ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

AUTOMATIZACIÓN DE REDES

AUTOMATIZACIÓN DE LAS TI

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TELECOMUNICACIONES

JAIME DARÍO OROSCO OROZCO

jaime.orosco@epn.edu.ec

DIRECTOR: CARLOS ALFONSO HERRERA MUÑOZ

carlos.herrera@epn.edu.ec

DMQ, abril 2023

CERTIFICACIONES

Yo, JAIME DARÍO OROSCO OROZCO declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

JAIME DARÍO OROSCO OROZCO

Certifico que el presente trabajo de integración curricular fue desarrollado por JAIME DARÍO OROSCO OROZCO, bajo mi supervisión.

CARLOS ALFONSO HERRERA MUÑOZ
DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

JAIME DARÍO OROSCO OROZCO

CARLOS ALFONSO HERRERA MUÑOZ

DEDICATORIA

Este trabajo va dedicado a mis padres, ellos son mi razón para seguir. Los dos han estado ahí cada vez que los necesitaba, tanto en el apoyo económico como emocional, sin ellos no estaría escribiendo estas líneas, los amo.

AGRADECIMIENTO

Agradezco a Dios por guiar mi camino y permitirme continuar siempre adelante y mejorando cada día, a mis padres Cristina Orozco y Jaime Orosco por estar ahí para mí a lo largo de mi carrera, a mi hermana Vanessa por ser una amiga y ayudarme a crecer como persona. A mi segunda familia, mis amigos que han sabido apoyarme y a quienes aprecio bastante, David, AnGeLiTa, Maritza, Alexander, Fernando, Christopher, Jeff, Jhon y Jandry. A mi tutor el Ing. Carlos Herrera por sus consejos, conocimiento y ser una guía para la realización de este trabajo. Y finalmente agradezco a Mayra Alejandra Pazmiño por su paciencia y siempre solucionar mis dudas con una sonrisa, desde que ingresé a la Universidad hasta la entrega de documentos finales.

ÍNDICE DE CONTENIDO

RESUMEN

La Automatización de las Tecnologías de Información (TI) permite digitalizar industrias completas, logra la conectividad entre los usuarios y brinda grandes beneficios para quienes la implementan. Varios fabricantes conocidos alrededor del mundo ofrecen sus servicios para automatizar el entorno de TI y usan tecnologías como el Aprendizaje Automático (ML) y la Inteligencia Artificial (IA).

En este trabajo se realiza una revisión de dos soluciones de Automatización de las TI que permite tener mayor claridad para implementar alguna de ellas en una red corporativa, así como dos de las herramientas más usadas cada una con distintos métodos para automatizar los servicios de TI, y la Arquitectura DNA de Cisco como una gran opción para digitalizar la empresa con innovaciones de hardware y software que le permiten enfrentar los desafíos del mundo actual.

Este trabajo contiene 3 capítulos, en el primer capítulo se presenta la definición, estructura y gestión de las TI, así como los beneficios que se obtienen al automatizar el entorno de TI, en el segundo capítulo se describen 2 soluciones y 2 herramientas de automatización de las TI, y se describe la Arquitectura DNA de Cisco principalmente sus innovaciones y breve funcionamiento de su estructura, en el tercer capítulo se presentan los resultados obtenidos como una comparativa entre los temas abordados en el capítulo 2.

PALABRAS CLAVE: Automatización, TI (Tecnologías de Información), DNA (Arquitectura de Red Digital).

ABSTRACT

Information Technology Automation allows the digitization of entire industries, achieves connectivity between users, and greatly benefits those who implement it. Several well-known manufacturers worldwide offer their services to automate the IT environment and use technologies such as Machine Learning (ML) and Artificial Intelligence (AI).

This document reviews two IT Automation solutions that allow greater clarity to implement any of them in a corporate network, as well as two of the most used tools, each with different methods to Automate IT services, and the Cisco DNA Architecture as a great option to digitize the company with hardware and software innovations that allow it to face the challenges of today's world.

This work contains 3 chapters, in the first chapter the definition, structure, and IT management are presented, as well as the benefits obtained by automating the IT environment, in the second chapter, 2 IT Solutions and 2 IT Automation tools are described. And the Cisco DNA Architecture is described mainly by its innovations and a brief structure operation, in the third chapter the results obtained are presented as a comparison between the topics addressed in chapter 2.

KEYWORDS: Automation, IT (Information Technology), DNA (Digital Network Architecture).

1 INTRODUCCIÓN

Las Tecnologías de Información hacen referencia a un conjunto de herramientas tanto de hardware como software utilizado para procesar, almacenar, crear o transmitir información. Las TI tienen su apogeo en la década de los 80 en donde áreas como la informática, la electrónica y las telecomunicaciones comenzaron a tener un mayor espacio para su desarrollo [1].

Por su parte la Automatización se define como el proceso mediante el cual se consigue realizar tareas con muy poca o ninguna intervención humana. De modo que la automatización de las TI se encarga de crear sistemas para que sustituyan los procesos de manera repetida sin necesidad de que el ser humano intervenga. Con ayuda de la Automatización de las TI se puede aportar al desarrollo de la empresa, dándole herramientas necesarias para la escalabilidad y ahorro de costes, permitiendo que el equipo de TI se encargue de elaborar planes estratégicos para mejorar el rendimiento y eficacia de la empresa, eliminando o minimizando errores humanos y mejorando la seguridad [2].

Es sustancial rescatar que al Automatizar el entorno de las TI se puede lograr grandes progresos para la empresa como crear modelos de seguridad de red, configuración de aplicaciones, disponibilidad del sistema, mejorar el rendimiento etc. La Automatización de las TI asiste a las empresas en su transformación digital, ya que mediante esta se puede adaptar, modificar y gestionar la infraestructura de TI así como los demás procesos existentes dentro de la empresa, el objetivo es que las actividades requeridas sean realizadas de manera eficiente y rápida, ahorrando recursos como tiempo y dinero [3].

Las tecnologías como la Inteligencia Artificial (IA) y Aprendizaje Automático (ML) son las que hacen posible los procesos de Automatización de TI, mediante un lenguaje de programación sencillo pero eficaz como Python se pueden lograr grandes resultados al ver reducida la carga de trabajo manual que realizan los centros de datos, y Automatizar la nube entre otras aplicaciones relevantes para el desarrollo de la empresa [4].

El presente trabajo se enfoca en la Automatización de las TI, se revisan dos soluciones planteadas, 2 herramientas utilizadas y se presenta la Arquitectura DNA de Cisco, su infraestructura e innovaciones, para lo cual ha sido necesario recopilar gran cantidad de información de empresas dedicadas al sector como Fortinet, Cisco, Juniper Networks, Dell SonicWall, Huawei, etc. En donde se puede evidenciar el gran avance tecnológico que ha tenido el sector de las Telecomunicaciones y redes de información.

1.1 OBJETIVO GENERAL

Estudiar la automatización de las TI en base a la arquitectura DNA de Cisco.

1.2 OBJETIVOS ESPECÍFICOS

1. Estudiar dos alternativas de soluciones de Automatización de las TI.
2. Estudiar las características de las herramientas de Automatización de las TI.
3. Describir las características de la arquitectura DNA de Cisco.

1.3 ALCANCE

La automatización de las TI nos permite gestionar dispositivos de red de manera automática, mejorando la eficiencia y reduciendo los gastos operativos y errores humanos. En el siguiente documento se implementan 3 fases.

1.3.1 FASE DE PLANTEAMIENTO

Estudiar dos alternativas de soluciones de automatización de las TI, conocer las diferencias entre ellas y sus aplicaciones.

Describir dos herramientas usadas para la automatización de las TI, características, infraestructura y configuraciones requeridas para su implementación.

1.3.2 FASE DE IMPLEMENTACIÓN

En la arquitectura DNA se describirá sus funciones principales, características y beneficios e innovaciones que permiten la automatización de las TI.

1.3.3 FASE DE RESULTADOS

Se presentará la comparación entre las soluciones de TI y las herramientas de automatización estudiadas en la fase de planteamiento, así como un análisis de la Arquitectura DNA de Cisco.

1.4 MARCO TEÓRICO

Con el pasar de los días la tecnología avanza, y las grandes y pequeñas empresas se ven en la necesidad de acelerar la transformación digital y de esta manera proporcionar una nueva experiencia a sus usuarios ofreciendo un mayor valor de personalización, conveniencia y satisfacción.

Para entender el proceso que se lleva a cabo y como se usan las tecnologías de información es necesario tener en cuenta varios conceptos básicos, pero de vital importancia para comprender esta temática.

1.4.1 DEFINICIÓN DE LAS TI

Las TI reciben este nombre por primera vez por la revista de Harvard Business Review (HBR) a mediados del siglo XX con la finalidad de distinguir las máquinas creadas especialmente para realizar ciertas funciones, y aquellas que eran usadas de manera general por la comunidad [5].

Las TI se definen también como una combinación de métodos y medios que ayudan a gestionar procesar y transmitir información en diferentes maneras ya sea como voz, video, texto, imagen, entre otros [5].

Junto con la transformación digital, aparecieron nuevas tecnologías, herramientas y términos que fueron dados a conocer como la automatización de las TI, este término hace referencia al proceso para crear sistemas y software que realizan procesos repetitivos y evitan la intervención humana, de tal manera que se acelere la infraestructura de TI, aporte escalabilidad, se reduzcan los errores humanos, exista mayor seguridad, se agilice el proceso y fundamentalmente represente un ahorro de tiempo y dinero [6].

1.4.2 ESTRUCTURA DE LAS TI

Para que el departamento de TI funcione de manera adecuada se deben cumplir tres pilares fundamentales que son:

Administración: Esta área es la encargada de la supervisión, implementación y funcionamiento del entorno de TI, esto incluye las aplicaciones, los sistemas, las redes etc. Los administradores también realizan otras tareas como actualizaciones de sistema operativo o software que lo requiera, capacitaciones, administración de datos y licencias así como el cumplimiento de los procesos comerciales [5].

Soporte: El equipo de soporte de TI es el encargado de dar solución a las problemáticas presentadas tanto con los equipos físicos como con el sistema operativo y aplicaciones, sus funciones también incluyen la gestión de activos del departamento, colaboran con la adquisición y manejo de datos, ayudan en el análisis de registros y cumplen con las normativas de soporte establecidos por la entidad [5].

Aplicaciones: Las aplicaciones usadas por los profesionales de TI son las que adquieren la información que posteriormente será analizada, éstas pueden provenir de terceros o desarrolladores de la misma empresa, las aplicaciones pueden ser implementadas con diversos lenguajes de programación y ser integradas con otras aplicaciones para mejorar su rendimiento. Los desarrolladores del departamento de TI implementan y monitorean sus aplicaciones para obtener los resultados deseados [5].

1.4.3 INFRAESTRUCTURA DE TI

Este término hace referencia a los elementos de una red como tal, que pueden ser tanto físicos como virtuales, puede ser implementado en una nube conocido como ***cloud computing***, o en las instalaciones de la compañía. El centro de datos que incluyen equipos como enrutadores, conmutadores, computadores, el cableado, el sistema operativo que usa, las aplicaciones, servidores etc [7].

En la Figura 1.1, se presenta un ejemplo de Infraestructura de las TI.

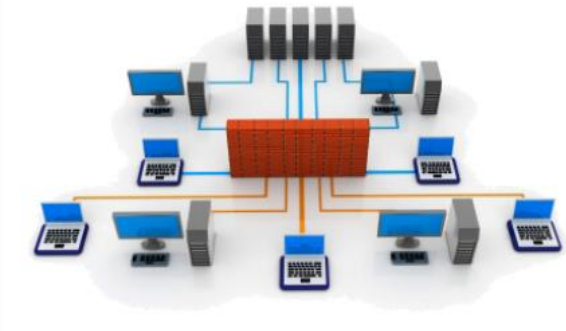


Figura 1.1. Infraestructura de las TI [8].

Los elementos que componen la Infraestructura de TI son utilizados para brindar servicios y soluciones de TI, existen 3 tipos de infraestructuras conocidas que son:

Infraestructura de TI tradicional: En este tipo de infraestructura, las empresas son dueñas de todos los elementos que la componen tanto en hardware como software, es decir los centros de datos, servidores, instalaciones, sistema de seguridad, sistema de almacenamiento, aplicaciones entre otros. Su funcionamiento se considera costoso ya que

contiene gran cantidad de equipos físicos y consumo de energía eléctrica, así como del espacio requerido para mantenerlo en óptimas condiciones [9].

Infraestructura de TI en la nube: En este tipo de infraestructura, las empresas tienen sus recursos de hardware y software recopilados en la nube esto incluye la capacidad de almacenamiento, de red y procesamiento, así como de una interfaz o puerto para que los usuarios puedan acceder sin inconvenientes a estos recursos virtuales. Este tipo de infraestructura ofrece una mayor escalabilidad, reducción de costos, y en cuanto a su funcionamiento es el mismo que el de una infraestructura física o tradicional [10].

Infraestructura de TI Hyperconvergente: En este tipo de infraestructura se unifican los dos conceptos anteriores, ya que se mantienen los recursos físicos de una infraestructura física, pero también se cuenta con los recursos virtualizados, se puede contar con una nube privada o híbrida, mejora notablemente la escalabilidad ya que permite una amplia carga de trabajo, además de requerir menor tiempo para su gestión e implementación.

En la Figura 1.2, se observa el diagrama de representación de la Infraestructura de TI Tradicional y Virtual.

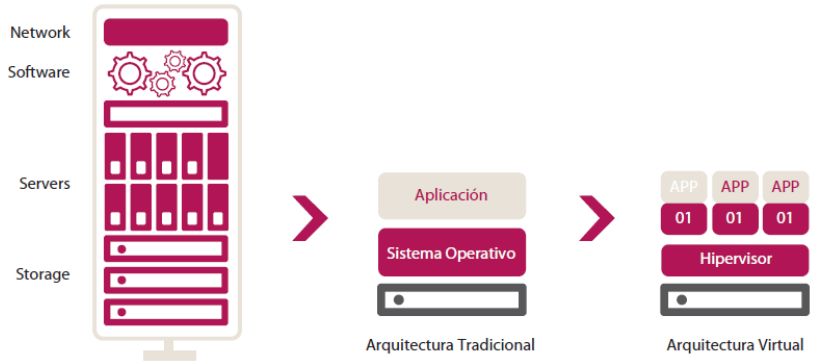


Figura 1.2. Infraestructura de TI Tradicional y Virtual [11].

Virtualización: Se conoce como virtualización a la creación mediante software que se utiliza para recrear un entorno o un recurso físico, tecnológico o de red, con el objetivo de optimizar los recursos de manera que en la empresa se requieran menos equipos físicos o de hardware y consecuentemente represente un ahorro para la empresa, aumentando la productividad del departamento de TI, teniendo alta disponibilidad de las aplicaciones y mejorando la capacidad de respuesta a los problemas suscitados [12].

1.4.4 SEGURIDAD

Se entiende como seguridad al conjunto de procedimientos y normas con los cuales se debe garantizar los pilares básicos como la confidencialidad, integridad, autenticidad y disponibilidad de la información. Hay que tener en cuenta que de tal manera que avanza la tecnología, avanzan los ataques cibernéticos, por lo que estar preparado para dichas amenazas es una necesidad primordial que debe cubrir una empresa o red corporativa y así proteger sus activos [7].

Existen tres niveles de seguridad que se conocen como Seguridad Perimetral, Seguridad de Punto Final y Seguridad de Datos.

Seguridad Perimetral: Este tipo de seguridad se encarga de proteger la red interna, es decir aquellas que provienen del Internet, se compone de dispositivos físicos cuya función es controlar el tráfico que fluye por la red corporativa, poseen herramientas avanzadas para prevenir y controlar amenazas informáticas, así como redes privadas virtuales para mantener comunicación segura con internautas externos [13].

Seguridad de Punto Final: Este tipo de seguridad es el encargado de detectar y eliminar ***malware*** que ya se encuentra en la red, es decir estas amenazas pasaron a la red interna, en muchos de los casos esto se da por acciones de los usuarios al instalar software de dudosa procedencia, páginas no verificadas, o en su defecto el uso de memorias USB previamente contaminadas. Esta seguridad se basa en la instalación de antivirus en el ordenador o servidor que lo requiera [14].

Seguridad de Datos: En este tipo de seguridad la base fundamental es la protección de la propiedad intelectual de la empresa, información valiosa o confidencial que pueda ser filtrada y llegar a manos equivocadas, en esta seguridad de datos se tienen soluciones robustas que trabajan junto con políticas de protección de datos, en redes corporativas se tiene administración centralizada desde donde se manejan estas herramientas y generan los reportes respectivos para la toma de decisiones [15].

1.4.5 BENEFICIOS DE AUTOMATIZACIÓN DE LAS TI

Varios de los equipos de seguridad de redes y TI tienen responsabilidades compartidas, lo que conlleva que el profesional de TI realice muchas funciones a lo largo de su jornada, muchas de estas funciones son procesos manuales que no requieren de experticia, además de esto atienden la necesidad de los usuarios y problemas puntuales para los cuales necesitan tiempo y gran cantidad de conocimiento y experiencia, por lo que

automatizar los procesos resulta vital para la continuidad de la empresa. A continuación, se describen las principales ventajas al automatizar la infraestructura de las TI [16].

Ahorro: Reducir los costos del departamento de TI no hace referencia a invertir menor cantidad de dinero en equipos o minimizar las capacidades del centro de datos, ya que esto repercutiría negativamente en la eficiencia de la empresa. Por el contrario, se trata de un enfoque inteligente ya que al automatizar los procesos se requiere de menos personal, también se puede utilizar software teniendo así soluciones escalables y promoviendo la movilidad operativa. Para citar un ejemplo se tienen los servidores virtuales, almacenamiento de datos, y utilizando de manera inteligente recursos como la virtualización se puede tener un gran impacto en la reducción de costes de la empresa [16].

Productividad: Un segundo gran beneficio que se obtiene al automatizar las TI es el aumento de la productividad. Esto se logra de varias maneras ya sea mediante un software de automatización de tareas el cual se encarga de optimizar lotes de producción, o también al mantener el equipo activo durante toda la jornada, es decir se ahorra el tiempo entre procesos que realiza el equipo electrónico y esto permite al operario de TI continuar con otras funciones específicas y avanzar en su trabajo optimizando los recursos de la empresa [16].

Disponibilidad: Otro gran beneficio que conlleva la automatización de TI es tener alta disponibilidad. Al automatizar los sistemas de guardado y recuperación de datos la empresa se prepara para una posible falla y en caso de que suceda algún imprevisto se pueda continuar con el proceso desde un punto en específico sin necesidad de reiniciar. Estos sistemas son críticos, ya que no contar con equipo de TI por minutos puede representar grandes pérdidas de dinero y perjudicar la reputación de la empresa [16].

Confiabilidad: En el departamento de TI los operarios realizan básicamente dos tipos de funciones, la primera cuya finalidad es el análisis y resolución de problemas a medida que estos surjan, y para esto se requiere de un gran conocimiento y habilidades técnicas. Y el segundo, realizar trabajo manual, presionando botones, guardando copias de seguridad de la información, cargando papel. Estos procesos que para el ser humano pueden volverse tediosos o aburridos y dar cabida a errores que impidan el desarrollo normal de actividades dentro del departamento, pueden ser automatizados de manera segura y confiable. Los sistemas automatizados ayudan a mantener el orden ya que permiten que los procesos sean ejecutados secuencialmente, que los datos a ingresar sean los adecuados y que se realice ***backup*** de la información cada cierto tiempo [16].

Rendimiento: Para que exista una mejora del rendimiento en el departamento de TI se solían implementar soluciones como actualizaciones de hardware o adquirir nuevos equipos, pero esto resulta muy costoso, además que el manejo de equipos sofisticados requieren de un experto en TI para su administración, todos estos inconvenientes se resuelven con la ayuda de un software de automatización, adicionalmente que mejora el rendimiento de los equipos al realizar tareas previamente programables de manera automática [16].

1.4.6 GESTIÓN DE LAS TI

A medida que los recursos de la empresa crecen se vuelve más complejo su administración, por lo cual tener las herramientas necesarias para gestionar los recursos de TI de manera correcta se vuelve una prioridad. A continuación, se presentan 3 herramientas usadas para realizar la gestión de los recursos de TI.

SNMP: Este protocolo de capa aplicación tiene como objetivo el monitorear y gestionar los elementos de la red, es un programa el cual debe ser ejecutado en cada equipo de la infraestructura de TI que se desea gestionar. SNMP contiene el Sistema de Gestión de Red (NMS), cuya función es la de ejecutarse en el servidor y realizar los requerimientos periódicamente para obtener la información [17].

En la Figura 1.3, se observa un ejemplo de Gestión con el Protocolo SNMP.

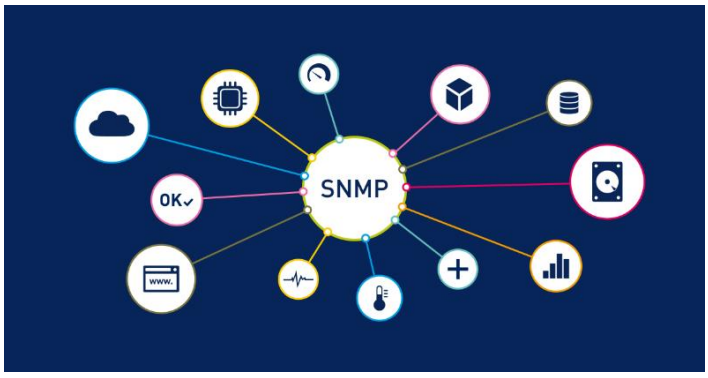


Figura 1.3 Gestión con el Protocolo SNMP [17].

NTA: Analizador de Tráfico de Red (NTA), es una herramienta muy potente para el monitoreo de trafico de red en tiempo real, cuenta con funciones como la gestión de direcciones IP, monitoreo específico de usuarios, aplicaciones, así como informes y alertas personalizables [18].

En la Figura 1.4, se muestra la Interfaz de NTA al capturar tráfico de red.

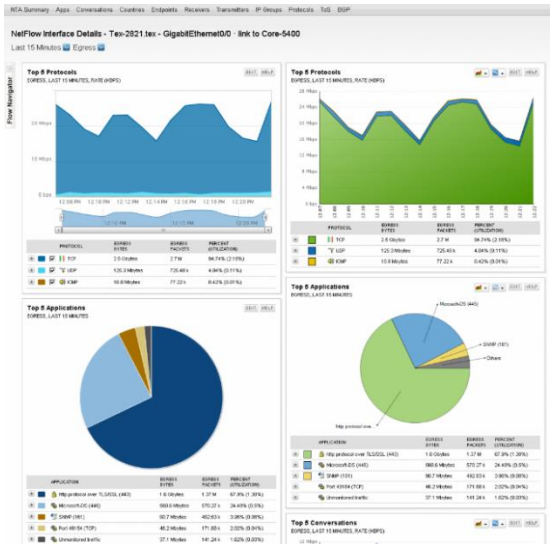


Figura 1.4. Interfaz de la herramienta NTA [19].

SAM: Monitor de aplicaciones y servidores (SAM), es una herramienta especializada en el monitoreo y gestión de aplicaciones, cuenta con notificaciones vía correo electrónico, y reinicio de los servicios de forma automática, tiene la capacidad de monitorear servidores y nubes híbridas, detecta problemas de red que influyen en el rendimiento de la aplicación analizada [20].

En la Figura 1.5, se muestra la herramienta de Gestión SAM.

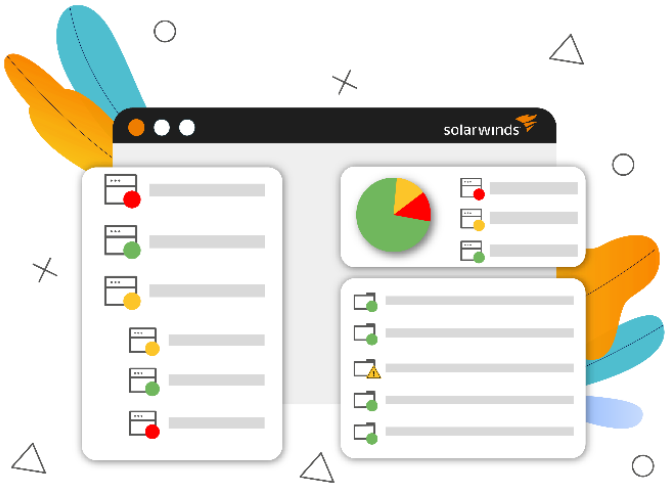


Figura 1.5. Esquema de monitoreo de aplicaciones SAM [20].

2 METODOLOGÍA

2.1 ALTERNATIVAS DE SOLUCIÓN DE AUTOMATIZACIÓN DE LAS TI

Se tienen diversas alternativas que pueden ser usadas para dar solución a las problemáticas presentadas con las nuevas tecnologías de información, entre ellas se pueden mencionar Cisco, Fortinet, Juniper Networks, DELL Technologies, Huawei. A continuación se presenta una breve introducción de cada una de ellas y se describen dos soluciones que en este capítulo han sido consideradas y mediante las cuales se pueden crear planes técnicos y estratégicos optimizando costos y garantizando la escalabilidad y confiabilidad de la información en soluciones integradas [21].

Cisco: Es una empresa fabricante fundada en el año de 1985 y cuyo objetivo es brindar soluciones de red y comunicaciones, también ofrece certificaciones que son necesarias para adquirir los conocimientos desde básicos hasta avanzados en el área de Redes y TI. Entre las principales soluciones que se pueden encontrar en cisco se tienen: Internet de las Cosas, ***Networking***, Seguridad, Software, Movilidad, servicios en la Nube entre otros. En la Figura 2.1, se observan algunas de las soluciones ofrecidas por Cisco [22].

Figura 2.1. Soluciones de TI dentro de Cisco [23].

Fortinet: Esta empresa brinda soluciones de TI, pero con un mayor enfoque en la seguridad de redes, esto debido a que a medida que aumentan las herramientas tecnológicas, también aumentan los ciberataques y las empresas necesitan defenderse de este tipo de amenazas. Cuenta con su propio sistema operativo conocido como FortiOS. Es un proveedor de excelencia y con soluciones innovadoras, dentro de ellas se tienen: Ciberseguridad, Redes empresariales, Seguridad en la Nube, Automatización de Redes entre otros [24].

Juniper: Fundada en 1996, Juniper Networks es una entidad dedicada a resolver problemas de ***Networking***. Su misión es conectar al mundo a través de la tecnología y

brindando servicios de calidad. Tiene una amplia gama de productos como switches, routers, software de gestión, equipos de seguridad, virtualización. También dispone de certificaciones que permiten a las personas capacitarse para administrar equipos Juniper, así como su sistema operativo Junos. Entre las soluciones y servicios que ofrece Juniper se tiene Automatización, Internet de las cosas, Seguridad en la nube, Centro de Datos, Redes definidas por software, entre otros [25].

DELL: Esta compañía es fundada en el año de 1984, empezó dedicándose a la producción y venta de computadoras, a medida que el tiempo transcurre, esta empresa fue expandiéndose a diferentes países y aumentando mayores servicios y productos como soporte de computadores personales, servidores, programas informáticos y proveedor de soluciones de infraestructura de TI. Dentro de las soluciones que ofrece DELL se encuentran la inteligencia artificial, Infraestructura de escritorio virtual, computación de alto rendimiento, Oracle, Microsoft, etc [26].

Huawei: Huawei es fundada en el año de 1987, esta empresa se dedica a desarrollar y proveer equipos de TI con el objetivo de mejorar la infraestructura de TI de sus clientes con ayuda de la digitalización. Cumple con estándares de calidad basados en la norma ISO 9000, ofrece soporte en todos sus productos y una experiencia personalizada, en cuanto a las soluciones de TI que plantea esta empresa se tienen soluciones de seguridad, centro de datos, Agile WAN, Gestión de Redes, Red de Gestión Autónoma (ADN), entre otros [27].

A continuación, se detallan dos soluciones implementadas por la marca Fortinet y Juniper.

2.1.1 FORTINET

Es una empresa que se dedica a la integración de múltiples funciones en una sola plataforma. Se encarga de proveer una seguridad amplia y con un rendimiento elevado en la infraestructura tecnológica de las redes corporativas. Mediante esta plataforma se pueden dar varios servicios como el filtrado web, antivirus, firewalls y control de las aplicaciones existentes [24].

Fortinet funciona bajo el objetivo de mantener segura la red de modo que ésta sea integrada, automática y escalable, previniendo así las amenazas y reduciendo el riesgo de intrusos [24].

Beneficios:

- ✓ Resguardo contra amenazas informáticas.

- ✓ Protección de los datos de la compañía y su propiedad intelectual.
- ✓ Aumentar el rendimiento de los usuarios.
- ✓ Aprovechar de mejor manera los recursos de red y el ancho de banda.
- ✓ Prevenir la pérdida de información relacionada con temas de seguridad.
- ✓ Administración de seguridad centralizada y economización de costos.
- ✓ Asesoramiento técnico y soporte directamente del fabricante.

A continuación, se describen dos de las soluciones usadas por Fortinet para mantener las empresas seguras y con un alto rendimiento tecnológico.

Redes Seguras: Fortinet tiene su enfoque basado en la seguridad de la red mediante una plataforma multiservicio, la cual está impulsada con inteligencia artificial (IA) permitiendo una alta productividad del sector de TI y agradable experiencia del usuario [28].

FortiGate: Este equipo es el componente principal de las redes seguras de Fortinet, tiene su propio sistema operativo el cual es diseñado por Fortinet y se conoce como FortiOS. Además, cuenta con procesadores de seguridad (SPU) lo que permite la convergencia completa de la red y evitan la necesidad de compra de productos de uso específico. A través de FortiGate se tiene servicios como firewalls, puertas de enlace Web seguras (SWG), Redes definidas por Software (SD-WAN), acceso a la red de confianza cero (ZTNA) y Redes inalámbricas 5G, cuenta también con protección contra amenazas en tiempo real [29].

Existen bastantes modelos de equipos FortiGate desde dispositivos de gama baja hasta gama alta debido a las diferentes necesidades de los clientes con lo cual se garantiza que FortiGate se adapte al entorno en el cual es utilizado.

En La Figura 2.2, se muestra el equipo FortiGate 80F.

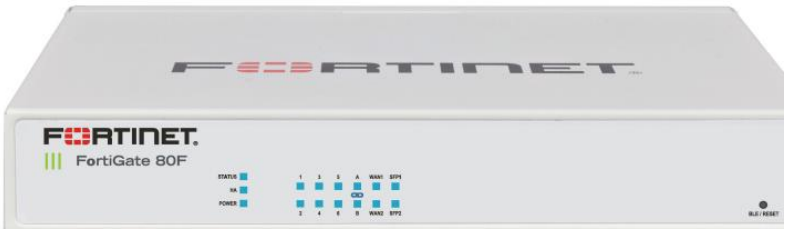


Figura 2.2. FortiGate 80F [30].

En cuanto a los parámetros técnicos que caracterizan a FortiGate 80F se tiene un rendimiento del Sistema de Prevención de Intrusos (IPS) de 1.4 Gbps, rendimiento de

Firewall de 1 Gbps, rendimiento de protección contra amenazas de 900 Mbps, cuenta con 8 puertos GbE, se puede tener hasta 1.5 millones de sesiones concurrentes. Este equipo es de fácil administración ya que todo se realiza a través de su interfaz web sin necesidad de usar comandos y cuenta con una consola de administración para tareas más avanzadas, y está diseñado para alrededor de 100 usuarios [30].

FortiGuard: La manera más eficaz para defenderse ante una amenaza o ataque es interrumpir dicha acción en el mismo instante que se produce. FortiGuard está diseñado para proteger aplicaciones, bloquear o permitir tráfico de red, y un constante análisis en tiempo real que le permite una respuesta ágil e inmediata a las amenazas ya sean conocidas o de día cero. Trabaja junto con ***Security Fabric*** quien se encarga de unir las soluciones de Fortinet y así enviar respuestas automatizadas, además de administrar y proteger la red con una sola plataforma convergente [31].

En la Figura 2.3, se muestran los servicios con los que cuenta FortiGuard.

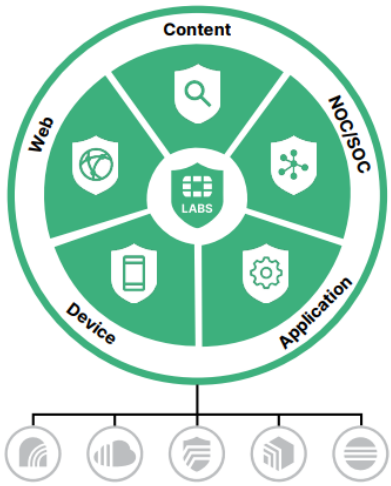


Figura 2.3 Servicios integrados que ofrece FortiGuard [31].

Contenido: Esta solución de seguridad de contenido está enfocada en el monitoreo y protección contra estrategias de ataques mediante archivos como por ejemplo amenazas internas de la empresa, ataques ***ransomware***, segmentación del Data center, y vigilancia en tiempo real de cualquier tipo de ***malware***. El proceso se realiza al retener el archivo y analizarlo en cuestión de milésimas de segundo con el aprovechamiento de técnicas usadas mediante Inteligencia Artificial y el Aprendizaje automático para dar un dictamen y determinar si el archivo es malicioso o no. El sistema Operativo FortiOS incluye también análisis de imágenes dinámico, reconstrucción de contenido, protección contra la perdida de datos e información (DLP). A su vez se cuenta con antispam mediante el uso de FortiMail lo que ayuda a la protección de correos maliciosos [32].

Web: Mediante esta solución se puede optimizar y dar seguimiento y protección a la información contra ataques que se basan en la web como pueden ser ***pishing***, sobrecarga a servidores DNS, filtrado de URLs, Redes definidas por Software (SD-WAN), acceso a la nube. Con el filtrado DNS se logra completa visibilidad del tráfico de red mientras analiza si se permite o no ciertos dominios considerados de riesgo elevado, si llega a ocurrir algún ataque se encarga de bloquear la salida de información y el intento de comunicarse con otros servidores de manera no autorizada, adicionalmente posee una herramienta de geolocalización que proporciona la ubicación de la región o zona de donde está llegando tráfico malicioso [32].

Dispositivo: Al implementar esta solución la empresa tiene seguridad contra ataques basados en dispositivos como por ejemplo detección de vulnerabilidades, uso de exploits, parches, sistema de prevención de Intrusos (IPS), identificación de tecnologías IoT. Mediante el IPS instalado de forma nativa se analiza el tráfico de red y con ayuda de una base de datos conocida como biblioteca que contiene miles de amenazas almacenadas son usadas para responder de manera automática ante cualquier ataque o amenaza [32].

Aplicación: Esta solución se trata de un conjunto de tecnologías que ayudan a proteger y optimizar el funcionamiento de las aplicaciones tanto en los terminales físicos como en la nube, algunos ataques que pueden ocurrir son control y entrega de aplicaciones (ADC), ataque de denegación de servicio (DoS), ataque de denegación de servicio distribuido (DDoS) y correo electrónico web seguro [32].

NOC/SOC: La solución Centro de Operaciones de Red (NOC) y Centro de Operaciones de Seguridad (SOC) se encargan de proporcionar una rápida identificación de los ataques o amenazas a la red corporativa, tratando casos como caza y detección de amenazas, evaluaciones constantes de la red, migración de equipos de red simplificada, gestión de la nube, todas están soluciones fueron previamente estudiadas y elaboradas por expertos de TI trabajando en conjunto en FortiLabs el cual es el laboratorio en donde se realizan investigaciones permanentes para continuar con el desarrollo de las mejores soluciones en el campo de TI que ayude a mejorar la experiencia del usuario y la de la empresa, brindando seguridad y confianza en sus equipos [32].

Seguridad en la Nube: La seguridad en la nube hace referencia a la protección de sistemas informáticos, es decir ayuda a mantener las aplicaciones, datos e infraestructura existente en línea, por lo general instalados en servidores virtuales con conexiones a internet que siempre están activas, en este contexto Fortinet ha desarrollado algunas

soluciones para dar cumplimiento a la seguridad virtual y mantener altos sus estándares de calidad [33].

FortiCNP: Esta plataforma implementada por Fortinet es una defensa nativa de la nube que ayuda a proteger su carga de trabajo, funciona con tecnología ***Risk Resource Insights*** (RRI), dando prioridad a los recursos críticos que conllevan información y así gestionar y administrar de manera eficaz el riesgo en la nube [34].

En la Figura 2.4, se muestran los servicios nativos que ofrece FortiCNP.

Figura 2.4 Servicios nativos que ofrece FortiCNP [34].

FortiWeb: Esta solución integral de Fortinet resuelve ataques que explotan vulnerabilidades tanto conocidas como desconocidas, incorpora opciones virtualizadas mediante máquina virtual (VM) para su convergencia en la nube contando con las mismas funcionalidades que un equipo físico. FortiWeb cuenta con la capacidad para detectar comportamientos extraños o anómalos relacionados con las aplicaciones que se encuentran en la nube lo que le permite bloquear ***exploits*** poco conocidos. Fortiweb también cumple con operaciones que minimizan las tareas manuales que conllevan mucho tiempo como encontrar falsos positivos, realizar ajustes a las reglas de seguridad y actualizaciones cuando sean necesarias [35].

En la Figura 2.5, se muestra el equipo FortiWeb 4000F.

Figura 2.5 FortiWeb 4000F [36].

FortiDevSec: DevSec proviene de las palabras desarrollo y seguridad. Esta solución unifica diferentes análisis de seguridad y ofrece un servicio completo en un solo punto de gestión [37]. Se caracteriza por usar varios tipos de scanner para realizar pruebas de seguridad, como las Pruebas estáticas de aplicaciones (SAST), que se encargan de escanear el código fuente de la aplicación. Pruebas dinámicas de aplicaciones (DAST), que se encargan de buscar vulnerabilidades a través del análisis front-end, Análisis de composición de Software (SCA) que es el encargado de la búsqueda de vulnerabilidades en bibliotecas o códigos de terceros, que generalmente son de código abierto y todo esto lo realiza de manera dinámica de acuerdo a la aplicación que es analizada por medio de parámetros como el lenguaje y ***frameworks*** usados por esa aplicación [38].

2.1.2 JUNIPER

Juniper Networks es una empresa que realiza el diseño y desarrollo de sus productos para posteriormente venderlos, ofrece servicios de ***Networking***, implementa soluciones que abarca los mercados de conmutación, enrutamiento y seguridad. Para su plataforma software cuenta con su propio sistema operativo JunOS lo que le permite lograr los objetivos comerciales de sus clientes. La Automatización de redes simplifica las operaciones para los equipos de ***Networking***, lo que hace que la red se vuelva más confiable, reduciendo errores por configuración. Es un sector muy amplio el conjunto completo de automatización ofrecido por Juniper dando como resultado una red escalable, flexible y con la seguridad necesaria para la empresa. A continuación, se describen dos soluciones ofrecidas por Juniper [39].

AIOps: Inteligencia Artificial para las Operaciones de TI (AIOps), esta solución optimiza la experiencia del usuario en el dominio de acceso ya sea inalámbrico, por cable o mediante SD-WAN, obteniendo una red más confiable, predecible y medible. AIOps trabaja en

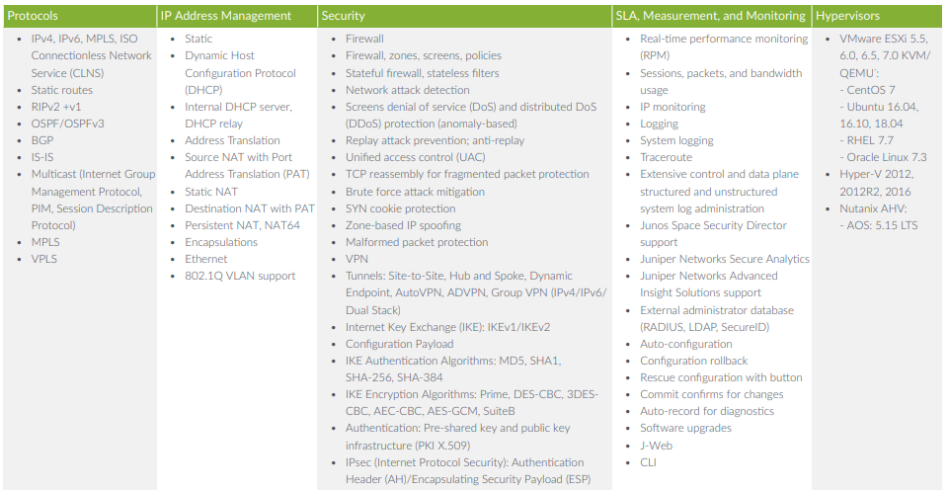
conjunto con Mist AI, que es una plataforma de inteligencia artificial en la nube, su función es la de monitorizar tráfico a un nivel granular en todos los puntos finales inalámbricos o cableados, optimiza la red de manera adinámica al usar microservicios ágiles, se componen de una amplia gama de puntos finales WLAN y son compatibles con tecnología bluetooth de baja energía (BLE), esto conlleva a una mayor facilidad para implementar servicios basados en la localización. AIOps proporciona un despliegue flexible es decir reconoce los equipos que se encuentran conectados y selecciona de manera automática los puertos requeridos, cuenta con actualización de software, gestión de la nube y servicios personalizados que se adaptan a las necesidades y requerimientos de los usuarios finales [40].

Seguridad en la Nube: Esta solución ofrecida por Juniper permite mantener los datos de manera privada y segura por medio de su infraestructura y el sistema informático, además Juniper cuenta con servicios de firewall, prevención de amenazas y políticas de seguridad que se aplican sin importar si las aplicaciones se encuentran en la nube o en las instalaciones físicas.

vSRX Virtual Firewall: vSRX se trata de un dispositivo virtual de seguridad que provee servicios de red, es ejecutado como una máquina virtual por medio de un servidor x86. vSRX es impulsado por el sistema operativo propio de la empresa, JunOS, que facilita los mismos servicios que la serie SRX, pero de manera virtualizada como son; Antivirus que se encargan de detectar y bloquear ***spyware***, ***Keyloggers***, ***adware*** y otros virus más por medio de protocolos como son POP3, SMTP, FTP, HTTP evitando así el filtrado de datos y pérdidas para la empresa. Cuenta con Antispam que analiza constantemente las URLs por posible ataque de Phishing, se basa en estándares como cifrado Open PGP (Muy buena Privacidad), el cual se usa para encriptar correos electrónicos. También cuenta con VPN, firewall centralizado, NAT, IPS, filtrado Web, además de análisis dinámico lo que lo hace más fuerte contra ***malware*** avanzado y se vale del aprendizaje automático para reducir el tiempo de toma de decisiones. Es compatible con otras soluciones de terceros y se pueden integrar sus aplicaciones por medio de APIs [41].

Para mantener segura la red cuenta nativamente con aplicaciones como AppTrack que se encarga de realizar seguimiento a las aplicaciones que son de alto riesgo y analiza el comportamiento del tráfico contribuyendo así con la gestión y control de la red. AppFW que realiza el control de las aplicaciones permitiendo o denegando tráfico, y brindando una mejora en la aplicación de políticas de seguridad de acuerdo con los grupos o aplicaciones que administre. AppQoS que limita el tráfico y lo prioriza manipulando el ancho de banda necesario en función de la información para mejorar la velocidad y el rendimiento de la red.

Esta solución puede usar varios CPU virtuales, específicamente hasta un máximo de 32 sin la necesidad de instanciar una nueva imagen, llegando hasta una velocidad de 98 Gbps. En la Figura 2.6, se muestran las especificaciones técnicas con las que cuenta vSRX [42].



Protocols	IP Address Management	Security	SLA, Measurement, and Monitoring	Hypervisors
• IPv4, IPv6, MPLS, ISO Connectionless Network Service (CLNS) • Static routes • RIPv2 +v1 • OSPF/OSPFv3 • BGP • IS-IS • Multicast (Internet Group Management Protocol, PIM, Session Description Protocol) • MPLS • VPLS	• Static • Dynamic Host Configuration Protocol (DHCP) • Internal DHCP server, DHCP relay • Address Translation • Source NAT with Port Address Translation (PAT) • Static NAT • Destination NAT with PAT • Persistent NAT, NAT64 • Encapsulations • Ethernet • 802.1Q VLAN support	• Firewall • Firewall, zones, screens, policies • Stateful firewall, stateless filters • Network attack detection • Screens denial of service (DoS) and distributed DoS (DDoS) protection (anomaly-based) • Replay attack prevention; anti-replay • Unified access control (UAC) • TCP reassembly for fragmented packet protection • Brute force attack mitigation • SYN cookie protection • Zone-based IP spoofing • Malformed packet protection • VPN • Tunnels: Site-to-Site, Hub and Spoke, Dynamic Endpoint, AutoVPN, ADVPN, Group VPN (IPv4/IPv6/ Dual Stack) • Internet Key Exchange (IKE): IKEv1/IKEv2 • Configuration Payload • IKE Authentication Algorithms: MD5, SHA1, SHA-256, SHA-384 • IKE Encryption Algorithms: Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, SuiteB • Authentication: Pre-shared key and public key infrastructure (PKI X.509) • IPsec (Internet Protocol Security): Authentication Header (AH)/Encapsulating Security Payload (ESP)	• Real-time performance monitoring (RPM) • Sessions, packets, and bandwidth usage • IP monitoring • Logging • System logging • Traceroute • Extensive control and data plane structured and unstructured system log administration • Junos Space Security Director support • Juniper Networks Secure Analytics • Juniper Networks Advanced Insight Solutions support • External administrator database (RADIUS, LDAP, SecureID) • Auto-configuration • Configuration rollback • Rescue configuration with button • Commit confirms for changes • Auto-record for diagnostics • Software upgrades • J-Web • CLI	• VMware ESXi 5.5, 6.0, 6.5, 7.0 KVM/ QEMU*: - CentOS 7 - Ubuntu 16.04, 16.10, 18.04 - RHEL 7.7 - Oracle Linux 7.3 • Hyper-V 2012, 2012R2, 2016 • Nutanix AHV: - AOS: 5.15 LTS

Figura 2.6 Especificaciones vSRX de Juniper [42].

2.2 HERRAMIENTAS USADAS PARA LA AUTOMATIZACIÓN DE LAS TI

Existen varias herramientas que nos ayudan a realizar de manera automática los procesos repetitivos en los diferentes dispositivos de capa 2 y capa 3, esto ayuda a que los profesionales de TI se enfoquen en tareas más específicas y obtener un mayor rendimiento y productividad. A continuación, se describen dos herramientas, que en este proyecto han sido consideradas como las más relevantes para la automatización de las TI.

2.2.1 ANSIBLE

Es una herramienta que fue desarrollada por Red Hat, mediante la cual se pueden realizar diversas tareas como gestionar servidores, aplicaciones y realizar configuraciones. Esta herramienta se destaca por realizar configuraciones en varios servidores, al mismo tiempo que facilita la práctica de software y el gestionamiento de la configuración e infraestructura [43].

Características: Su arquitectura se basa en el uso de controladores y nodos, es decir mediante el uso de máquinas virtuales y servidores web, los mismos que son interconectados mediante un lenguaje de programación llamado Python. No necesita de agentes para realizar sus funciones, lo que significa que no requiere de ningún software adicional para trabajar, realiza automatización de red y despliegue de aplicaciones. Esta

herramienta puede ser utilizada en varios sistemas operativos como Linux y MAC, a su vez también puede ser usada en Windows, pero mediante el uso de una máquina virtual. No se necesita de un vasto conocimiento en programación para utilizar Ansible, se considera un software libre o de código abierto [43].

En la Figura 2.7, se observa la arquitectura Ansible.

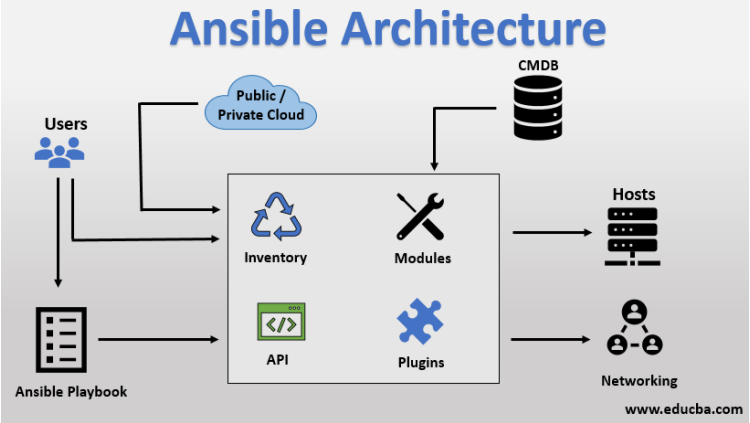


Figura 2.7 Arquitectura Ansible [44].

Para empezar a utilizar Ansible, éste necesita ser instalado en aquella máquina en donde se maneje la infraestructura (maquina controladora), y se puede utilizar apenas es instalado [43].

Ansible debe ser instalado tanto en la máquina controladora como en la máquina que funciona como administrada. Se deben tener en cuenta algunos requerimientos esenciales para utilizar Ansible en la máquina controladora [43]:

- ✓ Python 2.6
- ✓ paramiko
- ✓ PyYAML
- ✓ Jinja2
- ✓ httplib2
- ✓ Sistema operativo basado en Unix

En cuanto a los requisitos para la correspondiente instalación en la máquina administrada se necesita una versión de Python 2.5 o superior. Si se desea instalar en una máquina con sistema operativo Windows, se requiere de algunas dependencias adicionales como activar la comunicación remota y una versión de Power Shell mayor a 3.0 [43].

El comando para instalar Ansible en las distribuciones de

Fedora, RHEL, CentOS.

```
$ yum install ansible
```

Ubuntu, Debian, y compatibles

```
$ sudo apt-get install ansible
```

Ansible también puede ser instalado mediante el comando pip, el cual se encarga de encontrar, instalar y actualizar los paquetes que se requieran, así como sus dependencias, para lo cual se usa el siguiente comando [43].

```
$ pip install ansible
```

Configuración: Para su configuración, Ansible dispone de un archivo de inventario por default llamado host y se lo encuentra en la dirección /etc/ansible. Utiliza un sistema de grupos para realizar las configuraciones y que a su vez permita configurar varias máquinas a la vez. Cuando los hosts se encuentren registrados dentro de un grupo se puede empezar a realizar comandos sobre ellos. Se puede usar el módulo ping del cual dispone Ansible para probar conectividad con el host al cual se va a configurar. Como ejemplo de configuración se tiene un grupo de servidores web con el nombre de sitio1, sitio2, y sitio-dr, así como también se tiene un grupo de máquinas administradas llamadas sitio1, sitio2, sitio-db [43].

Teniendo los grupos configurados se puede empezar a realizar comandos para probar que pueden ser administrados, para esto se conecta de forma remota con las máquinas administradas mediante el protocolo ssh, esto quiere decir que en la máquina administrada no es necesario tener instalado Ansible [43].

El primer comando que se realiza es para comprobar conectividad con el servidor:

```
$ ansible sitio1 -u root -k -m ping
```

Con este comando se solicita la contraseña de ssh y se obtiene el siguiente resultado:

```
sitio1 | success >> {
 "changed": false,
 "ping": "pong"
}
```

Si se desea configurar el nombre de usuario simplemente se debe ir al archivo de inventario /etc/ansible/ansible.cfg y se deben añadir unas líneas de comandos, en este caso el host sitio1 del grupo de servidores tomará el nombre de root, y el host sitio2 tomará el nombre de Jaime. Existen también otros comandos que pueden ser utilizados como ansible_ssh_host el cual permite configurar un nombre de host distinto y el comando ansible_ssh_port el cual es capaz de configurar un puerto diferente como se muestra con el host sitio-dr. A su vez dentro del grupo de las máquinas administradas se tiene el host sitio-db cuyo nombre ha sido configurado como Dario y se le ha establecido una clave ssh con ayuda del comando ansible_ssh_private_key_file [43].

```
[servidores web]
Sitio1 ansible_ssh_user=root
Sitio2 ansible_ssh_user=jaime
sitio-dr
ansible_ssh_host=sitio.dr
ansible_ssh_port=65422
```

```
[Maquinas administradas]
sitio1
sitio2
sitio-db ansible_ssh_user=dario
ansible_ssh_private_key_file=/home/dario/.ssh.id_rsa
```

Para usar Ansible en el sistema operativo Windows se deben tener en cuenta varios requisitos como son:

- ✓ Crear algunas máquinas Windows en el inventario.
- ✓ Instalar Python-winrm el cual permite la conexión entre Ansible y Windows.
- ✓ Actualizar Powershell a la versión 3.0 o superior.
- ✓ Habilitar la comunicación remota de Windows.

La creación de las máquinas Windows en el inventario son originadas de la misma manera que se aprendió para el sistema operativo Linux, con la diferencia del comando ansible_connection el cual es configurado para ser usado mediante winrm y así poder conectar de manera remota con Windows Powershell. También se usan los comandos ansible_ ssh_user, ansible_ssh_pass, ansible_ssh_port [43].

```
[windows]
dc.ad.example.com
web1.ad.example.com
web2.ad.example.com
```

```
[windows:vars]
ansible_connection=winrm
ansible_ssh_user=jaime
ansible_ssh_pass=secreto
ansible_ssh_port=5986
```

Después de la creación del inventario con los usuarios para Windows, se necesita instalar winrm en la máquina que funciona como controladora, para esto se usa el comando pip.

```
pip install http://github.com/diyan/pywinrm/archive/master.zip.
```

Para asegurarnos que se esté trabajando con la versión correcta de Powershell en nuestra máquina se usa el siguiente comando con el cual se puede saber que versión se utiliza actualmente o si es el caso actualizarla [43].

```
$ PSVersionTable.PSVersion.Major
```

De la misma manera que se procedió a realizar un ping con el sistema operativo Linux, se realiza para Windows, pero en este caso el módulo se conoce como win_ping, sin embargo, su función es exactamente la misma, es decir verificar la conexión entre la máquina controladora y la administrada [43].

```
$ ansible web1.ad.example.com -u jaime -m win_ping
```

El resultado esperado al utilizar el comando anterior

```
web1.ad.example.com | success >> {
 "changed": false,
 "ping": "pong"
}
```

Luego de haber revisado su configuración básica es importante señalar un concepto esencial dentro de Ansible como lo es el “Playbook”; que hace referencia a las tareas de automatización, es decir las acciones que son escritas usando una estructura específica y que se ejecutan automáticamente en los hosts que se encuentran en el inventario de Ansible. A continuación, se muestra un ejemplo sencillo el cual realiza la instalación de apache sobre un inventario que tiene el nombre de “web”, se puede observar que tiene configurado el puerto 80 es decir el protocolo HTTP para que exista comunicación a la web, las tareas que va a realizar como, verificar si apache está presente, instalar la última versión de apache, copiar las configuraciones que están dentro del repositorio, y finalmente iniciar el servicio [43].

En la Figura 2.8, se presenta el script para instalar Apache por medio de Ansible.

```
---
- name: install and start apache
  hosts: web
  become: yes
  vars:
    http_port: 80
  tasks:
  - name: httpd package is present
    yum:
      name: httpd
      state: latest
  - name: latest index.html file is present
    copy:
      src: files/index.html
      dest: /var/www/html/
  - name: httpd is started
    service:
      name: httpd
      state: started
```

Figura 2.8 Script Implementado en Ansible [45].

2.2.2 PUPPET

Puppet es una herramienta de automatización de código abierto que sirve para administrar y gestionar infraestructuras de TI complejas, está escrito en lenguaje Ruby y usa su propio lenguaje de dominio específico (DSL) que facilita la conversión de la infraestructura como código para administrar y crear módulos. Puppet cuenta con dos versiones para su utilización, la primera que es Open Source Puppet que se puede descargar desde la página oficial, y la segunda que es una versión de paga y su nombre es Puppet Enterprise, esta última cuenta con algunas funciones más que la versión gratuita como el control de acceso basado en roles (RBAC), orquestación e informes de los análisis de rendimiento de la infraestructura que está siendo automatizada. Esta herramienta es considerada declarativa es decir que no se describen los pasos a donde se quiere llegar si no que se describe el estado en el que se quiere tener a una máquina o servidor. Puppet usa el modelo cliente-servidor en donde un servidor principal funciona como “Puppet máster” y los clientes se conocen como “Puppets” [46].

Flujo de Trabajo de Puppet: Mediante el flujo de trabajo se describe de manera secuencial los pasos que Puppet sigue de manera general para lograr la automatización de tareas. El Puppet máster es el encargado de recopilar la información de la máquina objetivo por medio del Factor, el cual representa a los nodos de la infraestructura, se obtienen los datos de configuración necesarios y son enviados al Puppet o cliente. Después de esto el Puppet máster es quien compara los detalles que se han definido en la configuración y procede a

crear un catálogo para ser enviados a los agentes de la máquina de destino. Tales configuraciones son aplicadas por la máquina ó servidor objetivo para lograr el estado que se desea. Una vez que la máquina de destino se encuentra en el estado que se desea, se envía un informe para el Puppet máster lo que guía al Puppet máster para conocer en que estado se encuentra el sistema, tal como fue definido inicialmente en el catálogo [47].

En la figura 2.9, se muestra el flujo de trabajo de Puppet.

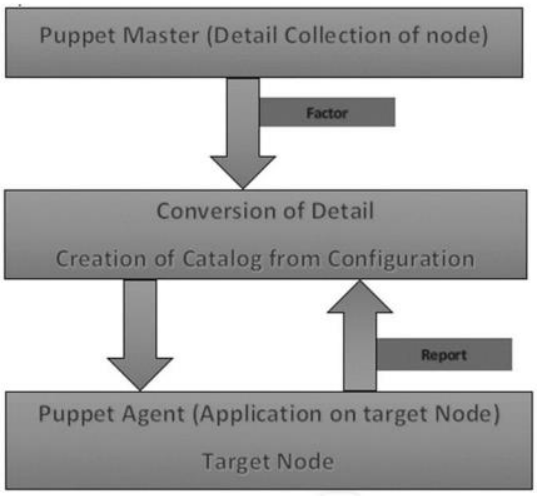


Figura 2.9 Flujo de Trabajo de Puppet [47].

Arquitectura Puppet: A continuación, se describen los elementos que conforman la Arquitectura de Puppet:

Puppet Máster: Es aquella máquina o servidor que maneja todos los aspectos que se relacionan con la configuración y el gestionamiento de datos que son aplicados a los nodos por medio de un Agente Puppet [47].

Agente Puppet: Son aquellas máquinas que se encuentran trabajando y que son administradas por el Puppet Máster, y para su funcionamiento se debe tener instalado un agente o software que permita la administración del máster [47].

Repositorio de Configuración: Es un repositorio en donde se guarda todos los datos e información relacionadas a la gestión y configuración de los nodos para ser extraídas cuando se requiera [47].

Hechos: Es la información referente al Puppet Máster y sirve para conocer el estado actual de un nodo, por medio de estos datos se pueden realizar cambios en cualquier Agente Puppet [47].

Catálogo: Los archivos de configuración o manifiesto que son descritos por Puppet se convierten en un lenguaje de compilación llamado catálogo para posteriormente ser aplicados a la máquina de destino [47].

En la Figura 2.10, se muestra la arquitectura usada por Puppet.

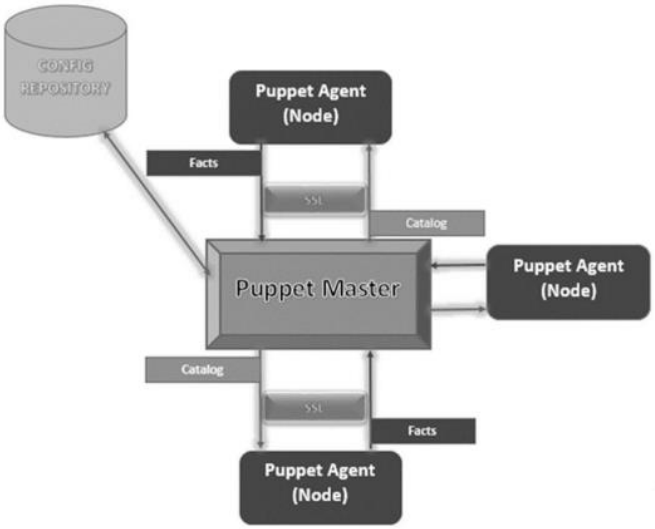


Figura 2.10 Arquitectura Puppet [47].

Configuración: Dentro de los requisitos para la instalación de Puppet se tiene; contar con al menos dos máquinas para que una tome el rol de máster y la otra funcione como cliente, y conexión de todos los sistemas ya sea mediante una red privada o pública [48].

Para iniciar su configuración primero se necesita ingresar al terminal y editar el archivo hosts.

```
# | sudo nano /etc/hosts
```

Luego se procede a añadir las siguientes líneas en el final del archivo /etc/hosts

```
10.132.14.239 puppetmaster puppet
10.132.14.240 puppetclient1
10.132.14.241 puppetclient2
```

En donde la primera dirección IP corresponde al Puppet máster, y las dos siguientes son clientes Puppet. Luego se procede a instalar el nodo maestro con ayuda de los siguientes comandos [48].

```
wget https://apt.puppetlabs.com/puppet7-release-focal.deb
sudo dpkg -i puppet7-release-focal.deb
```

Una vez descargado se procede a actualizar el caché e instalar el servidor Puppet [48].

```
sudo apt update
sudo apt install puppetserver -y
```

Ya instalado de manera correcta el siguiente paso es iniciar el servidor Puppet.

```
sudo systemctl start puppetserver
sudo systemctl enable puppetserver
```

Adicionalmente se debe descargar otro paquete para la configuración en la máquina cliente [48].

```
wget https://apt.puppetlabs.com/puppet7-release-focal.deb
sudo dpkg -i puppet7-release-focal.deb
```

A continuación, se instala el Agente Puppet.

```
sudo apt install puppet-agent -y
```

Completa la instalación se debe editar el archivo de configuración.

```
sudo nano /etc/puppetlabs/puppet/puppet.conf
```

Se agregan las siguientes líneas con el objetivo de definir el nodo maestro y cliente.

```
[main]
certname = puppetclient1
server = puppetmaster
```

Se inicia el Agente Puppet mediante los siguientes comandos.

```
sudo systemctl start puppet
sudo systemctl enable puppet
```

Para completar la configuración se necesita enumerar y firmar los certificados en uso, para lo cual en el Puppet Máster se escriben los siguientes comandos [48].

```
sudo /opt/puppetlabs/bin/puppetserver ca list --all
sudo /opt/puppetlabs/bin/puppetserver ca sign --all
```

Finalmente se comprueba que exista comunicación entre el Puppet máster y el cliente.

```
sudo /opt/puppetlabs/bin/puppet agent --test
```

Para entender un poco mejor su uso se describe un ejemplo simple en el cual se crea un módulo que instale apache2 y en su configuración se cree un archivo index.html, para esto lo primero que se hace es crear el fichero init.pp que es en donde Puppet busca los recursos del módulo y se agrega el siguiente contenido [48].

En la Figura 2.11, se presenta el módulo implementado en Puppet para instalar Apache2.

```
class apache {
    Package['apache package']  -> File['index.html'] ~>
Service['apache service']


  package { 'apache package':
     ensure => installed,
     name => "apache2",
   }
  file {'index.html file':
    ensure => file,
    owner => www-data,
    group => www-data,
    mode => 0640,
    source => "puppet:///modules/apache/index.html",
    path => "/vaw/www/index.html",
    }
   service {'apache service':
     ensure => running,
     name => "apache2",
    }
}
```

Figura 2.11 Script implementado en Puppet [49].

2.3 ARQUITECTURA DNA CISCO

La Arquitectura de Red Digital (DNA) tiene como función principal acelerar la digitalización de los negocios e industrias del mercado para ofrecer un mayor nivel de personalización, satisfacción y conveniencia, mejora la experiencia en el trabajo y con los usuarios finales lo que conlleva a mayor productividad y ganancias para la compañía, aprovecha la tecnología para tomar decisiones instantáneas y acertadas con base en datos previamente investigados analizados y almacenados, reduce costos para la empresa y minimiza errores humanos [50].

La Arquitectura DNA de Cisco hace referencia a una plataforma impulsada y controlada mediante software y cuyo objetivo es la simplificación de las operaciones de red que se realizan en la empresa a través de innovaciones como la automatización, virtualización y computación en la nube [51].

Características: La Arquitectura DNA funciona como una plataforma de transformación digital, en este sentido se toman en cuenta varias consideraciones para realizar su trabajo de manera correcta y sin contratiempos, está compuesta por hardware programable y con circuitos integrados que son específicos de la aplicación (ASIC) lo que permite una ingeniería más personalizada, usa protocolos y servicios de red con velocidades en el orden de los Gigabits, en cuanto al sistema operativo es construido en base a interfaces de aplicación programables (APIs), en el entorno de red también se encarga del enrutamiento, la interconectividad, la conmutación y la nube, automatiza las operaciones de TI, brinda visibilidad a través de APIs que son analizadas y de donde se obtiene información procesable, integra servicios en la nube ya sea pública o privada lo que proporciona escalabilidad. Dentro de los beneficios que se adquieren al implementar la Arquitectura DNA de Cisco se tienen; la reducción de costos mediante el hardware programable, la virtualización, la configuración y automatización de tareas [52].

Estudios han demostrado que implementar la automatización en la calidad de servicio (QoS) conlleva a un ahorro entre 200,000 y 1 millón de dólares, así como un ahorro en tiempo que representa el 200% en tiempo de configuración y 50% en resolver problemas debido a una menor cantidad de errores en configuraciones. Además, se tienen plataformas virtualizadas que ayudan a aprovechar de mejor manera los recursos de hardware, por citar un ejemplo un solo equipo puede realizar diversas funciones como enrutador, firewall, contenedor de aplicaciones etc. Además de que físicamente se requiere de menos espacio y pueden ser actualizables y administrables fácilmente por lo que se necesita menos especialistas en TI que se dirijan a realizar soporte en sectores alejados o remotos. Adicionalmente se usa la red como sensor, al reportar anomalías por medio de alertas que en muchos casos puede remediar el problema por sí misma, evitando así interrupciones en el sistema y salvaguardando la información [52].

Detecta amenazas y las resuelve rápida y eficazmente al ejecutar políticas de compensación o cuarentena en tiempo real, brinda excelente experiencia al usuario, y proporciona aplicaciones más rápidas que son integradas a la infraestructura de modo que éstas pueden obtener servicios de red en el instante que lo requieran. Cisco DNA también cuenta con la capacidad de integrarse con sistemas fuera de la red mediante APIs abiertas.

2.3.1 Servicios de la Arquitectura DNA de Cisco

El servicio principal de Cisco DNA es la conectividad, es decir permitir el tráfico IP entre las aplicaciones que usan los dispositivos electrónicos sin importar que éstos sean usados por el departamento de TI, empleados o usuarios finales. Estos flujos de datos pueden llegar

a ser muy complejos debido a los diferentes sistemas operativos usados por los equipos, la distancia que hay entre ellos o si se encuentran en movimiento o no, los flujos tanto de voz como video deben ser transmitidos sin interferencias y en tiempo real [53].

En la Figura 2.12, se presenta la red empresarial conectando a las aplicaciones con los usuarios y dispositivos.

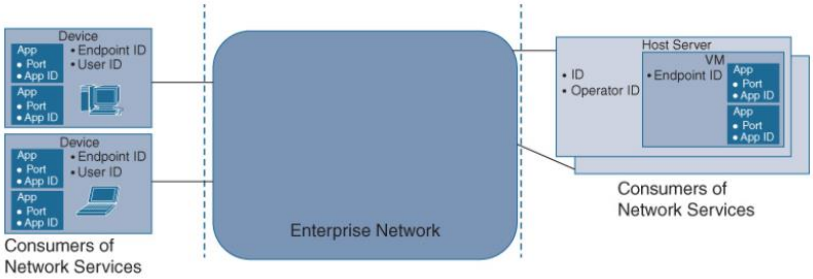


Figura 2.12 Conectividad por medio de la red DNA de Cisco [51].

Se tienen dos componentes principales que son el transporte y el envío del tráfico a través de la red. Y las políticas que se encargan de cómo la red trata dicho tráfico.

Transporte: Por medio del transporte Cisco DNA brinda una ruta que comunica dos o más usuarios, aplicaciones o equipos a través de la red. Comienza mediante una interfaz de acceso que puede ser física o lógica en donde ingresan paquetes IP y son transmitidos a los extremos del servicio. Cisco DNA usa la conmutación y el enrutamiento como un mecanismo de reenvío y de establecimiento de las rutas de entrada y salida, también usa las funciones de red como NAT, Protocolo Localizador de separación de ID (LISP), DHCP y servidores de mapas. La interfaz de usuario a red (UNI) define las rutas de entrada y salida además de funcionar como punto de demarcación entre la red y los usuarios [53].

Política: Las políticas que implementa Cisco DNA son utilizadas para tratar el tráfico de red que se asocia con el servicio, por ejemplo, si se requiere restringir cierto tráfico de red, la política que se usa es el filtrado de tráfico indeseado. La UNI es la encargada de dictaminar cuando se aplican estas políticas, si se tiene información muy valiosa y determinante, una política de seguridad que puede ser usada es el cifrado, también se usa para priorizar rutas de envío si así lo requiere y para recopilar los datos que son transmitidos. En servicios simples se usa el reconteo de paquetes IP, pero si una anomalía es detectada en un puerto se necesita de una recopilación de datos más estricta garantizando registros completos y que pueden ser usados junto con un sistema de detección de intrusos (IDS) o en su defecto un sistema de prevención de intrusos (IPS) [53].

En la Figura 2.13, se observa los servicios de la Arquitectura DNA de Cisco.

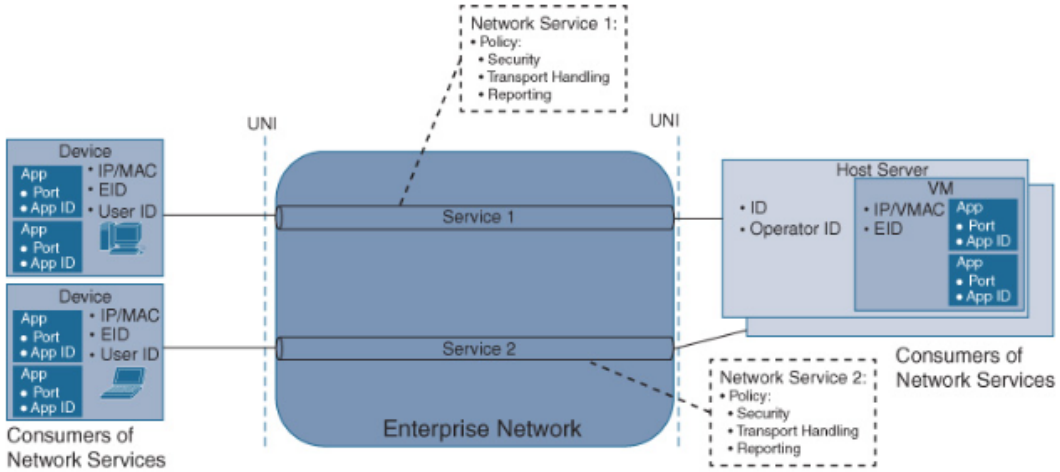


Figura 2.13 Servicios Transporte y Políticas de seguridad asociadas a Cisco DNA [51].

Funciones de Transporte: La función de transporte en Cisco DNA está dada por elementos físicos como conmutadores y enrutadores, y elementos virtuales como las funciones de red virtualizadas (VNF) dentro de esta función transporte se tiene el acceso a la red el cual se puede dar por medio de un puerto dedicado del conmutador o de manera inalámbrica mediante puntos de acceso. Independientemente de si es físico o lógico estos puntos están asociados y especificados por la UNI. Se debe tener en consideración que para que se cumpla la política de Cisco DNA todo dispositivo y sus aplicaciones deben pasar por la UNI para continuar a los puntos de aplicación de políticas (PEP), aquí se asocian las políticas con un servicio de la Arquitectura DNA por ejemplo un flujo de tráfico IP asociado con un segmento de red, en donde se adhieren los bits en los encabezados de los paquetes que llevan la información de la política a implementar. La Infraestructura transporte realiza segmentación que ayuda a definir los flujos de tráfico para los diferentes servicios, usa funciones de encriptación y están sujetos a funciones de seguridad como firewalls, IDS, IPS, filtrado y detección de anomalías, etc. Es importante mencionar que las funciones de red en la nube son parte de Cisco DNA y se usa las nubes privadas virtuales (VPC) para alojar las aplicaciones junto con enrutamiento virtual siguiendo las mismas consideraciones anteriores por su paso a través de la UNI y la PEP virtuales [54].

En la Figura 2.14, se observa la Infraestructura DNA de Cisco.

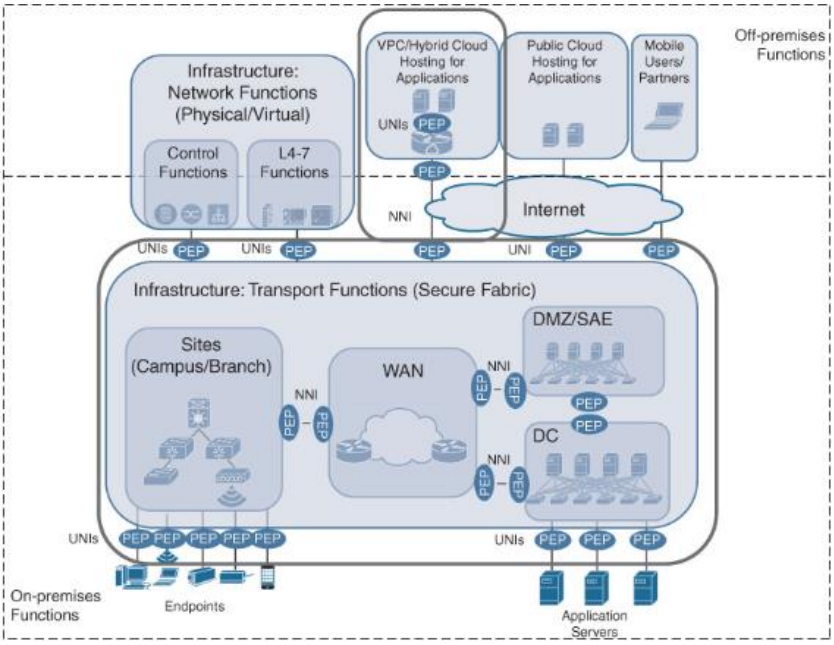


Figura 2.14 Infraestructura DNA de Cisco [51].

Funciones de Red: Para que las funciones de transporte se realicen adecuadamente necesita de ciertas funciones complementarias las cuales se dividen en dos que son:

Funciones de plano de control, que son responsables de ayudar a establecer la ruta de envío de paquetes como por ejemplo los reflectores de ruta y servidores DNS, DHCP que se encargan de ayudar en la comunicación entre los puntos finales y la red.

Funciones de plano de datos, que son aquellas que participan en la manipulación de tráfico de ser necesario como por ejemplo los servicios de aplicación de área amplia (WAAS), que pueden ser usadas para la optimización de la comunicación entre aplicaciones, funciones IDS, IPS para que se cumpla con políticas de seguridad [54].

Controladores: Los controladores realizan un papel importante en Cisco DNA ya que son los encargados de automatizar las funciones de red y transporte además de mantener e instanciar los servicios que ofrece Cisco DNA, por ejemplo si se requiere de ampliar la zona geográfica de la red, se instalan los elementos físicos necesarios y el controlador es el encargado de regular el inicio de la activación, así como de instalar complementos para su configuración, los controladores conocen la infraestructura como el tipo de equipo que se maneja, las tarjetas de línea, el sistema operativo y versión de firmware que usa, así como los grupos de dispositivos o aplicaciones que se forman para obtener un servicio de red [55].

Definición y Orquestación de Servicios: Este componente define los servicios de Cisco DNA a un nivel abstracto es decir de acuerdo a lo que el cliente requiera, mediante este componente se implementan políticas que rigen el acceso al servicio de la red por medio de la autenticación por ejemplo, una política de acceso puede establecer la autenticación o ingreso al servicio por medio de un usuario y contraseña o mediante algún otro mecanismo previamente elegido, también se puede regular el control de un grupo de usuarios para que éstos se puedan comunicar sólo con ciertos grupos de aplicaciones propias. Este componente posee una capa presentación, la cual se presenta mediante una GUI o interfaz de usuario la cual expresa de manera gráfica las políticas y servicios de Cisco DNA, también se puede presentar como una API. Sin importar su presentación los detalles para su funcionamiento se obtienen de los detalles del elemento de la red [55].

En la Figura 2.15 se observa un ejemplo de dicho funcionamiento al expresar los detalles de la intención de la red como “el tráfico es crítico en el punto de venta” y ser posteriormente abstraído.

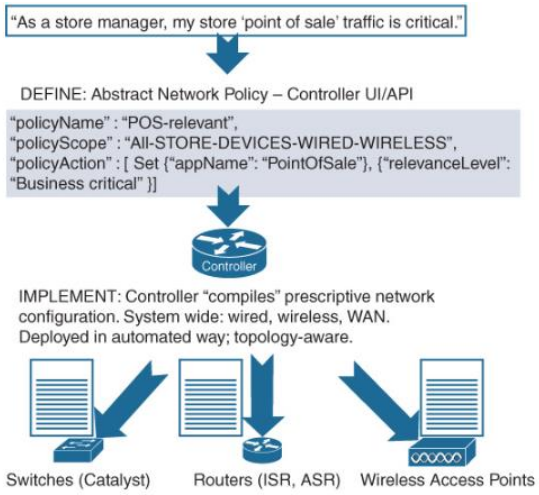


Figura 2.15 Ejemplo de Abstracción en la Arquitectura DNA Cisco [51].

Adicionalmente la capa de servicios y orquestación se encarga de crear las instancias de un servicio en las diferentes estructuras por medio de varios controladores de ahí toma el nombre de “Orquestación”, ya que se necesita que los controladores estén coordinados para instanciar o crear servicios de Cisco DNA [55].

En la Figura 2.16, se presenta la relación entre los controladores de Cisco DNA, los servicios y la Orquestación.

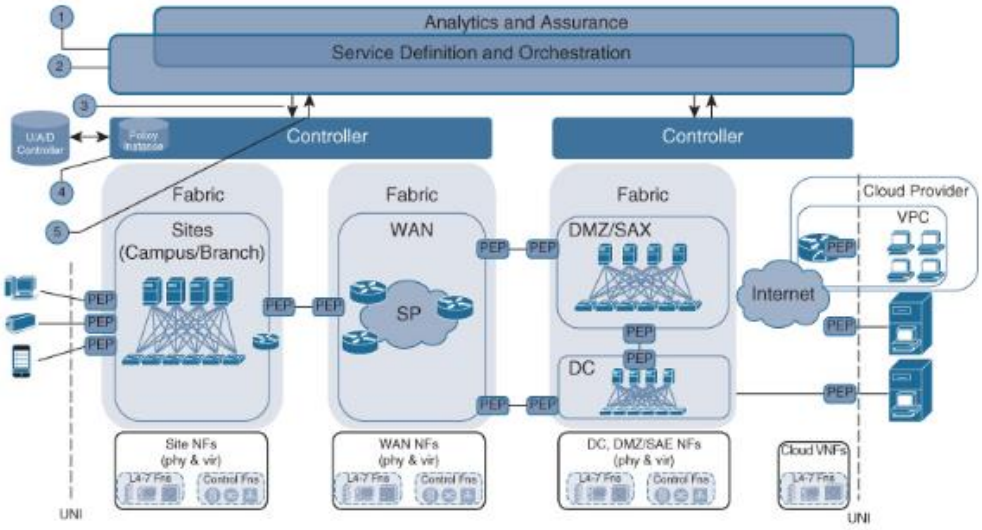


Figura 2.16 Bloques de la Arquitectura DNA de Cisco [51].

Plataforma de Análisis: Hasta ahora se ha visto que la Arquitectura DNA crean servicios de red a través de las funciones de transporte, de red y mediante controladores y políticas establecidas. Continuando con este proceso se tiene la plataforma de análisis, en la cual se da la confirmación de que la red efectivamente ha creado y está ejerciendo el servicio solicitado, además de un monitoreo constante para conocer el estado de la red y su correcto funcionamiento, también se encarga de recopilar datos y los analiza para obtener informes por medio de APIs, éstas son las responsables de conectar con los demás elementos de la red [55].

2.3.2 Innovaciones de Cisco DNA

En este apartado se describen las innovaciones que presenta Cisco DNA como son hardware y software flexibles, protocolos y virtualización.

Hardware Flexible: El Hardware es una parte importante de la red, la mejor inversión que se puede realizar para una mayor eficiencia en cuanto a infraestructura de red es una mezcla entre hardware y software trabajando en conjunto. Por medio del Hardware programable y flexible la red puede adaptarse a los cambios tecnológicos, funciones, protocolos y soluciones brindando así la base para la Arquitectura DNA de Cisco. Los circuitos integrados de silicio ASIC de red flexible los cuales están compuestos por millones de transistores y otros elementos electrónicos son diseñados cuidadosamente mediante codificación de lenguaje de descripción de hardware (HDL). Tecnología de la cual están

hechos los conmutadores y enrutadores y a través de los cuales se programan y ejecutan un grupo de tareas específicas como por ejemplo el manejo de tráfico, reenvío de paquetes, conmutación de etiquetas multiprotocolo (MPLS), analizado del tipo de paquete ya sea IPv4, IPv6, MPLS etc. Acciones de filtrado con listas de control de acceso (ACL), programación de paquetes y recolección de datos, entre otras [56].

En la Figura 2.17, se muestra el balance de costo, flexibilidad y programación que proporciona un ASIC.

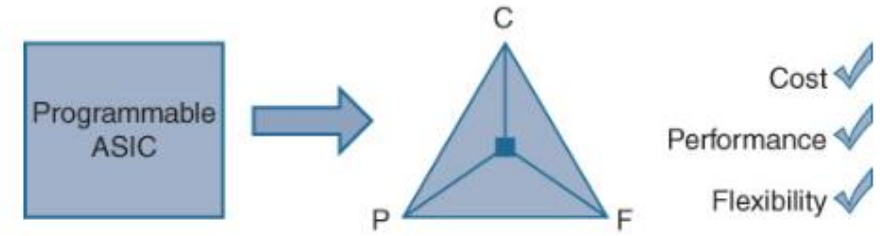


Figura 2.17 Beneficios ASIC [51].

Software Flexible: El software usado por la Arquitectura DNA de Cisco ha venido evolucionando con forme avanza el tiempo, desde Cisco IOS con funcionalidades que en su tiempo formaron la base para enfrentar la tecnología cambiante de hoy en día, hasta Cisco IOS XE que es la nueva generación y que se diferencia de su antecesor la admisión de CPU de múltiples núcleos, la capacidad de hospedar aplicaciones y contenedores adicionales y la adaptación a las plataformas de hardware en evolución. Adicionalmente dentro de la innovación de software se tiene las implementaciones de red que usan controladores de red, el primero creado por Cisco fue conocido como Módulo Empresarial del Controlador de Infraestructura de Políticas de Aplicaciones (APIC-EM), creado con el objetivo de proporcionar automatización de funciones y simplificar la resolución de problemas de red, con el paso del tiempo esta tecnología se convirtió en Cisco DNA Center que tenía las mismas capacidades que su antecesor y además llegó al mercado con nuevas funcionalidades como el monitoreo continuo de la infraestructura de red, informe de errores, recepción de información de cada dispositivo ya sea conmutador, enrutador, controlador inalámbrico, etc [57].

En la Figura 2.18, se observa de manera general las funciones que cumple Cisco DNA Center.

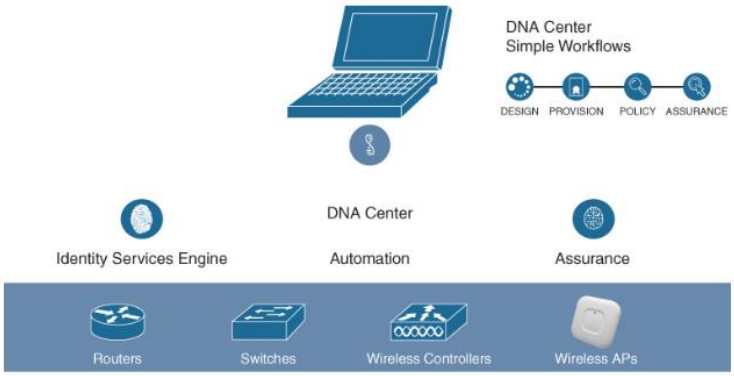


Figura 2.18 Cisco DNA Center [57].

Protocolos: Los Protocolos de Red son los que rigen como se crea y mantiene la red, así como la comunicación dentro de ella, desde su creación los protocolos no han tenido un mayor cambio, siendo los mayormente utilizados, protocolos de capa 2 y capa 3 como Spanning Tree (STP), Protocolo de enrutamiento en espera activa (HSRP), Protocolo de redundancia de enrutador virtual (VRRP), y protocolos de enrutamiento como OSPF, BGP. EIGRP. Sin embargo, con las nuevas tecnologías se requiere mayor capacidad de los protocolos usados, así tenemos red de área local virtual extensible (VXLAN) que es un protocolo de encapsulación y tiene la capacidad de ejecutar una red superpuesta, que no es más que una red virtual que se construye sobre una red física que tiene las características de escalabilidad, convergencia y estabilidad. Otro protocolo es el de separación de ID/Ubicación de Cisco (LISP) que ofrece un avance en el acceso a los dispositivos de redes y el enrutamiento, lo que permite la movilidad de los usuarios dentro de la red superpuesta, por medio de LISP se puede saber detrás de que enrutador se encuentra o conmutador se encuentra un dispositivo o el usuario [58].

En la Figura 2.19, se ilustra el concepto de superposición de una red.

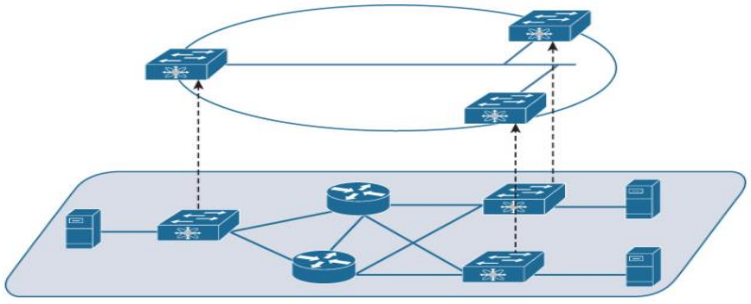


Figura 2.19 Superposición de redes [58].

Virtualización: Por medio de la Virtualización se pueden ejecutar funciones de red dentro de máquinas virtuales (VM). Su infraestructura es abierta ya que ofrece APIs en las capas de software para todos los usuarios, socios o terceros lo que conlleva mayor flexibilidad para su implementación con ayuda de las funciones de red Virtualizadas (NFV). En este entorno también aparece un concepto importante como es la nube privada virtual (VPC), que permite la reducción de costos ya que no se requiere de grandes infraestructuras de servidores para implementar sus aplicaciones. Para implementar una VPC se puede hacer uso de un enrutador virtual por ejemplo el CSR 1000v que se utiliza como NFV para brindar conectividad a toda la empresa convirtiéndose en una sucursal más de la red teniendo las mismas funciones de optimización, gestión y seguridad [59].

En la Figura 2.20, se muestra la combinación de funciones mediante Máquinas virtuales

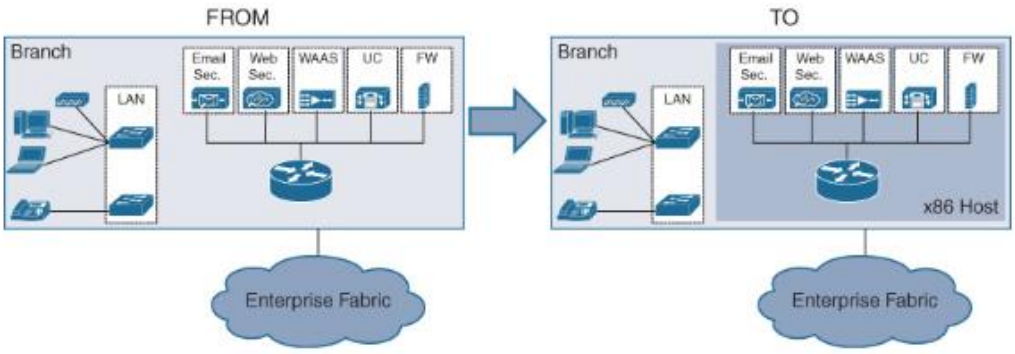


Figura 2.20 Esquema de Virtualización de Red [59].

3 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presenta una comparativa entre las soluciones de automatización de las TI descritas en el capítulo 2, detallando sus ventajas y desventajas para su implementación en una red corporativa, se compara las herramientas de automatización de TI y las innovaciones que hacen de la Arquitectura DNA de Cisco una gran opción para la digitalización de la empresa.

3.1 Resultados

3.1.1 Comparación entre las soluciones de Fortinet y Juniper

Las soluciones que presentan estos dos fabricantes cumplen con su función principal al ser capaces de automatizar los procesos de TI. Sin embargo, existen algunas diferencias entre

estas dos marcas que precisa a las empresas que requieren de sus servicios optar por alguno de ellos en particular.

Fortinet tiene un enfoque de automatización plasmado en la seguridad de la red, teniendo en cuenta la solución que ofrece en seguridad de la nube en donde el equipo FortiGate 80F el cual cuenta con muchas funciones tales como firewall, puertas de enlace web, filtrado de tráfico, antivirus, tiene un comportamiento automatizado ya que actualiza su software cuando es necesario, cuenta con filtrado URL único al poseer un proxy SSL por lo que el cifrado es realizado antes de que el paquete salga de FortiGate, su interfaz de usuario es bastante amigable e intuitiva y no presenta retardos en la respuesta ni errores informáticos (bugs), permite la reutilización de recursos ya que es un equipo físico que admite dominios virtuales y se puede usar desde otro lugar con las mismas funcionalidades y beneficios. Mientras que la solución SRX que ofrece Juniper es bastante flexible, admitiendo también aplicaciones basadas en la nube y en servidores físicos, su respuesta es automática ya que al detectar algún tipo de malware responde de manera inmediata, permite extender la red sin aumentar el costo al agregar módulos de expansión añadiendo escalabilidad a la empresa, su configuración se realiza de manera similar que con Fortinet teniendo una interfaz amigable, pero con un margen de mejora, en cuanto a costos se refiere, FortiWeb 80F es una solución asequible que se puede encontrar en Amazon por un precio de alrededor de los 2000 $ por otra parte Juniper SRX300 de similares características se lo puede encontrar por un precio de alrededor de los 3500 $. Ambas marcas ofrecen soporte técnico en sus equipos y cumplen adecuadamente.

Se puede abstraer que las dos soluciones presentadas son una gran opción para automatizar el entorno de TI, pero para las mismas funcionalidades e incluso teniendo un poco más de facilidad en cuanto a configuración de equipos y tomando en cuenta el dinero invertido Fortinet es una mejor opción.

En la Figura 3.1, se muestra las interfaces de FortiWeb (izquierda) y SRX de Juniper (derecha).

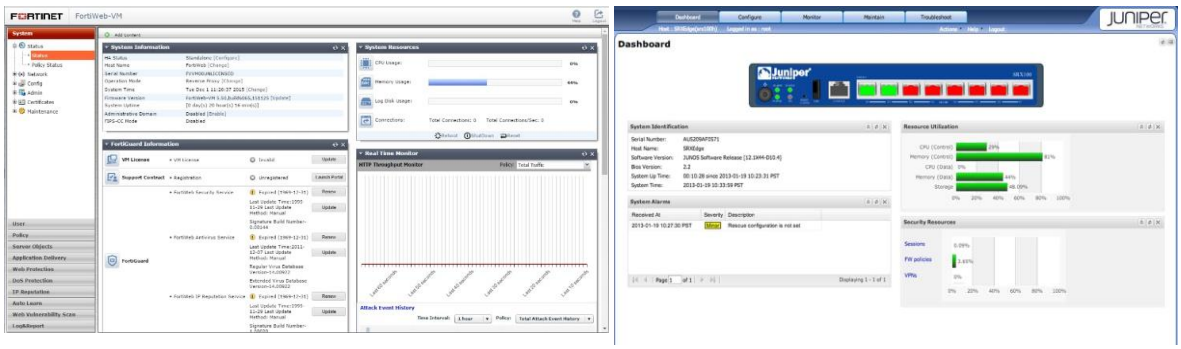


Figura 3.1 Interfaz FortiWeb y SRX Juniper [60].

3.1.2 Comparación entre las Herramientas Ansible y Puppet

Las herramientas de automatización de las TI Ansible y Puppet son ***open source*** y ambas tienen su versión de pago que trae funcionalidades adicionales para lograr un mayor alcance en la configuración, gestión de las TI, implementación de software, actualizaciones etc.

Ansible se conoce por su facilidad de manejo, dando un enfoque más flexible que no conlleva el uso de agentes, es decir de software adicional que deba ser instalado en equipos que van a ser configurados, por otra parte, Puppet se basa en el uso de agentes para automatizar los sistemas, esto puede ocasionar ciertos problemas ya que en algunos casos son sistemas un poco más cerrados como conmutadores o enrutadores y no se puede instalar un software complementario. Python es el lenguaje utilizado por Ansible y que es más sencillo de comprender ya que no se requiere de un gran conocimiento en programación al implementar los archivos o scripts de configuración. En cambio, Puppet usa lenguaje Ruby DSL que requiere mayor comprensión para empezar a programar infraestructura como código. Ambas herramientas acogen distintos criterios para realizar la automatización de tareas. Con la herramienta Ansible se sigue una automatización procedimental ya que para realizar sus funciones se emplean pasos a seguir mientras que Puppet usa una automatización declarativa es decir se define el estado sin la necesidad de declarar los pasos a su objetivo.

A pesar de que Puppet tiene una comunidad activa en donde existen varios colaboradores que comparten su trabajo y solucionan problemas. Ansible cuenta con más proyectos que requieren de ella y el soporte para esta herramienta es aún mayor, de acuerdo con la plataforma GitHub hasta mediados del 2022 las contribuciones que se realizaron para Puppet se han visto disminuidas.

Si tenemos en cuenta la comparativa realizada entre estas dos grandes herramientas se puede abstraer que Ansible es la opción preferida por las empresas a la hora de automatizar el entorno de TI por la facilidad de uso y contar con un gran soporte tanto por su fabricante como por la comunidad activa, no necesita de software adicional, su estructura basada en playbooks es clara. Sin embargo, si se trata de una infraestructura de TI compleja es decir alrededor de 1000 servidores, Puppet es una gran opción ya que es una herramienta más potente y cuenta con una interfaz más madura y se puede implementar en casi todos los sistemas operativos.

En la Figura 3.2, se muestra las interfaces de Ansible (izquierda) y Puppet (derecha).

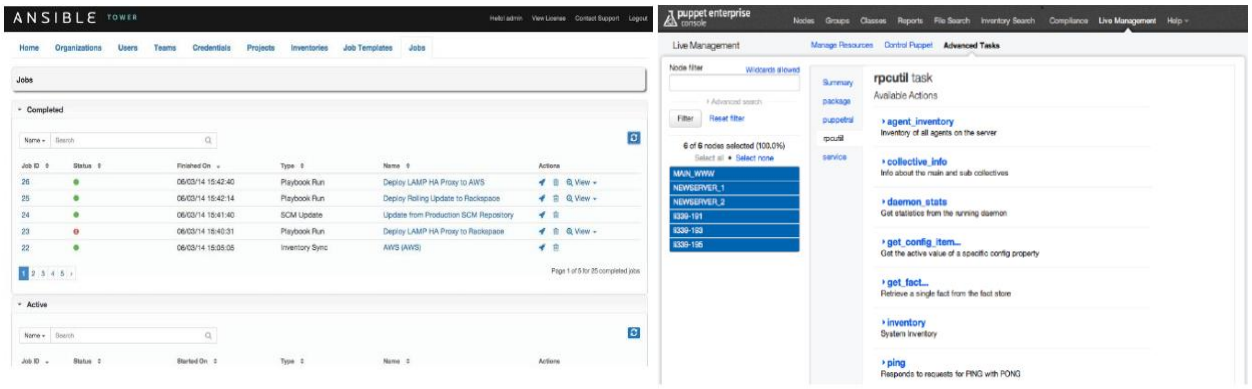


Figura 3.2 Interfaz Ansible y Puppet [61].

3.1.3 Análisis de la Arquitectura DNA de Cisco

De acuerdo con lo descrito en el capítulo 2 referente a la Arquitectura DNA de Cisco y su enfoque en la digitalización de la industria, se puede comprender que, a partir de una configuración inicial, un sin número de tareas pueden ser simplificadas. La tecnología sigue en expansión cada día y por medio del hardware flexible que tiene como su componente principal ASIC hechos de silicio los cuales son programados para su uso, y lo más importante para adaptarse a los cambios y lograr la automatización de la empresa.

Por medio de la implementación de Cisco DNA se tiene cubiertos todos los sectores tanto en gestión como en automatización, seguridad y virtualización, lo que hace de esta infraestructura muy completa y que permite la conectividad de los usuarios sin importar donde se encuentren. Si analizamos un poco más sus avances técnicos y tecnológicos se puede nombrar protocolos como VXLAN, LISP que brindan mayores avances para desarrollar el mundo virtualizado y que es en donde se obtiene mayor provecho debido a la reducción de costos, por medio de una red superpuesta en la infraestructura ya configurada, añadiendo escalabilidad y ofreciendo mayores beneficios, pero también manteniendo segura la red.

3.2 Conclusiones

- Existen varias soluciones planteadas para la automatización de las TI y sin importar el fabricante todas apuntan a mejorar la conectividad, rendimiento y economía de la empresa que las use, poniendo en consideración factores como costo de inversión inicial, interfaz amigable, tiempo de vida útil como los determinantes para escoger entre una solución u otra.

- La configuración de las herramientas de Automatización es sencilla y en el caso de Ansible al no requerir de software adicional para su funcionamiento puede estar lista para su uso en cuestión de minutos. Puppet al requerir de agentes para su funcionamiento demora un poco más, sin embargo, puede ser utilizado inmediatamente se complete la instalación del agente.
- Ansible cuenta con varios módulos usados para resolver trabajos abstractos que le permiten instalar paquetes y usar plantillas de acuerdo con la necesidad del operador. Posee requisitos simples y es una herramienta intuitiva de utilizar para aquellos se inician en la administración de configuraciones.
- Puppet es compatible con los sistemas operativos más usados en el medio, es sin duda la mejor opción si la empresa que se requiere automatizar es bastante grande, llegando a obtener beneficios en cuanto a costo y tiempo superiores a otras herramientas.
- La Arquitectura DNA de Cisco utiliza hardware y software flexibles lo que le permite mantenerse actualizada con las tecnologías y que son la base para la automatización de servicios e infraestructura de red.
- La Automatización del entorno de TI es una necesidad hoy en día, y contar con equipos adaptables como los que presenta la Arquitectura DNA de Cisco son la base para el futuro y los cambios tecnológicos que están por venir.

3.3 Recomendaciones

- Para lograr una digitalización completa de la empresa se requiere de una gran cantidad de dinero al inicio para invertir en equipos y servidores y manejar una red híbrida, dicha inversión se verá reflejada pronto debido a la mejora del rendimiento, y automatización de los servicios que ofrece.
- Se debe comparar precios al momento de adquirir un equipo que automatice la empresa, basándose en funcionalidad del dispositivo, compatibilidad con otros fabricantes, tiempo de vida útil, entre otros.
- Se debe realizar un estudio acerca de los Firewall de próxima Generación (NGFW), ya que la seguridad es un aspecto primordial y estos dispositivos tienen un enfoque a la automatización de estos servicios.

4 REFERENCIAS BIBLIOGRÁFICAS

[1] “" EL ORIGEN DE LAS TICS " by Isabel Zenteno.” https://prezi.com/kg1xnovnpwuy/el-origen-de-las-tics/ (accessed Dec. 08, 2022).

[2] “5 Ways to Automate Your IT Operations Now Leveraging Attune,” *ServerTribe*, Sep. 13, 2022. https://www.servertribe.com/5-ways-to-automate-your-it-operations-now-leveraging-attune/ (accessed Nov. 29, 2022).

[3] “¿Qué es la automatización? Ventajas e importancia de automatizar.” https://www.redhat.com/es/topics/automation (accessed Dec. 08, 2022).

[4] HIXSA, “La automatización TI impulsada por Inteligencia artificial,” *HIXSA Blog | Sobre el mercado de ITSM, RPA y Gestión documental*, Feb. 26, 2019. https://blog.hixsa.com/la-automatizacion-ti-impulsada-por-inteligencia-artificial/ (accessed Jan. 21, 2023).

[5] “What is Information Technology? Definition and Examples,” *Data Center*. https://www.techtarget.com/searchdatacenter/definition/IT (accessed Dec. 09, 2022).

[6] “¿Qué son las tecnologías de la información?,” *Ceupe*. https://www.ceupe.com/blog/que-son-las-tecnologias-de-la-informacion.html (accessed Dec. 09, 2022).

[7] “Seguridad Informática - Soluciones Amenazas Cibernéticas,” *icorp*. http://www.icorp.com.mx/solucionesTI/seguridad-informatica/ (accessed Dec. 08, 2022).

[8] “Plataforma TI (Hardware, Software),” *Sistemas de Información*, Oct. 11, 2017. https://mejorarinformacion.com/nivel-inferior/ (accessed Feb. 22, 2023).

[9] “¿Qué es la infraestructura de TI?” https://www.redhat.com/es/topics/cloud-computing/what-is-it-infrastructure (accessed Dec. 09, 2022).

[10] “What is Cloud Computing Infrastructure? | VMware Glossary,” *VMware*. https://www.vmware.com/content/vmware/vmware-published-sites/es/topics/glossary/content/cloud-computing-infrastructure (accessed Dec. 09, 2022).

[11] “La virtualización en empresas: Cómo te puede ayudar,” *Nunsys*. https://www.nunsys.com/virtualizacion/ (accessed Feb. 22, 2023).

[12] “Virtualización - Servidores y Escritorios de TI,” *icorp*. http://www.icorp.com.mx/solucionesTI/virtualizacion/ (accessed Dec. 08, 2022).

[13] “Seguridad perimetral,” *Ciberseguridad*. https://ciberseguridad.com/servicios/seguridad-perimetral/ (accessed Jan. 21, 2023).

[14] “¿Qué es la seguridad de punto final? | AppMaster.” https://appmaster.io/es/blog/que-es-la-seguridad-de-punto-final (accessed Jan. 21, 2023).

[15] “Seguridad de datos: En qué consiste y qué es importante en tu empresa.” https://www.powerdata.es/seguridad-de-datos (accessed Jan. 21, 2023).

[16] “Automatización de procesos: 5 principales beneficios en empresas.” https://www.fortra.com/es/recursos/guias/automatizacion-de-procesos-5-principales-beneficios-en-empresas (accessed Jan. 21, 2023).

[17] “¿Qué es SNMP? | Protocolo SNMP – Monitorización – Puerto SNMP - ManageEngine OpManager.” https://www.manageengine.com/es/network-monitoring/what-is-snmp.html (accessed Jan. 21, 2023).

[18] “List of Top Network Traffic Analysis (NTA) Tools 2023,” *TrustRadius*. https://www.trustradius.com/network-traffic-analysis-nta (accessed Jan. 21, 2023).

[19] A. L. A+ CCDA, CCNA, MCSE, ITILv3, MCSA, “Review: SolarWinds NetFlow Traffic Analyzer,” *Network Management Software - Reviews & Network Monitoring Tools*, Nov. 05, 2012. https://www.networkmanagementsoftware.com/review-solarwinds-netflow-traffic-analyzer-3-10-0/ (accessed Dec. 09, 2022).

[20] E. -dea N. SAS, “SolarWinds Server & Application Monitor.” https://www.e-dea.co/server-application-monitor (accessed Jan. 21, 2023).

[21] R. Ong, “About Us,” *Sirius Computer Solutions*. https://www.siriuscom.com/about-us/ (accessed Nov. 30, 2022).

[22] T. School, “¿Qué es Cisco? | Definición Redes Cisco,” *Tokio School*, Apr. 16, 2021. https://www.tokioschool.com/noticias/que-es-cisco/ (accessed Dec. 21, 2022).

[23] “Bridge to Possible,” *Cisco*. https://www.cisco.com/c/en/us/about/bridge-to-possible.html (accessed Dec. 21, 2022).

[24] J. Lemus, “Qué es Fortinet y cómo funciona,” *Vertical Ibérica*, Feb. 19, 2020. https://vertical-iberica.com/que-es-fortinet-y-como-funciona/ (accessed Dec. 05, 2022).

[25] “Enterprise IT Networking Products & Solutions | Juniper Networks US.” https://www.juniper.net/us/en/it-networking.html (accessed Dec. 21, 2022).

[26] “IT Infrastructure Solutions, Workforce technology, OEM.” https://www.dell.com/en-us/dt/solutions/index.htm (accessed Dec. 22, 2022).

[27] “Sobre Nosotros - HUAWEI Latin.” https://consumer.huawei.com/latin/about-us/ (accessed Jan. 22, 2023).

[28] “Soluciones de seguridad de redes para empresas,” *Fortinet*. https://www.fortinet.com/lat/solutions/enterprise-midsize-business/network-security.html (accessed Jan. 22, 2023).

[29] A. Garza, “¿Qué es y cómo es que funciona un Firewall FortiGate?,” *Quanti Solutions*, Feb. 15, 2022. https://quanti.com.mx/articulos/conociendo-el-firewall-fortigate/ (accessed Jan. 22, 2023).

[30] “fortigate-fortiwifi-80f-series.pdf.” Accessed: Dec. 30, 2022. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf

[31] “sb-portfolio-brief-fortiguard-ai-powered-security.pdf.” Accessed: Dec. 31, 2022. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-portfolio-brief-fortiguard-ai-powered-security.pdf

[32] “FortiGuard_Security_Services.pdf.” Accessed: Jan. 22, 2023. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGuard_Security_Services.pdf

[33] “¿Qué es seguridad en la nube o seguridad informática en la nube?,” *Fortinet*. https://www.fortinet.com/lat/resources/cyberglossary/what-is-cloud-security.html (accessed Jan. 22, 2023).

[34] “FortiCNP - Plataforma de protección de aplicaciones nativas de la nube,” *Fortinet*. https://www.fortinet.com/lat/products/public-cloud-security/cloud-native-protection.html (accessed Jan. 01, 2023).

[35] “Web Application Firewall (WAF) & API Protection,” *Fortinet*. https://www.fortinet.com/products/web-application-firewall/fortiweb (accessed Jan. 22, 2023).

[36] “Fortinet FortiWeb-4000F Hardware Only.” https://www.firewalls.com/fortiweb-4000f-hardware-only.html (accessed Jan. 22, 2023).

[37] “Seguridad de aplicaciones con FortiDevSec.” https://fortixpert.blogspot.com/2022/09/seguridad-de-aplicaciones-con.html (accessed Jan. 02, 2023).

[38] “Application Security Testing with FortiDevSec SaaS Application,” *Fortinet*. https://www.fortinet.com/products/fortidevsec (accessed Feb. 23, 2023).

[39] “Solutions & Technologies | Juniper Networks US.” https://www.juniper.net/us/en/solutions.html (accessed Jan. 12, 2023).

[40] “Juniper, con tecnología Mist AI.” https://www.westconcomstor.com (accessed Jan. 12, 2023).

[41] “vSRX Virtual Firewall | Juniper Networks US.” https://www.juniper.net/us/en/products/security/srx-series/vsrx-virtual-firewall.html (accessed Jan. 23, 2023).

[42] “vsrx-virtual-firewall-datasheet.pdf.” Accessed: Jan. 15, 2023. [Online]. Available: https://www.juniper.net/content/dam/www/assets/datasheets/us/en/security/vsrx-virtual-firewall-datasheet.pdf

[43] “ansible_configuration_management_2nd_edition.pdf.” Accessed: Oct. 30, 2022. [Online]. Available: https://profitbox.info/wp-content/uploads/2018/02/ansible_configuration_management_2nd_edition.pdf

[44] “Ansible Cheatsheet.” http://www.datadisk.co.uk/html_docs/ansible/ansible_cheatsheet.html (accessed Jan. 23, 2023).

[45] *Taller Casos de uso de automatización en infraestructura de TI con Ansible*, (May 04, 2022). Accessed: Jan. 23, 2023. [Online Video]. Available: https://www.youtube.com/watch?v=5mwDZ1Z2gFU

[46] jgarzas, “Simplifica drásticamente la administración de sistemas: Puppet en 10 min.,” *Javier Garzas*, May 16, 2014. https://www.javiergarzas.com/2014/05/puppet-en-menos-de-10-min.html (accessed Jan. 23, 2023).

[47] “puppet_tutorial.pdf.” Accessed: Dec. 22, 2022. [Online]. Available: https://www.tutorialspoint.com/puppet/puppet_tutorial.pdf

[48] “Cómo instalar Puppet en Ubuntu 20.04 LTS Focal Fossa,” *Noviello.it*, Apr. 28, 2021. https://noviello.it/es/como-instalar-puppet-en-ubuntu-20-04-lts/ (accessed Jan. 23, 2023).

[49] “jljg.pdf.” Accessed: Jan. 23, 2023. [Online]. Available: https://dit.gonzalonazareno.org/gestiona/proyectos/2012-13/jljg.pdf

[50] *Chapter 1 Why Transform Your Business Digitally?* Accessed: Jan. 23, 2023. [Online]. Available: https://learning.oreilly.com/library/view/cisco-digital-network/9780134723952/ch01.xhtml

[51] “Arquitectura de Red Digital (DNA) Cisco”.

[52] *Chapter 2 The Business Value of Cisco DNA*. Accessed: Jan. 23, 2023. [Online]. Available: https://learning.oreilly.com/library/view/cisco-digital-network/9780134723952/ch02.xhtml

[53] *Chapter 4 Introducing the Cisco Digital Network Architecture*. Accessed: Jan. 23, 2023. [Online]. Available: https://learning.oreilly.com/library/view/cisco-digital-network/9780134723952/ch04.xhtml

[54] *Chapter 5 The Cisco Digital Network Architecture Blueprint*. Accessed: Jan. 23, 2023. [Online]. Available: https://learning.oreilly.com/library/view/cisco-digital-network/9780134723952/ch05.xhtml

[55] *Chapter 6 Introduction to Cisco DNA Infrastructure*. Accessed: Jan. 23, 2023. [Online]. Available: https://learning.oreilly.com/library/view/cisco-digital-network/9780134723952/ch06.xhtml

[56] *Chapter 7 Hardware Innovations*. Accessed: Jan. 23, 2023. [Online]. Available: https://learning.oreilly.com/library/view/cisco-digital-network/9780134723952/ch07.xhtml

[57] *Chapter 8 Software Innovations*. Accessed: Jan. 23, 2023. [Online]. Available: https://learning.oreilly.com/library/view/cisco-digital-network/9780134723952/ch08.xhtml

[58] *Chapter 9 Protocol Innovations*. Accessed: Jan. 23, 2023. [Online]. Available: https://learning.oreilly.com/library/view/cisco-digital-network/9780134723952/ch09.xhtml

[59] *Chapter 10 Cisco DNA Infrastructure—Virtualization*. Accessed: Jan. 23, 2023. [Online]. Available: https://learning.oreilly.com/library/view/cisco-digital-network/9780134723952/ch10.xhtml

[60] “How to use the web UI.” https://help.fortinet.com/fweb/582/Content/FortiWeb/fortiweb-admin/web_based_manager.htm (accessed Feb. 10, 2023).

[61] “5. The Tower User Interface — Ansible Tower User Guide v3.8.6.” https://docs.ansible.com/ansible-tower/latest/html/userguide/main_menu.html (accessed Feb. 10, 2023).