

Área de Conocimiento de Tecnología de la Información y Comunicación

LEVANTAMIENTO DE UN SISTEMA DE RED LOCAL ÁREA NETWORK E IMPLEMENTACIÓN DE SERVIDORES VIRTUALIZADO PARA LA ADMINISTRACIÓN Y CONTROL DE INFORMACIÓN EN LA ORGANIZACIÓN “SUMINISTRO FARMACÉUTICOS”

Trabajo Monográfico para optar al título de Ingeniero en Electrónica

Elaborador Por:

Br. Omar Ewan Urbina Romero
Carnet: 2016-1212U

Tutor:

Msc. Dora Inés Reyes
Chávez

Resumen

El proyecto consiste en la implementación de una red local (LAN) en una organización dedicada al suministro farmacéutico, con el objetivo de administrar y controlar la información de manera eficiente. Para ello, se establecerá una infraestructura de servidores virtualizados que permitirá centralizar el almacenamiento de datos y la gestión de aplicaciones clave para la organización.

Como inicio del Proyecto se llevará a cabo la determinación de recursos iniciales de la organización para poder desarrollar el diseño y la planificación de la red LAN, considerando las necesidades específicas de la organización y garantizando la seguridad, disponibilidad y la escalabilidad de la red. Se definirán los requisitos de hardware y software necesarios para implementar la red, así como su topología.

Posteriormente, se procederá a la instalación y configuración de los servidores virtualizados, los cuales ejecutarán servicios como almacenamiento de datos, administración de usuarios, entre otros. Se utilizarán tecnologías de virtualización para optimizar los recursos y facilitar la administración de los servidores.

Además, se implementarán medidas de seguridad como firewalls y políticas de acceso restringido a la información sensible de la organización. Se establecerán procedimientos de copia de seguridad y recuperación de datos para garantizar la disponibilidad de la información en caso de fallos o pérdidas.

En resumen, el proyecto busca mejorar la eficiencia operativa y la seguridad de los datos en una organización de suministro farmacéutico, proporcionando una plataforma tecnológica robusta y escalable para su correcta administración.

Índice

I. Introducción.....	1
II. Objetivos	2
Objetivo General	2
Objetivos Específicos	2
III. Antecedentes	3
IV. Justificación	5
V. Marco teórico.....	6
Elementos que conforman una red estándar corporativa	6
Estándares para el diseño e implementación de red LAN.....	7
Flujograma del diseño de la red LAN bajo los estándares	10
VI. Análisis y presentación de los resultados	10
VII. Diseño metodológico.....	13
Análisis Causa – Raíz.....	16
Alcance Del Proyecto.....	17
Requerimientos de la organización	18
Limitación de recursos a terceros	18
Presupuesto del proyecto.....	19
VIII. Desarrollo del proyecto	20
Infraestructura de red	20
Selección de material y dispositivos	21
1. Cable de conexión de puntos de acceso Cat6	21
2. Determinación de Servidores	21
Servidor HP ProLiant ML150	23
Elección de Router y firewall.....	24
Selección de Switch y Patch panel	24
Patch panel	26
Respaldo de Energía.....	26
Base Rack	27

Optimización del Espacio.....	27
Ventilación y Refrigeración	28
Acceso y Mantenimiento.....	28
Escalabilidad	28
Elección de proveedor de Internet.....	28
Ubiquiti – AP	29
Conexiones eléctricas.....	29
IX. Despliegue físico de la red LAN	30
Selección de ubicación de la infraestructura	30
Instalación de cableado estructural	31
Ensamblaje y Armado de RACK	32
Instalación de switch y conexión de patch cord	36
Instalación de servidor Dell.....	37
Instalación de servidor HP Proliant y Bandeja.....	37
Instalación de Baterías y conexiones eléctricas	38
Conexiones de baterías a la corriente eléctrica comercial.....	39
Topología física.....	40
Instalación y configuraciones de servicios y sistemas operativos.....	40
Configuración de Red.....	40
Configuración de Servicio DHCP	42
Configuración Firewall y Política de restringida	44
Política de seguridad libre.	46
Configuración de VPN	46
Creación de Usuario para VPN	47
Configuración de VPN en host.....	48
Instalación y configuración de Antivirus	49
Virtualización de servidores	50
Configuración de Máquina virtual en el servidor.....	54
Instalación de Windows server 2016 en máquina virtual	57
Instalación de servicio de Active Directory	59
Implementación de servicio de respaldo	66
Configuración de disponibilidad y acceso a información.	72
Configuración de dispositivo wifi AP	77
Topología Lógica	78

X. Recomendaciones	80
XI. Conclusiones	82
XII. Referencias bibliográficas.....	83
<i>Bibliografía</i>	<i>83</i>

Contenido de Ilustraciones

<i>Ilustración 1 :Flujograma de estándares de la red LAN.</i>	10
<i>Ilustración 2: Muestras de datos antes del proyecto.</i>	12
<i>Ilustración 3: Muestras de datos después del proyecto.</i>	12
<i>Ilustración 4: Diagrama Causa Raíz</i>	16
<i>Ilustración 5: Vista aérea del edificio farmacéutico</i>	30
<i>Ilustración 6: Estructura de cableado</i>	32
<i>Ilustración 7: Medidas de Rack</i>	32
<i>Ilustración 8: Ensamblado de Rack</i>	33
<i>Ilustración 9: Medidas del Rack</i>	34
<i>Ilustración 10: Categorías de colores</i>	35
<i>Ilustración 11: Instalación de cable de red en patch panel</i>	35
<i>Ilustración 12: Pasos de ponchado Jack RJ45</i>	35
<i>Ilustración 13: Puerto de red en oficinas</i>	35
<i>Ilustración 14: Instalación de Switch</i>	36
<i>Ilustración 15: Interfaces de conexión Switch y patch panel</i>	37
<i>Ilustración 16: Servidor Dell</i>	37
<i>Ilustración 17: Instalación de rack de Servidor Dell</i>	37
<i>Ilustración 18: Servidor Proliant sobre bandeja</i>	38
<i>Ilustración 19: Instalación de Baterías de respaldo APS</i>	38
<i>Ilustración 20: Vista toma eléctrico</i>	39
<i>Ilustración 21: Conexiones de baterías a la Fuente</i>	39
<i>Ilustración 22: Conexión de servidores en baterías</i>	39
<i>Ilustración 23: Topología física e la red LAN Estándar</i>	40
<i>Ilustración 24: Captura de pantalla de interfaz física de Fortinet</i>	41
<i>Ilustración 25: Login Inicial de Fortinet</i>	42
<i>Ilustración 26: Selección de Interfaces Fortinet</i>	42
<i>Ilustración 27: Configuración red LAN interna</i>	43
<i>Ilustración 28 Configuración de DHCP</i>	43
<i>Ilustración 29 Configuración de parámetros de Política</i>	44

<i>Ilustración 30 Vista de Política Restringido</i>	45
<i>Ilustración 31 Creación de Bloqueo de dirección web</i>	45
<i>Ilustración 32 Vista de política libre.</i>	46
<i>Ilustración 33 Configuración de SSL-VPN.</i>	46
<i>Ilustración 34 Establecimiento de Credenciales vpn.</i>	47
<i>Ilustración 35 Configuración Forti-Client</i>	48
<i>Ilustración 36 Configuración Forti-Client</i>	49
<i>Ilustración 37. Vista de consola de Eset (Descarga de archivo de instalador)</i>	50
<i>Ilustración 38 Descarga de ISO Esxi (Captura de pantalla en la plataforma)</i>	51
<i>Ilustración 39 Boot de Sistema de virtualización</i>	52
<i>Ilustración 40 Selección de disco de instalación</i>	52
<i>Ilustración 41 Configuración de IP estática</i>	53
<i>Ilustración 42 Navegación grafica del servidor</i>	54
<i>Ilustración 43 Creación de maquina virtual</i>	55
<i>Ilustración 44 Selección de parámetros de virtualización</i>	55
<i>Ilustración 45 Selección de recursos de máquina Virtual</i>	56
<i>Ilustración 46 Carga de sistema operativo para MV</i>	57
<i>Ilustración 47 Menú de instalación Windows Server 20216</i>	58
<i>Ilustración 48 Proceso de instalación de Windows server 2016</i>	58
<i>Ilustración 49 Login y panel de control Windows server 2016</i>	59
<i>Ilustración 50 Proceso de configuración de Active Directory</i>	60
<i>Ilustración 51 Proceso de configuración de Active Directory 1.1</i>	60
<i>Ilustración 52 Proceso de configuración de Active Directory 1.2</i>	61
<i>Ilustración 53 Controlador de dominio</i>	62
<i>Ilustración 54 Proceso de configuración de Active Directory 1.3</i>	62
<i>Ilustración 55 Proceso de configuración de Active Directory 1.4</i>	63
<i>Ilustración 56 Proceso de configuración de Active Directory 1.5</i>	64
<i>Ilustración 57 Proceso de configuración de Active Directory 1.5</i>	64
<i>Ilustración 58 Proceso de configuración de Active Directory 1.6</i>	65
<i>Ilustración 59 Unión de cliente a servidor de dominio</i>	65

<i>Ilustración 60. Conexión local veeam a servidor</i>	67
<i>Ilustración 61 Creación de repositorio de respaldo</i>	67
<i>Ilustración 62 Selección de carpeta para repositorio</i>	68
<i>Ilustración 63 Menú de configuración de repositorio</i>	68
<i>Ilustración 64. Selección de servidor</i>	69
<i>Ilustración 65. Selección de repositorio</i>	70
<i>Ilustración 66 Configuración de respaldo</i>	70
<i>Ilustración 67 Finalización de estado de trabajo</i>	71
<i>Ilustración 68 Vista de proceso de respaldo de maquina virtual</i>	71
<i>Ilustración 69 Visualización de archivos de respaldo</i>	72
<i>Ilustración 70 Permisos de accesos a información</i>	73
<i>Ilustración 71 Selección de nuevo trabajo</i>	74
<i>Ilustración 72 creación de trabajo de respaldo 1.1</i>	75
<i>Ilustración 73 creación de trabajo de respaldo1.2</i>	75
<i>Ilustración 74. creación de trabajo de respaldo 1.3</i>	76
<i>Ilustración 75. creación de trabajo de respaldo 1.5</i>	76
<i>Ilustración 76 creación de trabajo de respaldo 1.4</i>	76
<i>Ilustración 77: Diseño de red LAN con topología logica estrella.</i>	79

Contenido de Tablas

<i>Tabla 1: Gastos del proyecto</i>	1
---	---

I. Introducción.

La tecnología de la información y la comunicación (TIC) se ha vuelto fundamental en el desarrollo y éxito de cualquier organización. En particular, las redes LAN y la virtualización de servidores se han convertido en herramientas indispensables para la gestión y control de la información en las empresas. En este sentido, la organización "Suministro farmacéuticos" enfrenta el reto de mejorar su sistema de información para optimizar sus procesos internos y ofrecer un mejor servicio a sus clientes y usuarios.

Por lo tanto, en este trabajo se plantea el diseño metodológico del levantamiento de un sistema de Red Local Área Network e implementación de servidores virtualizados para la administración y control de información en la Organización "Suministro farmacéuticos". Se abordarán aspectos como la identificación de requerimientos, el análisis de la infraestructura actual, el diseño de la red, la selección de servidores y software, la virtualización de servidores, la configuración de los sistemas, la capacitación de usuarios, el mantenimiento y soporte, la implementación de medidas de seguridad y la evaluación de resultados.

El diseño metodológico abarca diversas etapas, desde la identificación de requisitos hasta la configuración de servicios como el router y Windows Server. Esto permitirá una visión completa de la estructura del sistema y garantizará la ejecución exitosa del proyecto. Se espera que la implementación de estas medidas permita mejorar la eficiencia y productividad de la organización, así como una mayor satisfacción de sus clientes y usuarios. Además, se busca contar con un soporte y mantenimiento adecuado que proporcione la actualización constante de los sistemas y la adaptación a nuevas tecnologías en el futuro.

II. Objetivos

Objetivo General

-) Implementar una infraestructura de red LAN estándar y un servicio en Windows server, para la gestión de usuarios y dispositivos finales, que cumpla con los requisitos de protección y disponibilidad de la información generada por los usuarios en la organización.

Objetivos Específicos

1. Determinar la infraestructura del área junto con las diferentes necesidades que requiere la organización para una elaboración apropiada de un sistema de red LAN.
2. Implementar servidores virtualizados que permitan a la organización tener una mayor flexibilidad y escalabilidad en sus sistemas, así como una mayor eficiencia en el uso de los recursos de hardware y software.
3. Establecer medidas de seguridad adecuadas de acuerdo a la disponibilidad y confidencialidad de la información de la organización, tales como firewalls y sistemas de respaldo.

III. Antecedentes

En el ámbito de la industria farmacéutica y de suministros médicos, la implementación de sistemas de información y comunicación eficientes, y seguros, es fundamental para garantizar la calidad, la trazabilidad, la disponibilidad de los productos y servicios que se ofrecen. Además, estos sistemas pueden ser esenciales para cumplir con las regulaciones y normativas que rigen el sector de salud y para optimizar la gestión de los recursos. (Manghani, K., 2015).

La virtualización de servidores y la implementación de redes de área local (LAN) son tecnologías ampliamente utilizadas en la actualidad para mejorar la eficiencia, la escalabilidad y la flexibilidad de los sistemas de información y comunicación en las organizaciones. Según diversos estudios, estas tecnologías pueden permitir reducir costos de hardware, simplificar la administración de sistemas y mejorar la seguridad y el rendimiento de las redes y los servidores (Dabiri & Lim, 2016).

En referencia a proyectos anteriores similares, la universidad nacional de ingeniería, en el compendio de su biblioteca se encontraron 2 trabajos monográficos como fuente de soporte y apoyo en la determinación de alcance del presente protocolo, los cuales son:

En el centro de documentación FEC de la universidad nacional de ingeniería se pudo apreciar un trabajo monográfico **“Diseño de red LAN y radio enlace por microondas para acceso a internet en la escuela de la comunidad el Coyolito del Departamento de Estelí.CD”**, por el Br. David Josué Gaitán Rugama, en donde plantea proyectar un sistema de red LAN usando los principios de la tecnología de radio propagación demostrando cómo expandir y conectar otros lugares por medio de un sistema de red.

En la documentación FEC de la universidad nacional de ingeniería podemos apreciar una vez más un monográfico de redes cuyo título es “**Diseño de Red FTTH para la Zona de la Laguna de Apoyo**”, escrita por Br. Erick Danilo Arroliga Grijalba, como base del proyecto se es implementar un dispositivo de alta eficiencia como lo es la fibra óptica en la red para obtener la confiabilidad y seguridad en el transporte de datos, esta es una tecnología que retomaremos en este protocolo.

En la documentación expuesta como trabajo monográfico, para optar al título de ingeniero electrónico es el realizado por Zambra y López (2015), bajo el tema “**Diseño de una Red LAN para la empresa comercial Edgar Detrinidad s.a (CEDETSa)**”, en el que presentan como objetivos el diagnóstico y análisis de la red LAN existente en la empresa CEDETSa, para determinar posibles deficiencias y así proponer el diseño de un nuevo sistema de red que optimice recursos de dicha empresa.

Como trabajo monográfico para optar por el título de ingenieros electrónicos Castellón y Gutiérrez (2016), desarrollaron el tema “**Configuración e instalación de una PBX virtual a través de Elastix basado en Asterisk en la Agencia aduanera ADENICA-Managua**”, en el cual plantean como objetivo unificado el análisis de las condiciones del sistema telefónico, para mostrar una nueva alternativa mediante la implementación de VoIP con Asterisk, al mismo tiempo que explican su instalación, configuración y las tablas comparativas de costo entre la comunicación telefónica actual y la propuesta.

IV. Justificación

La implementación de un sistema de Red Local Área Network (LAN) y servicios virtualizados en la organización "Suministro Farmacéuticos" tiene como objetivo principal mejorar la administración y el control de la información. Este proyecto se justifica debido a la necesidad de mejorar los tiempos de respuesta de la compañía ya que la meta de la empresa de entregar lo solicitado por el cliente es de 10 horas o menos y en promedio actualmente, se encuentran en 20 horas, por lo tanto, se debe de contar con una infraestructura tecnológica robusta y eficiente que conceda optimizar los procesos de la organización, mejorar la gestión de la información y asegurar la disponibilidad y confidencialidad de los datos.

La implementación de una red LAN permitirá a la organización conectar sus diferentes equipos de cómputo en una red local, lo que facilitará la comunicación y el intercambio de información entre ellos. Además, el uso de servicios virtualizados permitirá a la organización tener una mayor flexibilidad y escalabilidad en sus sistemas, así como una mayor eficiencia en el uso de los recursos de hardware y software.

Esta iniciativa se basa en diversas normas y recomendaciones, como las establecidas por la Asociación de la Industria de las Tecnologías de la Información (CompTIA) y la Asociación de la Industria de la Computación (ACM), entre otras.

En conclusión, la implementación de un sistema de Red LAN y servicios virtualizados en la organización "Suministro Farmacéuticos" representa una inversión estratégica que facilitará mejorías en la gestión de la información y así optimizar los procesos de la organización, con el fin de brindar un mejor servicio a sus clientes.

V. Marco teórico

Elementos que conforman una red estándar corporativa

Una red de computadoras es un conjunto de dispositivos interconectados que comparten recursos y datos entre sí. Para que este sistema funcione de manera eficiente, se requiere de una serie de elementos fundamentales, con sus respectivas fuentes que proporcionan un análisis profundo sobre cada componente (Hernández, 2012-2013).

1. **Nodos (Dispositivos Finales):** Los dispositivos finales o nodos son esenciales para el propósito de una red, que es compartir recursos y comunicarse. Cualquier dispositivo capaz de usar la red para comunicarse se considera un nodo (Stallings, 2017).
2. **Medios de Transmisión:** El medio de transmisión actúa como un portador de las señales entre emisor y receptor. Puede ser cableado, como el par trenzado, coaxial o de fibra óptica, o inalámbrico, como radiofrecuencia, microondas, infrarrojos o satelital (Comer, 2018).
3. **Dispositivos de Interconexión de Red:** Los dispositivos de interconexión como switches, enrutadores y puntos de acceso son cruciales para facilitar la comunicación entre dispositivos en la red (Kurose & Ross, 2020).
4. **Dispositivos de Seguridad de Red:** Los firewalls y los sistemas de prevención de intrusiones protegen las redes de accesos no autorizados y monitorean posibles amenazas (Cheswick, Bellovin, & Rubin, 2019).

5. **Servidores y Servicios de Red:** Estos dispositivos robustos y especializados proveen servicios a la red y pueden especializarse en tareas como archivos, impresión, correo electrónico y otros (Stallings, 2017).

6. **Software de Red:** El software de red, incluyendo los sistemas operativos y protocolos de comunicaciones, es imprescindible para el funcionamiento y gestión de la red (Tanenbaum & Wetherall, 2011).

7. **Topología de Red:** La topología define el diseño y la estructura física o lógica de la red. Topologías comunes incluyen la estrella, anillo, malla, bus y árbol, cada una con ventajas y limitaciones específicas (Laudon & Laudon, 2016).

8. **Elementos de Virtualización de Red y SDN:** La virtualización de red es un método para gestionar recursos de red mediante software. Las Redes Definidas por Software (SDN, por sus siglas en inglés) separan la capa de control de la capa de datos, proporcionando una gestión de red más dinámica y adaptable (Nadeau & Gray, 2013).

Estándares para el diseño e implementación de red LAN

En la implementación de una red LAN corporativa, se deben considerar una serie de estándares que garantizan la interoperabilidad, la seguridad y la eficiencia de la red. Estos estándares son desarrollados por organizaciones reconocidas a nivel mundial y proporcionan directrices para prácticamente todos los aspectos de las redes. Estos son:

1. **IEEE 802.3:** Este estándar define el Ethernet, que es la tecnología predominante utilizada en redes LAN cableadas. Cubre aspectos como la topología de red, los métodos de acceso y las velocidades de transmisión (IEEE, 2018).
2. **IEEE 802.11:** Conocido como Wi-Fi, este conjunto de estándares define las comunicaciones inalámbricas LAN. Se actualiza periódicamente para incluir avances como mayor velocidad y seguridad (IEEE, 2020).
3. **ANSI/TIA-568:** Este estándar especifica los requisitos para el cableado de telecomunicaciones en edificios comerciales, incluyendo las categorías de cable, distancias máximas y métodos de prueba (ANSI/TIA, 2021).
4. **ISO/IEC 27001:** Este estándar internacional proporciona requisitos para un sistema de gestión de seguridad de la información (SGSI), relevante para proteger la información procesada por la red LAN (ISO/IEC, 2013).
5. **ANSI/EIA/TIA-942:** Es un estándar para el diseño e instalación de infraestructuras de centros de datos, incluyendo redes LAN corporativas que se alojan en dichos centros (ANSI/EIA/TIA, 2012).
6. **ISO/IEC 11801:** Proporciona pautas para el cableado de sistemas de comunicación de datos y voz, incluyendo especificaciones para el cableado estructurado tanto de cobre como de fibra óptica (ISO/IEC, 2017).

7. **Control Objectives for Information and Related Technologies (COBIT):** Es un marco de trabajo para el desarrollo, implementación, monitoreo y mejora de las políticas de TI y seguridad de la información.
8. **NFPA 75:** La National Fire Protection Association establece estándares para la protección contra incendios específicos para la tecnología de la información, incluyendo los centros de datos (National Fire Protection Association, 2013).
9. **ASHRAE Standards:** La American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) establece recomendaciones para el control ambiental en centros de datos, como la temperatura, la humedad y la filtración del aire (American Society of Heating, Refrigerating and Air-Conditioning Engineers, 2011).
10. **Uptime Institute's Tier Standard:** El Uptime Institute ofrece un sistema de clasificación (Tier) para los centros de datos que evalúa la infraestructura de acuerdo con la disponibilidad y redundancia de los sistemas críticos (Uptime Institute, 2014).
11. **ISO/IEC 20000:** Define las mejores prácticas en la gestión de servicios de TI, lo que ayuda a garantizar la entrega de servicios eficaces y fiables (ISO, 2018).
12. **CIS Critical Security Controls:** Anteriormente conocidos como los controles críticos de SANS, son un conjunto recomendado de acciones para la defensa cibernética que proporciona medidas efectivas para prevenir los tipos de ataques más comunes y peligrosos.

Flujograma del diseño de la red LAN bajo los estándares

En la siguiente imagen se muestra el flujograma del diseño de la red LAN bajo los estándares utilizados para el levantamiento del proyecto. Ver figura de abajo.

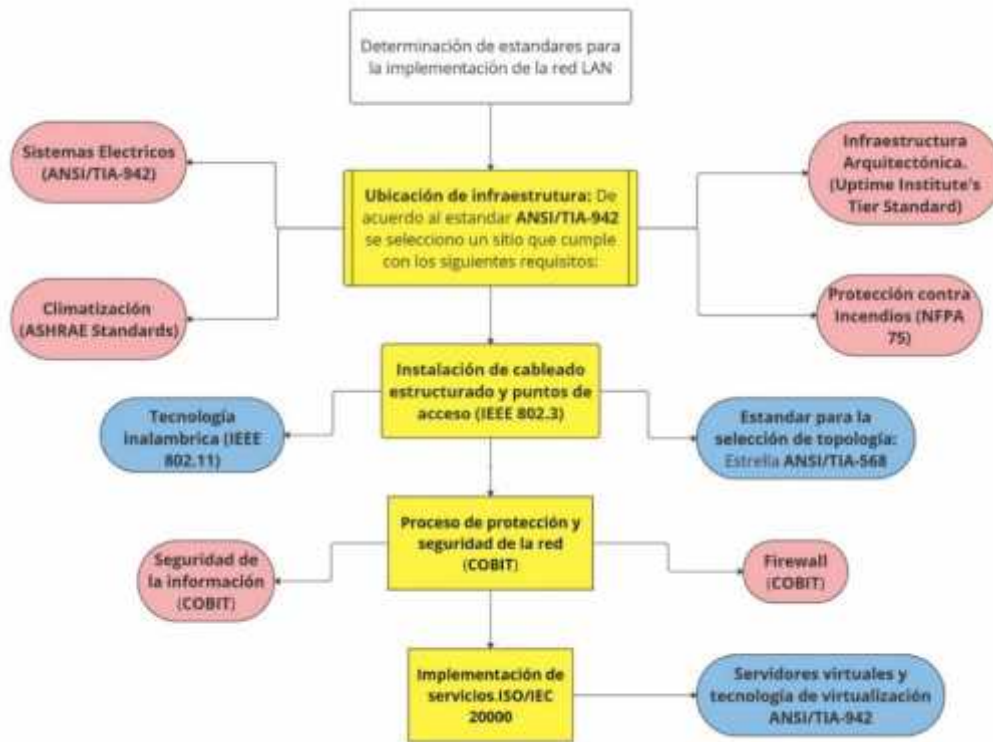


Ilustración 1 :Flujograma de estándares de la red LAN.

Fuente: Recursos Propios

VI. Análisis y presentación de los resultados

Para determinar el estado de la empresa, previo al proyecto, se realizó un estudio estadístico que se obtuvo de una sesión de causa raíz y lluvia de ideas que se condujo con los líderes de operaciones, la métrica ideal para medir el éxito del proyecto, que es el indicador clave de rendimiento de la empresa "Tiempo de respuesta", que se refiere al tiempo en horas que se tarda en entregar los químicos solicitados, desde que el cliente los ordena, hasta que son recibidos por el solicitante. La meta de la empresa es que este proceso tome 10 horas o menos.

Debido al número mínimo de muestras que se requieren para conducir los análisis estadísticos, en los que se obtengan resultados con un nivel de confianza de un 95%, que es estándar en la industria, se tomaron 1 muestras diaria por treinta días donde se midió eligiendo un usuario al azar, el periodo de tiempo desde que se recibe la orden de parte del cliente, hasta que se entrega, dicho testeó empezó el 21 de abril de 2022 y culminó el 20 de mayo de 2022.

Algunos conceptos importantes a tomar en cuenta son, N: Número de muestras; Media: Promedio de las muestras; Desviación Estándar: Calcula la dispersión de los datos; Mínimo: Es el valor mínimo de las muestras; Máximo: Es el valor máximo de las muestras; Percentil x%: El valor de x en el percentil representa el porcentaje de la población que se encuentra debajo del valor del percentil. Mediana: La mitad de las muestras están abajo del valor de la mediana y la otra mitad arriba de la mediana.

Para el análisis, se utilizó la herramienta de análisis estadístico Minitab 20.1, y se condujeron 2 análisis: El primero fue un resumen gráfico estadístico, que nos muestra un análisis de las muestras y su distribución y el segundo análisis, fue un análisis de capacidad del proceso para determinar si con las condiciones actuales en ese momento, era estadísticamente posible que el proceso alcanzara la meta de 10 horas o menos.

En la siguiente imagen se puede observar el análisis de capacidad confirma que, con las condiciones actuales, el proceso no es capaz de alcanzar la meta de 10 horas.

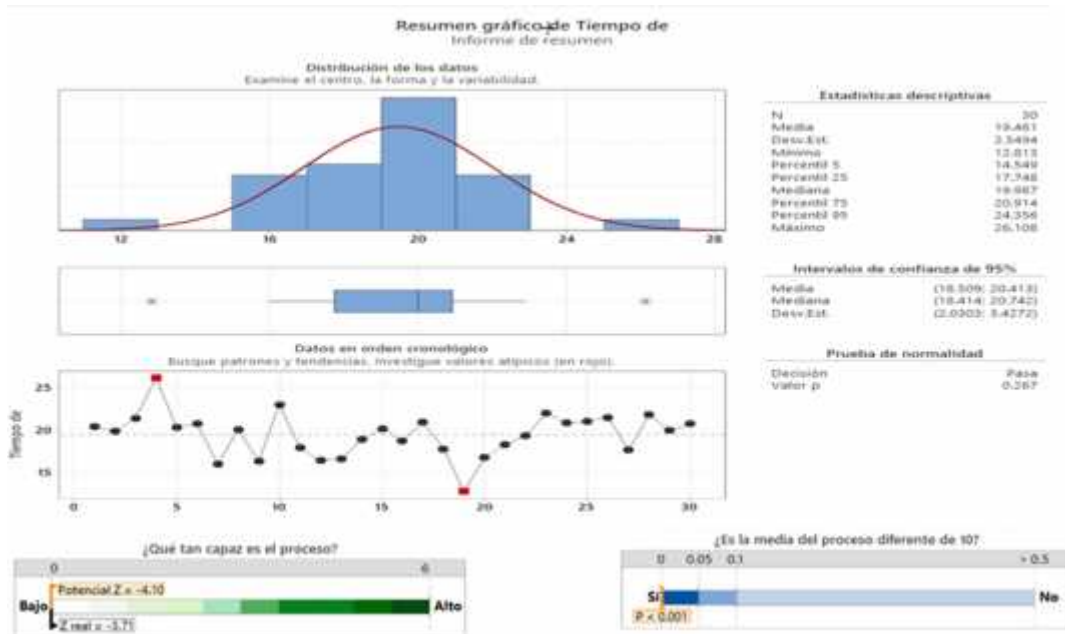


Ilustración 2: Muestras de datos antes del proyecto.

Fuente: Recursos propios

Luego de culminar el proyecto, se volvió a repetir el mismo proceso de recolección de otras 30 muestras del 9 de noviembre 2022 al 8 de diciembre 2022, para comparar la capacidad, en donde se concluyó que el proceso ahora si es capaz de estar en el objetivo de 10 horas y dentro de límite superior de especificación, resultados que se muestran en la imagen siguiente.

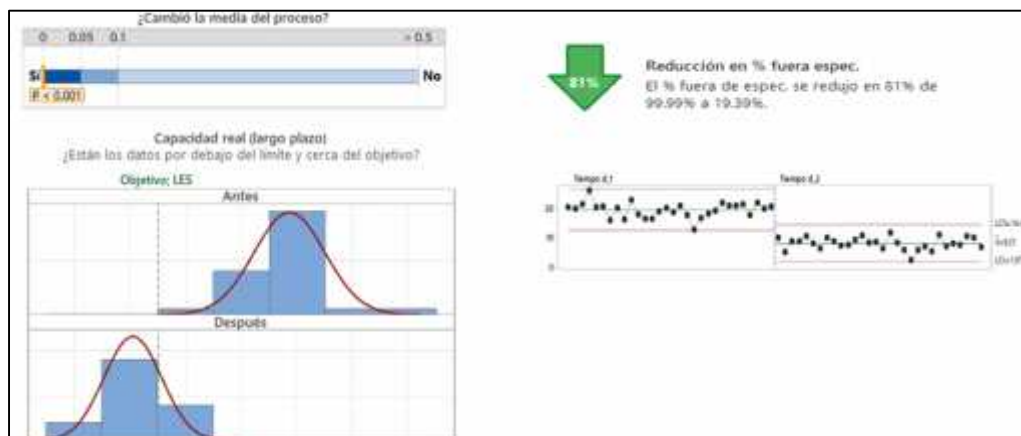


Ilustración 3: Muestras de datos después del proyecto.

Fuente: Recursos propios

VII. Diseño metodológico

Ubicación de estudio:

La ubicación del sistema red del proyecto estará dirigido al municipio de Managua.

Área de estudio:

Sistemas de Redes en Telecomunicaciones.

Tipo de investigación: Estratégica

La utilización de una investigación estratégica es comprender y predecir los patrones de comportamiento dentro de los sectores productivos, lo cual es imprescindible para el desarrollo e innovación tecnológica.

Cómo ciertas condiciones pueden afectar los procesos y resultados, permitiendo así diseñar o perfeccionar la tecnología para maximizar su eficacia y eficiencia. El objetivo primordial de esta metodología es proporcionar un marco que oriente el desarrollo tecnológico de manera que sea capaz de responder adecuadamente a las necesidades y desafíos de la industria.

Por otro lado, la base teórica obtenida de fuentes variadas y confiables como publicaciones académicas, expertos en la materia y recursos en línea, constituye un pilar crucial para el éxito de la implementación tecnológica, en este caso, de un sistema de red.

Esta sólida formación teórica posibilita no solo identificar falencias y errores potenciales que podrían impactar a los usuarios finales, sino también anticipar soluciones prácticas, lo que resulta en un proceso de implementación más informado y efectivo.

La teoría, en este contexto, se convierte en la herramienta que guía la práctica, asegurando que los resultados sean robustos, confiables y satisfagan las expectativas de los usuarios.

Estrategia de investigación

En la implementación se tomará como estrategia una serie de preguntas cualitativa para poder assimilar las necesidades principales de los clientes e investigación de sus procesos de gestión para poder encontrar una manera de ampliar la disponibilidad y automatización de algunos procesos que se presenta diariamente, se usará los siguientes parámetros:

1. **Identificación de requerimientos:** se llevará a cabo una reunión con los responsables de las distintas áreas de la organización, con el fin de identificar sus necesidades y requerimientos en cuanto al uso de tecnologías de la información y comunicación.
2. **Análisis de la infraestructura actual:** se realizará un diagnóstico de la infraestructura actual de la organización, con el fin de determinar si es necesario hacer ajustes o mejoras a la misma, para asegurar la compatibilidad con los nuevos sistemas que se implementarán.
3. **Diseño de la red:** se definirán los requerimientos de la red LAN que se implementará, teniendo en cuenta el tamaño de la organización, la cantidad de usuarios y la cantidad de dispositivos que se conectarán a la red. Se definirán también las políticas de seguridad y se según estándares para garantizar la integridad y confidencialidad de la información.
4. **Selección de servidores y software:** se elegirán los servidores que se utilizarán para la implementación de los sistemas de información, así como el software que se instalará en ellos.

5. **Virtualización de servidores:** se procederá a la virtualización de los servidores, utilizando software especializado para ello, con el fin de maximizar el uso de los recursos y optimizar el rendimiento de la red.

6. **Configuración de los sistemas:** se procederá a la instalación y configuración de los sistemas de información que se utilizarán en la organización, como el sistema de gestión de inventarios, el sistema de gestión de clientes, el sistema de facturación, entre otros.

7. **Pruebas y ajustes:** se realizarán pruebas exhaustivas de los sistemas implementados, con el fin de detectar posibles problemas y hacer los ajustes necesarios para garantizar el correcto funcionamiento.

8. **Capacitación de usuarios:** se brindará capacitación a los usuarios de la organización, con el fin de que puedan utilizar correctamente los sistemas de información implementados y maximizar su uso.

9. **Mantenimiento y soporte:** se establecerá un plan de mantenimiento y soporte para los sistemas de información, con el fin de asegurar su correcto funcionamiento a lo largo del tiempo.

Con la implementación de este plan de trabajo, se espera lograr una mejora significativa en la administración y control de la información en la organización "Suministro farmacéuticos", lo que permitirá mejorar la eficiencia y productividad de la misma, así como una mayor satisfacción de sus clientes y usuarios.

Análisis Causa – Raíz

En este diagrama en la ilustración 4 se muestra el resultado de definición e identificación de Causa Raíz, que se llevó a cabo en conjunto con los líderes del departamento de operaciones de la compañía y el departamento de Informática, donde se identificaron los requerimientos. Ver figura de abajo.

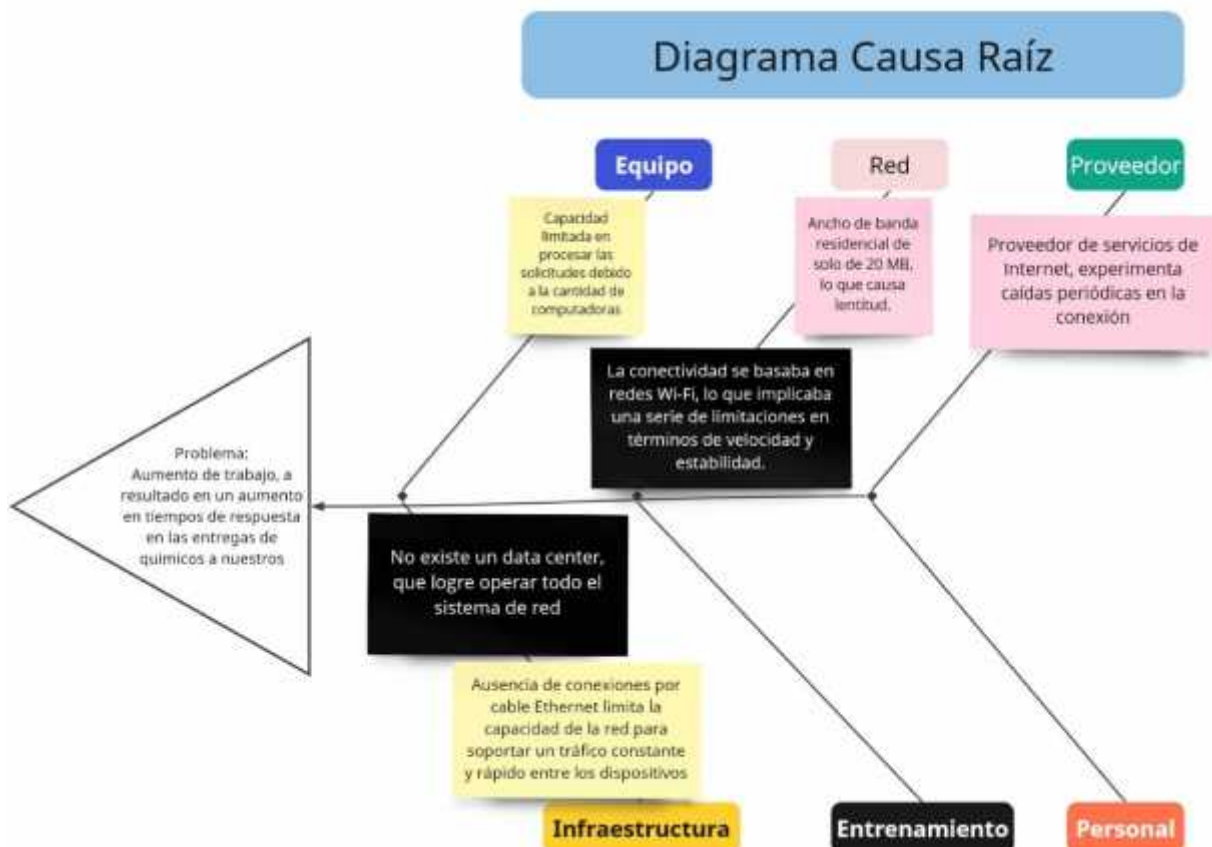


Ilustración 4: Diagrama Causa Raíz

Fuente: Recursos propios

Es importante mencionar que solo se tomaron en cuenta las causa-raíces que provenían del área de informática y que además se llevó a cabo durante la etapa de descubrimiento y en conjunto con la recolección de datos para reafirmar las necesidades de la empresa.

Alcance Del Proyecto

Se pretende implementar una estructuración de red LAN estándar para la mejora de tiempos de respuesta de ejecución de un proceso, asegurando la información de los usuarios, que esta puede ser utilizada de manera fácil y rápida mediante la disponibilidad y privacidad.

En el cumplimiento de objetivos se necesitarán servicios y herramientas que se brindará a través de esta infraestructura, siendo está regida por estándares de flexibilidad y escalamiento a las necesidades de la organización estos con el fin de solucionar dichos problemas o gestionar más rápido tramites internos.

Los servidores virtualizados brindaran alojamiento y servicios seguros bajo normas de gestión y control mejorando los recursos físicos disponibles, evitando errores y tiempos ocioso de los servicios por parte del servidor. El hardware y software tendrán recursos eficientes al ser virtualizado ayudando en el consumo energético y fácil de administrar, siendo punto puntual en el alcance del proyecto.

El sistema de red determinara el uso del tráfico de banda ancha y privacidad de la red evitando proveer o acceder información indebida o cualquier otro dato que perjudique a la organización y/o usuarios.

Tomaremos las medidas adecuadas para garantizar la confidencialidad de nuestros servicios e información de la organización, utilizaremos firewalls, antivirus, control de acceso y sistemas de respaldo para salvaguardar toda exigencia, información o necesidad de nuestros usuarios protegiendo su identidad.

Requerimientos de la organización

La organización identificó por medio de una serie de reuniones mejoras sobre red LAN de la empresa. Se plantearon peticiones para aumentar la velocidad y estabilidad de la conexión, así como para fortalecer la seguridad de los datos. Además, se discutieron propuestas para optimizar la distribución del ancho de banda y mejorar la accesibilidad de los recursos compartidos. Se destacó la importancia de implementar medidas proactivas para detectar y resolver problemas de red de manera eficiente, con el objetivo de garantizar un rendimiento óptimo en todas las operaciones internas.

Una forma de mejorar la red LAN existente era retomando la mejor parte de la misma, sin embargo, la red que estaba funcionando en las instalaciones no se podía reutilizar ya que la misma carecía de elementos claves y de muchas vulnerabilidades y se optó por reconstruirla bajo los siguientes requerimientos.

1. Mejora en el ancho de banda.
2. Conexiones física de cable de red ethernet en puntos de acceso.
3. Administración de equipos de cómputo y usuario.
4. Instalación de servidores de gestión de archivos y respaldo.
5. Optimización de recursos informáticos hardware y software (virtualización).
6. Seguridad, disponibilidad y política en la red.

Limitación de recursos a terceros

Se limitará la infraestructura al uso de servicios necesarios locales, sin embargo, para el uso de ciertas tecnologías no se podría cubrir sin el soporte de proveedores especializado que brindan estas soluciones que para una red LAN estándar sobrepasa los requerimientos y recursos a utilizar.

Para determinar un servicio a tercerizado es necesario comprender que ante un bien común se garantiza la solución por medio de un costo/beneficios, tales como correo, antivirus, y una seguridad avanzada con licenciamiento.

La estructuración de red empezará a proveer nuevos servicios a clientes como lo son consultas en línea con médicos de turno y números de teléfonos a doctores privados estos sistemas no forman parte de la red estándar, pero son un recurso disponible sin embargo solo se mencionarán los recursos de tercero que se ejecutan dentro de la red y se administran por parte del área correspondiente.

Presupuesto del proyecto

El presupuesto de inversión que generará la empresa para implementar el proyecto será de 20.000 mil dólares previendo los gastos por instalación, mantenimiento, compras, teniendo esta cifra como un estimado inicial tomando en cuenta que luego que la empresa exprese su objetivo y las ganancias del servicios suban su valor, esta aumentará tanto el número de compras como ofrecer otros servicios a las necesidades.

En dicho presupuesto entra las compras materiales, tanto como la mano de obra y el mantenimiento para la instalación de dicha, al no poseer un capital alto nos ajustamos a él para poder emprender nuestra compañía, un estimado en los materiales adquiridos está a continuación.

Los servicios de contratación para la empresa de pago mensuales no están reflejados como en las compras ya que estos no son adquisiciones directas de la misma incluyendo también el alquiler de equipos de protecciones a la red.

VIII. Desarrollo del proyecto

Infraestructura de red

El proceso de establecer una infraestructura de red adecuada, se basa en selección de los materiales y componentes, considerando atentamente por los estándares, como sus características individuales. Esta elección ha sido determinante para respaldar el levantamiento de la infraestructura de red, asegurando su estabilidad y rendimiento

Esta elección de los dispositivos se basó en diversos factores, que abarcan desde la capacidad para gestionar la carga de tráfico esperada, la durabilidad a largo plazo y la compatibilidad con las tecnologías de red actuales y futuras. Se otorgó prioridad a la elección de cables de alta calidad, los cuales cuentan con eficientes capacidades de transmisión y aislamiento adecuado, con el objetivo de minimizar las posibles interferencias.

Además, los elementos cruciales de la red, como enrutadores, conmutadores y puntos de acceso, se seleccionaron en función de su habilidad para manejar de manera eficaz la cantidad de dispositivos conectados y así garantizar una comunicación fluida y segura. No menos importantes, la redundancia y la escalabilidad se convirtieron esenciales, lo que asegura que la infraestructura esté preparada para futuras expansiones sin comprometer su estabilidad.

En última instancia, esta selección cuidadosamente elaborada de materiales establece nuevos inicios para una infraestructura de red fiable y de alto rendimiento, lo cual es esencial para abordar las cambiantes demandas de conectividad en constante evolución.

Selección de material y dispositivos

1. Cable de conexión de puntos de acceso Cat6

El cable Cat6, también conocido como Categoría 6, es una elección debido al estándar IEEE 802.3 que indica que para gigabit ethernet sobre cobre se requiere al menos cable Cat5e. el cable utp cat 6 no solo ofrece una mayor capacidad de transmisión de datos y una reducción significativa en la interferencia, sino que también garantiza una conexión más estable y confiable la selección puede resultar ventajosa a largo plazo, especialmente para entornos que requieren altas velocidades de transferencia de datos y un rendimiento constante.

Ficha técnica del cable Cat6

Velocidad de transmisión: Hasta 10 Gbps (Gigabits por segundo).

Frecuencia: Hasta 250 MHz.

Tipo de cable: Par trenzado blindado (STP) o no blindado (UTP).

Conectores: Conectores RJ-45 en ambos extremos.

Distancia máxima de transmisión: Aproximadamente 100 metros.

Mejora en la calidad: Mayor cancelación de eco y reducción de diafonía.

Aplicaciones: Ideal para redes Ethernet Gigabit, VoIP, videoconferencias y transferencia de datos de alta velocidad

2. Determinación de Servidores

La elección de utilizar un servidor para alojar servicios en red se basa en las ventajas significativas que brinda en términos de rendimiento, seguridad y gestión.

Los servidores están especialmente diseñados para manejar eficientemente cargas de trabajo intensivas, proporcionando recursos dedicados para servicios críticos como sistemas, bases de datos y almacenamiento en red.

Para tomar una decisión informada sobre la elección de un servidor, fue necesario evaluar la proyección de la carga de trabajo, lo que implica retomar el análisis anterior, para determinar los recursos requeridos en términos de procesamiento, memoria y almacenamiento para asegurar un rendimiento óptimo.

La escalabilidad se convierte en un factor crítico, ya que el servidor debe ser capaz de expandirse de manera efectiva para atender el crecimiento futuro de la empresa. Asimismo, las opciones de redundancia y tolerancia a fallos desempeñan un papel vital, garantizando la continuidad del negocio incluso en situaciones imprevistas.

El servidor Dell PowerEdge R430 se solicitó por sus características y costos de inversión para la virtualización de máquinas gracias a su ficha técnica sólida y capacidades destacadas. Con el procesador Intel Xeon E5-2600 v4, el R430 brinda un rendimiento óptimo entre potencia y eficiencia. Con una capacidad que llega a los 384 GB de memoria RAM DDR4, proporciona un amplio espacio para ejecutar múltiples máquinas virtuales simultáneamente, sin comprometer el rendimiento en ningún momento.

El servidor R430 garantiza una administración de almacenamiento eficiente con ocho unidades de disco duro de 2,5 pulgadas o cuatro unidades de disco duro de 3,5 pulgadas.

Esta característica permite la creación de una infraestructura de almacenamiento versátil y adaptable a las necesidades cambiantes de la virtualización. Su diseño compacto y altamente escalable también lo convierte en una solución ideal para entornos con restricciones de espacio físico.

Ficha Técnica – Servidor Dell:

Procesador: Procesadores Intel Xeon E5-2600 v4 (hasta dos procesadores).

Memoria: Hasta 384 GB de memoria RAM DDR4.

Almacenamiento: Compatibilidad con hasta ocho unidades de disco duro de 2,5 pulgadas o cuatro unidades de disco duro de 3,5 pulgadas.

Conectividad: Opciones de red flexibles, incluyendo Ethernet 1 GbE y 10 GbE.

Dimensiones: Chasis compacto y escalable.

Gestión: Herramientas de administración remota Dell iDRAC para una gestión sencilla y eficiente.

Servidor HP ProLiant ML150

También se tomó la decisión de implementar un servidor HP ProLiant ML150 como servidor de archivos de datos. Esta elección se basó en la robustez y las capacidades específicas del servidor para manejar eficientemente el almacenamiento y el acceso a datos críticos. Equipado con características avanzadas, el HP ProLiant ML150 se posiciona como una solución confiable para la gestión de archivos en la empresa.

Ficha Técnica – Servidor ProLiant:

Procesador: Procesador Intel Xeon Escalable.

Memoria: Hasta 1.5 TB de memoria RAM DDR4.

Almacenamiento interno: Opciones de unidades de disco duro y unidades de estado sólido (SSD).

Conectividad: Múltiples puertos de red para conectividad Ethernet.

Capacidad de almacenamiento: Escalabilidad para adaptarse a necesidades de almacenamiento en crecimiento.

Redundancia: Opciones de fuentes de alimentación redundantes.

Elección de Router y firewall

La elección del enrutador en la gestión de la red empresarial es esencial para un funcionamiento eficiente y seguro. Este dispositivo, como centro de dirección del tráfico, debe ser seleccionado cuidadosamente. Aspectos cruciales incluyen capacidad de procesamiento y velocidad, medidas de seguridad como cortafuegos y VPN, así como administración remota y actualizaciones frecuentes. La escalabilidad y la implementación de Quality of Service (QoS) también son fundamentales para garantizar rendimiento y priorización de tráfico.

Un modelo comúnmente considerado, el FortiGate 30E, ejemplifica esta elección. Con su procesador de alto rendimiento y capacidad de inspección profunda de paquetes, ofrece una protección eficaz contra amenazas avanzadas. Su capacidad de VPN, escalabilidad y opciones de administración remota también influyeron en la decisión.

Ficha técnica - FortiGate 30E:

Procesador: System-on-a-Chip (SoC) específico para seguridad.

Rendimiento del firewall: Hasta 950 Mbps.

Rendimiento de IPS: Hasta 300 Mbps.

VPN: Hasta 200 Mbps.

Interfaces: 5 puertos GbE RJ45.

Alimentación a través de Ethernet (PoE): No disponible.

Dimensiones: 20.8 cm x 16.8 cm x 3.7 cm.

Selección de Switch y Patch panel

Switch, permite una distribución inteligente de datos entre los dispositivos conectados, mejorando la velocidad y reduciendo la congestión en comparación con los concentradores.

Esto resulta en una comunicación más rápida y confiable entre los equipos, lo que a su vez mejora la productividad y la colaboración. Estos se utilizan para una mayor ampliación en los puntos de acceso y conexiones interna a la red de la empresa.

En el proceso de selección de un switch adecuado, es fundamental considerar ciertos parámetros esenciales. La capacidad de puertos del switch debe ser suficiente para cubrir las necesidades presentes y futuras de la red. Además, el rendimiento de transferencia es un aspecto crítico, asegurando que los datos fluyan sin problemas incluso en momentos de alta demanda. Las características de administración, como la capacidad de VLAN y QoS, permiten una gestión eficiente del tráfico y la priorización de ciertos tipos de datos y sobre la seguridad en la conexión como habilitar o deshabilitar puertos específicos.

El dispositivo seleccionado, el Catalyst 2960S, se escogió debido a su reconocida marca en el ámbito de redes y su relación calidad-precio destacada. Cisco, el fabricante, es conocido por su excelencia en productos de redes. Además, el Catalyst 2960S ofrece una combinación sólida de características, lo que lo convierte en una opción eficiente y confiable para nuestra infraestructura.

Ficha técnica del Cisco Catalyst 2960S:

Capacidad de conmutación: Hasta 176 Gbps.

Número de puertos Ethernet: 24 puertos Gigabit Ethernet.

PoE: Opción de PoE para alimentación de dispositivos.

Características de administración: Soporte para gestión remota y seguridad avanzada.

Tamaño: Factor de forma compacto y montable en rack.

Calidad de Servicio (QoS): Priorización de tráfico para un rendimiento óptimo.

Patch panel

Un patch panel que cumple con la característica de Cat6 y ofrece 48 puertos es esencial para garantizar una conexión de red eficiente y de alta velocidad. El estándar Cat6 asegura una transmisión de datos confiable y de alto rendimiento, crucial para mantener la integridad de las tecnologías empleadas. Contar con 48 puertos en el patch panel permite una correspondencia perfecta con los 48 puertos del switch, para una organización ordenada y facilitando la expansión futura de la red. En conjunto, estas características aseguran una conectividad sólida y sin problemas en la infraestructura de red de la empresa.

Respaldo de Energía

Es necesario contar con un respaldo de energía en los servidores es esencial para garantizar la continuidad y disponibilidad de los servicios críticos de la organización. Los servidores almacenan y gestionan datos y aplicaciones fundamentales para las operaciones diarias.

Un corte de energía súbito puede resultar en la interrupción de estos servicios, lo que podría generar pérdida de datos, tiempo de inactividad costoso y daño a la reputación de la empresa.

Un sistema de respaldo de energía, como UPS (Sistema de Alimentación Ininterrumpida) o generadores, entra en acción durante fallos de energía, proporcionando una fuente temporal de electricidad.

Esto permite a los servidores apagarse adecuadamente y mantener la integridad de los datos. Además, el respaldo de energía evita la pérdida de productividad y ayuda a mantener la confianza de los clientes al asegurar que los servicios estén disponibles en todo momento.

Se ha decidido seleccionar una batería SRT3000RMXLA-NC marca APC, con una capacidad de 3000 VA y 120 V, diseñada para montarse en un rack. Esta elección se fundamenta en sus características destacadas que la hacen idónea para asegurar la continuidad de energía en los servidores.

Ficha técnica - SRT3000RMXLA-NC

Capacidad de Potencia: 3000 VA (vatios-amperios) con una potencia nominal de 2700W

Voltaje de Entrada y Salida: Funciona con un voltaje de entrada y salida de 120 V,

Conectividad: Entrada NEMA L5-30P y 8 salidas NEMA 5-20R junto con 1 salida NEMA L5-30R, permitiendo la conexión de múltiples dispositivos.

Duración de Batería y Recarga: Tiempo típico de recarga de 3 horas y vida de batería de 3 a 5 años, asegurando una fuente confiable de energía en caso de cortes.

Tiempo de Descarga de Batería: 1 hora bajo potencia de entrega máxima

Topología y Forma de Onda: Topología de doble conversión en línea y forma de onda senoidal,

Base Rack

Una base de rack proporciona un entorno seguro y organizado para montar equipos, dispositivos y componentes, contribuyendo a la eficiencia operativa y la gestión efectiva de los sistemas tecnológicos. Algunos puntos clave a considerar son:

Orden y Organización: permite colocar los equipos de manera ordenada y estructurada, lo que facilita la administración y el mantenimiento. Los cables y conexiones también pueden gestionarse de manera más efectiva.

Optimización del Espacio

La base de rack utiliza el espacio vertical en lugar del espacio horizontal, lo que ayuda a aprovechar al máximo la superficie disponible en un centro de datos o espacio de trabajo

Ventilación y Refrigeración

Las bases de rack están diseñadas con espacios abiertos entre los equipos, lo que permite una mejor circulación del aire y una adecuada refrigeración. Esto ayuda a prevenir el sobrecalentamiento y asegura un rendimiento estable y duradero de los dispositivos.

Acceso y Mantenimiento

Permiten un acceso más fácil a los equipos para tareas de mantenimiento y resolución de problemas. Esto reduce el tiempo de inactividad en caso de problemas y facilita la instalación de nuevos componentes

Escalabilidad

Las bases de rack son altamente escalables, lo que significa que pueden adaptarse a las necesidades cambiantes de la empresa. Nuevos equipos y dispositivos pueden ser fácilmente añadidos o reemplazados sin afectar la disposición general.

La elección de una base de rack de 4 postes abierta estándar se basa en su practicidad y versatilidad ya que toda la estructura convergerá en una habitación de 3 metros de largo por 3.5 metros de ancho y 3 metros de profundidad. Su diseño abierto permite un buen acceso a los equipos desde ambos lados contribuyendo a la eficiencia operativa.

Elección de proveedor de Internet

En un análisis rápido de diferentes proveedores de internet serios para empresas se escogió como proveedor 'Equipos y Sistemas' como nuestro proveedor de internet debido a su reputación de confiabilidad y atención a la cliente práctica, lo que garantiza una experiencia de conexión fluida y además de brindar el costo beneficio más rentable.

Ubiquiti – AP

Para la distribución de señal WiFi en la empresa se escogió el UAP-AC-LITE para proporcionar una cobertura WiFi de alta calidad y estable. Con su diseño compacto y transmisión de datos, el UAP-AC-LITE se adaptó perfectamente a nuestras necesidades de conectividad, brindando una experiencia fluida a nuestros usuarios en todo el edificio.

Ficha Técnica del UAP-AC-LITE:

Modelo: UAP-AC-LITE

Estándar WiFi: 802.11ac

Velocidad máxima de datos: 867 Mbps en la banda de 5 GHz y 300 Mbps en la banda de 2.4 GHz.

Antenas: 2x2 MIMO (Multiple Input Multiple Output)

Rango de cobertura: Hasta 122 metros (400 pies)

Puertos Ethernet: 1 puerto Ethernet 10/100/1000 Mbps

Alimentación: PoE (Power over Ethernet) 24V

Administración: Compatible con UniFi Controller para una gestión centralizada y sencilla.

Dimensiones: 160 x 160 x 31.45 mm (6.3 x 6.3 x 1.24 pulgadas)

Peso: 170 g (6 oz)

Montaje: Montaje en techo o pared

Toma Eléctrico para rack

Conexiones eléctricas

En las conexiones eléctricas necesarias de los dispositivos como, switch, ap, router, etc. se escogió comprar una extensión para rack de 8 tomas, que iría directamente conectado de las baterías de respaldo de los servidores hasta los dispositivos para su conexión de 110v bajo los estándares de tomas especiales de la ANSI/EIA/TIA-942.

IX. Despliegue físico de la red LAN

Selección de ubicación de la infraestructura

La selección de esta ubicación específica para el centro de datos se basa en varios criterios estratégicos y de seguridad. Primero, la ubicación se encuentra dentro de las instalaciones de la empresa en un área visible y fácil el acceso al personal de TI y reduce los tiempos de respuesta en caso de problemas o mantenimiento. Además, al concentrar todos los componentes de la red en un solo lugar, se simplifica la administración y el monitoreo de la infraestructura. La decisión de ubicar el centro de datos en el área mostrada en la ilustración, se debe a su seguridad física, ya que se encuentra en una zona protegida y controlada, lo que reduce el riesgo de intrusiones no autorizadas.

La habitación designada para el centro de datos está dimensionada para proporcionar un espacio adecuado para los equipos y la infraestructura necesarios. Con medidas de 3 metros de ancho, 3.5 metros de largo y 3 metros de altura, ofrece suficiente espacio para la instalación de racks, servidores y otros dispositivos de red. El acceso a la habitación se realiza a través de una entrada principal asegurada con llave y sin ventana esta habitación también cuenta con una climatización propia, ubicada en la parte superior de una de la pared lateral izquierda, posteriormente se observó que hace una modificación en la parte superior del cielo Razo para gestión del cableado con una abertura de dimensiones de 100 cm de ancho y 60 cm de largo, garantiza un acceso conveniente y seguro al centro de datos. Ver Ilustración 5.



Ilustración 5: Vista aérea del edificio farmacéutico

Fuente: Recursos propios

Instalación de cableado estructural

La implementación de la infraestructura de cableado para red LAN establecido bajo los estándares de TIA/EIA para asegurar la calidad y el rendimiento de la red. Los detalles de la instalación son los siguientes:

La ubicación del datacenter en el edificio corporativo se definió estratégicamente para permitir un acceso eficiente a los puntos de red distribuidos a través de las distintas áreas. Desde esta ubicación central, se desplegaron un total de 1,582 metros de cableado Categoría 6 para la conexión de todos los puntos de acceso, estos puntos fueron determinado por cada una de la ubicación de los usuarios. El cableado UTP recorre encima del cielo raso que pasa por todo el edificio y se distribuye hacia las diferentes áreas mediante el descenso por canaletas de color blanco en conexión con cajas plexo 2 por 4, garantizando así una integración estética y funcional con la infraestructura del edificio

Las áreas que se beneficiaron de esta implementación incluyen la recepción con 1 punto de acceso, contabilidad con 9 puntos, operaciones con 9 puntos, atención al cliente con 11 puntos, el área legal con 3 puntos y ventas con 3 puntos, sumando un total de 36 puntos de acceso conectados por jack hembras (ANSI/TIA, 2017).

En el extremo correspondiente al datacenter, los cables fueron terminados en un patch panel, donde se utilizó el estándar de cableado por color T568B para las terminaciones en ambos extremos, cumpliendo con los requisitos de categoría 6. Posteriormente, se realizaron las conexiones entre el patch panel y cada puerto del switch a través de patch cords de categoría 6 para mantener la coherencia y asegurar el rendimiento óptimo de la red (ANSI/TIA, 2017).

En la siguiente ilustración se podrá apreciar la infraestructura del cable por medio de líneas azules indicación numérica de cada uno de los puntos de conexión. Ver figura de abajo.

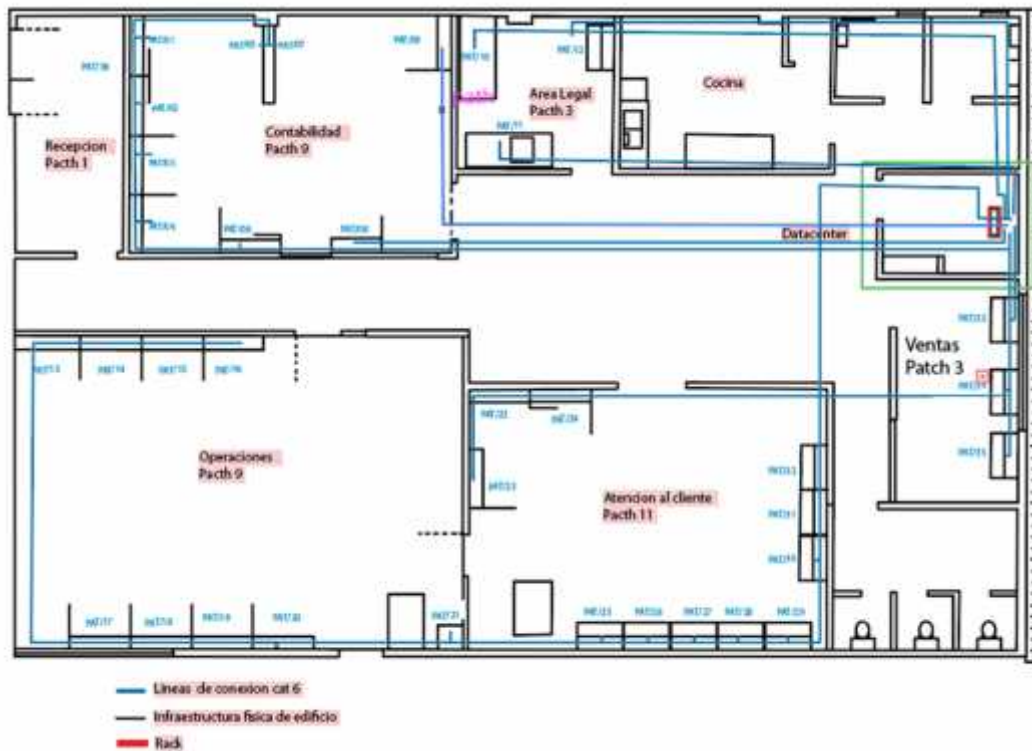


Ilustración 6: Estructura de cableado

Fuente: Recursos propios

Ensamblaje y Armado de RACK

Para la instalación del rack fue necesario ensamblar y atornillar cada una de su parte individuales, como se puede observar en la imagen, solo es la unión de diferente parte específica en medida, sujetadas por tornillos. Ver figura de abajo.

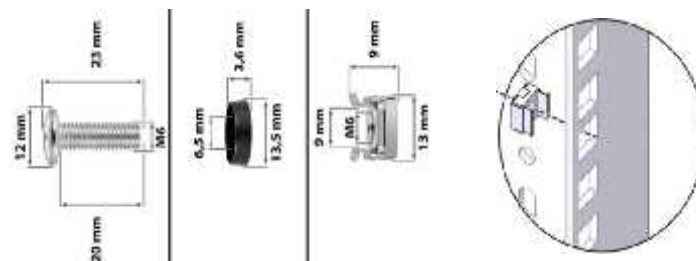


Ilustración 7: Medidas de Rack

Referencia de la imagen: Guía de instalación de carriles
https://docs.oracle.com/cd/E65081_01/html/E65041/gnmnx.html#scrollto

c

La imagen de la ilustración abajo se muestra de manera gráfica y detallada el armado completo del rack, un componente esencial en la configuración de un data center. Para asegurar la estabilidad y la seguridad del rack, es imprescindible fijarlo al suelo de manera adecuada. Ver figura de abajo.

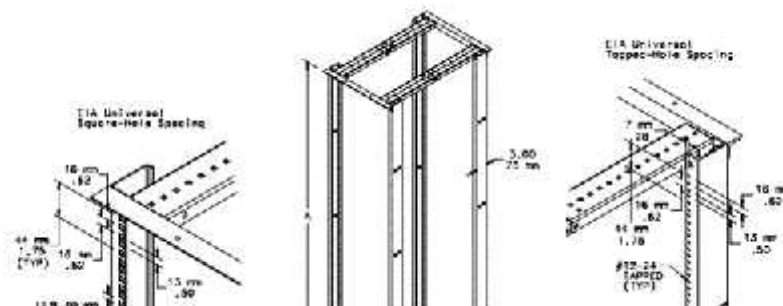


Ilustración 8: Ensamblado de Rack

Según: 4Post Open Frame, Autor: nvent Hoffman (Pag.2)

Para lograr esto de manera efectiva, se recomienda el uso de pernos de suelo especialmente diseñados para esta tarea. Estos pernos, fabricados con materiales robustos como acero galvanizado, presentan una combinación única de resistencia a la corrosión y durabilidad.

En la parte superior del Datacenter, en el cielo se realizó una abertura de 60 centímetros de largo y 50 de ancho, donde se conecta la pared trasera junto con el centro de ambas paredes laterales, esta abertura se realizó para la poder introducir el cable cat6 desde el data center a los diferente puntos conexión distribuido en todo el edificio dando un total de 26 cables.

Instalación de patch panel y organizador

La instalación de un patch panel en un rack es para asegurar la organización efectiva de la infraestructura de red. se eligió en la más alta posición de 45 y 44 U ya ocupa 2 espacios, generalmente para medir las posiciones en un rack están basada en unidades de (U) que corresponde a 1.75 pulgadas, el rack instalado en el datacenter tiene en la parte inferior de 1U hasta 45U, cada U tiene ubicaciones para tornillo y fijación de componentes. Ver figura de abajo.

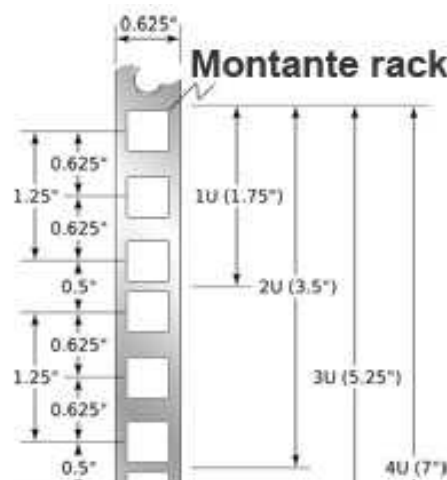


Ilustración 9: Medidas del Rack

Referencia de la imagen: Según: 4Post Open Frame, Autor: nvent Hoffman (Pag.2)

El patch panel se colocó en esa posición, alineando sus orificios de montaje con los del rack., Con el panel en su lugar, se procede a conectar los cables en categoría B, desde la parte trasera del panel a los puertos numerados o etiquetados en la parte frontal.

La categoría T568A Y T568B, solo es un protocolo de ordenamiento basado en la posición y colores del en conexión del cable cat6 para su debida eficiencia en el momento de transmitir datos estos colores se encuentran indicados en la parte trasera del patch panel, así mismo como el recubrimiento de los hilos del cable de red. Ver Ilustración 10

T568A		T568B	
Blanco/Verde		Blanco/Naranja	
Verde		Naranja	
Blanco/Naranja		Blanco/Verde	
Azul		Azul	
Blanco/Azul		Blanco/Azul	
Naranja		Verde	
Blanco/Marrón		Blanco/Marrón	
Marrón		Marrón	

Ilustración 10: Categorías de colores

Según: <https://www.profesionalreview.com/2020/02/29/cable-rj45/>

Una vez realizadas las conexiones en la parte trasera de del patch panel, se organiza por medio de etiquetas cada punto de cable y se asegura la gestión de cables, utilizando abrazaderas y guías para evitar enredos. Este proceso de instalación del patch panel en el rack contribuye significativamente a mantener una infraestructura de red ordenada y eficiente. Ilustracion11

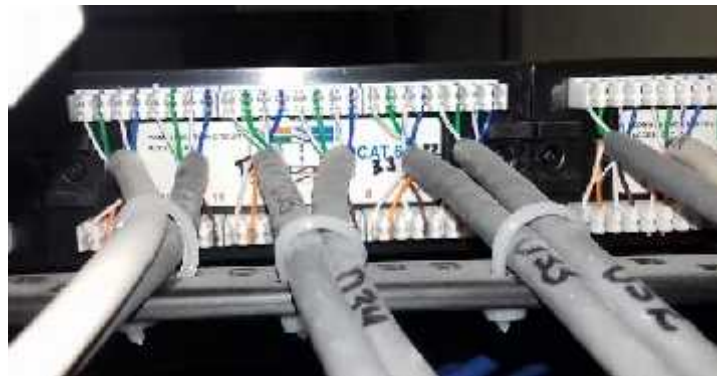


Ilustración 11: Instalación de cable de red en patch panel

Fuente: Recursos propios

En el otro extremo de la conexión del cable cat6 se encontrarán los distribuido en el acceso físico de conexión en la empresa, que estarán ubicada en una caja 2 x 2 plásticas previamente instalada por el equipo de contrición y diseño del edificio, esta contendrá 1 punto de acceso el cual se un Jack RJ45, para una futura conexión de un patch Cord. Ilustración 12 y 13.



Ilustración 12: Pasos de ponchado Jack RJ45

Fuente: Manual de Instalaciones de redes pag. 87



Ilustración 13: Puerto de red en oficinas

Fuente: Recursos propios

En la parte inferior del patch panel se coloca un organizador de cables para mantener la orden y evitar ocupar más cable de lo debido para las conexiones incluyendo la facilidad a acceso y futuras intervenciones físicas, el organizador se estableció en la posición 35U del rack.

Instalación de switch y conexión de patch cord

Para la instalación de switch cisco se escogió en la posición 34U debajo del organizador de cable, siguiendo el mismo procedimiento de colocar tornillos en patch panel es fijado en los dos postes -frontales del rack.

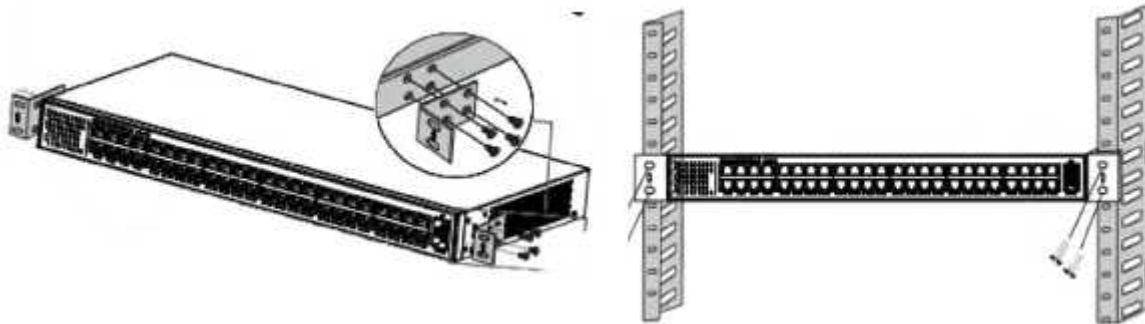


Ilustración 14: Instalación de Switch

Segun: Grand streams gwn7816 Managed Network Switch Installation Guide

Instalando previamente unas agarraderas de metal a ambos lados del switch para poder proceder a la colocación en el rack.

Se instalarán patch Cord de los puntos conectados en el patch panel que son los puertos 1 al 26 a los mismos números de puerto del switch, con una longitud de 25 cm máximo cada patch cord para dar movilidad interna si presentaría un caso necesario.

Una vez finalizado el proceso de conexión de los 26 patch cord, la alimentación del switch será proporcionada por la toma eléctrica del rack, con una instalación en la parte de atrás del rack en con una alineación en el lugar 33U. Ilustración 14.

Ilustración 15: Interfaces de conexión Switch y patch panel

Fuente: Recursos propio



Instalación de servidor Dell

Para la instalación del servidor Dell se necesitaron dos varas de soporte, que se sujetaran en cada uno de los postes en particular estas varas especiales ya vienen incluida con la compra del servidor y se conectan en cada uno de los postes sin la colocación de tornillos ya que estarán sujetado bajo presión en la posición 17U, ya que se necesitara cerca de los dispositivos de Respaldo de energía. Vista ilustración 16 y 17

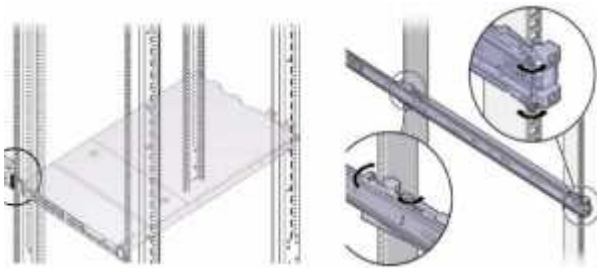


Ilustración 17: Instalación de rack de Servidor Dell

Fuente: Grand streams gwn7816 Managed Network oracle

Dell Installation Guide



Ilustración 16: Servidor Dell

Fuente: Recursos propios

Instalación de servidor HP Proliant y Bandeja

Para poder instalar un servidor de torre en este caso el servidor HP ProLiant ML150, es necesario instalar una bandeja donde pueda descansar el servidor, se escogió ponerlo en la posición 6U del rack.

En la parte superior de la bandeja el servidor Proliant ocupa una altura de 43,39 cm equivalente a 9U en distancia, considerando que el servidor dell está en la posición 17U y restando los 6U de partida quedan 11 U disponible de los cuales 9U son usador por la altura del servidor HP dando un espacio de 2U entre el servidor Dell y el servidor HP. Ver Ilustración 18



Ilustración 18: Servidor Proliant sobre bandeja

Fuente: Recursos Propios

Algunos dispositivos entregados por el proveedor de Internet o ISP, que son necesario la conexión a internet, instalando una segunda bandeja en debajo del switch en la posición 33U. Vista de instalación de servidor HP ProLiant y bandeja.

Instalación de Baterías y conexiones eléctricas

En la instalación de las baterías de respaldo es similar a la instalación del servidor Dell con las varillas de soporte para poder sostenerse en los 4 poste del rack, esta posee ranuras para la colocación de tornillos para rack, se colocaron en la posición 1U-2U, y la segunda batería en 3.5U- 5.1U, estableciendo un espacio de separación para ventilación y no provocar sobre calentamiento por contacto directo entre las baterías. Ver figura de abajo.



Ilustración 19: Instalación de Baterías de respaldo APS

Fuente: Recursos propios

Para las conexiones eléctricas a la energía comercial, se conectarán únicamente las baterías por medio de tomas especiales de enclavamiento NEMA L15-30R, aun que la corriente que soportan son 240v a 30A, se seleccionaron por su sistema protección anti- desconexión accidental, con una alimentación de 110v a 20A, cada toma está separado por un disyuntor electromagnético cada uno. Ver Ilustración 20 y 21



Ilustración 20: Vista toma eléctrico

Según: Ficha técnica nema L15-30R



Ilustración 21: Conexiones de baterías a la Fuente

Fuente: Recursos propios

Conexiones de baterías a la corriente eléctrica comercial

Las conexiones del puerto de alimentación de las baterías, estarán directamente conectada a los servidores, en la alimentación de los dispositivos como switch y dispositivos proporcionados por el proveedor de internet (ISP) por medio de la regleta anteriormente mencionada de 8 tomas de rack, que la alimentación de la misma será por las baterías logrando un total de 2.5 horas de respaldos entre las dos baterías, tiempo suficiente para guardar y proteger datos y evitar daño a los sistemas operativos instalados. Ver imagen de abajo.



Ilustración 22: Conexión de servidores en baterías

Fuente: Recursos propio

Topología física

El siguiente diagrama proporcionará una representación visual de la disposición instalada en la estructura del rack, lo que facilitará una comprensión más completa de la arquitectura de la red LAN en el data center. Este diagrama incluirá los elementos mencionados anteriormente, brindando una visión clara y detallada de cómo están distribuidos y conectados los componentes clave de la red. Ver imagen de abajo.

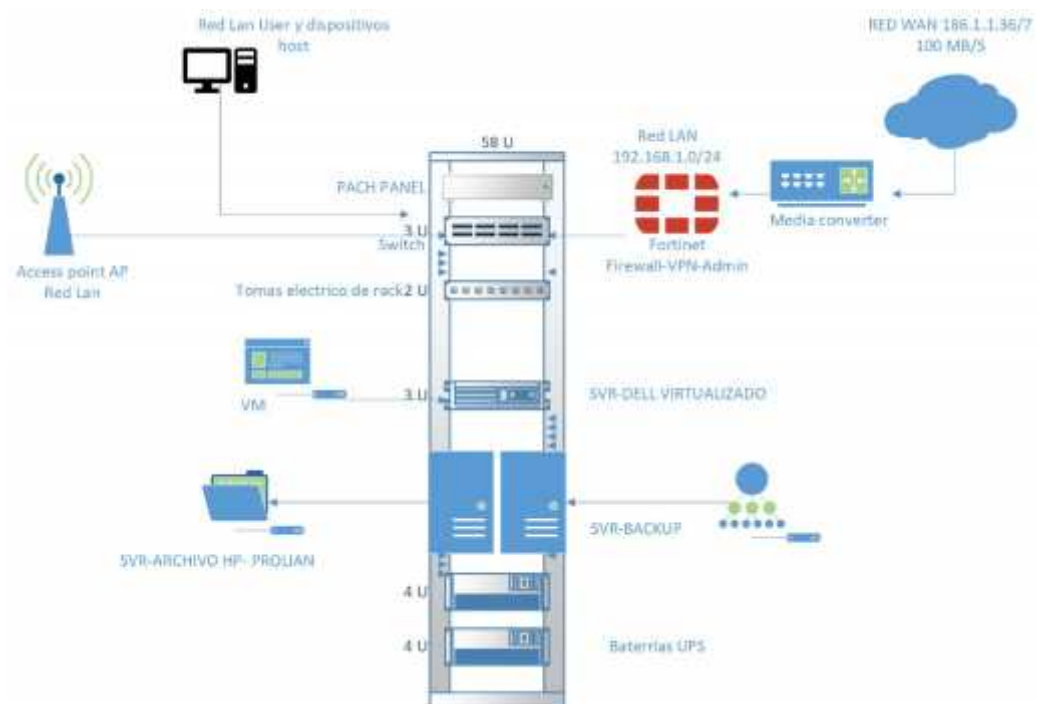


Ilustración 23: Topología física e la red LAN Estándar

Fuente: Recursos propio

Instalación y configuraciones de servicios y sistemas operativos

Configuración de Red

La implementación de seguridad en una red es fundamental para resguardar la integridad, confidencialidad y disponibilidad de la información y los sistemas. Con el aumento de amenazas cibernéticas, desde ataques de malware hasta intrusiones por personal externo o interno, la seguridad en la red se vuelve crucial para proteger los datos sensibles y garantizar el funcionamiento ininterrumpido de los servicios.

En la configuración inicial el proveedor ISP, ha hecho entrega una conexión de fibra óptica con una tasa de velocidad de 80 Mb/s incluyendo un dispositivo convertido de fibra a cable ethernet, llamado 'conversor' junto con el dispositivo de seguridad FortiGate 30E, que el dispositivo conversor estará conectado directamente al puerto WAN del FortiGate. Ver Ilustración 24.



Ilustración 24: Captura de pantalla de interfaz física de Fortinet

Fuente: Recursos propio

El FortiGate 30E será establecido como seguridad inicial ante la red por su característica de análisis de firewall y constantes actualizaciones de firmware (protección de hardware), por medio de análisis y monitoreo en la red y web, filtrando contenidos web, políticas en la red, administración de VPN (Redes Privadas Virtuales).

Estas políticas de seguridad y reglas contenidas en el Fortinet son necesarias configurarlas en el dispositivo sin embargo el fabricante ofrece algunas políticas sencillas por defecto. Configuraremos lo siguientes aspecto en el dispositivo:

- a. Servicio DHCP
- b. Servicio De Firewall
- c. Política De Seguridad Restringida
- d. Política De Seguridad Libre
- e. Configuración De VPN

Configuración de Servicio DHCP

Para la poder configurar estos servicios, conectaremos el cable de conexión que nos ha brindado el nuestro proveedor de internet en el puerto llamado WAN, posterior mente un cable de red de cualquier puerto del Fortinet a nuestra pc o laptop, por defecto la dirección 192.168.1.0/24 está establecida en el Fortinet nos colocaremos una dirección IP de este segmento y pondremos en el navegador la dirección 192.168.1.99, nos permitirá abrir en el navegador la interfaz gráfica del Fortinet. Ver Ilustración 25.

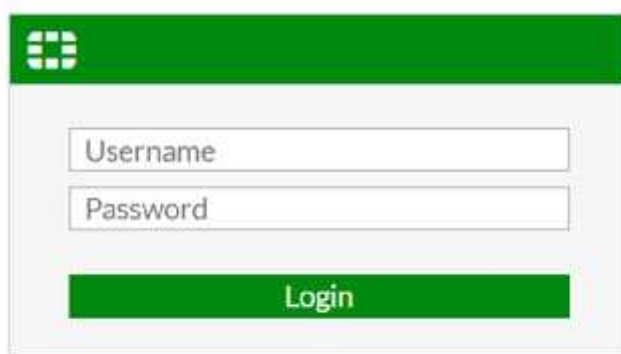


Ilustración 25: Login Inicial de Fortinet

Fuente: Recursos propio

Por defecto la primera vez las credenciales son admin y la contraseña la dejaremos en blanco y nos pedidera cambia la contraseña, Para habilitar el servicio de DHCP en el FortiGate se puede realizar desde la interfaz web en las opciones de **System > Network > Interface**. Ver Ilustración 26.



Ilustración 26: Selección de Interfaces Fortinet

Fuente: Recursos propio

Se crea una nueva regla de interfaz, donde rellenaremos los campos con los datos que utilizaremos, pero antes se configurara la interfaz física del puerto llamado WAN y ingresaremos la IP publica entregada de nuestro ISP.

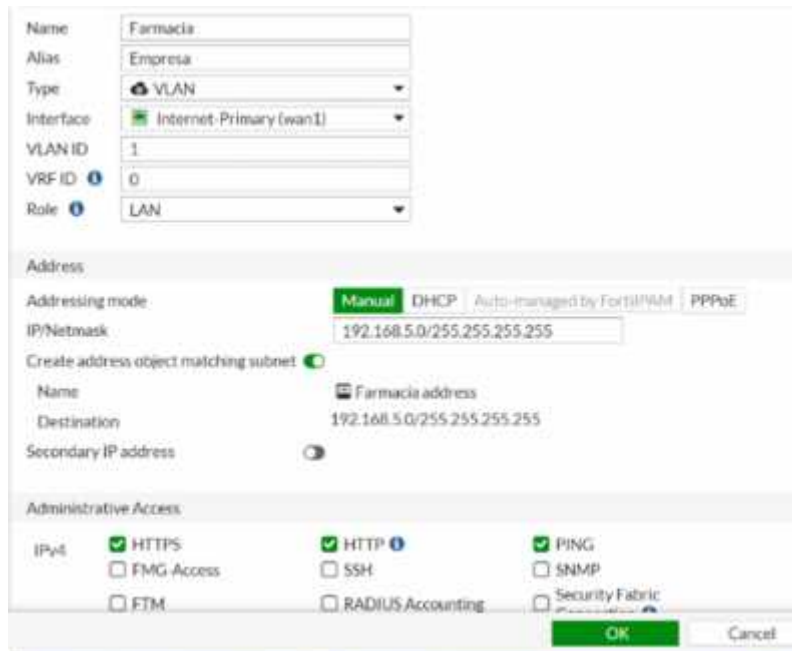


Ilustración 27: Configuración red LAN interna

Fuente: Recursos propio

En las opciones de este apartado estará la opción del DHCP server, una vez habilitada pedirá el rango de las direcciones IP, se puede asignar uno o a varios puertos de del Fortinet. Cabe de mencionar que el parámetro puesto en nuestro Fortinet son 192.168.0.1 como Gateway, en la red de 192.168.0.0/24 con 253 IP disponibles. Ver imagen de abajo.

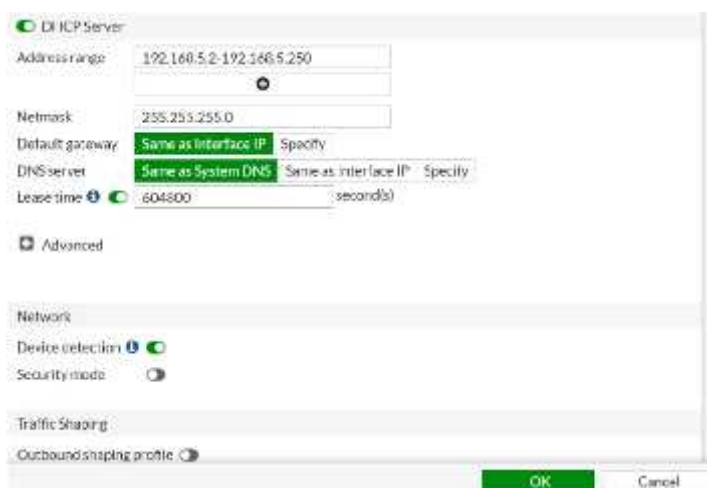


Ilustración 28 Configuración de DHCP

Fuente: Recursos propio

Configuración Firewall y Política de restringida

En el panel de control, se selecciona “Policy & Objects” desplegando una opción llamada “Firewall”. Las políticas de firewall estén habilitadas. Se puede configurar políticas de firewall para controlar el tráfico entrante y saliente según los requisitos de seguridad, en las opciones “Incoming Interface” se selecciona la red LAN que el firewall estaría analizando y protegiendo. Ver imagen de abajo.

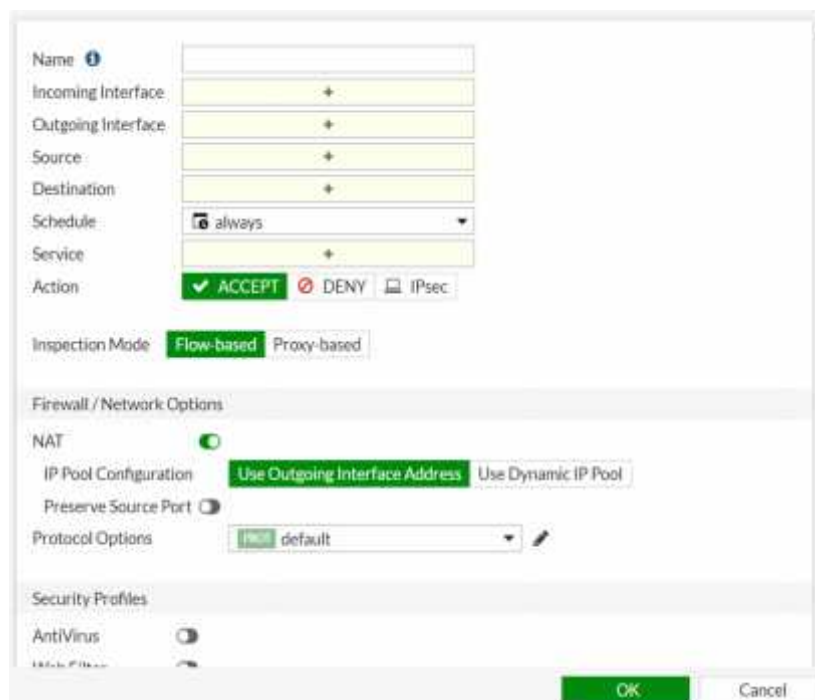


Ilustración 29 Configuración de parámetros de Política

Fuente: Recursos propio

Se selección en “source” la interfaz de ALL ya que se estaría obteniendo el rango de origen todas las direcciones IP de la LAN, una forma de concepto y orden en las reglas internas del firewall hemos llamo a esta regla “Restringido”

Por defecto se crean 5 reglas de navegación en el cuadro de “security Profiles” estas reglas se puede editar seleccionándolas, no se recomienda hacerlo en el apartado de seguridad.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
Restringido	all	all	always	ALL	ACCEPT	Enabled	<ul style="list-style-type: none"> AV-General WEB Limitado APP Limitado default

Ilustración 30 Vista de Política Restringido

Fuente: Recursos propio

Sin embargo, la empresa desea bloquear todo lo que son redes sociales, para esto se crea una regla en el apartado de “security Profiles” en el menú principal, seleccionando web filter, seleccionando el boton de crear nueva regla, se nos desplegara un menú, escribiendo el nombre de la regla en este caso Block redes sociales, en las opciones inferiores se puede observar una opción llamada URL Filter, si se selecciona crear block se introduce la dirección que se desea bloquear por ejemplo www.facebook.com, así mismo se agregarían todas las páginas restringida y en el apartado del firewall se agregaría la política llamada block redes sociales.

Block invalid URLs

URL Filter

URL	Type	Action	Status
www.facebook.com	Simple	Exempt	Enable

Ilustración 31 Creación de Bloqueo de dirección web

Fuente: Recursos propio

Política de seguridad libre.

Es importante controlar la navegación por parte de los usuarios ya que el firewall es el encargado de analizar lo que navegan y a la disponibilidad de estos accesos sin embargo ahí usuarios que tiene autorizaciones, se crea nuevamente en el firewall un apartado llamado “Unrestricted” en la selección de fuentes agregaremos de forma manual la dirección ip o Mac que quisiéramos liberar, también se procede a quitar todas las políticas en “security Profiles” y segregaría una ya por defecto en las lista de selección llamada “no-inspection”



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
UNRESTRICTED	192.168.0.106	all	always	ALL	ACCEPT	Enabled	no-inspection	All

Ilustración 32 Vista de política libre.

Fuente: Recursos propio

Configuración de VPN

En la configuración del VPN, se tiene en cuenta que existen dos formas de establecerlo las cuales son SSL Y IPSEC ambas configuraciones son excelente para la conexión remoto de la empresa, sin embargo, se escogió la configuración de SSL por la ventaja que tiene sobre IPSEC, que es la liberación y recuperación de la conexión es decir IPSEC pierde momentáneamente la conexión para levantar el servicio de VPN y SSL no necesita perder dicha conexión para establecer comunicación con el servicio vpn, para poder configurar esta opción en el menú principal del Fortinet se selecciona **VPN>SSL-VPN Settings**.

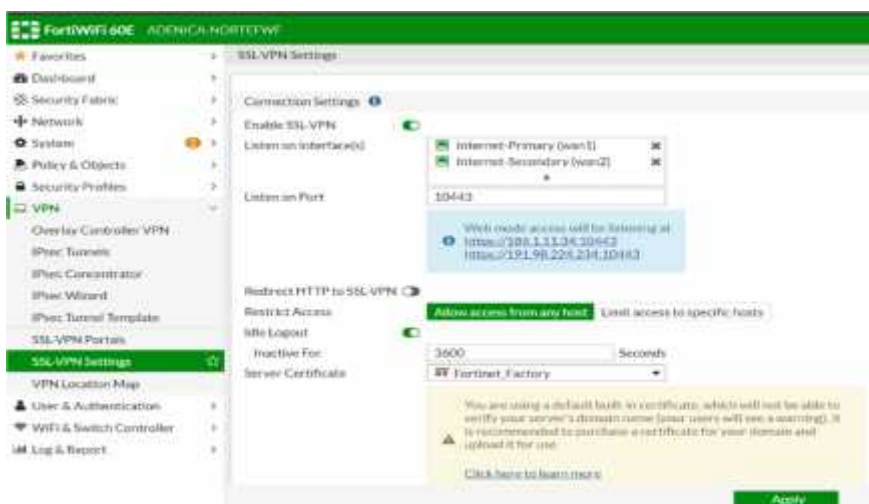


Ilustración 33 Configuración de SSL-VPN.

Fuente: Recursos propio

Se habilita la opción **Enable SSL-VPN**, posteriormente se selecciona la IP pública a la cual se realizará la conexión, en este ejemplo se seleccionaron dos IP por si un proveedor de internet no podría brindar el servicio de internet temporalmente, se puede establecer la configuración predeterminada del puerto 443, pero se decidió establecerlo en 10443 solo por no ser estándar, en la opción **Idle logout** si se habilita para poder guardar la contraseña en futuras conexiones.

Creación de Usuario para VPN

El acceso remoto para la empresa se proporciona en los usuario y contraseña establecidos en el Fortinet, navegando en el menú principal **User & Authentication > Create New**, se ingresa un nombre de usuario en este caso **Oromero** y una contraseña, el resto de paso es información general de comentarios se next hasta finalizar el proceso.

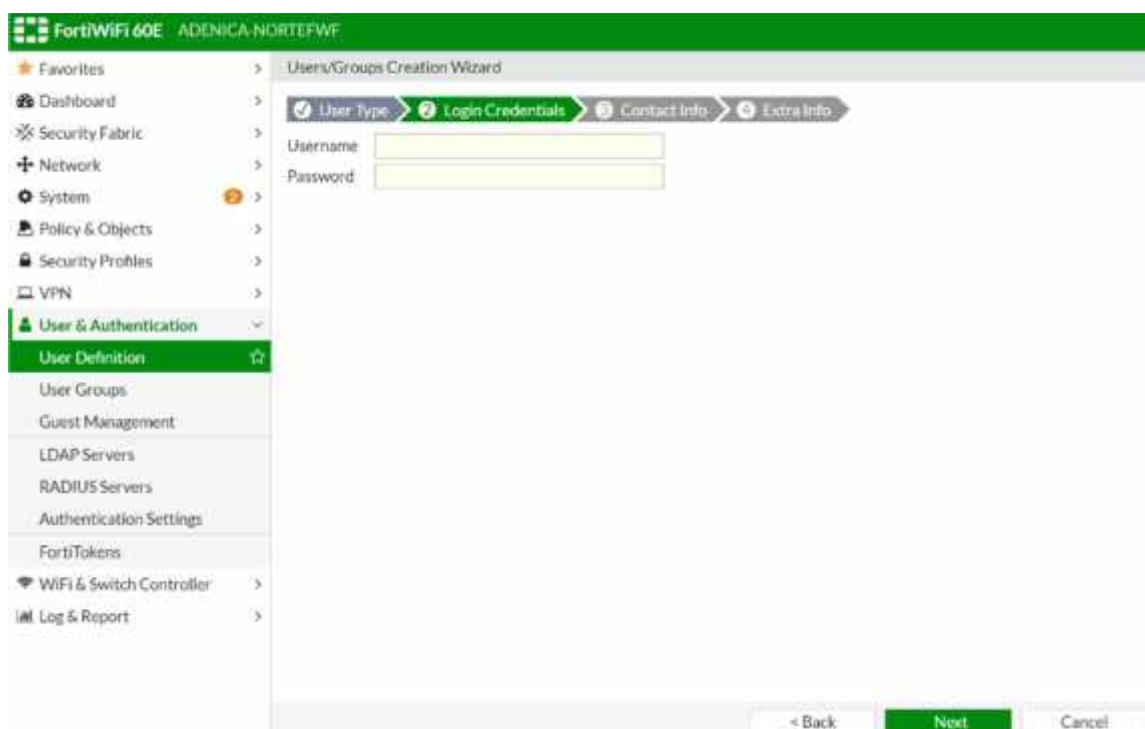


Ilustración 34 Establecimiento de Credenciales vpn.

Fuente: Recursos propio

Configuración de VPN en host

La implementación del VPN en el Host consiste en la instalación de una aplicación llamada Forticlient, existen 3 versiones diferentes en la página oficial de Fortinet, se implementará únicamente la aplicación que solo contenga la configuración VPN llamada **Forticlient- Remote Access**.



Ilustración 35 Configuración Forti-Client

Fuente: Recursos propio

En la aplicación instalada aceptamos los permisos y se procede a añadir los datos en la pestaña de SSL-VPN Ingresando el nombre de conexión y la descripción, en remote Gateway colocamos la dirección pública configurada en el Fortinet, se habilita el puerto customize junto con el número de puerto, posteriormente se agrega el nombre de usuario y dando click en guardar llevara a la página principal a la aplicación, se ingresa la contraseña y la conexión estaría establecida.



Ilustración 36 Configuración Forti-Client

Fuente: Recursos propio

La aplicación establece una conexión segura al usuario al internet de la impresora evitando usar aplicaciones de terceros, ya es un servicio propio de Fortinet.

Instalación y configuración de Antivirus

Para la seguridad y protección de cada usuario, servidor o dispositivo final, se estableció como política interna hacer uso de Antivirus, en el mercado actual existen diferentes soluciones para estos servicios de protección, como son McAfee, Eset, Avast y Kaspersky.

Aunque siendo Avast una solución de servicios gratuito, no ofrecía servicio de administración en la nube, despliegue de tareas, análisis programado, y protección ante alteraciones de información, a diferencia de los demás antivirus, se optó por seleccionar Eset como sistema de protección, por su fácil administración de políticas en la nube y aun precio adecuado.

En el panel de administración de antivirus se observa el menú de política del antivirus y la opción de descarga para el instalador de equipos y servidores por defecto este es un proceso de dar siguiente hasta finalizar la instalación en cada host, actualmente la consola de Eset por defecto tienes habilitada muchas herramientas de protección entre ellos un firewall, junto con

el equipo técnico de soporte de Eset, se encargan de notificar y modificar alguna política de protecciones.

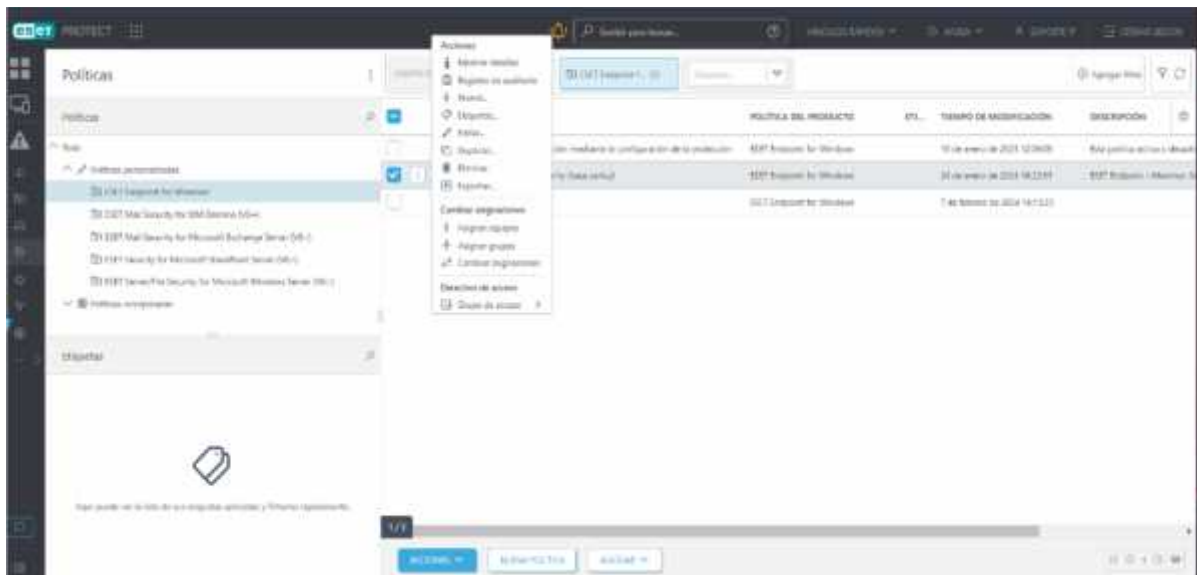


Ilustración 37. Vista de consola de Eset (Descarga de archivo de instalador)

Fuente: Recursos propio

Virtualización de servidores

En la implementación de un servidor es necesario tener la mejor administración de todos los recursos que dispone, utilizarlo únicamente por un sistema operativo ya sea Linux o Windows no se estaría aprovechando al máximo en su recurso, para esta solución se implementó como sistema operativo VMware - ESXi que permite la fácil administración y virtualización de diferentes sistemas operativos.

El software VMware ESXi es un sistema operativo que se instala directamente en el hardware del servidor, en este caso del servidor Dell PowerEdge R430 al ser un servicio de paga es necesario adquirir una licencia de uso.

En la instalación del sistema operativo de virtualización el proveedor VMware, requiere en la creación de una cuenta de VMware Customer Connect de aspecto gratuito, en las opciones de la cuenta se puede observar, **Productos y cuentas > Todos los productos**. VMware vSphere se mostrará un icono de descargar producto.

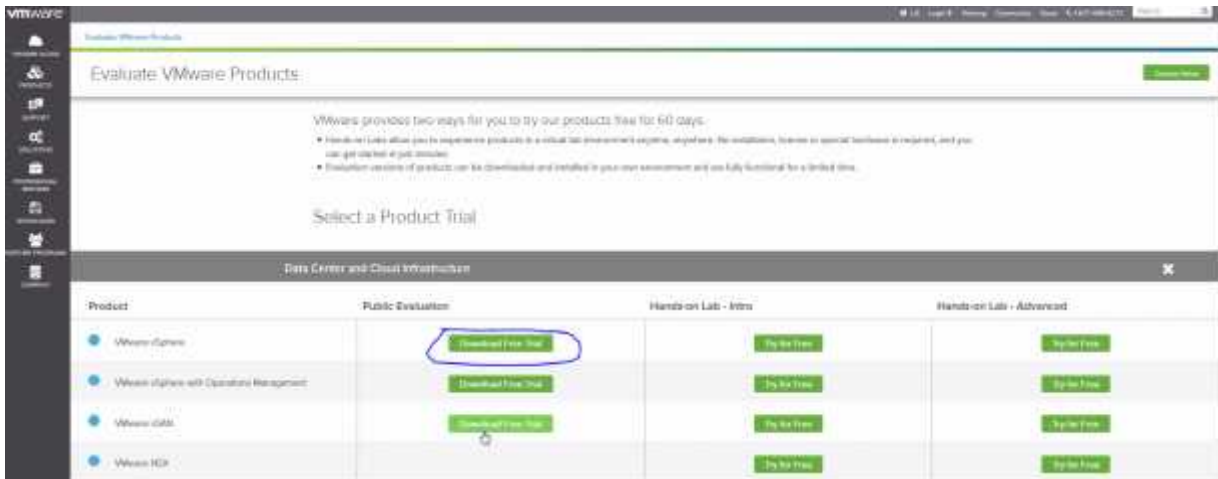


Ilustración 38 Descarga de ISO Esxi (Captura de pantalla en la plataforma)

Fuente: Recursos propio

Una vez obtenida la imagen iso de VMware ESXi, es esencial flashear una USB compatible con nuestro servidor, el servidor Dell PowerEdge R430 es compatible con memoria USB 2.0 y 3.0, por lo tanto, se utiliza el programa RUFUS para poder integrar la imagen ISO a la USB posteriormente insertando y encendiendo el servidor, presionando al mismo tiempo la tecla F12, para poder iniciar en el modo BOOT.

En el siguiente menú se seleccionará la opción del nombre del sistema operativo ESXi, se utilizó la versión 6.7.0, ya que es una versión estable y probado a través de algunos años.



Ilustración 39 Boot de Sistema de virtualización

Fuente: Recursos propio

Después empezará a cargar los archivos en memoria para poder realizar la instalación, empezaremos con la instalación después de ver un mensaje de compatibilidad. Se pulsa enter. En este caso se tiene en cuenta un host físico donde estás haciendo la instalación, aparecerán todos los discos que contiene y se debe elegir donde instalarlo, sin embargo, se hizo un arreglo en la BIOS marcando en el gestor de almacenamiento como RAID 1, seleccionando una única opción en disco donde instalar.

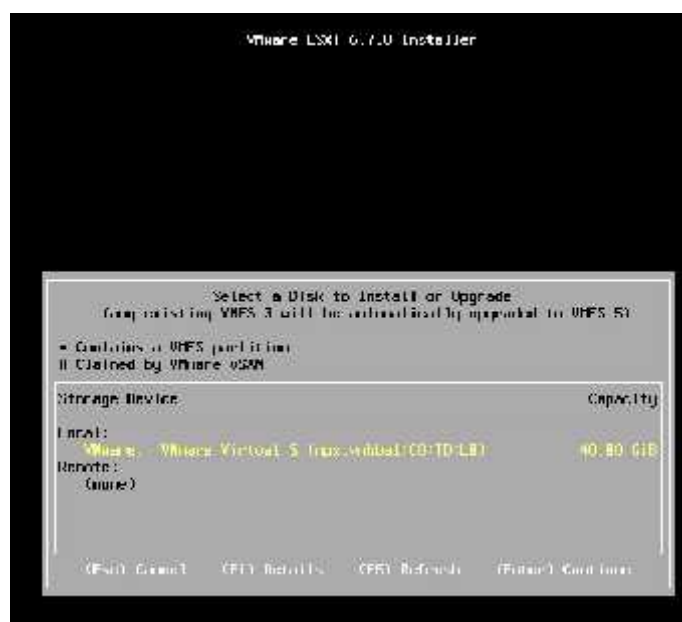


Ilustración 40 Selección de disco de instalación

Fuente: Recursos propio

Posteriormente la instalación del programa solicitara, la selección de idioma y una contraseña compleja de 9 caracteres como mínimo con combinaciones de mayúsculas, números y minúsculas.

Una vez que haya terminado la instalación el servidor se reiniciara, iniciando los servicios de virtualización obteniendo una dirección IP por DHCP.

En la pantalla del servidor se coloca una IP fija en este caso será la 192.168.0.252, en el acceso de las configuraciones apretando la tecla F2.

Se abrirá una ventana solicitando la contraseña previamente estableciendo, las opciones de Red en el servidor junto con otras configuraciones se mostraran y se seleccionara la opción de **Configure Management Network>IPV4**.

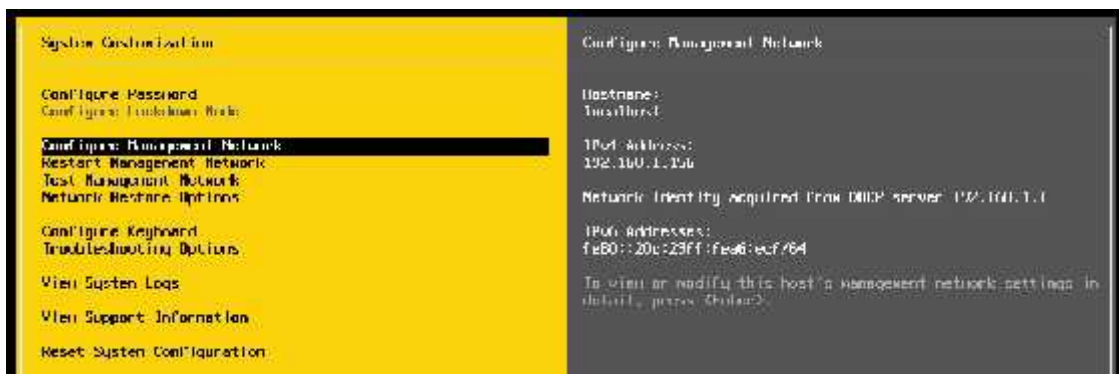


Ilustración 41 Configuración de IP estática

Fuente: Recursos propio

Una vez finalizado este proceso se recomienda cerrar la sesión y reiniciar el servidor para que los cambios establecidos puedan ser ejecutados.

En la administración del servidor se deberá acceder a la interfaz a través de cualquier equipo de cómputo que este dentro de la misma red del equipo ESXI colocando la IP en cualquier navegador este mostrará un mensaje de advertencia o no dependiendo del navegador, simplemente se selecciona la opción de proceder o continuar en la página web, mostrando el panel de inicio de nuestro servidor.



Ilustración 42 Navegación gráfica del servidor

Fuente: Recursos propio

Por defecto en la configuración del programa el usuario root es el único usuario disponible para acceder a la administración junto con la navegación web.

No es recomendable el cambio de usuario por motivos de privilegio o la creación de nuevas configuraciones siendo el usuario root con mayor autorización en el equipo.

Configuración de Máquina virtual en el servidor

En la configuración de una máquina virtual será necesario descargar la imagen ISO correspondiente, hay que tener en cuenta que esta imagen ISO debe estar en nuestro equipo al momento de seleccionarlo desde la consola de ESXI, una vez iniciado sesión en la página web de ESXI y suponiendo que se encuentra nuestro sistema operativo en el Datastore comenzaremos con el proceso de instalación de la primera máquina virtual en este caso Windows server 2016

Para ello en el menú derecho se observa una opción de “máquinas virtuales”, se selecciona la opción de “Crear/regar máquina virtual”.



Ilustración 43 Creación de maquina virtual

Fuente: Recursos propio

Como se creará una nueva máquina virtual a partir de una ISO previamente descargada seleccionaremos la opción “Crear una nueva máquina virtual”, se escoge el nombre, la compatibilidad, el tipo de sistema operativo y la versión del sistema operativo:

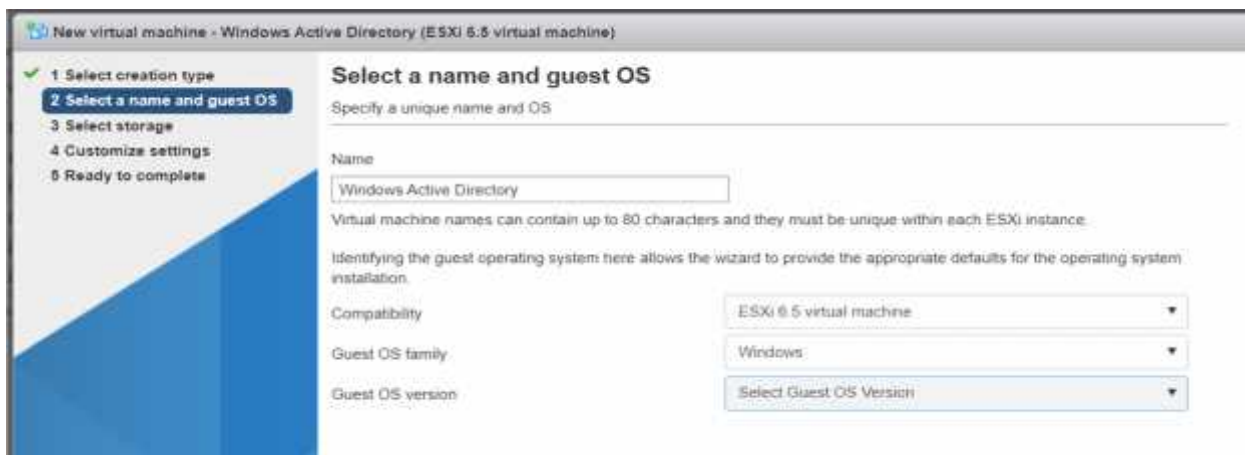


Ilustración 44 Selección de parámetros de virtualización

Fuente: Recursos propio

En la siguiente venta el programa pedirá seleccionar cuanto almacenamiento se le asignara a la máquina virtual, en este caso como solo es un Windows server 2016 a instalar y contendrá el servicio de Active Directory (AD) para la administración y gestión de usuarios se le asignara 60GB de 40TB Disponible luego en la opción de siguiente.

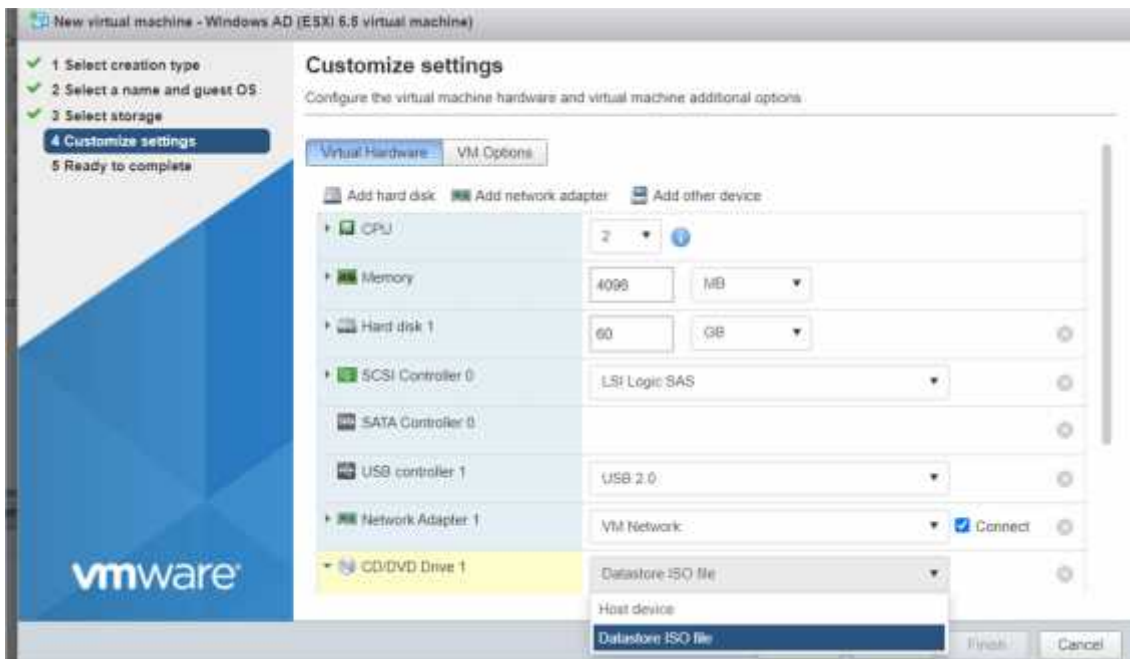


Ilustración 45 Selección de recursos de máquina Virtual

Fuente: Recursos propio

En la tercera pestaña se selecciona la configuración cuanto memoria RAM y cantidad de núcleos en junto con la selección de la imagen ISO a utilizar, se establecerá una configuración de 2 núcleos y 4 GB de memoria RAM.

En la parte inferior se observa la opción de Datastore file, abriendo una ventana nueva en el reposito de nuestra computadora podremos crear nuevos directory y seleccionar el ISO correspondiente seleccionada desde el dispositivo en uso.

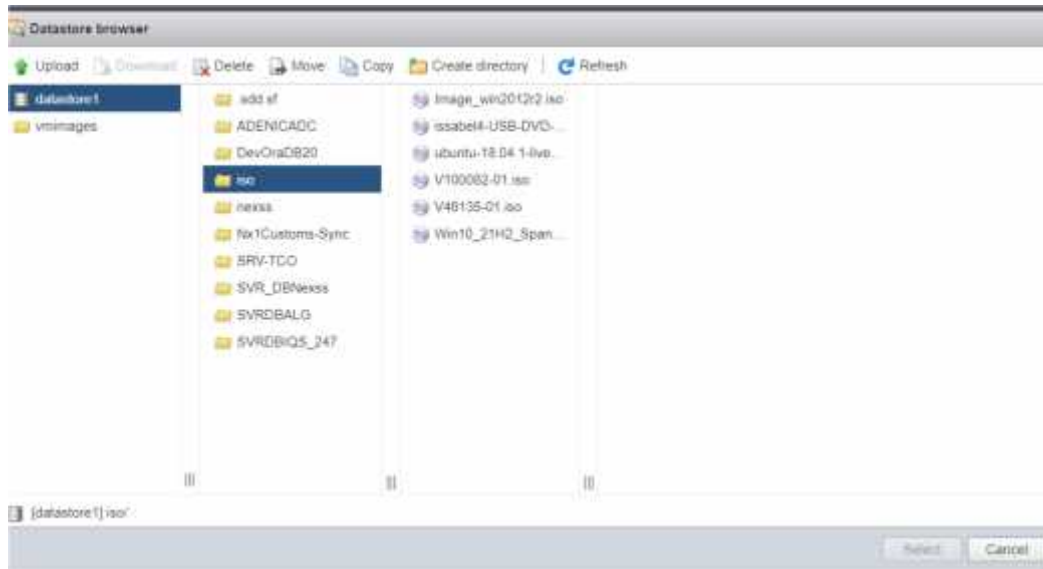


Ilustración 46 Carga de sistema operativo para MV

Fuente: Recursos propio

Escogido el sistema operativo correcto se devolverá a la ventana anterior dando finalizar la configuración, las por defecto la máquina virtual estará apagada. Dando clic en el botón de encender se iniciará el proceso de una ventana mostrando menú de instalación de Windows server 2016 una vez completado se podrás usar totalmente la máquina virtual.

Instalación de Windows server 2016 en máquina virtual

En el apartado de inicialización del servidor Dell PowerEdge R430 a través de la interfaz gráfica web la máquina virtual estará apagada, se mostrará un botón llamado encender máquina virtual, al pulsarlo se abrió una ventana externa dentro del navegador mostrando el logo de vmware, seguidamente, se mostrará el menú de azul de Windows server para su instalación.



Ilustración 47 Menú de instalación Windows Server 2016

Fuente: Recursos propio

En esta parte de la instalación se muestra un botón de siguiente, posteriormente se observará un menú de que solicitara el tipo de versión de Windows server, se estableció la versión de entrono grafico Datacenter x64, en la siguiente venta aparecerá la aceptación de términos y condiciones, una vez aceptado se escogió la opción de custom, mostrando la única partición de disco de 60GB establecido en la creación de la máquina virtual, comenzara a instalarse el sistema Operativo.

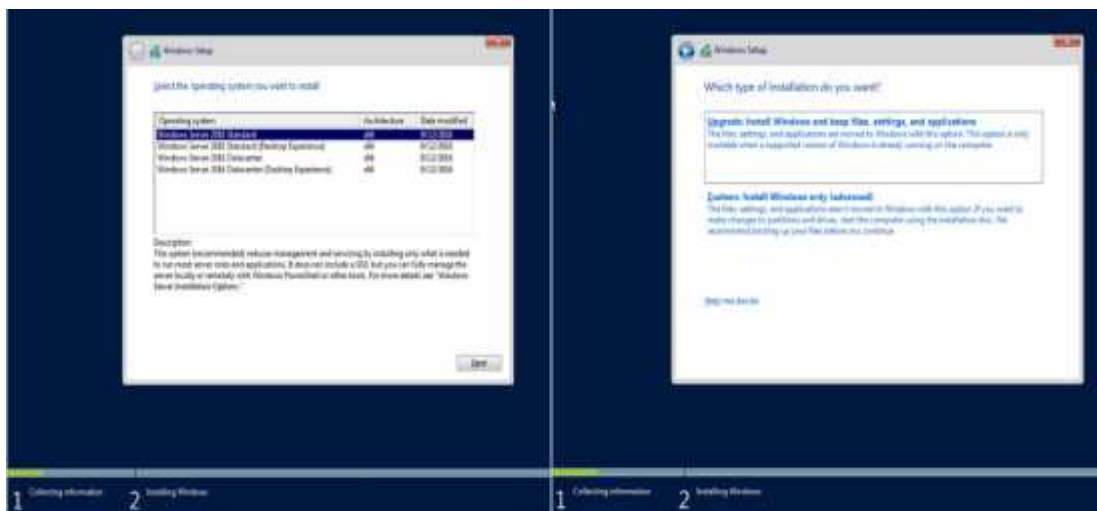


Ilustración 48 Proceso de instalación de Windows server 2016

Fuente: Recursos propio

Una vez finalizado el proceso de copia de los archivos del sistema operativo solicitará un reinicio, al finalizar el reinicio la máquina virtual (más adelante mencionada como MV) inicializara con normalidad el inicio de sesión de Windows, se ingresaran como usuario predeterminado el administrador y una contraseña segura para el uso de la MV, al iniciar el Windows server se mostrara el panel de control para la asignación de roles y característica.

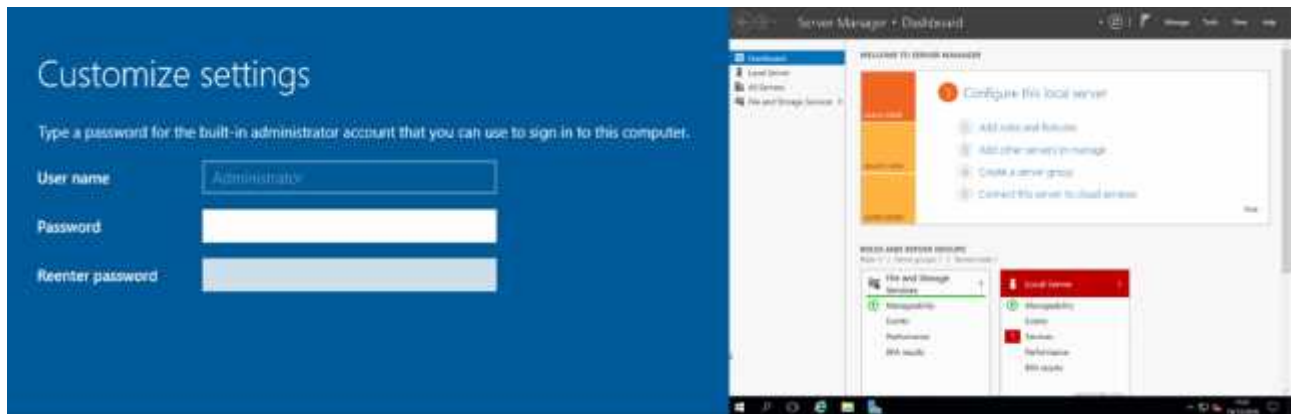


Ilustración 49 Login y panel de control Windows server 2016

Fuente: Recursos propio

Instalación de servicio de Active Directory

En el sistema operativo Windows server 2016 previamente instalado en el servidor Dell PowerEdge R430, dentro de la máquina virtual es necesario brindarle una IP estática ya que por predeterminado sistema operativo ESXI en el servidor Dell genera una conexión puente en su interfaz física de Ethernet a la interfaz virtual dando una IP del mismo segmento de la red LAN. Esta configuración se puede modificar internamente en dentro de la máquina virtual, en la parte inferior a la derecha podremos observar un icono de una computadora de escritorio, al momento de seleccionar dicha opción se abrirá una ventada mostrando “Cambiar opciones del adaptador”.

En las opciones de funciones de red se seleccionó la ruta de protocolo de internet versión 4 (IPV4), aquí se abrirá una nueva ventana digitando la dirección IP de DHCP a Estática, por preferencia de la empresa se decidió dejar en 192.168.0.251/24.

En la implementación del proceso de servicio de **Active Directory**, es importante dirigirse al panel de “**Administrador de servidor**”, herramienta que se inicia automáticamente cuando se abre Windows Server. En caso contrario, solo se abrirá el menú **inicio**.

En el panel de control “**Administrador de servidor**”, se puede observar la opción de “**Administrar**” contigua a la selección se desplegará un menú mostrando la indicación de “**Agregar roles y características**”.



Ilustración 50 Proceso de configuración de Active Directory

Fuente: <https://www.profesionalreview.com/2018/12/17/active-directory-windows-server-2016/>

Dará comienzo el asistente para la instalación del controlador de dominio. En la primera pantalla, Como cumplimos con las recomendaciones, se habilitará el botón “**Siguiente**”.

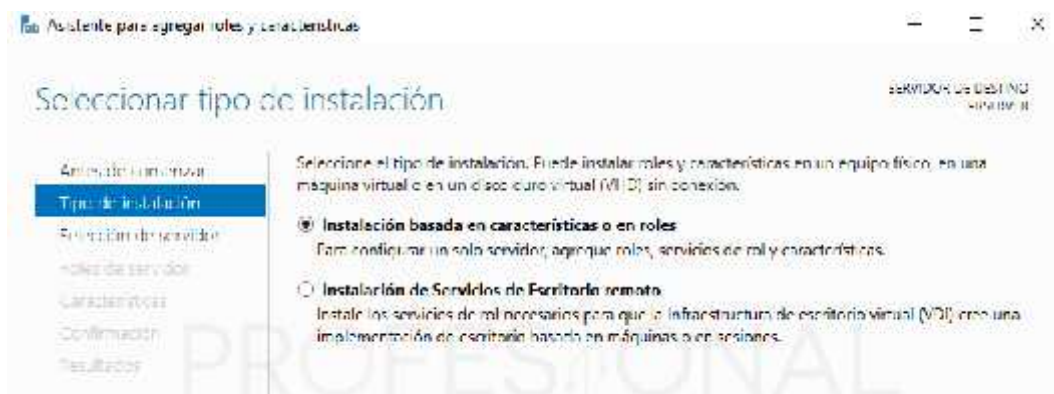


Ilustración 51 Proceso de configuración de Active Directory 1.1

Fuente: <https://www.profesionalreview.com/2018/12/17/active-directory-windows-server-2016/>

En la siguiente ventana tendremos que **seleccionar el servidor** que será el encargado de hacer esto. Como solo tenemos uno, pues ya estará añadido de forma predeterminada. Pulsamos en “**Siguiente**”, Recordando, que no contamos con el servicio de DNS en nuestra red, se seleccionara la casilla de “**Servidor DNS**” para que Windows server nos proporcione estos servicios necesarios internamente.

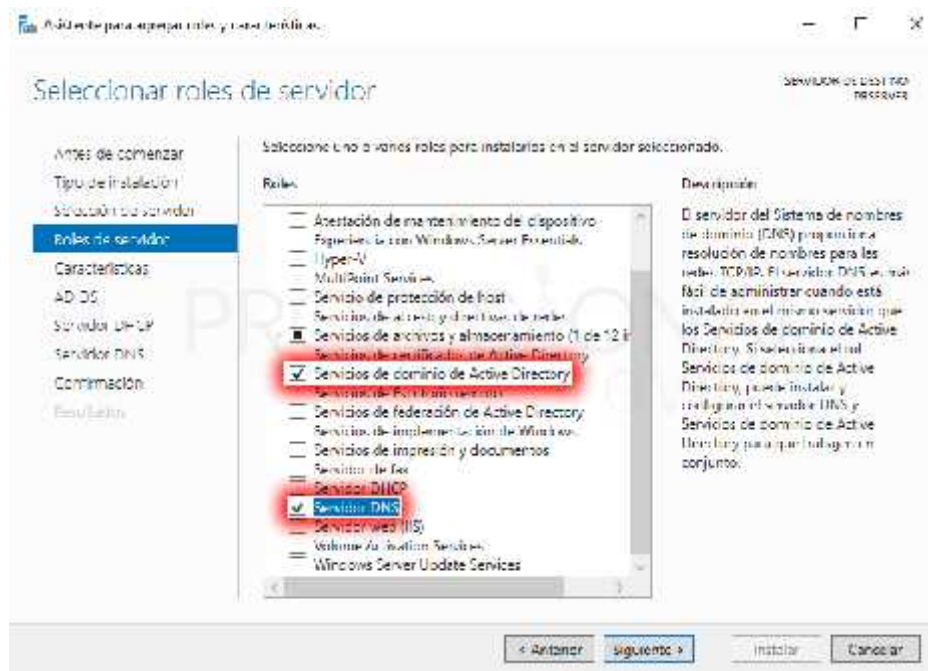


Ilustración 52 Proceso de configuración de Active Directory 1.2

Fuente: <https://www.profesionalreview.com/2018/12/17/active-directory-windows-server-2016/>

Ahora solo aparecerán sendas ventanas para informarnos de las características que vamos a instalar son el rol DNS y Active Directory. Se pulsará por recomendación de Microsoft “**Siguiente**”, Finalmente, veremos un resumen de todo lo que vamos a realizar en nuestro servidor. El proceso seguramente llevará un rato. Nosotros debemos darle en “**Instalar**”

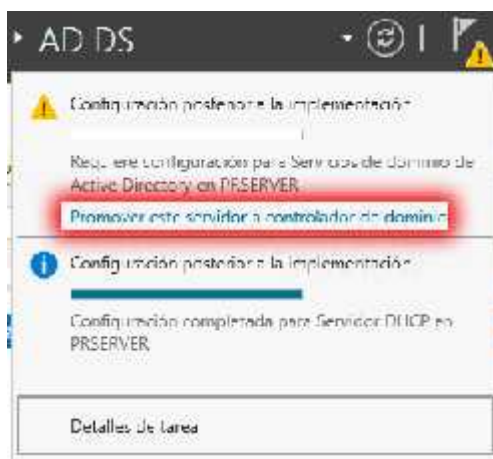


Ilustración 53 Controlador de dominio

Fuente: <https://www.profesionalreview.com>

En configuración sobre el servidor como controlador de dominio. Se establecerá como la creación de un servicio interno agregando un nuevo dominio, lo que implica crear un árbol y un bosque, esto se encuentra en la parte **icono de Notificaciones** en el panel de control. Se podrá observar la opción de **“Promover este servidor a controlador de dominio”**.

En Windows integra un asistente de configuración para el nuevo dominio. Elegimos la opción **“Agregar un nuevo bosque”** y colocamos un nuevo nombre en la casilla de dominio en este caso será el nombre de la empresa Farmacéutica



Ilustración 54 Proceso de configuración de Active Directory 1.3

Fuente: <https://www.profesionalreview.com/2018/12/17/active-directory-windows-server-2016/>

En la siguiente ventana, se configura una serie de parámetros. En nuestro caso vamos a dejar las opciones que vienen ya predefinidas, y colocaremos una contraseña para cuando necesitemos reiniciar Active Directory. (no es la contraseña del administrador del servidor). Seguidamente se asignará un nombre **NetBIOS** al dominio que deseamos crear. Este hecho es muy importante, porque será el nombre se utilizará para conectar los equipos en el dominio. Cuando lo tengamos, pasaremos a la siguiente ventana, y luego a la siguiente.



Ilustración 55 Proceso de configuración de Active Directory 1.4

Fuente: <https://www.profesionalreview.com/2018/12/17/active-directory-windows-server-2016/>

Ahora situado en la pantalla final, en donde, tras esperar unos segundos, nos aparecerá activa la opción de **“Instalar”**. Se podrá pasar de las advertencias que nos aparecen, ya que justo más abajo nos notificará que las comprobaciones son correctas.

Una vez terminado las instalaciones, comenzar a gestionar el directorio activo creando usuarios u otros objetos. por nuestra parte se crearán un usuario para luego utilizarlo en una conexión desde un equipo externo como cliente.

En las opciones del panel de control de nuestra maquina virtualizada se buscará la opción de **Herramientas>Centro de administración de Active Directory.**



Ilustración 56 Proceso de configuración de Active Directory 1.5

Fuente: <https://www.profesionalreview.com/2018/12/17/active-directory-windows-server-2016/>

Se abrirá una nueva ventana, conteniendo en la parte izquierda el bosque creado con nombre el nombre introducido anteriormente, para ver todo el dominio y unidades organizativas. Se debe de bajar hasta el final del menú de en medio, en donde encontraremos la unidad de “Users”.

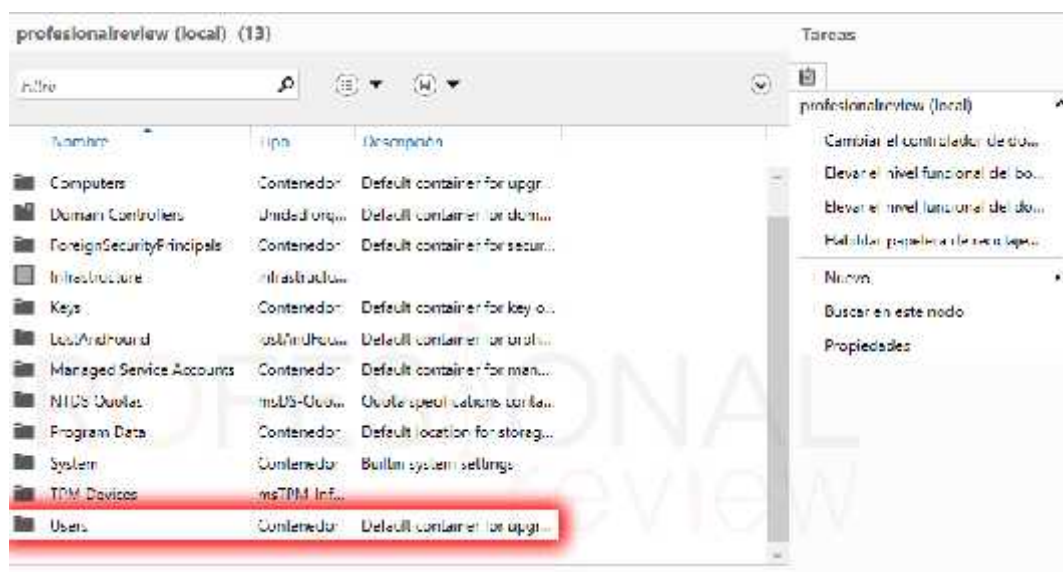


Ilustración 57 Proceso de configuración de Active Directory 1.5

Fuente: <https://www.profesionalreview.com/>

Una vez seleccionado la unidad User en la parte izquierda veremos una opción llamada “Nuevo” nos abrirá un menú de formulario para la creación de un nuevo usuario de dominio, junto con diferente para metros de la cuenta.



Ilustración 58 Proceso de configuración de Active Directory 1.6

Fuente: <https://www.profesionalreview.com/2018/12/17/active-directory-windows-server-2016/>

Para comprobar que nuestras configuraciones fueron exitosas, se usara un equipo externo antes mencionado conectado a la red, abriendo una ventana en el explorador de tarea, seleccionando “este equipo”, dirigiendo a la opción de **propiedades>Dominio o grupo de trabajo**.

En la opción de dominio escribimos el nombre de dominio nos pedirá ingresar usuario contraseña por defecto el nombre de usuario es administrador y la contraseña es la establecida en la configuración del Active Directory, completado correctamente este proceso nos indicara que hemos agregado correctamente el host al dominio.

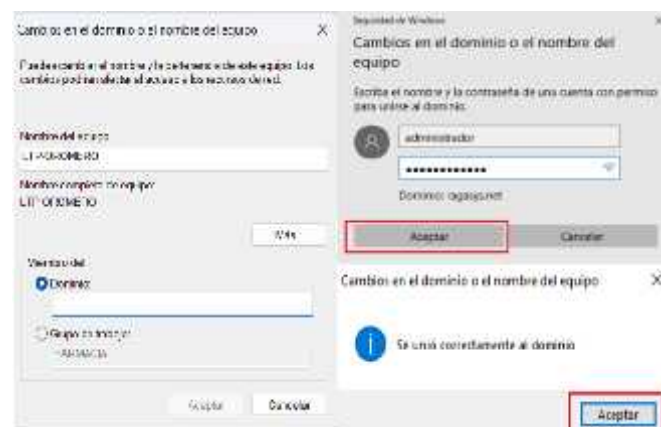


Ilustración 59 Unión de cliente a servidor de dominio

Fuente: Recursos Propios

El servicio de administración para cada equipo de la empresa, se encuentra levantado, y se podrá gestionar cambio de contraseña, suspensión de cuentas, creación y modificación de ella, junto con el ordenamiento de cada equipo por nombre registrado en el servicio de Active Directory.

Implementación de servicio de respaldo

Una buena práctica en informática es crear respaldo ante un acontecimiento de fuerzas mayores como daños a los sistemas operativo de los servidores principales o virtualizados. Mencionado lo anterior se decidió establecer un servidor físico con sistema operativo de Windows como gestor de respaldo de archivos compartidos, máquinas virtuales y documentación sensible

Para esta labor se utilizó el servidor HP ProLiant ML150, inicialmente se instaló la versión de Windows server 2019 con nombre de quipo DataFile , junto con 3 disco duros, individuales, 1 TB establecido como el disco principal que contiene el sistema operativo con letra de identificación C , el segundo y y 3 disco son de 4TB cada uno, el segundo disco con letra D será nombrado como “Compartidas” en este disco se crearan todas las carpetas que se compartirán a usuarios claves con acceso a ellas, en el disco 3 con letra F será nombrado Backup.

Para comenzar con el proceso de respaldo de las máquinas virtuales se utilizará un programa llamado Veeam Backup & Replication, el software es de uso gratuito con algunas limitantes de no crear más 50 tareas respaldos, la principal descarga del programa se puede encontrar en la página oficial de Veeam, se solicitará crear una cuenta y navegar hasta los productos para comenzar su descarga.

Al momento de instalar el programa solo nos pedirá permisos de instalación y un nombre de cuenta de acceso este puede ser cualquier nombre, en este caso se colocó el nombre de la empresa Una vez finalizado el proceso de instalación se mostrará un menú validando la conexión local a los servicios de respaldos.

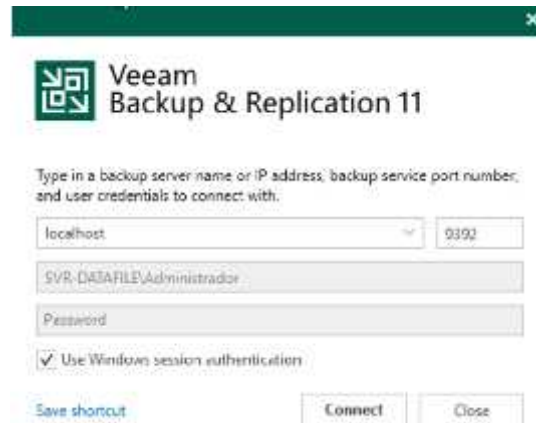


Ilustración 60. Conexión local veeam a servidor

Fuente: Recursos Propios

En el menú principal de la aplicación de respaldo veeam, tendremos que declarar en qué lugar se desea guardar los datos a respaldar, en la aplicación se conoce como almacenamiento, en menú inferior ahí se selecciona la opción de **BackupInfrastructure >Backuprepositories > add backup.**

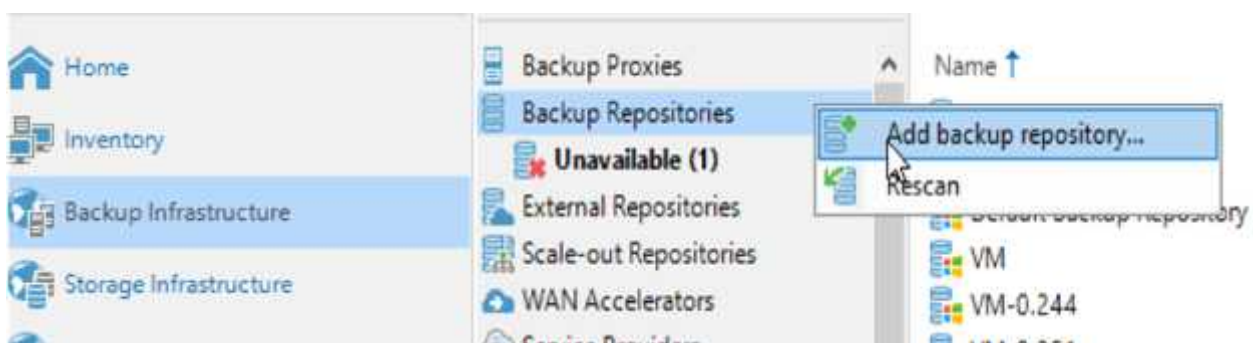


Ilustración 61 Creación de repositorio de respaldo

Fuente: Recursos Propios

Se abrirá una nueva ventana para poder crear la dirección de almacenamiento en el servidor de una forma local seleccionándola o creándose directamente del asistente de creación de repositorio del programa veeam, se tiene en cuenta en este proceso que toda la información a respaldar de las máquinas virtuales se estará enviando por nuestra red, conforme a la creación del repositorio con el nombre de carpeta llamado VM, se dará siguiente hasta finalizar el proceso.

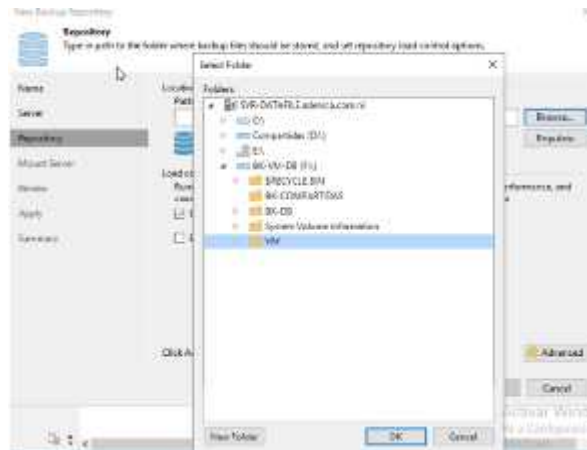


Ilustración 62 Selección de carpeta para repositorio

Fuente: Recursos Propios

Este proceso permitió la creación de un repositorio de almacenamiento local en el disco del servidor DataFile, en la sesión del menú de la izquierda se encuentra una opción de llamada Home, esta opción ayuda en la ruta de realizar el respaldo de las MV, dirigiendo en el apartado de **Jobs >Backup>virtual Machine**, mostrando una nueva ventana de paso que se estableciera el nombre del proceso de respaldo llamado BK-W2016.

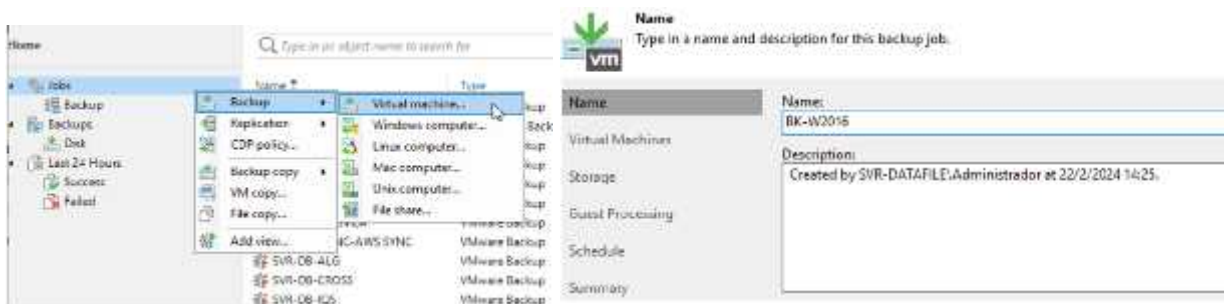


Ilustración 63 Menú de configuración de repositorio

Fuente: Recursos Propios

En la siguiente ventana, se mostrara un cuadro vacío en blanco que contendrá en la parte de la derecha un botón llamado Add si se pulsa nos redireccionara a una sub ventana para añadir y otorgar acceso a las máquinas virtuales, seleccionando en la parte inferior un icono de servidor con nombre de “Host” al momento de seleccionarlo se coloca la dirección IP del servidor y comenzara una búsqueda dentro de la red mostrando posteriormente el servidor deseado, se procede a seleccionarlo, retornando en la ventana de principal aparecerán diferentes direcciones IP que todas MV que contiene el servidor se selecciona y se da siguiente.

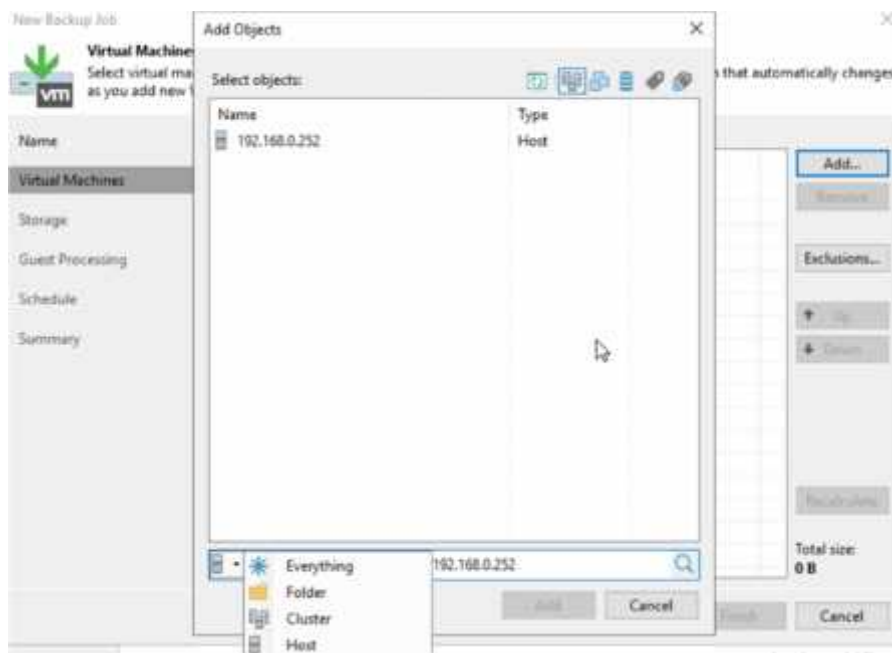


Ilustración 64. Selección de servidor

Fuente: Recursos Propios

En la ventana de **storage** se mostrará un menú desplegable con algunos repositorios predeterminados, se seleccionó el repositorio previamente creado llamado “VM” aquí se está establece la ruta de programa para el trabajo de respaldo, en la ventana siguiente solo daremos continuar, posteriormente se observará en la venta de **Schedule** que contiene las casillas para una configuración de trabajo automático.

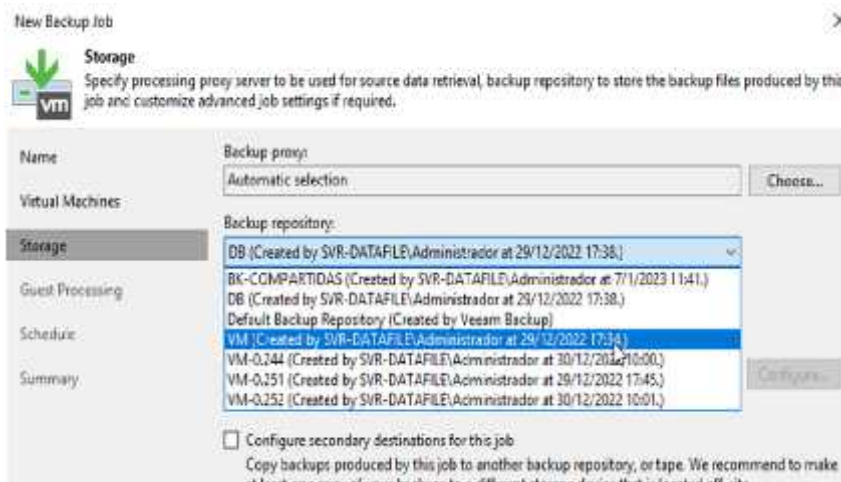


Ilustración 65. Selección de repositorio

Fuente: Recursos Propios

En las opciones de trabajo automático previamente mostradas se puede apreciar las indicaciones de correr diariamente la tarea asignada, en la opción de "Days" se seleccionó los días de semana y los sábados establecidos como los días de respaldo a las 10 P.M de la noche cabe de mencionar si se están haciendo uso de cualquier máquina virtual ya sea Linux o Windows al momento de la hora exacta en la ejecución de la tarea de respaldo esta no sufrirá ninguna afectación.

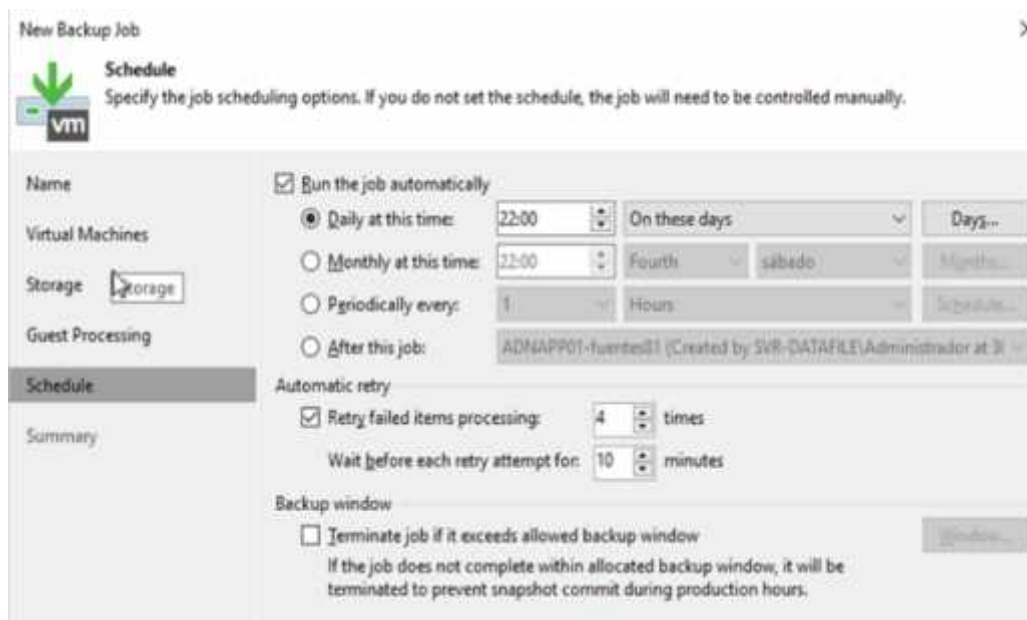


Ilustración 66 Configuración de respaldo

Fuente: Recursos Propios

En las opciones inferiores se muestran un apartado de cuantos intentos permitidos tiene la aplicación de veeam para poder volver a ejecutar la tarea si esta no pudo ser cumplida en este caso se estableció 4 veces en un intervalo de 10 minutos, en la siguiente venta solo damos siguiente y la aplicación veeam terminara de carga el proceso finalizado.

Terminado el proceso la aplicación tendrá un cuadro inferior llamado "run the job", al momento de seleccionar la opción y dar finalizar se comenzará la tarea de respaldo inmediatamente.

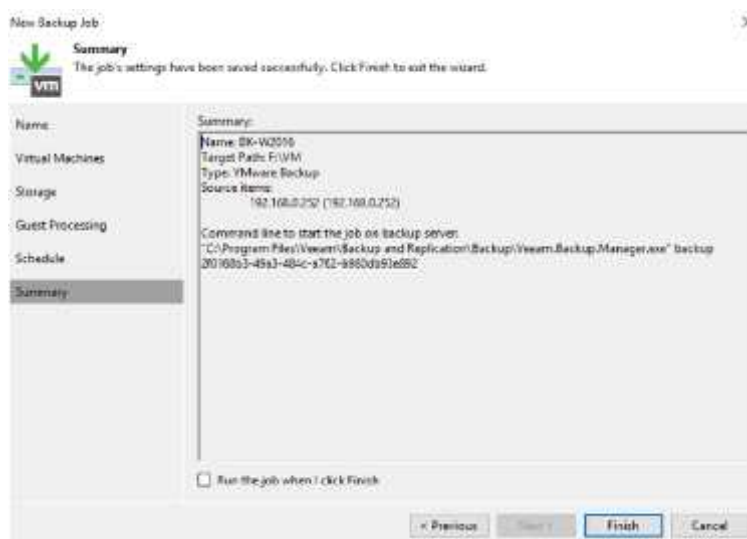


Ilustración 67 Finalización de estado de trabajo

Fuente: Recursos Propios

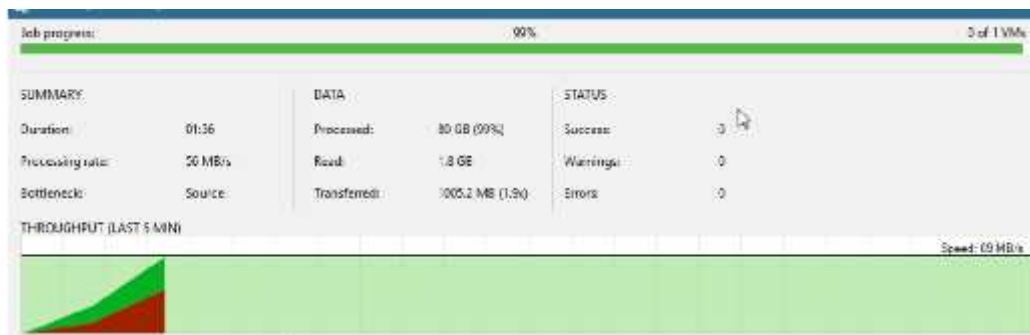


Ilustración 68 Vista de proceso de respaldo de maquina virtual

Fuente: Recursos Propios

El progreso de respaldo se puede apreciar 2 barras verdes, en la parte superior se encuentra el proceso general de la tarea principal, en la parte de en medio se observa características de as tarea, como tiempo transcurrido, peso de la máquina virtual, errores y advertencias, en la parte inferior se contempla de una forma gráfica la transferencia de megas por segundos, al finalizar el trabajo de se puede apreciar los nuevos archivos creados por el programa veeam en la dirección dada del repositorio.

Estos archivos como tal no se pueden abrir, se tendría que restaurar la máquina virtual en el servidor para poder analizar la información interna de la máquina virtual o se podría instalar la MV en el equipo local, sin embargo, esto significaría que tendríamos que instalar todo atravez de la aplicación VMware para Windows lo que no es recomendable por los recursos expuesto.

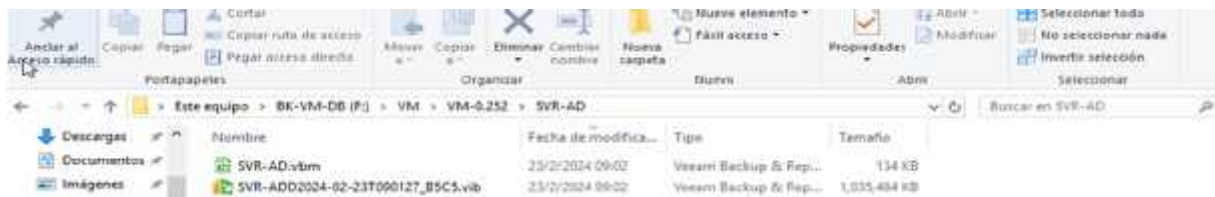


Ilustración 69 Visualización de archivos de respaldo

Fuente: Recursos Propios

Configuración de disponibilidad y acceso a información.

Es importante saber que para asignar privilegio de acceso a la información se tiene que tomar en cuenta que usuarios podrán acceder atravez de ella, en la parte de la empresa es necesario que los usuarios de cada área puedan compartir información entre sí, se conoce que el uso de otro medio como correo o dispositivos USB no son prácticos o inseguros, ya que es información que se tiene que estar revisando o actualizando constantemente.

Para esta solución se creó una carpeta compartida por área en el servidor de archivos y cada carpeta compartida se añadió a solo las personas correspondientes por medio del servicio de

administración Active Directory (AD), esto se estableció de la misma manera que unir un equipo al dominio en este caso se unió el servidor de archivo.

En creación de estas carpetas nos dirigimos al disco D llamado compartidas en el servidor de archivos, se creará la primera carpeta llamada "Administración ", los cuales solo se agregarán los usuarios autorizados, en este apartado se ejecutó clic derecho en el disco, nueva carpeta posterior mente se nombra la carpeta, posterior mente se selecciona **propiedades>uso compartido>compartir**, se desplegará un menú de selección de usuario, y se escribirá el ID del usuario que se estableció en el AD, en la parte derecha se muestra los permisos si es solo lectura(solo podrá observar la documentación) o lectura y escritura (podrá alterar la documentación).

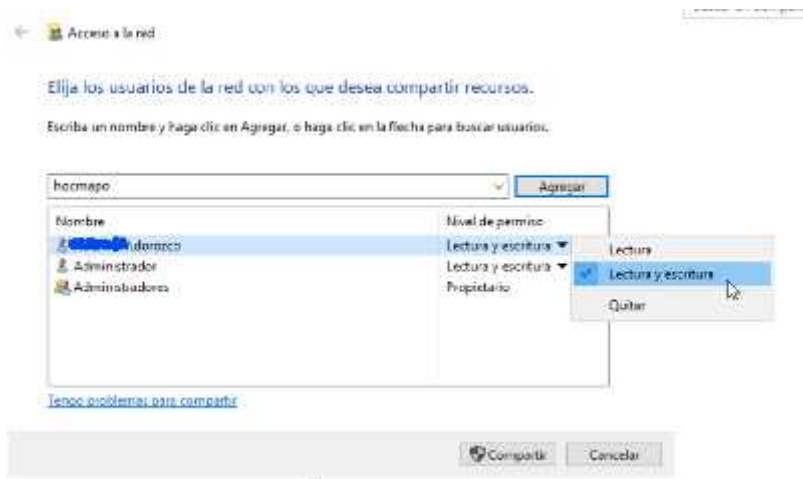


Ilustración 70 Permisos de accesos a información

Fuente: Recursos Propios

Se tiene en cuenta que este proceso se llama SMB (Server Message Block) es un protocolo cliente / servidor que gobierna el acceso a archivos y directorios completos, así como a otros recursos de red como impresoras, enrutadores o interfaces abiertas a la red. El intercambio de información entre los diferentes procesos de un sistema (también conocido como comunicación entre procesos) que consiste en el tráfico en la red si un usuario cliente elimina un archivo por error accidental o a propósito este se perderá completamente.

Para evitar esto crearemos un proceso de respaldo de cada carpeta compartida en un periodo de 7 días hábiles para una recuperación de archivo, la aplicación en su proceso de mantenimiento eliminara los respaldos mayores de los días establecidos, para esto usaremos la aplicación veeam Agent. De igual manera que se descargó la aplicación veeam backup & replication, en la página de web oficial de veeam, se encontrara la opción de descarga, una vez descargada en el dispositivo a instalar en este caso el servidor de archivos, se aceptó Acepte todos los términos y condiciones se procedió a la instalación, es sencilla y finalizará automáticamente.

En las opciones de aplicación veeam mostrará una opción de crear nuevo trabajo, Se abrirá el asistente posteriormente se debe especificar el nombre del trabajo y se acciona **Siguiente**. Después de eso, se seleccionó el tipo de copia de seguridad mostrando 3 opciones, las cuales son; respaldo completo (todo el equipo), volumen (respaldo de discos únicamente), Archivos (solo selección de carpetas específicas y sub carpetas).

Conforme a los requerimientos propuesto en este documento se estableció la opción 3 archivo, se desplegará un sub menú, para seleccionar la ruta que carpeta respaldar, en ese apartado se seleccionó todas las carpetas compartidas.

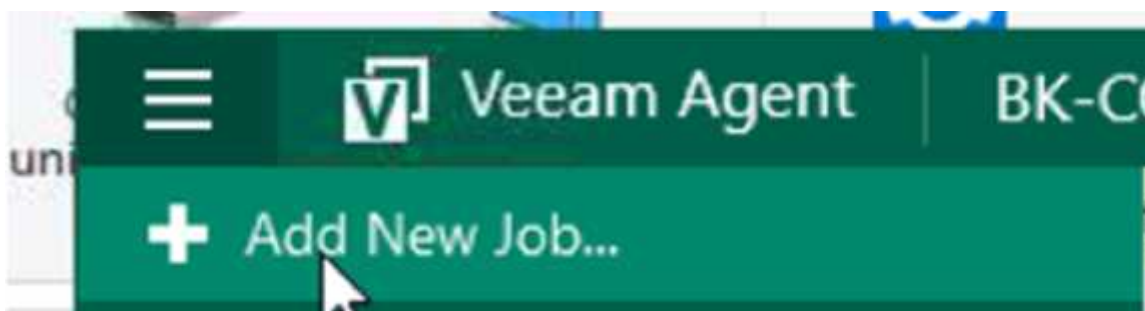


Ilustración 71 Selección de nuevo trabajo

Fuente: Recursos Propios

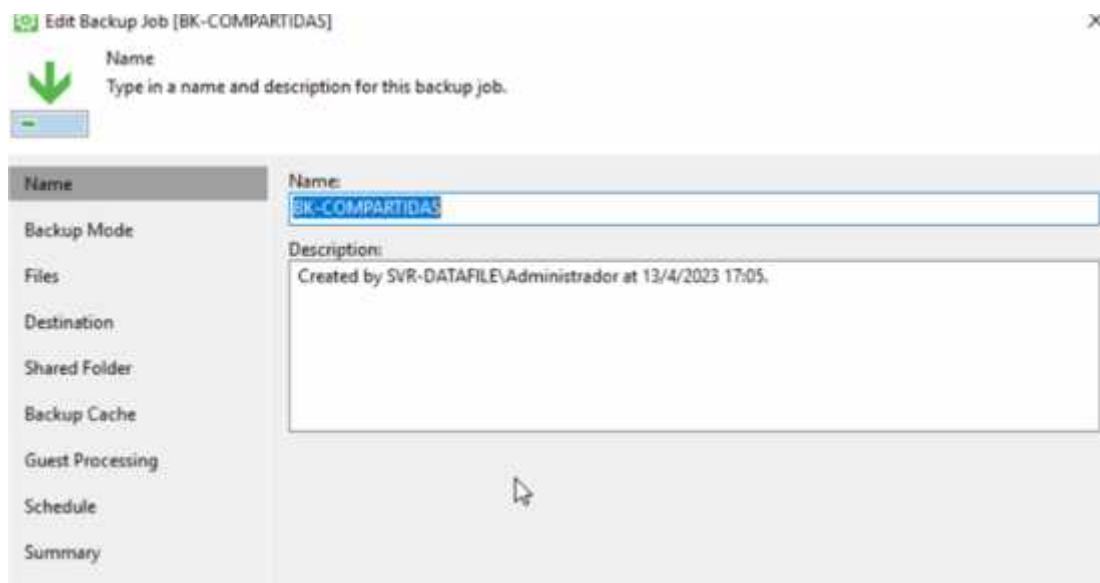


Ilustración 72 creación de trabajo de respaldo 1.1

Fuente: Recursos Propios

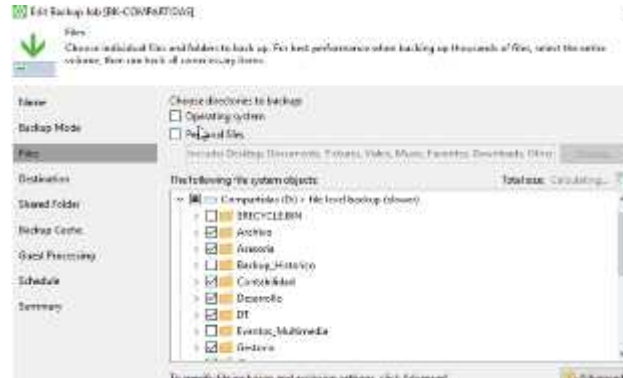
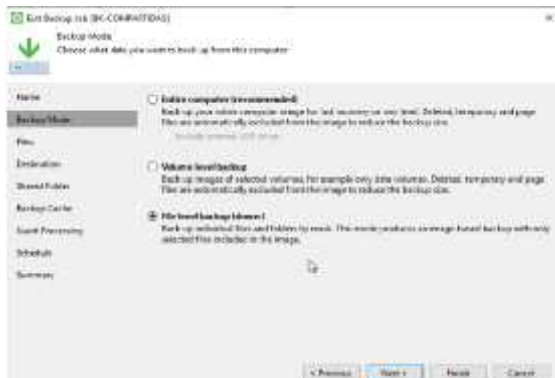


Ilustración 73 creación de trabajo de respaldo1.2

Fuente: Recursos Propios

posteriormente se escogió como los datos se respaldaría ya que será en el mismo servidor se optó la opción almacenamiento local, para finalizar se escoge el destino y bajo del destino se muestra una opción de días de respaldo se dejó por defecto 7 días. Luego de esto la finalización del trabajo será automático y se ejecutará.

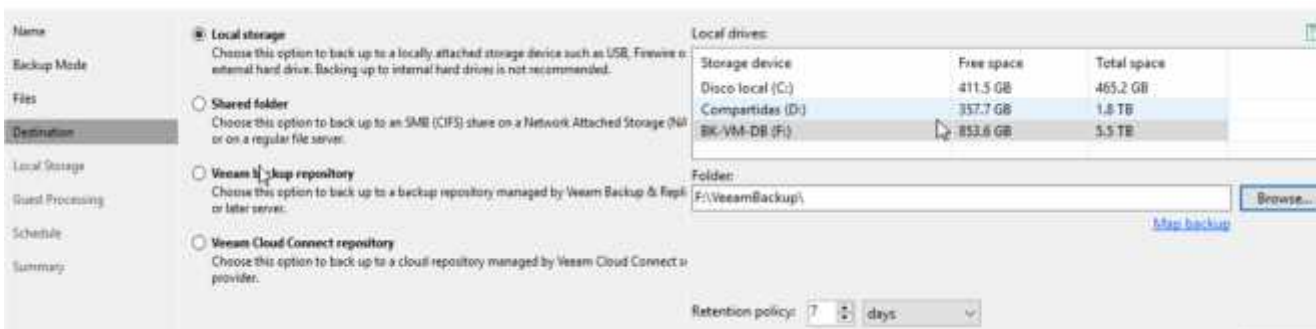


Ilustración 74. creación de trabajo de respaldo 1.3

Fuente: Recursos Propios

Al ejecutarse el programa podemos observar en la aplicación unas barras verdes indicando un 100% una vez finalizado el trabajo se podrá comprobar yendo a la carpeta de destino seleccionada para validar los datos creado.

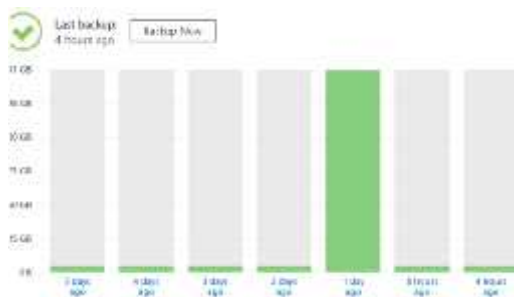


Ilustración 76 creación de trabajo de respaldo 1.4

Fuente: Recursos Propios



Ilustración 75. creación de trabajo de respaldo 1.5

Fuente: Recursos Propios

Configuración de dispositivo wifi AP

Hoy en día es importante una conectividad de internet en cada dispositivo móviles o fijos como sea posible ya sea por comunicación, uso de aplicaciones contenida en la red interna de la empresa además de un medio alámbrico, se brindó una solución inalámbrica por medio del dispositivo profesional Ubiquiti Ap-lite

Para la configuración de este dispositivo se descargó su software basado en java en su página oficial no es necesario hacer ningún tipo de cuenta para poder acceder de este recurso gratuito, pero si es necesario instalar previamente java SDK V11, las instalaciones de ambos recursos son automatizadas y predeterminada de aceptar términos y condición y continuar siguiente hasta finalizar.

El Equipo AP tiene múltiples funciones tales como la facilidad de crear vlan interna de él y propagación, protección de analizadores de IP (Evita que programas maliciosos conozca dispositivos en la red), genera hasta 5 redes de Wi-Fi diferentes, soporte de red troncal en su entrada principal.

Conociendo estas ventajas, se procedió a colocar el dispositivo AP en medio del edificio y haciendo mediciones de cobertura por analizadores de estabilidad de red gratuitos, se llegó a la conclusión que los 100 metros de cobertura que especifica el dispositivo cubría de forma eficiente todo el edificio.

En la aplicación instalada en el servidor AD, Ubiquiti nos pedirá crear un usuario y contraseña local para acceder a las configuraciones del dispositivo, posteriormente nos aparecerá el dispositivo en la red, al seleccionarlo observaremos las configuraciones red del dispositivo cambiaremos estos parámetros a una IP estática.

Al finalizar los ajustes de parámetros del dispositivo AP se podrá observar que el dispositivo fue adoptado, en la parte de configuraciones del dispositivo indica una serie de parámetros anterior mente mencionada como creación de red wifi 2.4 G O 5G, como solo queremos una red wifi que funciones como distribución de nuestra red se seleccionó la opción bridge, asignado le un nombre red llamado “Operativa” tomando en cuenta que toda el segmento de red será el mismo del principal y las políticas controladas por el Fortinet.

En el caso de la red llamada operativa solo se conectarán equipo de la empresa y usuarios como invitados o personal propio de la empresa, pero con dispositivos personales se creará una sub red dentro del mismo Ubiquiti llamada Invitados esta no está en estado Bridge estará en otro segmento de red que mismo dispositivo AP creará el enrutamiento del segmento interno con el de invitados.

En caso de la red de invitados tendrá el segmento 192.168.1.0/24, para las mismas políticas de restricciones se mantendrán igual, sin acceso a redes sociales o contenido indebido, todo esto se seguirá administrando desde el router principal que es Fortinet como se observó en la creación y validación de las políticas.

Topología Lógica

En siguiente ilustración se podrá apreciar gráficamente las cómo está diseñada la red LAN sobre la topología estrella lógicamente, donde dispositivos se conectan a través de un switch central. Esta configuración proporciona múltiples direcciones y IP y como estas interconectas entre sí para adecuada la comunicación proporcionando tanto como, numero de segmento, referencia de servicio y características de la red, entorno virtualizado de Windows Server, donde se ejecuta Active Directory para la gestión centralizada de usuarios, grupos y políticas de seguridad.

Además, la infraestructura incluye dos servicios dedicados: uno para la administración de archivos, proporcionando un almacenamiento centralizado y seguro para los datos de la empresa, y otro para realizar copias de seguridad y garantizar la disponibilidad de la información crítica en caso de fallos del sistema.

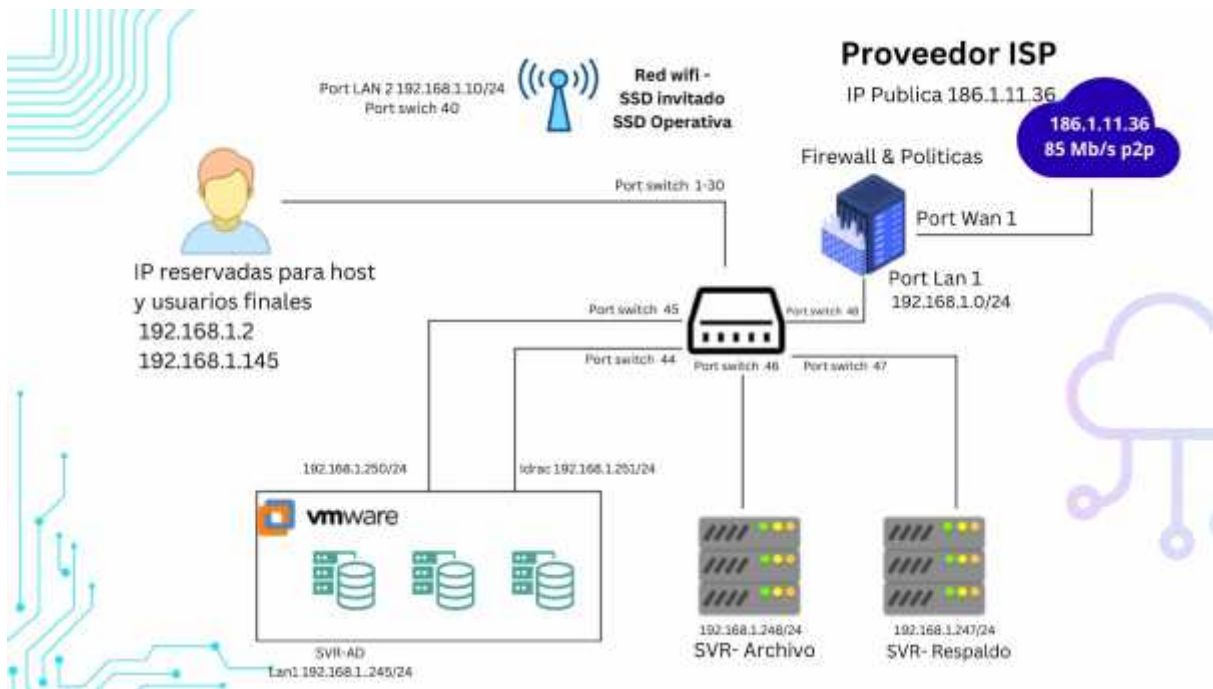


Ilustración 77: Diseño de red LAN con topología lógica estrella.

Fuente: Recursos propios

X. Recomendaciones

Al implementar un sistema de levantamiento de red local en una sociedad, es crucial tener en cuenta varios factores para garantizar su eficacia y beneficios. Aquí algunas recomendaciones:

1. **Planificación y diseño:** Antes de implementar el sistema, realiza una planificación detallada y un diseño de la red local, teniendo en cuenta las necesidades específicas de la sociedad, como el tamaño, la ubicación geográfica, y los requisitos de seguridad.
2. **Escalabilidad:** Asegúrate de que el sistema sea escalable para adaptarse al crecimiento futuro de la sociedad y sus necesidades de conectividad.
3. **Seguridad:** Implementa medidas de seguridad robustas para proteger la red local contra amenazas cibernéticas, incluyendo firewalls, sistemas de detección de intrusiones, y políticas de acceso adecuadas.
4. **Fiabilidad y disponibilidad:** Diseña la red para garantizar la fiabilidad y disponibilidad del servicio, implementando redundancia en los puntos críticos y configuraciones de alta disponibilidad cuando sea necesario.
5. **Gestión centralizada:** Utiliza herramientas de gestión centralizada para facilitar la administración y monitorización de la red, permitiendo una rápida detección y resolución de problemas.

6. Capacitación y concienciación: Proporciona formación adecuada a los administradores de red y usuarios finales sobre el uso seguro y eficiente de la red, así como sobre los procedimientos de respuesta ante incidentes de seguridad.
7. Respaldo y recuperación: Implementa políticas de respaldo y recuperación de datos para proteger la integridad de la información almacenada en la red local y garantizar la continuidad del negocio en caso de fallos o desastres.
8. Monitoreo y análisis de rendimiento: Utiliza herramientas de monitoreo de red para realizar un seguimiento del rendimiento y la utilización de la red, identificando posibles cuellos de botella o problemas de rendimiento que puedan afectar la experiencia del usuario.
9. Cumplimiento normativo: Asegúrate de que la implementación del sistema cumpla con los requisitos legales y regulatorios aplicables, especialmente en lo que respecta a la protección de datos y la privacidad de la información.
10. Evaluación continua: Realiza evaluaciones periódicas del sistema para identificar áreas de mejora y asegurarte de que sigue cumpliendo con los objetivos y necesidades de la sociedad.

Al seguir estas recomendaciones, podrás implementar un sistema de levantamiento de red local que proporcione conectividad segura, confiable y eficiente para la sociedad.

XI. Conclusiones

La implementación de la red LAN ha cumplido con el objetivo general de establecer una infraestructura estándar segura para la comunicación y la transferencia de datos dentro de la organización. Como resultado, se ha mejorado notablemente la conectividad y el intercambio de información interdepartamental, facilitando así una gestión más integrada y eficiente. La capacidad de la red para soportar la creciente demanda de datos refleja la efectividad de la infraestructura en responder a las necesidades operativas de la organización, así como su capacidad para proteger la información crítica.

La virtualización de servidores ha sido una estrategia clave, permitiendo una administración de recursos informáticos significativamente más eficiente. Esta flexibilidad y escalabilidad subrayan la capacidad de la organización para adaptarse rápidamente a las necesidades cambiantes del sector farmacéutico, optimizando el rendimiento y reduciendo costos operativos. La infraestructura implementada, basada en Linux, promete una continua adaptación y mejora de los recursos tecnológicos. Además, la seguridad de los datos se ha incrementado con la implementación de un servidor de Active Directory (AD), que ha reforzado la integridad y confidencialidad de la información sensible farmacéutica al administrar efectivamente los accesos de usuarios.

Finalmente, la implementación de la red LAN y la virtualización de servidores han mejorado la eficiencia operativa, ya que han sentado una base firme para la innovación tecnológica continua en la industria farmacéutica. Este proyecto ha establecido los pilares para una operación más ágil, apoyando el desarrollo y crecimiento sostenible de la organización en un mercado competitivo. De esta manera, se ha alcanzado el propósito de este trabajo, evidenciando cómo una infraestructura tecnológica robusta y segura es esencial para el avance y la adaptabilidad de una organización en el dinámico sector farmacéutico.

XII. Referencias bibliográficas

Bibliografía

1. González, L. (2022). *Introducción a las Redes* (1st ed.).
2. Millan Esteller, J. M. (2012). *Instalaciones de megafonía y sonorización*. Ediciones Paraninfo, S.A.
3. Pressman, R. S. (2010). *Ingeniería de Software* (7th ed.). Editorial McGraw-Hill. 9786071503145
4. Juan José Yunquera Torres, Proyecto Final de Carrera “Diseño de una red WIFI para la E.S.I.”. Universidad de Sevilla, 2005.
5. F. Brunetti, J. Moreno, R. Ceres, L. Calderón, J.L. Pons, XXV Jornadas de
6. Automática “Redes inalámbricas de área personal al servicio de los discapacitados y de las personas mayores”. Ciudad Real, 2004.
7. Cabrera, J. L., & Santos González, M. (2014). *Sistemas Operativos en red*. Editorial RA-MA. <https://elibro.net/ereader/unicaragua/62454>
8. Castillo Montenegro, E. J., & Tercero Mendoza, N. A. (2016, octubre). *Evaluación de la infraestructura de red LAN, bajo la norma ISO/IEC 27002:2013, en la Alcaldía Municipal de San Ramón, Matagalpa, primer semestre 2016*. <https://repositorio.unan.edu.ni/4783/1/5767.pdf>
9. Cisco Systems. (2011). *Cisco CCNA Exploration 4.0 | Módulo 3: Conmutación y Conexión Inalámbrica de Lan* (Vol. 3). <https://www.elsolucionario.org/cisco-ccna-exploration-4-0-cisco-systems-modulo-3-conmutacion-y-conexion-inalambrica-de-lan/>
10. Etecé. (2021, Julio 16). *Sistema Operativo*. Concepto. <https://concepto.de/sistema-operativo/#ixzz7bUCkLiBc>

11. Etecé. (2021, agosto 5). *Fibra Óptica*. Concepto. <https://concepto.de/fibra-optica/#ixzz7bTwTrPTo>,
12. Hallberg, B. (2007). *FUNDAMENTOS DE REDES* (4th ed.). Editorial McGraw-Hill. https://www.academia.edu/11018001/Fundamentos_De_Redres_4ta_Edicion_Bruce_Hallberg
13. Hernández, M. (2012-2013). *Introducción a redes*. <https://www.fcca.umich.mx/descargas/apuntes/academia%20de%20informatica/Introducci%C3%B3n%20a%20Redes%20%20M.H.B/APUNTES%20INTRODUCCION%20A%20REDES/INTRODUCCION%20A%20REDES.pdf>
14. Olifer, N., & Olifer, V. (2009). *Redes de computadoras: principios, tecnología y protocolos para el diseño de redes* (7th ed.). Editorial McGraw-Hill. 9701072499, 9789701072493
15. Olivares Sáez, C. (2016). *1 NIC/MAU (Tarjeta de red) "Network Interface Card"*. DocPlayer. <https://docplayer.es/10897623-1-nic-mau-tarjeta-de-red-network-interface-card.html>
16. Rodríguez, F. F., Leonardo, R. M., Aquino, Y. M., & González Tejada, E. (2018). *Historia y Origen de las Redes*. Redes Informáticas. <http://redesinformaticas4to.blogspot.com/p/origen.html>
17. Sánchez Lasaosa, S. (2015). *Elementos de una Red de Área Local*. <https://silviasanchezlasaosa.wordpress.com/2015/04/10/elementos-de-una-red-de-are-local/>
18. Sánchez López, M. (2015-2017). *I.E.S. Miguel Sánchez López C.F.G.M. Sistemas Microinformáticos y Redes. Módulo Profesional Sistemas Operativos en Red. - PDF Free Download*. DocPlayer. <https://docplayer.es/203873854-I-e-s-miguel-sanchez->

lopez-c-f-g-m-sistemas-microinformaticos-y-redes-modulo-profesional-sistemas-operativos-en-red.html

19. Stallings, W. (2004). *Comunicaciones y Redes de Computadoras* (7th ed.). Editorial ALHAMBRA. <https://richardfong.files.wordpress.com/2011/02/stallings-william-comunicaciones-y-redes-de-computadores.pdf>
20. Tanenbaum, A. S. (2008). *Sistemas Operativos Distribuidos* (2nd ed.). <https://maritzaescobar.files.wordpress.com/2010/08/prentice-hall-tanenbaum-sistemas-operativos-distribuidos.pdf>
21. Stallings, W. (2017). *Redes de computadoras: Un enfoque descendente*. Pearson Educación.
22. Comer, D. E. (2018). *Redes de computadoras y de Internets*. Pearson Educación
23. Kurose, J. F., & Ross, K. W. (2020). *Redes de computadoras: Un enfoque superior hacia abajo*. Pearson Educación.
24. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2019). *Firewalls y seguridad en Internet: Protección de redes en el ciberespacio*. Addison-Wesley.
25. Tanenbaum, A. S., & Wetherall, D. J. (2011). *Redes de computadoras*. Pearson Educación.
26. Laudon, K. C., & Laudon, J. P. (2016). *Sistemas de información gerencial*. Pearson Educación.
27. Nadeau, T. D., & Gray, K. (2013). *SDN: Software Defined Networks*. O'Reilly Media, Inc.
28. ISACA. (2019). *COBIT 2019*.
29. National Fire Protection Association. (2013). *NFPA 75: Standard for the Fire Protection of Information Technology Equipment*. NFPA.

30. ISO. (2018). *ISO/IEC 20000-1:2018 Information technology — Service management — Part 1: Service management system requirements*. International Organization for Standardization.
31. Uptime Institute. (2014). *Tier Standard: Topology*. Uptime Institute.
32. American Society of Heating, Refrigerating and Air-Conditioning Engineers. (2011). *Thermal Guidelines for Data Processing Environments*. ASHRAE.
33. IEEE. (2007). *IEEE Standard 493-2007 (IEEE Gold Book): Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*. Institute of Electrical and Electronics Engineers.
34. Center for Internet Security. (2021). *CIS Controls v8*.

ANEXOS

Cantidad	Descripción	Precio unitario	Importe
1	Rack 7ft en aluminio color negro oficina	\$1,200.00	\$1,200.00
1	Organizador Horizontal 2ur sencillo	\$10.00	\$10.00
2	Bandeja para Rack de 19x10	\$50.00	\$100.00
12	Canaleta color blanco 2.5mts 3vias	\$57.43	\$689.16
1	Panel de conexión 48p	\$387.93	\$387.93
19	Placa keyston de 2 cavidades	\$15.51	\$294.69
19	Caja universal plástico color blanco	\$25.99	\$493.81
25	Jack RJ 45 CAT6	\$19.82	\$695.69
1	Pinza ponchadora de impacto para Jack RJ45	\$298.82	\$298.82
55	Metros Cable UTP cat 6 negro exterior	\$19.82	\$1,100.82
1	Switch de red 48 puertos TP Link	\$1,853.45	\$1,853.45
1	Traslado de material	\$80.50	\$80.5
10	Caja universal plástico color blanco	\$11.59	\$115.90
5	Canaleta color blanco 2.5mts 3vias	\$65.43	\$327.15
1	Servidores Dell PowerEdge R430	\$4,800	\$4,800
1	Regleta servidor 8 puertos	\$30	\$30
1	Servidore torre HP Prolian	\$1,500	\$1,500
1	Ubiquiti AP-LITE	\$110	\$110
5	Jack RJ45 CAT 6	\$1	\$8
2	Baterías APS 3,000KVA	\$1,400	\$2,800
2	Tapas ciegas plas	\$5.00	\$10.00
2	canaleta color blanco 1via	\$5.00	\$10.00
1	broca 3/8	\$7.00	\$7.00
1	PZ broca 12x5/16	\$6.00	\$6.00
1	broca 5/16	\$7.00	\$7.00
2	pza. broca 1/4	\$6.00	\$6.00
1	Servicio de Internet y fortinet (Mensual)	\$400.00	\$400.00
3	Licencias de Window server	\$80.00	\$240.00
Total			\$17,581.92

Tabla 1: Gastos del proyecto

Fuente: Recursos Propios