregar páginas web para ser bloqueadas .....	32
Imagen 32: Centro de información del Synology NAS .....	33
Imagen 33: Información de cada recurso en el Synology NAS .....	34
Imagen 34: Análisis del almacenamiento.....	35
Imagen 35: Actualización del DSM.....	35
Imagen 36: Inventario de equipos de la empresa ABC Uniformes S.A. de C.V.....	39
Imagen 37: Ingreso al sistema cPanel .....	40
Imagen 38: Crear cuentas de correo electrónico .....	40
Imagen 39: Ingresar datos de usuario.....	41
Imagen 40: Configuración en Outlook.....	41
Imagen 41: Configuración de datos del servidor de correo.....	42
Imagen 42: Configuración del servidor de salida.....	42
Imagen 43: Opciones avanzadas .....	43
Imagen 44: Probar configuración de la cuenta.....	43
Imagen 45: Correo configurado correctamente.....	43

## 2. Índice de diagramas.

	Pág.
Diagrama 1: Diagrama de red de la empresa ABC Uniformes S.A. de C.V.....	16
Diagrama 2: Diagrama de configuración de las políticas de seguridad. ....	27

### **3. Introducción**

Una de las soluciones y servicios de seguridad para empresas es implementar un sistema de seguridad perimetral. Todas las empresas, independientemente de su tamaño y del sector al que se dediquen, actualmente tienen algún tipo de sistema de seguridad perimetral para defensa de ataques informáticos. Dichos sistemas son responsables de la seguridad del sistema informático de una empresa contra amenazas externas, como virus, gusanos, troyanos, ataques de denegación de servicio, robo o destrucción de datos, etc.

Los sistemas de seguridad perimetral proporcionan protección dentro de las capas del modelo OSI. En un primer grupo nos encontramos con las tres primeras capas que son la física, el enlace de datos y la red, en donde se debe dar protección contra amenazas como ataques de hackers, las intrusiones o el robo de información en las conexiones remotas. En un segundo grupo abarca las capas de transporte, sesión, presentación y aplicación que es todo el contenido que se transporta por la red, el sistema de seguridad perimetral para contenido proporciona protección contra amenazas como malware, gusanos, el spam y los contenidos web no apropiados para las empresas. Dicho lo anterior y en conjunto con la evolución de las amenazas, que hoy en día parece haber superado toda seguridad informática, ha propiciado que el campo dedicado a la seguridad informática se enfoque en el desarrollo de equipos dedicados a controlar dichas amenazas [1].

Cuando se habla de seguridad perimetral, nos referimos metafóricamente en levantar una barrera o frontera imposible de vencer entre nuestra red interna e Internet. Es de suma importancia condicionar y controlar, qué datos entran a nuestra organización o salen de ella. Además de permitir al administrador dentro de la red controlar los puntos de entrada, sin olvidarse del resto de los servicios internos, para protegerlos frente a una posible intrusión.

Como administradores de una red no podemos pensar que existe un sistema de seguridad que no contenga vulnerabilidad, es decir, que la seguridad sea total, ya que nos llevaría a descuidar el mantenimiento de la red y a no contar con nuevas políticas de seguridad que se pueden llegar a implementar. Al implementar nuevas políticas de seguridad, se pueden controlar puntos importantes dentro de la empresa, como mantener todos los equipos actualizados, realizar estudios de vulnerabilidades o una correcta planificación de copias de seguridad (backup) [7].

Para el caso de la Estancia Profesional de la cual se ocupa el presente proyecto, las actividades se desarrollaron prestando el servicio al cliente de la empresa TB&Talent S.A. de C.V.: Artículos Básicos de Calidad en Uniformes y Equipos S.A. de C.V. De tal manera, el siguiente escrito está dirigido a la implementación de estrategias y políticas de seguridad dentro de la red de dicha empresa, con el objetivo de minimizar la vulnerabilidad del activo, aumentando la eficacia y nivel de seguridad del sistema.



#### **4. Antecedentes:**

Proyectos terminales.

Administración de una red corporativa [2].

Este proyecto nos habla de la finalidad de administrar una red corporativa en una empresa, y de la importancia de asegurar la confiabilidad y la disponibilidad de la información, mediante el diseño de un protocolo de seguridad. Tiene relación con mi proyecto de estancia, ya que hace referencia a la seguridad que debe haber en la red informática dentro de una empresa, levantamiento y configuración de servidores. Así como adoptar nuevas tecnologías que mejor cumplan con las demandas de la empresa, y la implementación de un servidor Web seguro. La diferencia de este proyecto con el mío es que se enfoca más a la virtualización de servidores y las aplicaciones que tienen las máquinas virtuales dentro de la empresa.

Administración de una red profesional [3].

El proyecto trata de cómo la red interna de una empresa puede tener un rendimiento óptimo, llevando a cabo una adecuada configuración de autenticación y autorización de servicios. Así como de llevar una correcta administración de los servidores, switches, routers y un manejo apropiado de las contingencias en la red, entre muchas otras actividades que se requieren para su buen funcionamiento. Una diferencia de este proyecto con el mío es que se enfoca más en la auditoría de cada uno de los equipos de red utilizados dentro de la empresa, y de su distribución dentro de la misma.

Medidas de Seguridad en Servidores VPN de una red corporativa [4].

El proyecto trata de la implementación de tecnologías que ayudan a proteger los datos, de alteraciones de terceras personas, usuarios o hasta del mismo software. El propósito es proporcionar una comunicación segura, brindar el acceso sólo a personal capacitado, y aumentar la productividad y flexibilidad al ampliar la red corporativa. La diferencia con mi proyecto, es que éste va dirigido a la implementación de medidas de seguridad con base sólo a servidores VPN de la red de la empresa, con el objetivo de minimizar vulnerabilidades de los bienes y recursos.

Análisis y gestión de recursos para brindar seguridad en una red empresarial [5].

En este proyecto se desarrollan varias actividades dentro de una empresa, algunas de éstas son: la identificación de los recursos propios de la empresa para su red de computadoras y cómo es que ellos manejan la seguridad de sus datos. Se hace un análisis de las medidas y políticas de seguridad, de la creación de una VPN para la transmisión de información confidencial, de políticas dentro de un firewall para el bloqueo de acceso de datos maliciosos a servidores y clientes. A diferencia de mi proyecto, éste se basa en su mayoría al análisis de las medidas de seguridad que se implementan dentro de la empresa.

Auditoria de la seguridad de los equipos de cómputo de la Central Termoeléctrica Valle de México [6].

En este proyecto se propone la realización de una estancia profesional en la que se llevará a cabo una auditoria de los equipos de cómputo de una red LAN, del departamento de programación y control, para identificar riesgos, amenazas o posibles vulnerabilidades a las que está expuesto dicho departamento. A diferencia de mi propuesta lo que se plantea es sólo realizar un informe detallado de los riesgos que pudiera tener cada uno de los equipos, así como de dar solución y evitar vulnerabilidades de los equipos a nivel físico y lógico.

Administración de una red corporativa [7].

En este proyecto se realiza la administración de la red dentro de una empresa, su objetivo principal es de utilizar el hardware y software proporcionados para hacer una red más eficiente y aumentar su nivel de seguridad mediante el uso de un firewall. La diferencia radica en que mi proyecto propone la implementación de estrategias que nos permitan mantener una eficacia y nivel óptimo de seguridad para poder resguardar el activo dentro de la empresa.

## **5. Justificación.**

La seguridad e integridad de una red de computadoras dentro de una empresa es primordial y de suma importancia para salvaguardar toda la información almacenada. Los ataques por red y pérdidas de información ocasionan un gran trastorno y no solo la imagen si no también el funcionamiento y progreso de una empresa se ven afectados.

Considerando lo limitado que son los recursos hoy en día y la actual necesidad en el sector empresarial, se plantea la necesidad de implementar un cerco de seguridad dentro de la red para proveer diferentes servicios de seguridad que nos permitan controlar el tráfico de datos que pasan por la red de la empresa, dichos servicios pueden ser tanto inalámbricas como los basados en cable; también los que permiten accesos a cuentas de correo electrónico, administración de dominios empresariales, hospedaje y dominios Web entre otros. Para ello se requiere implantar un sistema de seguridad que dependería de personal con una determinada capacidad de análisis, proporcionando un único origen para administrar la información del sistema e identidad de un servidor, identificando los problemas de configuración y administrando todos los servicios instalados en el mismo.

La implementación de las mejores tecnologías para establecer una seguridad perimetral que es de suma importancia dentro de una red empresarial, se deducen a través de estudios y la demanda que dependerá de cada empresa.

La finalidad de esta estancia es contribuir con este fin para que toda la información esté resguardada de cualquier tipo de ataque informático. De allí que se establezca una seguridad perimetral robusta para el control de accesos y protección de los servicios informáticos que garantice un correcto aprovechamiento de la infraestructura y garantizar la integridad y confidencialidad de la información.

## **6. Objetivos:**

### 6.1.General:

Analizar, diseñar e implementar medidas que permitan establecer una seguridad perimetral mejorando la eficacia y nivel de seguridad de la red dentro de la empresa.

### 6.2.Específicos:

- ✓ Identificar y verificar la ubicación y condición de cada uno de los componentes que conforman la red (hardware y software).
- ✓ Analizar los elementos hardware y software que conforman la red empresarial para identificar y definir los posibles riesgos, amenazas o vulnerabilidades que pudieran presentar.
- ✓ Crear, modificar e implementar estrategias y políticas de seguridad para establecer un mayor nivel de seguridad que nos permitan contrarrestar las posibles amenazas que puedan llegar a afectar el sistema.
- ✓ Aplicar una metodología de control en el sistema para garantizar la seguridad dentro de la red (autenticidad, confidencialidad, disponibilidad, integridad, privacidad y auditoria).

## **7. Marco teórico.**

Antes de seguir con el desarrollo del proyecto, es necesario atender y definir conceptos que se utilizan en el presente reporte.

### ➤ Red empresarial de computadoras.

Es una red de computadoras que resulta de interconectar las distintas redes existentes de una organización completa, diseñada para cubrir todas sus necesidades de comunicación. Compuestas por centralitas, ordenadores o redes de área local y unidas mediante enlaces privados o públicos [10].

➤ Seguridad en redes.

Es mantener bajo protección los recursos y la información con que se cuenta en la red. A través de procedimientos basados en políticas de seguridad.

➤ Virtualización de servidores.

Es el proceso de crear una representación virtual basada en software, en lugar de una física. La virtualización se puede aplicar a servidores, aplicaciones, almacenamiento y redes, y es la manera más eficaz de reducir los costos de TI y aumentar la eficiencia y la agilidad de los negocios de cualquier tamaño [11].

➤ Firewall.

Es un sistema en la red que monitorea el tráfico de la información que se traslada en la misma -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Los firewalls han constituido una primera línea de defensa en seguridad de la red. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet. Un firewall puede ser hardware, software o ambos [12].

➤ Synology NAS.

El almacenamiento conectado en red (NAS por sus siglas en inglés), es el nombre dado esta nueva tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento con computadoras personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un sistema operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

En este tipo de servidores nos referiremos al Synology NAS, que es muy útil para proporcionar el almacenamiento centralizado a computadoras clientes en entornos con grandes cantidades de datos. El NAS puede habilitar sistemas fácilmente y con bajo costo con balance de carga, tolerancia a fallos y servidor web para proveer servicios de almacenamiento

Las soluciones de almacenamiento de Synology NAS se han diseñado para ayudar a administrar sus activos digitales. Se dispone de un conjunto de paquetes de valor añadido para facilitar la vida diaria empresarial, con opciones administrativas flexibles, además de herramientas para salvaguardar su DiskStation y los datos de valor [16].

➤ Fortinet.

Empresa que se dedica a ofrecer una seguridad amplia, verdaderamente integrada y de alto rendimiento en toda la infraestructura de TI. Proporciona seguridad en redes y contenido, así como productos de acceso seguro que comparten inteligencia y trabajan juntos para formar un tejido cooperativo. Tienen un tejido de seguridad que combina procesadores de seguridad, un sistema operativo intuitivo e inteligencia de amenazas aplicada para brindarle una seguridad comprobada, un rendimiento excepcional y una mejor visibilidad y control, a la vez que facilita la administración.

Tienen una amplia plataforma de firewall empresarial, FortiGate, está disponible en una amplia gama de tamaños y factores de forma para adaptarse a cualquier entorno y proporciona una amplia gama de funciones de seguridad y redes de próxima generación. Los productos complementarios se pueden implementar con FortiGate para permitir una infraestructura de seguridad de extremo a extremo simplificada que cubra:

- Seguridad de la red
- Seguridad del centro de datos (física y virtual)
- Seguridad en la nube
- Acceso seguro (por cable e inalámbrico)
- Seguridad de infraestructura (conmutación y enrutamiento)
- Seguridad del contenido
- Seguridad de aplicaciones [13].

➤ FortiGate.

Sirve para proteger las redes empresariales de ataques, spam, y otros peligros informáticos. Esta solución ha crecido mucho en estos últimos tiempos por la relación costo-calidad.

FortiGate es un Firewall basado en hardware desarrollado por Fortinet. El sistema de FortiGate es el único sistema que puede detectar y eliminar virus, gusanos y otras amenazas basadas en contenido, sin afectar al rendimiento de la red, incluso para aplicaciones en tiempo real como la navegación Web. Las soluciones de FortiGate también incluyen:

- Firewall
- Filtrado de contenido
- VPN
- Antivirus
- Antispam
- Detección y prevención de intrusos y gestor de tráfico
- Balanceo de carga
- Alertas por e-mail

Estas características hacen de FortiGate un sistema rentable, conveniente, potente y seguro de las soluciones de seguridad de red disponibles [14].

➤ Políticas de seguridad.

Es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una empresa para llevar a cabo los objetivos de seguridad de la información dentro de la misma.

Las políticas de seguridad definen lo que está permitido y lo que está prohibido, permiten definir los procedimientos y herramientas necesarias, expresan el consenso de los “dueños” y permiten adoptar una buena actitud dentro de la organización [15].

El objetivo de dichas políticas es mostrar el posicionamiento de la organización con relación a la seguridad y servir de base para desarrollar los procedimientos concretos de seguridad.

Las políticas deben contener claramente las prácticas que serán adoptadas por la compañía. Y éstas deben ser revisadas, y si es necesario actualizarlas periódicamente.

Las políticas deben de definir:

- Los objetivos principales y su importancia dentro de la empresa.
- El compromiso de los altos cargos con la misma.
- La filosofía respecto al acceso de datos.
- Responsabilidades relacionadas al tema.
- La base para diseñar normas y procedimientos referidos a:
  - ✓ Clasificación y control de los datos.
  - ✓ Organización del sistema de seguridad.
  - ✓ Plan de contingencia.
  - ✓ Prevención y detección de vulnerabilidades.
  - ✓ Administración del activo.
  - ✓ Seguridad física y lógica.
  - ✓ Privilegios del personal a cargo.

Al establecer las políticas de seguridad que mejor se adapten a la empresa, se podrá desarrollar las normas y procedimientos de seguridad que serán la guía para la realización de las actividades dentro de la misma.

Por lo tanto, dichas políticas son establecidas mediante un documento que sirve de referencia para definir los objetivos que se desea alcanzar al establecer un sistema de seguridad; además se establecen las medidas que deben implementarse para tener la certeza de alcanzar dichos objetivos.

## **8. Desarrollo del proyecto.**

Antes de empezar con el análisis del sistema, se realizó un recorrido para obtener un panorama amplio de la infraestructura, al mismo tiempo se verificó a fondo las condiciones de todo el hardware que conforma la red: cableado, servidor, switch, firewall, router, computadoras, entre otras cosas.

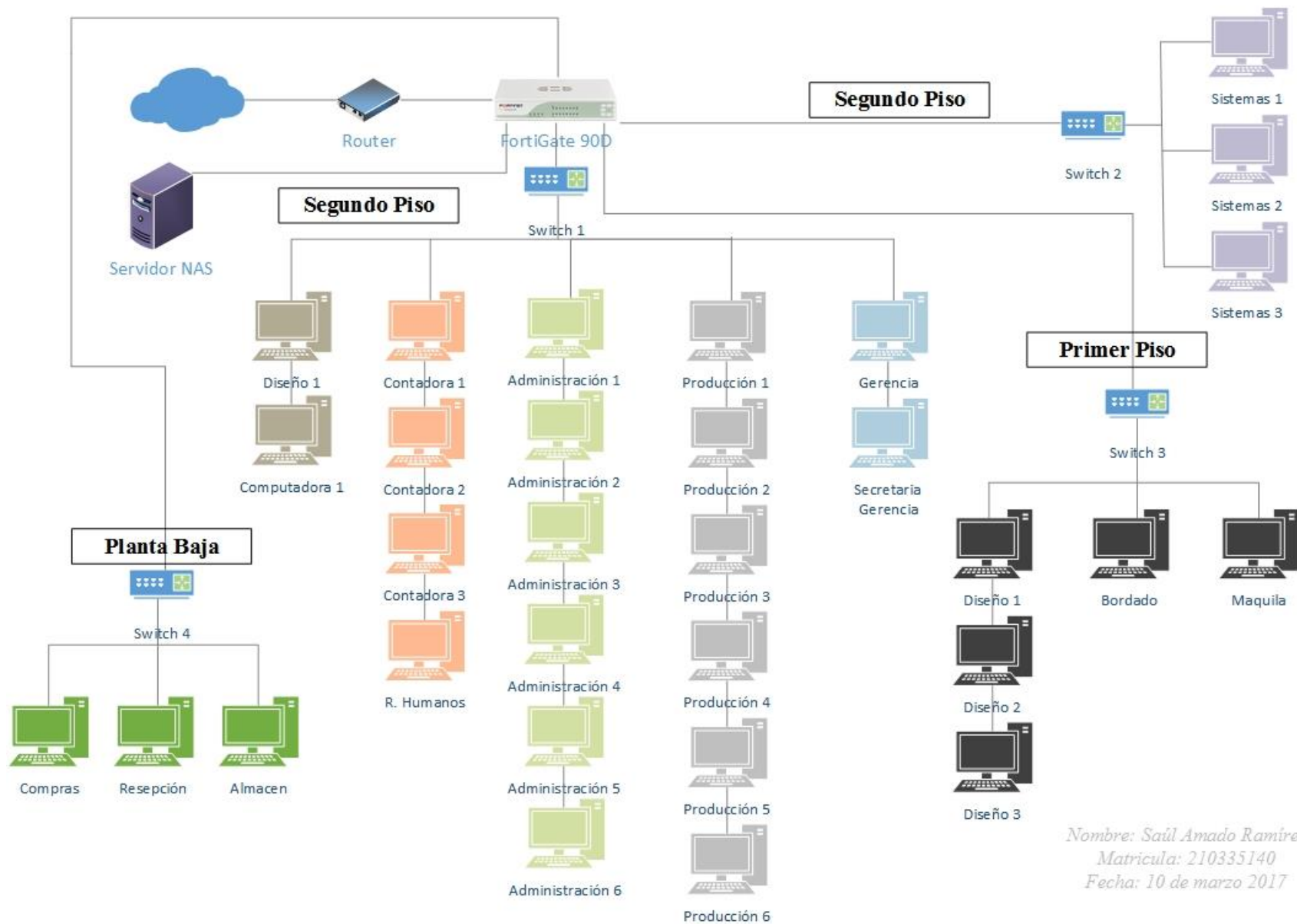
Se inspeccionó cada nodo dentro de la red, así como el cable que enlaza a cada uno de ellos y no se encontraron daños al cableado. Sólo se hicieron pequeños cambios en las canaletas que transportan los cables de red, se trasladaron las canaletas pegándolas a la pared para no dañar el cable, ya que estos atravesaban los pasillos y eran pisados por los empleados de la empresa. Se le notificó al encargado del área de sistemas antes de realizar dichos cambios y se dio el visto bueno para realizarlos.

También se observaron equipos que por el tiempo que fueron adquiridos ya se encuentran obsoletos, se notificaron todas estas observaciones al encargado del área y se realizó un inventario de todos los equipos que están operando en la empresa. Queda a observación del personal del área de sistemas realizar los cambios de equipo o realizar una actualización de dichos equipos.

Terminado el proceso de inspección se procedió a diseñar un diagrama de red de todo el edificio dividido por zonas, con el objetivo de tener una perspectiva más amplia del área de trabajo. Dicho diagrama se realizó con Visio, que es un software que se utilizó en el entorno de Windows.

En el diagrama de red podemos observar de una manera sencilla como está constituida la red de la empresa Artículos Básicos de Calidad en Uniformes y Equipos S.A. de C.V.





Nombre: Saúl Amado Ramírez  
 Matricula: 210335140  
 Fecha: 10 de marzo 2017

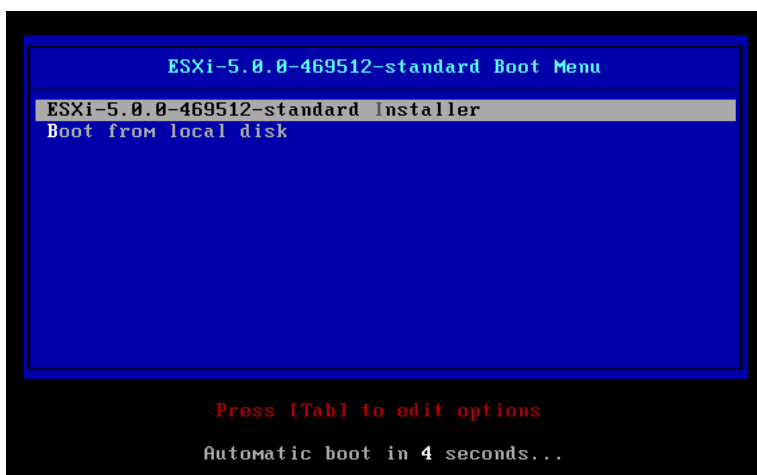
Diagrama 1: Diagrama de red de la empresa ABC Uniformes S.A. de C.V.

## 8.1. Virtualización de un servidor con VMware vSphere ESXi 5.

ESXi 5 permite ser instalado desde un USB booteable, pero normalmente lo hacemos desde un CD-ROOM. La instalación es muy sencilla, sólo nos llevará algunos minutos debido a que estamos hablando de un sistema operativo que no llega a los 300 MB.

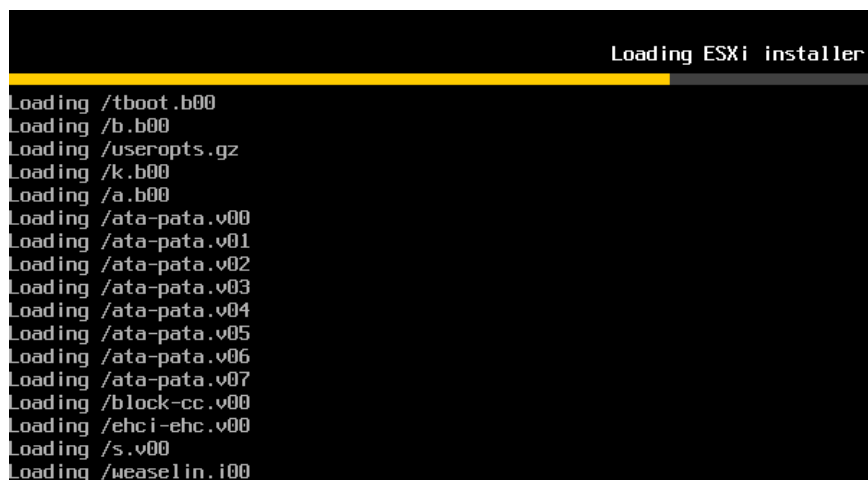
VMware es un sistema de virtualización por software. Y un sistema virtual por software es un programa que simula un computador o un hardware con características determinadas. Cuando se ejecuta el simulador, proporciona un ambiente de ejecución similar a todos los efectos de un sistema físico, con CPU, BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, puerto Ethernet y disco duro.

La primera pantalla que veremos tras bootear será la que adjunto a continuación, donde la primera opción por defecto es la de cargar el sistema para instalarlo (dejamos por defecto marcada esa opción).



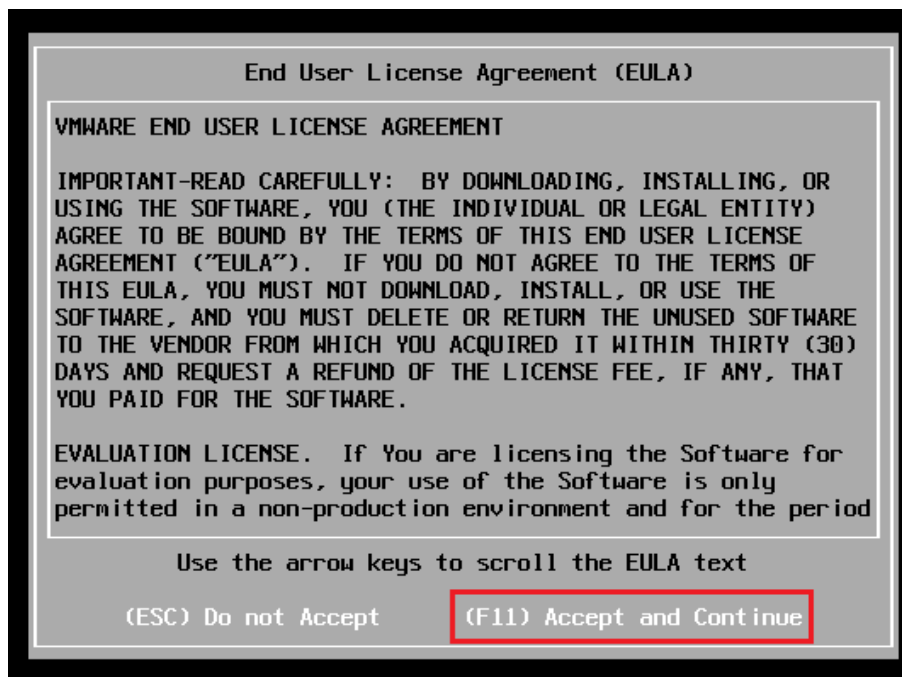
*Imagen 1: Instalación de ESXi 5.0.*

Después del primer paso, comenzará a cargarse los módulos necesarios para la instalación.



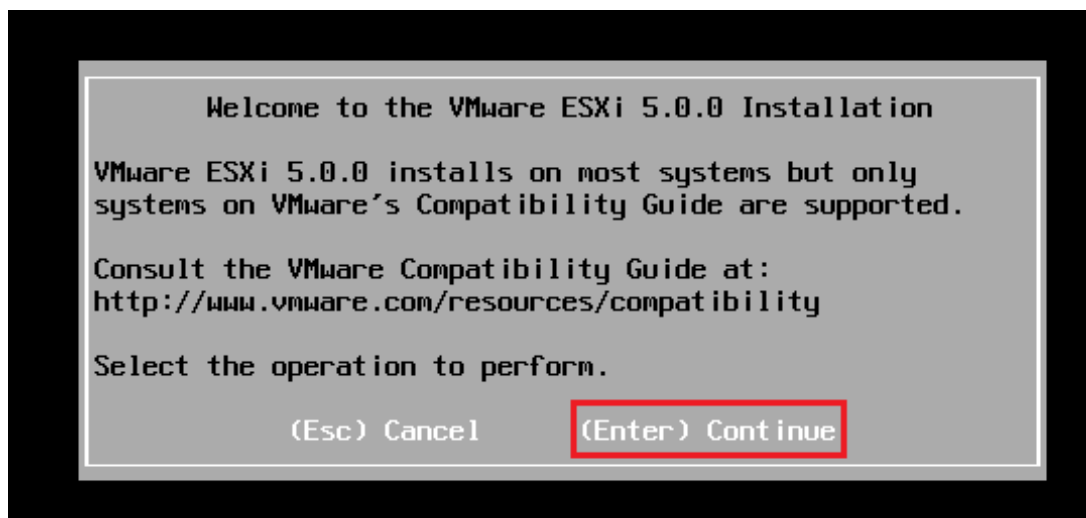
*Imagen 2: Descarga de los módulos de instalación.*

A continuación, aparecerá la siguiente pantalla donde debemos aceptar los términos de la licencia (EULA) con la tecla **F11**.



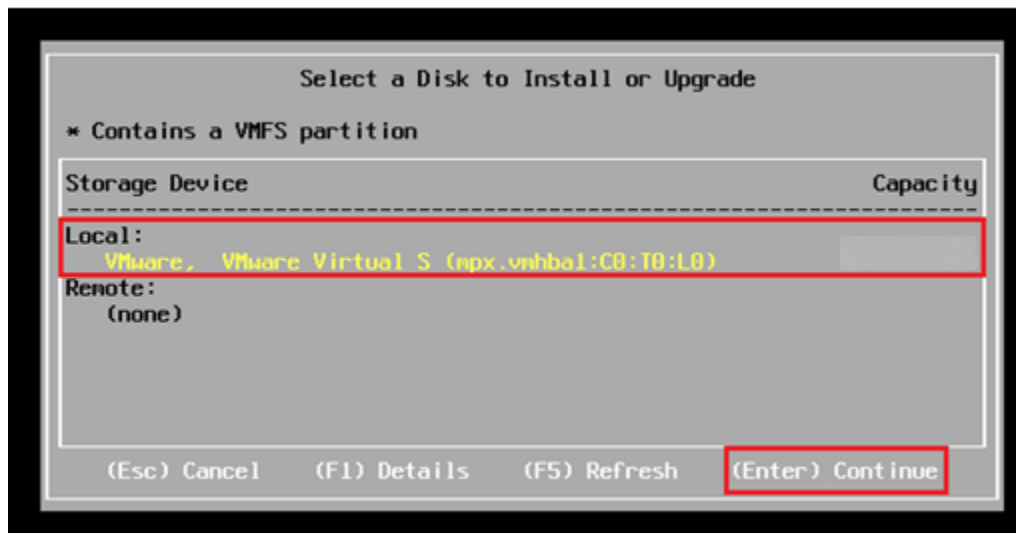
*Imagen 3: Aceptar términos de la licencia.*

Seguidamente el instalador nos da la bienvenida y nos recomienda consultar la compatibilidad del hardware para ESXi 5.0.0, continuamos la instalación presionando **Enter**.



*Imagen 4: Continuar con la Instalación.*

En la siguiente pantalla, nos enseñará el asistente los discos duros detectados, ya sea local o remoto, en nuestro caso, seleccionamos el disco duro en el que instalaremos ESXi 5, y continuamos con el asistente.



*Imagen 5: Detección de discos duros.*

Elegimos la configuración del idioma para el teclado.



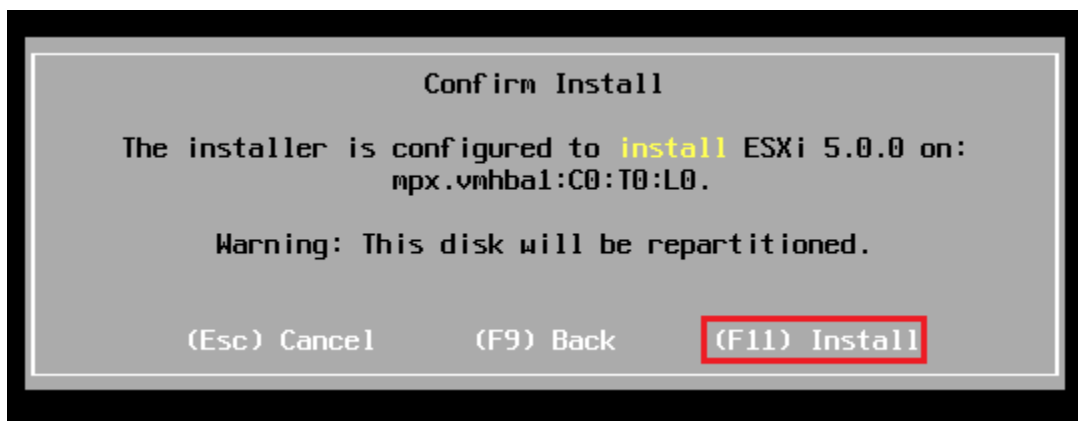
*Imagen 6: Selección del idioma.*

Y a continuación, deberemos de introducir la contraseña para el usuario “root” que es la que nos permite administrar y gestionar nuestro servidor. Es posible instalarlo sin clave, pero para poder administrar el servidor, debemos de establecer una contraseña, por lo que recomendamos introducir una.



*Imagen 7: ingresar una contraseña.*

Introducido la contraseña, nos queda confirmar la instalación presionando **F11**



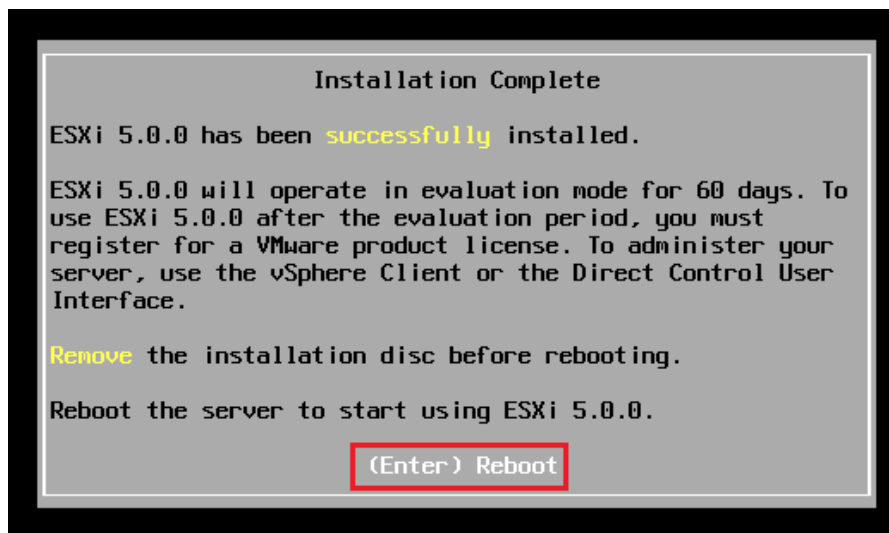
*Imagen 8: Confirmar la Instalación.*

Ahora solo nos queda esperar que termine la instalación.



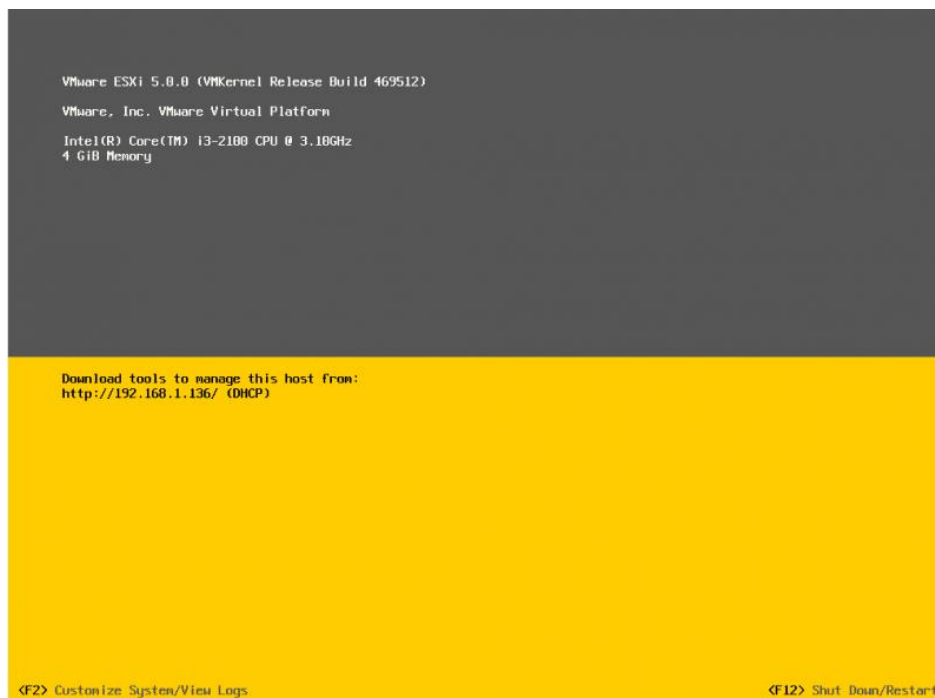
*Imagen 9: Estatus de porcentaje de instalación.*

Al terminar la instalación, nos da una serie de información, como usar **vSphere Client** para la administración del mismo, remover el disco de instalación y presionar **Enter** para su Reinicio.



*Imagen 10: Reiniciar para terminar la instalación.*

Tras el arranque de VMware **ESXi**, puesto que la dirección IP se le asignó a través de DHCP, nos indica la IP del servidor (fundamental para poder administrar).



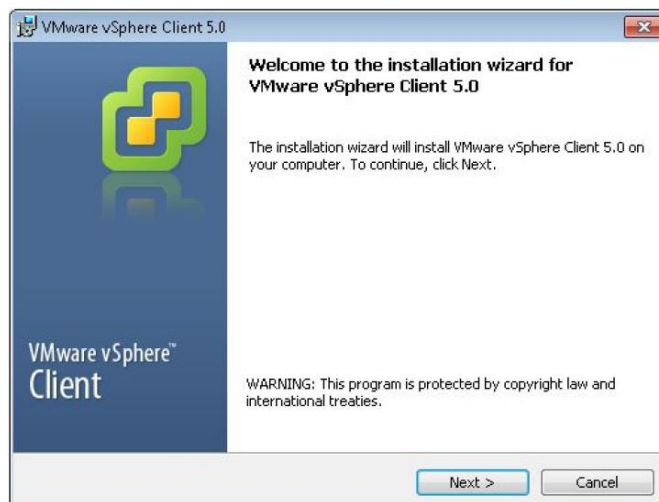
*Imagen 11: Inicio de VMware ESXi 5.0.*

Ahora ya podemos acceder a nuestro servidor VMware ESXi 5.0 desde cualquier equipo de la red (sea virtual o físico) dentro de la empresa ABC Uniformes S.A. de C.V.

## 8.2. Administrar y gestionar un servidor VMware ESXi usando VMware vSphere Client.

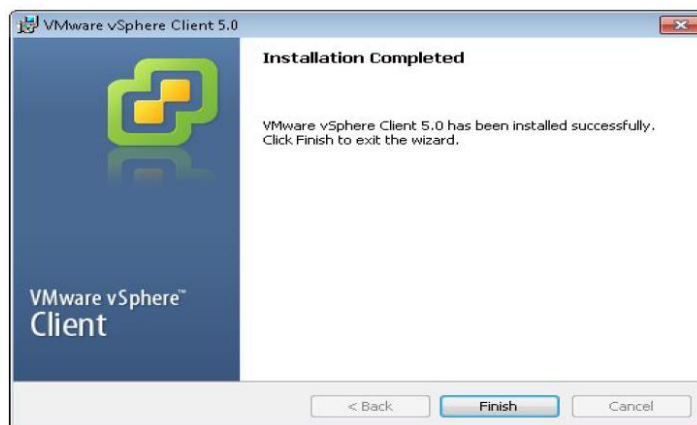
Se instala VMware vSphere Client en alguno de los equipos físicos del departamento de sistemas dentro de la empresa ABC Uniformes. Permitiendo a los usuarios ejecutar aplicaciones, con seguridad y poder responder con mejor eficacia a las necesidades de la empresa, optimizando los activos de la misma.

Se ejecuta el archivo VMware vSphere Client (proporcionado por el departamento de sistemas) y seleccionamos el idioma. Se inicia el asistente de instalación y seguimos las instrucciones.



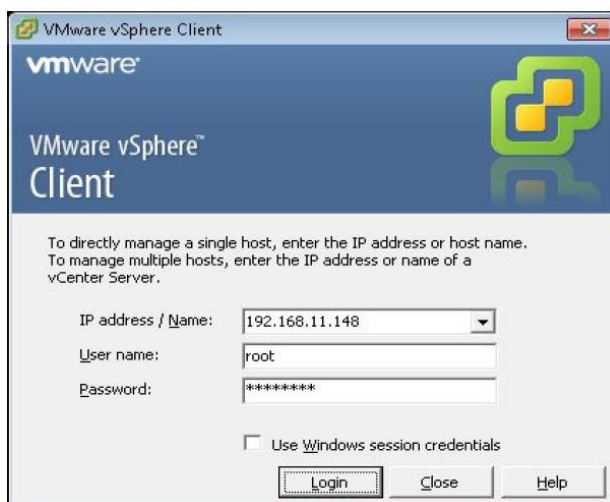
*Imagen 12: Inicio de la instalación de VMware vSphere Client.*

Leemos los términos de la licencia, y pulsamos “Next” en el caso de estar de acuerdo, introducimos nombre de usuario y de organización, pulsamos “Next”. Indicamos la carpeta de instalación, volvemos a pulsar “Next”. Damos click en Install, de esta manera se inicia el proceso de instalación de VMware vSphere Client. Después de algunos minutos el asistente nos indica que el proceso ha terminado, por ultimo pulsamos “Finish”: como se muestra en la Imagen.



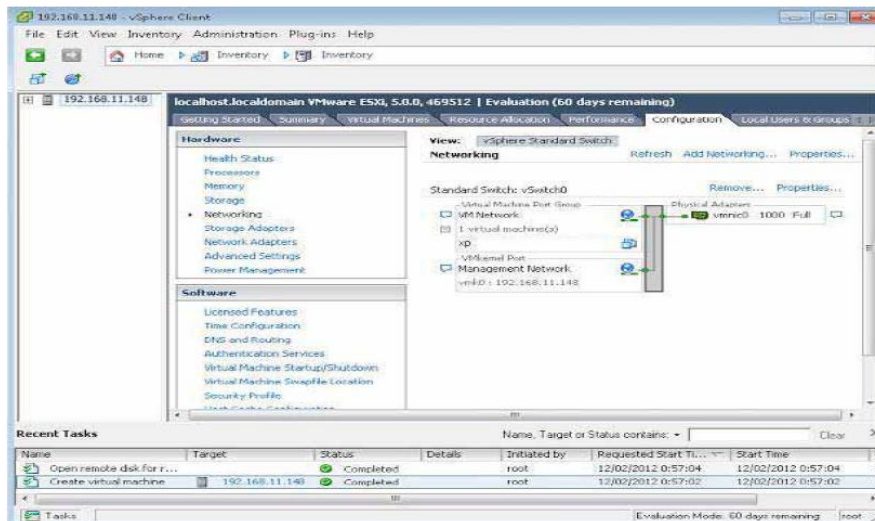
*Imagen 13: Finalizamos el proceso de instalación.*

Ejecutamos VMware vSphere Client, nos solicita la IP del servidor VMware ESXi previamente configurada, además ingresamos la contraseña del usuario “root”, después de introducir los datos requeridos pulsamos “Login”, como se muestra en la imagen.



*Imagen 14: Iniciar VMware vSphere Client.*

El asistente nos manda un mensaje de que existe un certificado de seguridad en el servidor ESXi, marcamos la casilla y pulsamos “Ignore”. Se inicia VMware vSphere Client y nos muestra el servidor ESXi que hemos creado.



*Imagen 15: Interfaz de VMware vSphere Client.*

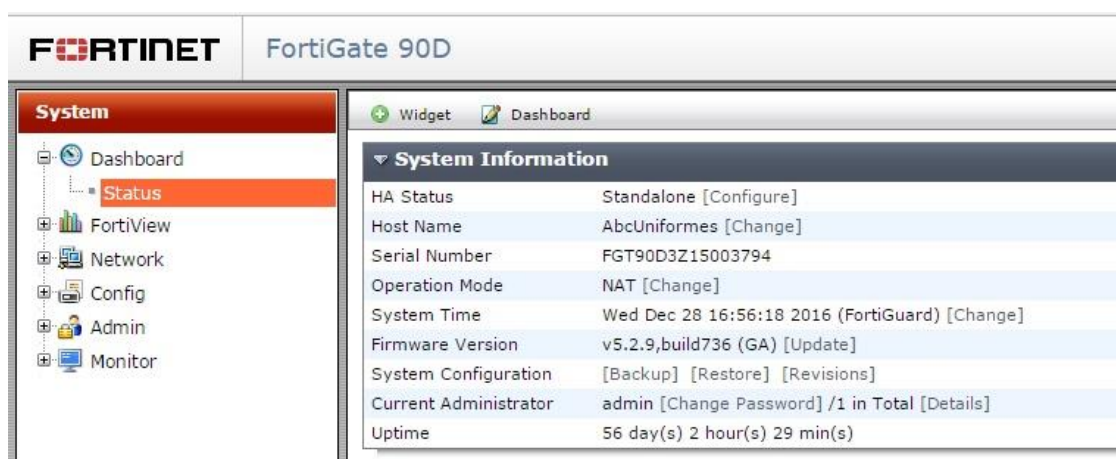
Ya instalado el software, procedemos a crear máquinas virtuales que nos permitirán la instalación y administración de recursos necesarios que se demandan dentro de la empresa, algunos recursos son software como SAI, COI, NOI, que se instalan en dichas máquinas virtuales para tener centralizada la información y ser utilizada por el personal cuando así lo requieran.



Posteriormente se desarrollaron estrategias de impacto que representan un cambio significativo en el sistema dentro de la red, que nos permitieron reducir de forma significativa los riesgos y eventos de desastre que no se habían realizado y ponían en peligro el activo de la empresa (hardware, software, datos y documentación). La mayoría de las estrategias se establecieron en el FortiGate 90D, que es un firewall desarrollado por Fortinet. Dichas estrategias se describen a continuación.

### 8.3. Configuración del equipo FortiGate 90D.

Información del FortiGate 90D son los siguientes:



The screenshot displays the Fortinet FortiGate 90D web interface. The top navigation bar includes the Fortinet logo and the device name 'FortiGate 90D'. A left-hand menu is titled 'System' and contains options for Dashboard, Status (highlighted), FortiView, Network, Config, Admin, and Monitor. The main content area shows 'System Information' with the following details:

System Information	
HA Status	Standalone [Configure]
Host Name	AbcUniformes [Change]
Serial Number	FGT90D3Z15003794
Operation Mode	NAT [Change]
System Time	Wed Dec 28 16:56:18 2016 (FortiGuard) [Change]
Firmware Version	v5.2.9,build736 (GA) [Update]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	56 day(s) 2 hour(s) 29 min(s)

*Imagen 16: Información del FortiGate 90D.*

#### 8.3.1. Configuración de Interfaces

##### a) Configuración de las Interfaces Internal, WAN1 y WAN2

Las interfaces están numeradas desde **port1...port10**, por lo tanto, se pueden utilizar cualquier port para configurar cada interface. Tal como se muestra en la imagen 2. Navegamos en: **System >> Network >> Interface** y editamos cada una de las Interfaces necesarias.

Ejemplo para configurar la interface Internal:

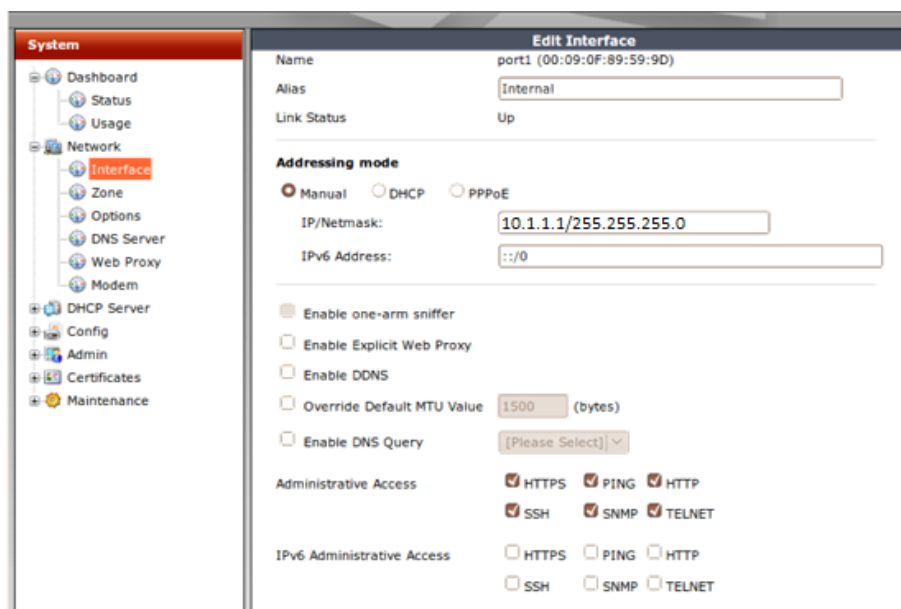


Imagen 17: Configuración de la Interface Internal.

b) Dentro del menú **System** encontramos la opción **Network >> Interfaces** y se encuentran configuradas las siguientes interfaces.

- Configuración wan1 (TELMEX).
- Configuración wan2 (IUSACELL).
- Configuración Internal.
- Configuración Internal 5.

Status	Name	Members	IP/Netmask	Type
<b>Hardware Switch (1)</b>				
+	internal	1 3 5 7 9 11 13 2 4 6 8 10 12 14	10.1.1.1 255.255.255.0	Hardware Switch (4)
<b>Physical (12)</b>				
+	internal5 (wan1)		187.170.164.119 255.255.255.0	Physical
+	internal6		0.0.0.0 0.0.0.0	Physical
+	internal7		0.0.0.0 0.0.0.0	Physical
+	internal8		0.0.0.0 0.0.0.0	Physical
+	internal9		0.0.0.0 0.0.0.0	Physical
+	internal10		0.0.0.0 0.0.0.0	Physical
+	internal11		0.0.0.0 0.0.0.0	Physical
+	internal12		0.0.0.0 0.0.0.0	Physical
+	internal13		0.0.0.0 0.0.0.0	Physical
+	internal14		0.0.0.0 0.0.0.0	Physical
+	wan1 (Telmex)		192.168.1.99 255.255.255.0	Physical
+	wan2 (Iusacell Plus)		192.168.100.15 255.255.255.0	Physical
<b>WAN Link Load Balancing (1)</b>				
+	wan-load-balance			WAN Link Load Balancing
<b>WiFi (2)</b>				
+	Ventas	(SSID: Ventas)	10.1.5.1 255.255.255.0	WiFi
+	Ventas VIP	(SSID: VentasVIP)	10.1.6.1 255.255.255.0	WiFi

Imagen 18: Lista de Interfaces configuradas.

### 8.3.2. Configuración de Políticas:

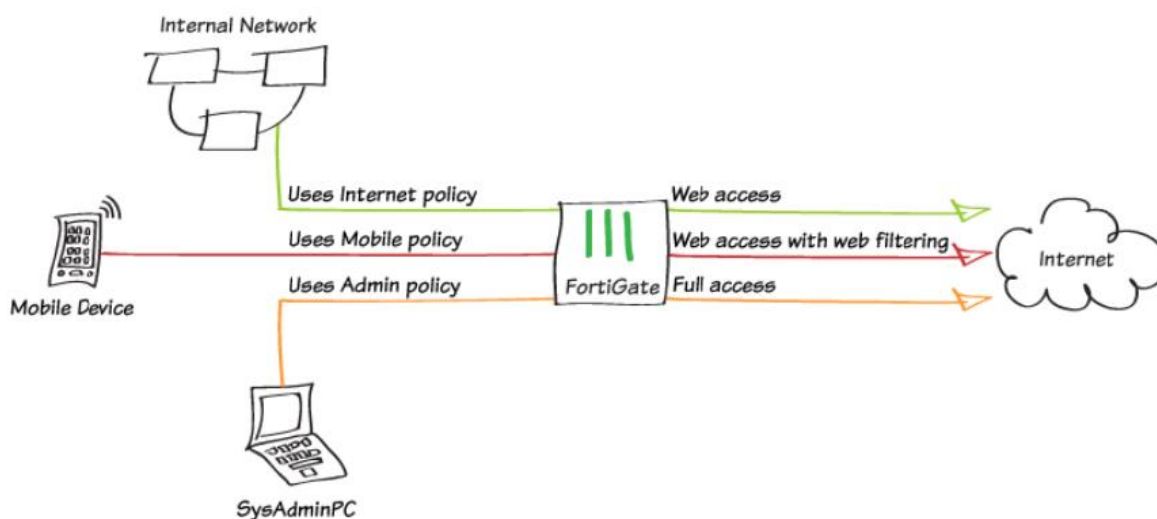


Diagrama 2: Diagrama de configuración de las políticas de seguridad.

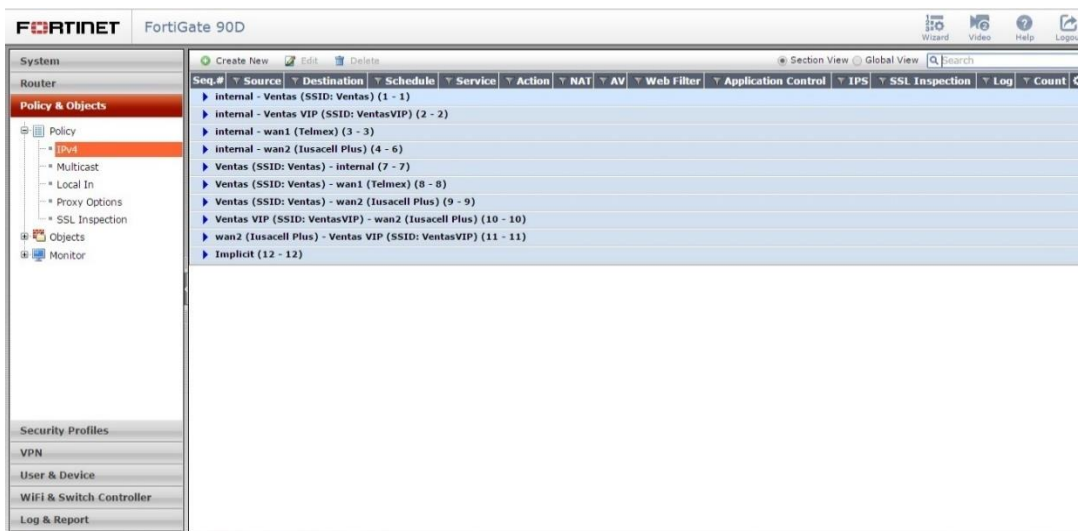
A través de las políticas de Firewall, podremos configurar los permisos y/o negaciones para equipos (host) que envíen tráfico para la Internet, así como también para la red. Esto lo hacemos desde: Firewall >> Policy >> Policy donde podremos crear o editar las políticas de firewall.

- Definimos un nombre para la política, será llamada Internet.
- Agregar la interface para la red local y la interface del enlace de internet.
- En Source y Destination Address seleccionar All.
- Definamos los servicios para HTTP, HTTPS y DNS.
- Asegurémonos que la política tenga NAT habilitado.
- Para poder ver resultados más adelante habilitemos la opción de Log Allowed Traffic y seleccionemos Security Events o All Sessions.



Imagen 19: Configuración de una nueva política de seguridad.

Dentro del menú **Policy** en la opción **Policy >> Policy** tenemos las siguientes políticas.



*Imagen 20: Políticas de seguridad aplicadas en la red.*

Estas políticas permiten la comunicación entre ambos segmentos de red y además nos ayudan a mantener un cerco de seguridad en la red dentro de la empresa. Para las políticas con usuarios acceso a servicios de internet se activa la opción de Web Filter y Application Control.

No sólo es aplicar medidas de seguridad dentro del firewall, sino que también se monitorean constantemente para identificar los tipos de dispositivos conectados a nuestra red, cableada o inalámbrica. Además, el FortiGate puede monitorear las redes y coleccionar información acerca de los dispositivos operando en nuestras redes.



*Imagen 21: Monitoreo de políticas de seguridad.*

### 8.3.3. Configuración de Objetos y Grupos.

- a) Ingresamos al menú Policy & Objects > Addresses y damos clic en el botón de Create New.

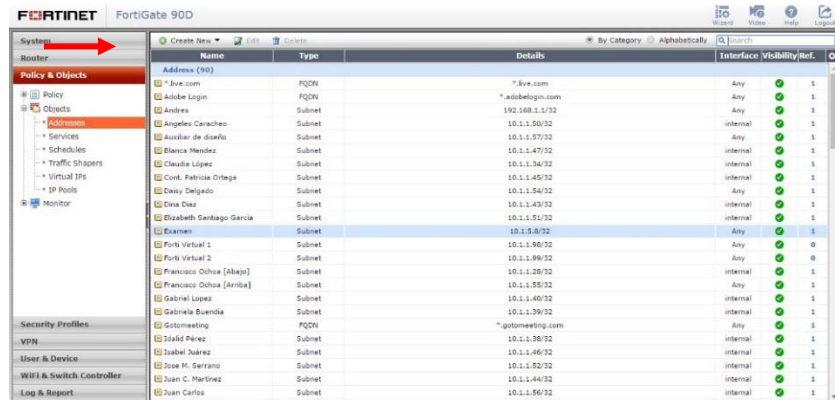


Imagen 22: Creación de un nuevo objeto.

- b) Podemos seleccionar entre dos tipos de objetos Direcciones (Address) o Grupos de Direcciones (Address Group). Para nuestro ejemplo crearemos un objeto de dirección.

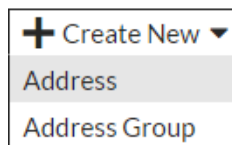


Imagen 23: Crear un objeto de dirección.

- c) Llenamos los campos necesarios (Nombre, tipo y el objeto como tal) sin utilizar espacios ni caracteres especiales como “\* ñ/> <¡!‘¿?” o palabras con tildes y damos clic en el botón de OK.

The screenshot shows the 'New Address' configuration form. The fields are filled as follows:

- Name: RED\_LOCAL
- Type: IP Range
- Subnet / IP Range: 192.168.0.0/24
- Interface: any
- Show in Address List:
- Comments: (empty)

At the bottom, there are 'OK' and 'Cancel' buttons.

Imagen 24: Llenado de los campos para crear el objeto.

Todos los objetos creados en el menú de Addresses deben de ser utilizados en política, de lo contrario el objeto por sí solo no ejecuta ninguna acción.

- d) En el menú **Firewall Objects** en la opción **Address >> Groups** se configuran los grupos ocupados dentro de las políticas.

*Imagen 25: Creación de un Grupo en el FortiGate.*

- e) En el menú **Firewall Objects** en la opción **Traffic Shaper >> Shared** se configura el consumo de tráfico de transmisión de datos que requieren ciertas políticas para evitar el mal funcionamiento de los equipos y aplicaciones críticas que se tienen dentro de la sucursal.

*Imagen 26: Configuración del tráfico de Transmisión.*

- f) En el menú **Firewall Objects** en la opción **Virtual IPs >> Virtual IPs** se configuran los equipos o dispositivos que tienen un NAT y requieren que el servicio que proporcionan sea público por la información que maneja.

*Imagen 27: Configuración de equipos con NAT.*

### 8.3.4. Configuración de Perfiles de Seguridad.

- a) En el menú **Security Profiles** en la opción **Web Filter>>Profiles** se encuentran los perfiles de bloqueo para páginas web.

Dentro de cada perfil se tienen diferentes categorías con subcategorías dentro de cada una, con opción para poderlas bloquear, monitorear o permitir.

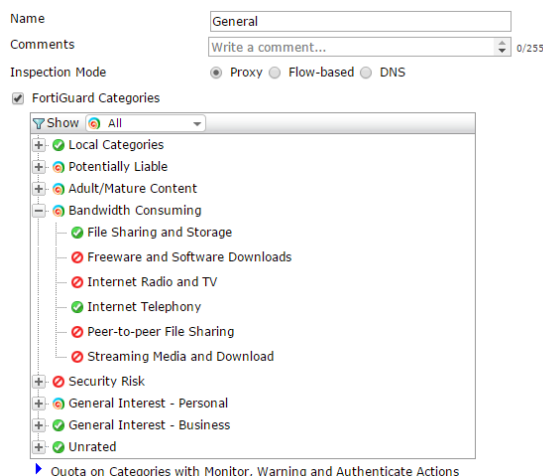


Imagen 28: Configuración del Web Filter.

- b) En el menú **Security Profiles** en la opción **Application Control>>Application Sensors** se encuentran los perfiles de bloqueo para aplicaciones.

En estos perfiles podemos bloquear las aplicaciones o servicios que ocupan algunas páginas web o programas instalados en los equipos de cómputo (antivirus, web chat, video en línea, etc.).

Name: Sucursal\_Del Valle  
Comments: Comments 0/255

Category	Popularity	Technology	Risk	Action	Application
	👤👤👤👤	All	All	Monitor	012mail, 1und1.Mail, 51.Com_Mail ... [Show all 105]
				Monitor	Amazon.AWS_S3, DNS, FTP ... [Show all 25]
				Block	Boomeranggmail, Gmail, Gmail_Attachment ... [Show all 5]
				Monitor	All Other Known Applications
				Monitor	All Other Unknown Applications

Imagen 29: Monitoreo de aplicaciones y servicios.

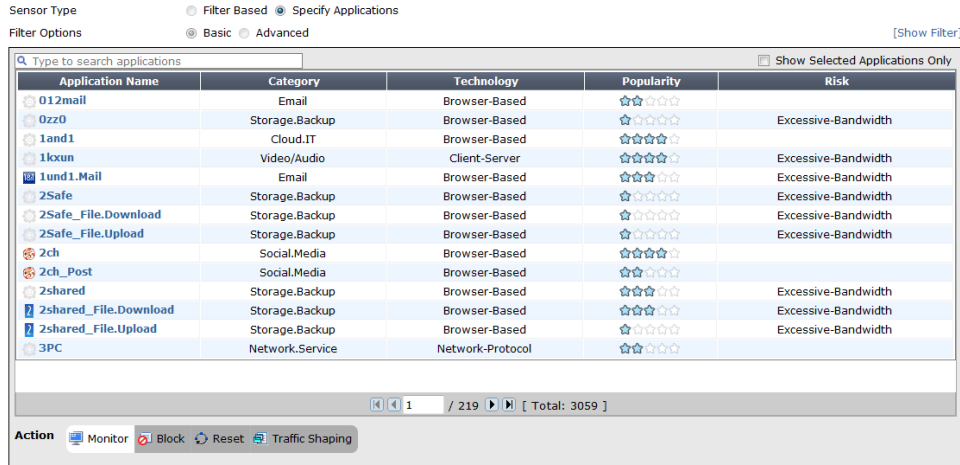


Imagen 30: Bloqueo de aplicaciones y servicios.

- c) En el menú **Security Profiles** en la opción **Web Filter >> Rating Overrides** se agregan los las URL en las categorías de Web Filter.

En esta parte se agregan las páginas web que requieren ser bloqueadas o permitidas en las categorías de los perfiles de Web Filter, para esta opción se agregaron las URL que fueron proporcionadas por los usuarios de la sucursal.

#	Enable	URL	Override Category	Category
2	✓	65.50.225.98	custom1	Unrated
18	✓	69.20.23.1	custom1	Unrated
3	✓	74.205.6.223	custom1	Unrated
72	✓	88.80.202.146	custom2	Information Technology
71	✓	172.28.224.152	custom2	Unrated
70	✓	173.199.5.16	custom2	File Sharing and Storage
7	✓	173.203.12.184	custom1	Web Hosting
8	✓	173.203.12.185	custom1	Unrated
9	✓	173.203.12.185:8080	custom1	Unrated
10	✓	173.203.12.185:8081	custom1	Unrated
11	✓	173.203.12.186	custom1	Unrated
12	✓	173.203.12.186:8080	custom1	Unrated
13	✓	173.203.12.186:8081	custom1	Unrated
14	✓	173.203.12.187	custom1	Unrated
15	✓	173.203.12.187:5444	custom1	Unrated
69	✓	189.254.22.30/WebServicesAMB/WS_HSA/datosaut.asmx	custom2	Unrated
56	✓	190.90.112.136	custom2	Unrated
55	✓	200.33.74.126	custom2	Unrated
50	✓	200.33.84.128	custom2	Unrated
47	✓	201.140.109.99	custom2	Health and Wellness
21	✓	201.140.109.99/novaweb/services/ImageProcessor.rem	custom1	Health and Wellness
22	✓	201.148.87.141	custom1	Unrated
23	✓	201.157.45.101	custom1	Unrated
40	✓	201.157.56.23:8081/interpretacion/login/auth	custom2	Unrated
38	✓	201.175.34.103	custom2	Unrated
26	✓	207.97.245.99	custom1	Information Technology
28	✓	216.195.72.47	custom2	Business
68	✓	216.203.82.59	custom2	Health and Wellness

Imagen 31: Agregar páginas web para ser bloqueadas.



## 8.4. Administración y gestión de tareas avanzadas de un servidor Synology NAS.

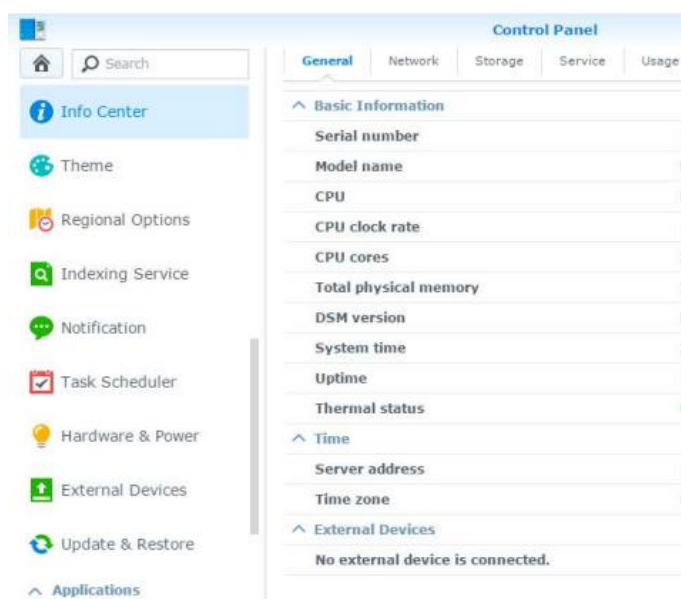
Synology ha desarrollado múltiples herramientas relacionadas con soluciones de almacenamiento, ayudando a todos los usuarios dentro de la red de la empresa a responder a diferentes demandas de almacenamiento. De modo que su servidor Synology NAS DS 416 cuenta con un CPU de doble núcleo, 1 GB de RAM, dos puertos Gigabit LAN, tres puertos USB3.0, cuenta con cuatro bandejas de almacenamiento para introducir cuatro discos duros con capacidad de hasta 10 TB cada uno, siempre un rendimiento superior. La gestión del servidor se simplifica en DSM, sin importar la cantidad de servidores que posea. Administrar filas de servidores es tan sencillo como administrar uno solo.

DiskStation Manager (DSM) es un sistema operativo intuitivo, basado en web, que se encuentra en cada NAS de Synology. Se ha diseñado para ayudarle a gestionar sus datos: documentos, fotos, música, vídeos y otras formas importantes de activos digitales. DSM ofrece un gran número de aplicaciones y servicios para proporcionar así una mayor productividad en el trabajo.

Synology incluye diversas funciones de gestión que le permiten comprobar la información del sistema, supervisar los recursos del sistema, gestionar los servicios de notificación, restaurar o actualizar DSM, acceder a aplicaciones con una conexión independiente, indexar archivos multimedia para aplicaciones, etc.

### 8.4.1. Comprobar la información del sistema.

El centro de información ofrece una visión general del estado del Synology NAS y de otros dispositivos conectados. Vaya a Panel de control > Centro de información para comprobar la información siguiente.



*Imagen 32: Centro de información del Synology NAS*

#### 8.4.2. Verificar registros del sistema.

El Centro de registros es una aplicación centralizada de administración de registros que nos permite visualizar y administrar los registros de servicios del Synology NAS de manera sencilla y eficiente.

#### 8.4.3. Supervisar recursos del sistema.

Con el Monitor de recursos podemos supervisar el uso de la CPU, el uso de la memoria, la utilización del disco y el flujo de red. Puede elegir entre supervisar en tiempo real o visualizar los datos anteriores.

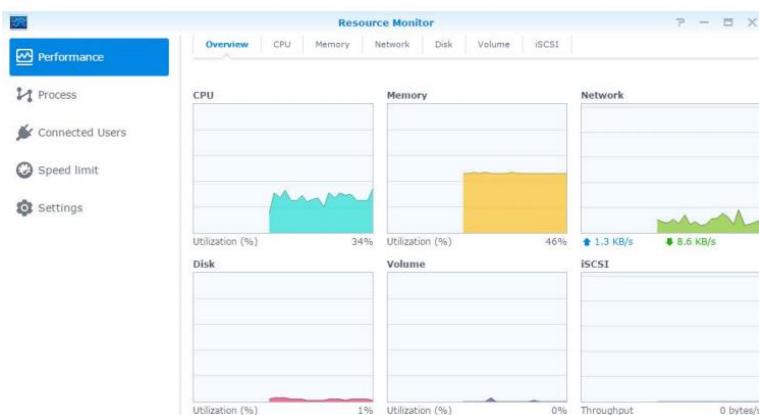


Imagen 33: Información de cada recurso en el Synology NAS.

#### 8.4.4. Analizar el uso del sistema.

El Analizador de almacenamiento nos permite observar de manera rápida las tendencias de uso general del Synology NAS, crear tareas para analizar espacios de almacenamiento y generar informes detallados sobre el uso del volumen.



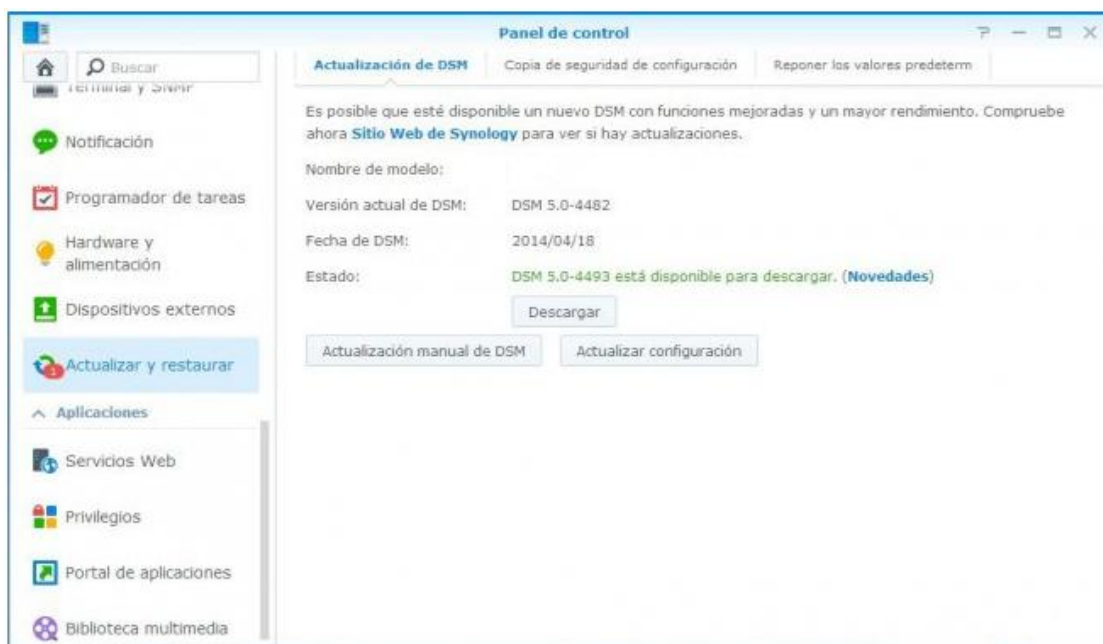
Imagen 34: Análisis del almacenamiento.

#### 8.4.5. Automatizar tareas.

Para programar y ejecutar servicios o scripts a horas predefinidas entramos a Panel de control > Programador de tareas. En este apartado se crearon y administraron tareas para ejecutar automáticamente scripts previamente definidos, vaciar las papeleras de reciclaje de las carpetas compartidas, o iniciar y detener ciertos servicios. Todo se hace bajo las necesidades de almacenamiento dentro de la empresa.

#### 8.4.6. Actualizar DSM o restaurar los valores predeterminados.

En el Panel de control > Actualizar y restaurar, cada vez que vamos a Actualización de DSM, el sistema comprobará si está disponible un nuevo DSM para su descarga y mostrará a continuación el resultado en texto verde o rojo. Si los resultados indican que el DSM más reciente está listo para su descarga, aceptamos para que el sistema descargue automáticamente el último DSM y, a continuación, realizar la actualización, también se pueden realizar copias de seguridad y restaurar configuraciones del sistema o restaurar su dispositivo Synology NAS a su configuración original de fábrica. También podemos configurar un programa para instalar actualizaciones de DSM de manera automática para que el Synology NAS esté siempre actualizado.



*Imagen 35: Actualización del DSM.*

Una nota importante es que, aunque los datos almacenados en el Synology no se borran en el proceso de actualización, siempre es recomendable hacer una copia de seguridad.

## 9. Resultados.

Se obtuvieron dos máquinas virtuales con un sistema Windows Server 2008 R2 (64 bits), necesarias para la empresa, ya que se instalaron programas como NOI, COIN, SAI, que funcionan en este sistema operativo, necesarias para la administración de la nómina, así como la administración de los productos que se manejan dentro de la misma.

Cada máquina tiene las siguientes características:

- Un procesador.
- Dos virtuales sockets, cada uno con dos cores.
- Memoria RAM de 4 GB.
- Disco duro de 80 GB.
- Tarjeta de Video.
- Lector de CD.
- Un puerto USB.
- Un puerto Ethernet.

El software utilizado dentro de la empresa se repartió en estas dos máquinas virtuales, pudiendo cada usuario acceder a los programas cuando sean requeridos de una manera más accesible y sencilla. Compartiendo de manera fácil el software y hardware en los equipos de la red, estableciendo así el acceso y control de la información que se maneja en la empresa más estricto a nivel usuario. Dicha información compartida entre los usuarios por medio de la plataforma virtual se verificó que funcionara de forma correcta.

Con respecto a las políticas de seguridad que se crearon dentro del Firewall y que se describieron con anterioridad, se obtuvo un mejor rendimiento de la red y se instaló un cerco de seguridad que permite a cada usuario compartir de manera segura la información. Ya que no se le permite a la mayoría de los usuarios utilizar aplicaciones móviles y de computadora, ya que se puede poner en riesgo la información y la seguridad de la red.

Se realizó el cambio de un servidor de archivos Synology NAS DS 212j a un DS 416, se hizo una copia de seguridad de toda la información existente del servidor anterior para pasarla al nuevo, y se configuró de acuerdo a las necesidades de la empresa. El servidor se dejó actualizado al DSM 6.1 que es el más reciente, y funcionando correctamente. El servidor anterior tenía una capacidad de almacenamiento de 2.87 TB en formato RAID 1, dicho servidor ya estaba comprometido al 93% de su capacidad. Con el Synology NAS DS 416 se aumentó la capacidad de almacenamiento hasta de 11 TB en el mismo formato RAID 1, con esto se redujo el porcentaje en el que estaba comprometido el anterior servidor; teniendo el actual sólo el 43% comprometido de la capacidad total de almacenamiento.

## **10. Análisis y discusión de resultados.**

Con las mejoras realizadas a cada una de las máquinas virtuales tanto en capacidad de almacenamiento como en el número de sockets y la memoria RAM, como respuesta, se obtuvo una plataforma robusta con un mejor rendimiento, además se tiene la opción de seguir creando máquinas virtuales si así lo requiere la empresa.

Con las políticas de seguridad actualizadas se estableció un perímetro de seguridad con el cual la información puede ser compartida con mayor seguridad y sólo se le permite a cada uno de los usuarios que laboran dentro de la empresa y dependiendo el departamento tener acceso a la información requerida y necesaria para desarrollar sus actividades diarias.

A cada usuario se le da un nombre que lo identifica, así como su clave de acceso para poder entrar a sus carpetas dentro del servidor de archivos Synology NAS DS 416, para que sólo pueda hacer cambios dentro de su carpeta de almacenamiento.

Con la implementación y actualización de estrategias que se tenían dentro de la empresa se logró tener un mayor control de la información que maneja cada usuario, además se tiene una supervisión constante de los activos con que cuenta la empresa.

## **11. Conclusiones**

El diseño de un diagrama de red sirvió de antecedente para ver la distribución de cada equipo, así como conocer las adecuaciones que se realizaron; cumpliendo con las expectativas para el cual se formuló el proyecto de Estancia con el cliente de la empresa T&B Talent S.A. de C.V.: ABC Uniformes S.A. de C.V. De esta manera se logró el objetivo principal, el cual era analizar, diseñar e implementar medidas que permitan establecer un cerco seguro, a través de estrategias dirigidas a mejorar la seguridad de la red, así como realizar las actualizaciones correctas de las políticas de seguridad existentes dentro de la empresa.

La realización de este proyecto ha permitido la obtención de una mayor comprensión de la distribución y seguridad existente en la red de computadoras dentro de una empresa, así como también me permitió adquirir nuevos conocimientos enfocados hacia la importancia de mantener una red segura mediante la investigación y la práctica laboral para el diseño de soluciones de problemas que se presentaron en la red de la empresa en la cual desarrollé la estancia.

Gracias a la realización de este proyecto y la correcta planeación de los cambios que se realizaron con respecto a la seguridad de la red, puedo afirmar que se tiene un mejor control de la información que maneja cada usuario y de manera global de toda la información con la que cuenta la empresa.

## 12. Referencias Bibliográficas.

- [1] Instituto Internacional de Seguridad Cibernética [en línea] ¿Cómo definir un plan de seguridad informática? [Consulta el 10 de noviembre de 2016] Disponible en: <http://www.iicybersecurity.com/seguridad-logica-seguridad-perimetral.html>
- [2] D. Lozano Gambo, “Administración de una red corporativa”, proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2015.
- [3] J. L. Matlacala Martínez, “Administración de una red profesional”, proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2010.
- [4] S. P. Ávila Campos, “Medidas de Seguridad en Servidores VPN de una red corporativa”, proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2015.
- [5] D. Avila Castillo, “Análisis y gestión de recursos para brindar seguridad en una red empresarial”, proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2015.
- [6] J. V. Juárez Guerrero, “Auditoria de la seguridad de los equipos de cómputo de la Central Termoeléctrica Valle de México”, proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2015.
- [7] R. M. Muñoz Villasana, “Administración de una red corporativa”, proyecto terminal, División de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana Azcapotzalco, México, 2015.
- [8] C. M. Fabuel Díaz, “Implantación de un sistema de seguridad perimetral”, proyecto de carrera, Escuela Universitaria de Ingeniería Técnica de Telecomunicación, Universidad Politécnica de Madrid, España, 1998.
- [9] Instituto Nacional de Tecnologías de la Comunicación. Seguridad Perimetral. En: *incibe* [en línea]. Noviembre 2010. [Consulta: 9 de noviembre de 2016]. Disponible en: [https://www.incibe.es/extfrontinteco/img/File/demostrador/monografico\\_seguridad\\_perimetral.pdf](https://www.incibe.es/extfrontinteco/img/File/demostrador/monografico_catalogo_seguridad_perimetral.pdf)
- [10] Colegio Cardenal Sancha. Redes. Sección 2 En: *Redes de Comunicaciones* [en línea]. [Consulta: 7 de marzo de 2017]. Disponible en: <http://info-redes.tripod.com/seccion2.html>
- [11] Vmware [en línea]. ¿Qué es una virtualización? [Consulta el 07 de marzo de 2017] Disponible en: <http://www.vmware.com/latam/solutions/virtualization.html>

[12] CISCO [en línea]. ¿Qué es un firewall? [Consulta el 07 de marzo de 2017] Disponible en:

[http://www.cisco.com/c/es\\_mx/products/security/firewalls/what-is-a-firewall.html](http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html)

[13] Fortinet [en línea]. Sobre nosotros [Consulta el 07 de marzo de 2017] Disponible en:

<https://www.fortinet.com/corporate/about-us/about-us.html>

[14] NKsistemas [en línea]. FortiGate – Firewall perimetral [Consulta el 07 de marzo de 2017] Disponible en:

<https://nksistemas.com/fortigate-firewall-perimetral/>

[15] Universidad Nacional Autónoma de México [en línea]. Seguridad Informática [Consulta el 07 de marzo de 2017] Disponible en:

<http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php>

[16] Synology Inc. [en línea]. NAS [Consulta el 15 de marzo de 2017] Disponible en:

<https://www.synology.com/es-mx/dsm/6.1/features>

### 13. Anexos.

#### 13.1. Inventario de equipos.

En la siguiente imagen se muestra parte del inventario de cada uno de los equipos con los que cuenta la empresa.

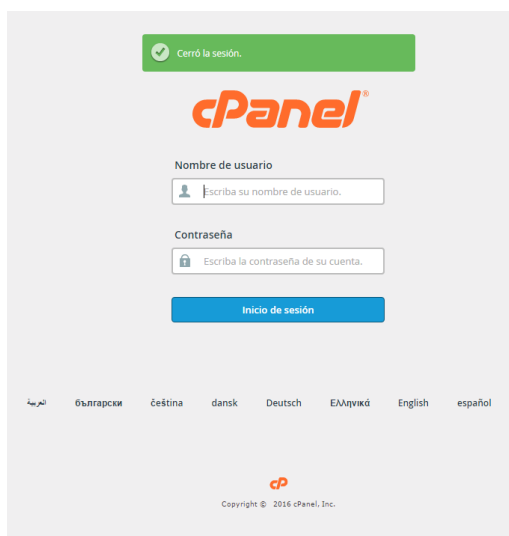
A	B	C	D	E	F	G	H	I	J	K	
1	NOMBRE DE USUARIO	IP	PROCESADOR	PC	MONITOR	ELIMINADOR PC	TECLADO	MOUSE	NO BREAK	IMPRESORA	OFFICE
3	Raúl Pérez	10.11.41	AMD E1-2000 APU with Radeon™ HD Graphics	HP Pavilion 20 All in one PC SN: 3CF00010M4		Eliminador HP SN: F10C110014620 INV: ADAP002	Logitech Keyboard K120 SN: 3C10C2 INV: sin número	HP Wireless Mouse 24000 SN: 7CDA90094M INV: sin número	SN: 986000025 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R200 INV: sin número	
4	José Manuel Sereno	10.11.52	AMD E1-2000 APU with Radeon™ HD Graphics	HP Pavilion 19 All in one PC SN: 3CM11907V4 INV: PC207		Eliminador HP SN: F12751310700960 INV: sin número	HP SK-3063 SN: 4491A-KB2063 INV: TEC024	HP Wireless Mouse SK2063 SN: H4MS2063 INV: MOUSE02	SN: 986000033 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R233 INV: MPF023	
5	Eliáneth Sotomayor	10.11.51	AMD E1-2000 APU with Radeon™ HD Graphics	HP Pavilion 19 All in one PC SN: 3CM11907V4 INV: PC207		Eliminador HP SN: VCPV10B7H4F02A INV: ADAP038	Logitech Keyboard K120 SN: CH-09VUS2-4475-24G-03AK-AS INV: sin número	HP Wireless Mouse SK2063 SN: H4MS2063 INV: MOUSE02	SN: 986000784 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R233 INV: MPF019	
6	Yolanda López	10.11.24	AMD A6-4300 APU with AMD Radeon™ HD Graphics	HP A6-4300 23.5" PC SN: 3CF9500MCP INV: sin número		Eliminador HP SN: VCPV10B7H4F02A INV: ADAP038	HP Keyboard SN: BCY10A5Y18C00A INV: sin número	HP Mouse SN: FCYV10C2850ACF INV: sin número	SN: 986000033 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R203 INV: MPF015	
7	Said Silva	10.11.50	AMD E1-2000 APU with Radeon™ HD Graphics	HP Pavilion 19 All in One PC SN: 3CM1200004 INV: PC205		Eliminador HP SN: F10C110014620 INV: ADAP002	HP Keyboard SN: BA0Y10A4H4PPEVQ INV: sin número	HP Wireless Mouse 24000 SN: 7CDA90094M INV: sin número	VICA S800 SN: 986000045 INV: sin número		
8	Diego Delgado	10.11.54	Intel® Core™ i3-2100 CPU @ 3.10GHz	HP Pav Slimline z5-1225a PC SN: M0C210K62 INV: CPJ002	Samsung S19E50N SN: ZUM4MTHC40095X INV: MOUNT01	No tiene	Dell SK-815 SN: CA10C4W5-7836-85R-054P INV: MOUNT01	Mouse PC-04425 SN: L200M4215 INV: MOUSE028	VICA S800 SN: 986000038 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R203 INV: MPF028	
9	Julio Vargas	10.11.49	Intel® Core™ i3-2100 CPU @ 3.10GHz	HP Pavilion P7-300LA SN: M0K120K03B INV: sin número	Samsung S19E50N SN: ZUM4MTHC40095X INV: MOUNT01	No tiene	HP KU-1000 SN: 8EY190E1V81000 INV: TEC017	Mouse Easy line SN: L33953315 INV: sin número	VICA S800 SN: 986000024 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R211 INV: MPF027	
10	Mauricio de la Cruz	10.11.36	Intel® Core™ i3-2120 CPU @ 3.10GHz	Dell Vostro SN: 3870075325 INV: CPJ005	Monitor Dell E1916 SN: CN14N0V14480-25A-0PYS	No tiene	HP SK-3063 SN: BCY10A5Y18C00A INV: TEC006	HP FBNVLC09V55F4 SN: FBNVLC09V55F4 INV: MOUSE05	VICA S800 SN: 986000035 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R212 INV: MPF018	
11	Isabel Sánchez	10.11.46	Intel® Core™ i3-3220 CPU @ 3.30GHz	HP ENVY 20 TouchSmart AIO SN: 3CM2370VGF INV: PC039		HP AC ADAPTER SN: VCPV10B73E1PD INV: ADAP038	HP SN: BCY10A5Y18C00A INV: sin número	HP Wireless Mouse 24000 SN: 7CDA90094M INV: sin número	VICA S800 SN: 986000042 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R212 INV: sin número	
12	Plabén Vázquez	10.11.33	Intel® Core™ i5-310M CPU @ 2.50GHz	Laptop HP Pavilion dm4 SN: 2CE22L2H INV: LAP015		HP AC ADAPTER SN: VB65V08CX15HB INV: ADAP015	HP AC ADAPTER SN: F132102822166 INV: ADAP017	HP Mouse Easy line SN: L33953315 INV: MOUSE019	VICA S800 SN: 986000028 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R212 INV: MPF018	
13	Gabriel López	10.11.40	Intel® Core™ i5-2450M CPU @ 2.50GHz	HP ENVY 20 TouchSmart AIO SN: 3CM2370VGF INV: PC039		HP AC ADAPTER SN: VCPV10B73E1PD INV: ADAP038	HP SK-3063 SN: BCY10A5Y18C00A INV: TEC007	HP Mouse SN: FCDF0A9V30G0C INV: MOUSE014	VICA S800 SN: 986000040 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R211 INV: MPF015	
14	Pilar Villegas	10.11.35	Intel® Core™ i5-3330S CPU @ 2.70GHz	HP Pavilion Slimline z5-1225a PC SN: M0C209794 INV: CPJ007	LCD Monitor HACER SN: MHLHPAA0023718638595		HP p1109 SN: BAUY10E8H-H0692 INV: TEC018	HP Mouse SN: FBNVLC09V55F4 INV: sin número	VICA S800 SN: 986000021 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R212 INV: sin número	
15	Isidoro Pérez	10.11.38	Intel® Core™ i3-2120 CPU @ 3.10GHz	HP ENVY 20 TouchSmart AIO SN: 3CM2370VGF INV: PC039		HP AC ADAPTER SN: VCPV10B73E1PD INV: ADAP038	HP SK-3063 SN: BCY10A5Y18C00A INV: TEC019	HP Mouse SN: FCDF0A9V30G0C INV: MOUSE014	VICA S800 SN: 986000034 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R212 INV: sin número	
16	Dina Díaz	10.11.43	Intel® Core™ i3-3220 CPU @ 3.30GHz	HP ENVY 20 TouchSmart AIO SN: 3CM2370VGF INV: PC039		HP AC ADAPTER SN: VCPV10B73E1PD INV: ADAP038	HP SK-3063 SN: BCY10A5Y18C00A INV: TEC019	HP Wireless Mouse 24000 SN: 7CDA90094M INV: sin número	VICA S800 SN: 986000023 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R2049 INV: MPF024	
17	Minerva Ortega	10.11.42	Intel® Core™ i3-3220 CPU @ 3.30GHz	HP ENVY 20 TouchSmart AIO SN: 3CM2370VGF INV: PC039		HP AC ADAPTER SN: VCPV10B73E1PD INV: ADAP038	HP SK-3063 SN: BCY10A5Y18C00A INV: TEC019	HP Wireless Mouse 24000 SN: 7CDA90094M INV: sin número	VICA S800 SN: 986000023 INV: sin número	Brother MFC-3870CW SN: UE3872L4F1R2049 INV: MPF024	

Imagen 36: Inventario de equipos de la empresa ABC Uniformes S.A. de C.V.

### 13.2. Manual para dar de alta un correo electrónico en cPanel.

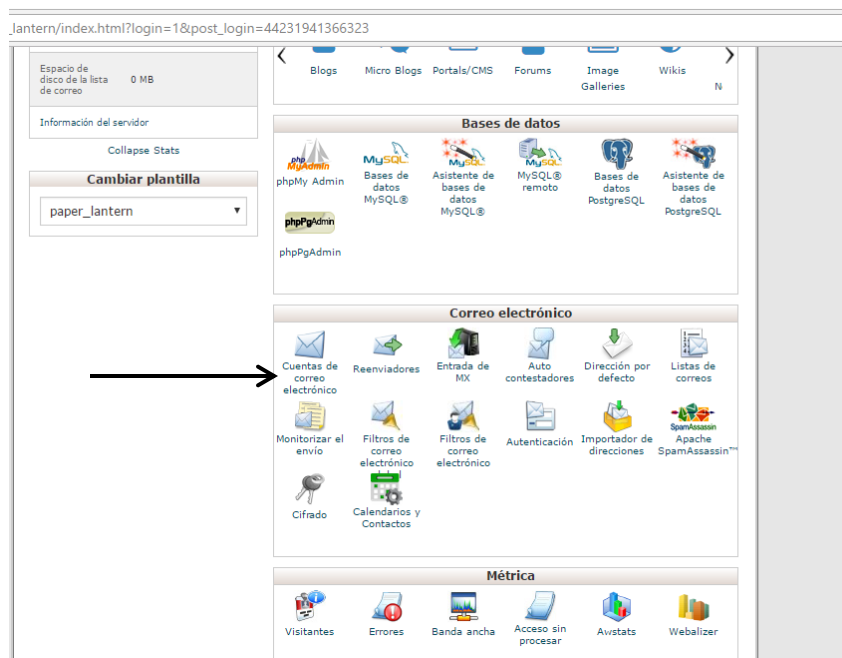
Para crear un correo electrónico, es necesario dar de alta al usuario desde el “cPanel Customer Portal” ingresando a la dirección <http://67.23.252.12/cpanel>

Ingresar usuario y contraseña (consultar archivo Administración TBT – ABC para ver clave de autenticación).



*Imagen 37: Ingreso al sistema cPanel.*

Después de haber ingresado, dirigirse al apartado del correo electrónico y seleccionar “Cuentas de correo electrónico”.

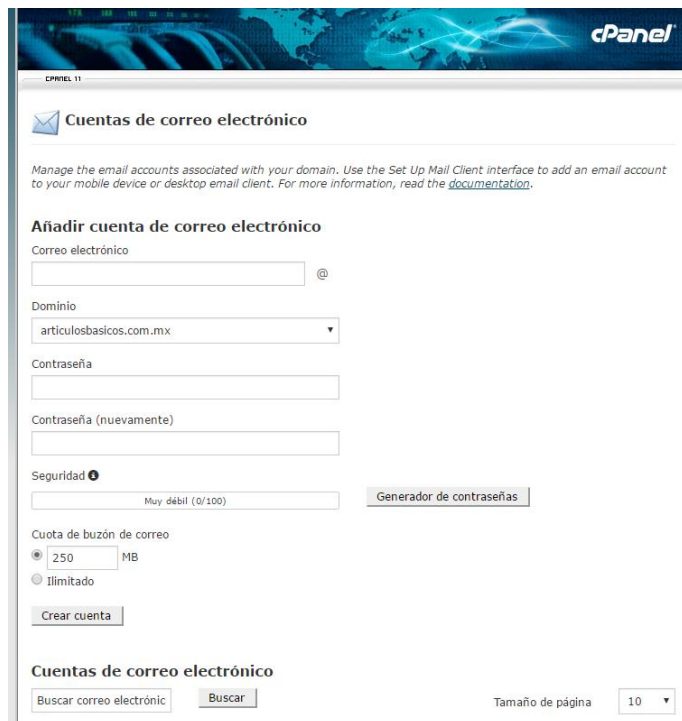


*Imagen 38: Crear cuentas de correo electrónico.*



En “Cuentas de correo electrónico” se añaden los datos del usuario a registrar, seleccionando como Dominio “articulosbasicos.com.mx”.

Para la contraseña, es necesario seguir el formato alfanumérico siguiente:  
4rt1cul05b451c05.xxxx

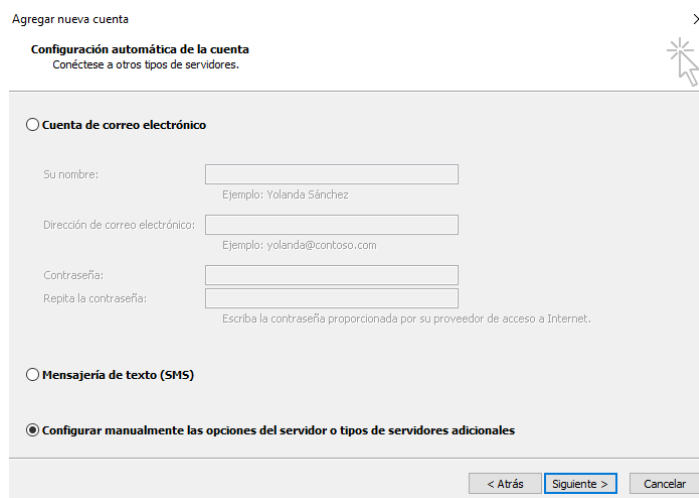


The screenshot shows the cPanel interface for adding an email account. The page title is "Cuentas de correo electrónico". Below the title, there is a section for "Añadir cuenta de correo electrónico". The form includes fields for "Correo electrónico", "Dominio" (set to "articulosbasicos.com.mx"), "Contraseña", and "Contraseña (nuevamente)". There is also a "Seguridad" section with a "Generador de contraseñas" button and a "Cuota de buzón de correo" section with radio buttons for "250 MB" (selected) and "Ilimitado". A "Crear cuenta" button is at the bottom of the form. Below the form, there is a search section for "Cuentas de correo electrónico" with a "Buscar" button and a "Tamaño de página" dropdown set to "10".

*Imagen 39: Ingresar datos de usuario.*

Una vez creado el correo electrónico, se procede a hacer la configuración en Outlook.

En el asistente de configuración de Outlook, seleccionar la opción “Configurar manualmente las opciones del servidor o tipo de servidores adicionales”.



The screenshot shows the Outlook "Agregar nueva cuenta" wizard. The title is "Agregar nueva cuenta". Below the title, there is a section for "Configuración automática de la cuenta" with a sub-note "Conéctese a otros tipos de servidores." and a close button. Below this, there are three radio button options: "Cuenta de correo electrónico", "Mensajería de texto (SMS)", and "Configurar manualmente las opciones del servidor o tipos de servidores adicionales" (which is selected). The "Cuenta de correo electrónico" section has fields for "Su nombre:" (with an example "Yolanda Sánchez"), "Dirección de correo electrónico:" (with an example "yolanda@contoso.com"), "Contraseña:", and "Repita la contraseña:". A note below the password fields says "Escriba la contraseña proporcionada por su proveedor de acceso a Internet." At the bottom, there are buttons for "< Atrás", "Siguiete >", and "Cancelar".

*Imagen 40: Configuración en Outlook.*

En “Configuración de correo electrónico de Internet”, ingresar la información del usuario y del servidor.

Para el servidor de correo entrante y saliente (SMTP), ingresar: smx11.hostdime.com.mx

En “Entregar nuevos mensajes a:”, se deja habilitada la opción “Nuevo archivo de datos de Outlook” si se trata de un usuario nuevo. Si se cuenta con el archivo .pst de un usuario existente, seleccionar “Archivo de datos de Outlook existente” y agregar la ruta donde se encuentra el archivo.

Agregar nueva cuenta

**Configuración de correo electrónico de Internet**  
Estos valores son necesarios para que la cuenta de correo electrónico funcione.

**Información sobre el usuario**  
Su nombre: Aaron Lopez  
Dirección de correo electrónico: nas@articulosbasicos.com.mx

**Información del servidor**  
Tipo de cuenta: POP3  
Servidor de correo entrante: smx11.hostdime.com.mx  
Servidor de correo saliente (SMTP): smx11.hostdime.com.mx

**Información de inicio de sesión**  
Nombre de usuario: aaron sistemas@articulosbasicos  
Contraseña: \*\*\*\*\*  
 Recordar contraseña  
 Requerir inicio de sesión utilizando Autenticación de contraseña segura (SPA)

**Configuración de la cuenta de prueba**  
Después de rellenar la información de esta pantalla, le recomendamos que pruebe su cuenta haciendo clic en el botón. (Requiere conexión de red.)  
Probar configuración de la cuenta ...  
 Probar configuración de la cuenta haciendo clic en el botón Siguiente

**Entregar nuevos mensajes a:**  
 Nuevo archivo de datos de Outlook  
 Archivo de datos de Outlook existente  
Examinar

Más configuraciones ...

< Atrás Siguiente > Cancelar

Imagen 41: Configuración de datos del servidor de correo.

Después, dentro de la misma ventana, dirigirse a “Más configuraciones...” y en la pestaña “Servidor de salida” habilitar la opción “Mi servidor de salida (SMTP) requiere autenticación” y también seleccionar “Utilizar la misma configuración que mi servidor de correo de entrada”.

Configuración de correo electrónico de Internet

General Servidor de salida Conexión Avanzadas

Mi servidor de salida (SMTP) requiere autenticación

Utilizar la misma configuración que mi servidor de correo de entrada

Iniciar sesión utilizando

Nombre de usuario: [ ]

Contraseña: [ ]

Recordar contraseña

Requerir Autenticación de contraseña segura (SPA)

Iniciar sesión en el servidor de correo de entrada antes de enviar correo

Aceptar Cancelar

Imagen 42: Configuración del servidor de salida.

En la pestaña “Avanzadas” se elige el puerto de entrada y salida. En POP3 asignar el puerto 995 y en SMTP asignar el puerto 465. También es necesario habilitar la opción “Este servidor precisa una conexión cifrada (SSL)” y en “Usar el siguiente tipo de conexión cifrada”, seleccionar “SSL” y finalmente “Aceptar”

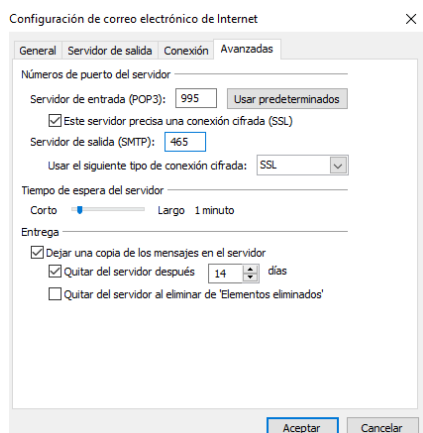


Imagen 43: Opciones avanzadas.

Es posible verificar que la configuración es correcta, mediante la opción “Probar configuración de la cuenta...” de no estar correcta, se pueden verificar los errores.

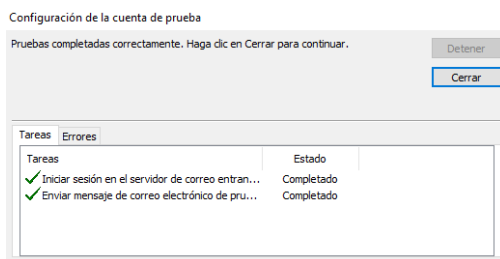


Imagen 44: Probar configuración de la cuenta.

Al finalizar la instalación, se abrirá automáticamente la bandeja de entrada con el correo ya configurado.

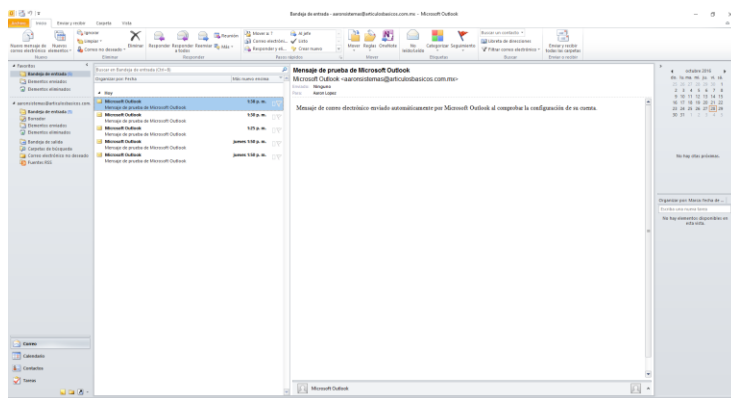


Imagen 45: Correo configurado correctamente.