



Facultad 2

Trabajo de Diploma para optar por el título de
Ingeniero en Ciencias Informáticas

Arquitectura para la gestión del equipamiento activo de redes basado en políticas

Autora: Lisandra Lazara Pedroso Guerra

Tutores: MSc. Mónica Peña Casanova
Ing. Yenlys Guerra Dávila

La Habana, 5 de junio del 2019



Pensamiento

“Si avanzo sígueme, si me detengo empújame y si retrocedo mátame...”

Ernesto Che Guevara.

Declaración de autoría

Declaro ser autora de la presente tesis que tiene por título: “Arquitectura para la gestión del equipamiento activo de redes basado en políticas” y reconozco a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la misma, con carácter exclusivo. Para que así conste firmo la presente a los __/__/2019.

Lisandra Lazara Pedroso Guerra

Firma del Autor

MSc. Mónica Peña Casanova

Firma del Tutor

Ing. Yenlys Guerra Dávila

Firma del Tutor

Datos de contacto

Tutor 1:

MSc. Mónica Peña Casanova

Graduada en 1997 de Ingeniera en Telecomunicaciones, máster en ciencias y profesora auxiliar, imparte Teleinformática en la facultad 2 y actualmente se desempeña como decana en la misma.

Universidad de las Ciencias Informáticas

Email: monica@uci.cu

Tutor 2:

Ing. Yenlys Guerra Dávila

Graduada en 2007 de Ingeniera en Ciencias Informáticas, profesora asistente, imparte Sistemas Operativos en la Facultad 2, Instructora CISCO y actualmente se desempeña como Subdirectora del Centro de Telemática.

Universidad de las Ciencias Informáticas

Email: yguerra@uci.cu

Agradecimientos

Quiero agradecerle a mi madre por ser mi columna vertebral, por llorar cuando yo lloraba y darme fuerzas cuando yo más necesitaba, gracias mami por ser como eres y estar en esta etapa de mi vida estudiando tanto como yo, ahora sí te digo ¡Lo conseguimos!

Al hombre de mis sueños mi padre, gracias por malcriarme y darme todos los consejos que siempre corría a pedirte, gracias DADDY por entenderme y soportar a tu niña cuando llegaba con algo nuevo de la escuela.

A mi hermano Alexander por estar al tanto de su princesa, por tenerme paciencia en todo momento y siempre decirme que el que persevera triunfa, pues si ale triunfé. A mi familia que estando lejos siempre están presente, que a cualquier hora en mis días de prueba estaban al tanto de mí. A los que ahora no están aquí también gracias que en estos cinco años siempre tenía que buscar un momento para ponerlos al tanto de cómo iba, gracias a todos porque somos muchos.

Quiero agradecer a mis dos tutoras, gracias profe Mónica por confiar en mi para algo tan importante en su vida profesional y servirme a mí en algo tan importante como mi trabajo de diploma. Gracias profe Yenlys por haberme guiado y ser hoy la persona que hizo posible que cada uno de mis miedos en el trabajo práctico fuera vencido. Gracias a esos profes que me formaron en estos 5 años y a muchos de ellos gracias por ser hoy más que profes, ser buenos amigos.

Sí, llegó el momento de agradecer a esa familia que he conseguido en solo 5 años, mi grupo el 02 sin prefijo delante porque les quiero agradecer a todos los que comenzaron, a los que se han ido y a los que quedamos de esa FICI gracias chicos sin ustedes este camino hubiera sido muy aburrido. A mi chivo expiatorio tengo que agradecerle por soportar mis quemaderas en esta recta final a cualquier hora ¡Gracias Jorgito! Jeniffer Justiz Viñales no porque te mencione ahora te quita importancia gracias por ser la primera persona con quien hable en esta universidad y por estar ahí no solo en los buenos y malos momentos sino también en los peores, gracias por fajarte conmigo para hacerme entender las cosas, gracias por ser mi mejor amiga todo este tiempo sin ti no hubiera hecho todas mis locuras universitarias. A mis amigos de la calle, a los que están y a los que están lejos ahora mismo, gracias por entender mis ausencias en fechas significativas y por hacerme desconectar de los estudios cuando más necesitaba, gracias chicos por ser esa mala pero necesaria influencia en mi vida. Gracias a todos.

Dedicatoria

Quiero dedicarles esta tesis a mis dos pilares fundamentales, mis padres. Gracias por estar ahí y ser parte de esta etapa de mi vida sin ustedes no lo hubiera logrado.

Resumen

El avance de las Tecnologías de la Información y las Comunicaciones (TIC) conllevan a una creciente demanda de los servicios de información y de las infraestructuras que abarcan equipos de todos tipos. Dentro de estas infraestructuras se encuentra los principales motivos para efectuar una correcta gestión en los equipos activos que albergan los servicios, ya que de ellos depende el hecho de brindar un servicio con calidad y seguridad. La gestión integrada basada en políticas se presenta como una opción viable dado que permitirá el intercambio de información de gestión en entornos heterogéneos y dispersos, a través de un modelo común de información vinculando las necesidades del negocio con la infraestructura de la organización.

En el presente trabajo se desarrolló un procedimiento para el diseño de infraestructuras TI, para alinear la operación del mismo se propone una arquitectura capaz de enmarcar la gestión del equipamiento activo basado en políticas, que permite a las entidades mejorar su gestión de recursos informáticos al construir redes altamente escalables y flexibles. En la propuesta se utiliza el Método de Diseño Basado en la Arquitectura (ABD) y el Método de Evaluación de Arquitecturas (ATAM), se valida la calidad del procedimiento propuesto a través de Redes Petri.

Palabras clave: Arquitectura, gestión de red, procedimiento, políticas, simulación, tecnologías.

Abstract

The advancement of Information and Communication Technologies leads to a growing demand for information services and infrastructures that include equipment of all types. Within these infrastructures are the main reasons to carry out a correct management in the active equipment that houses the services, since the fact of providing a service with quality and safety depends on them. Integrated management based on policies is presented as a viable option since it will allow the exchange of management information in heterogeneous environments, through a common information model linking business needs with the infrastructure of the organization.

In the present work a procedure for the design of IT infrastructures was developed, to align the operation of the same an architecture is proposed capable of framing the management of the active equipment based on policies, which allows the entities to improve their management of computing resources when building highly scalable and flexible networks. The proposal uses the Architecturally Based Design Method (ABD) and the Architectural Assessment Method (ATAM), the quality of the proposed procedure is validated through Petri Networks.

Keywords: *Architecture, network management, procedure, policies, simulation, technologies.*

Índice

Introducción	1
Capítulo I Fundamentación teórica	7
1. Introducción	7
1.1. Conceptos Relacionados	7
1.2. Gestión de redes	7
1.2.1. Elementos del sistema de gestión de red	8
1.2.2. Áreas funcionales de la gestión de redes	8
1.2.3. Evolución de la gestión de redes	10
1.2.4. Elementos generales de la Filosofía de diseño de redes Top-Down	12
1.3. Componentes de la gestión integrada de redes	12
1.3.1. Aspectos esenciales para la gestión de equipamiento activo en las redes	13
1.3.2. Protocolos y estándares	13
1.4. Metodología a utilizar	16
1.4.1. Metodología de ingeniería a utilizar siguiendo la filosofía Top Down	17
1.5. Herramientas y métodos a utilizar	18
1.5.1. Herramientas de simulación de red	18
1.5.2. Lenguaje de Modelado	21
1.5.3. Métodos para validar la simulación	22
1.6. Estado del arte	23
1.7. Conclusiones del Capítulo	26
Capítulo II Diseño lógico y físico de la arquitectura	27
2. Introducción	27
2.1. Fase de diagnóstico del negocio y propuesta para el diseño de la arquitectura	27
2.2. Propuesta de la metodología	27
2.2.1. Factores del negocio	28
2.2.2. Requerimientos del negocio	29
2.2.3. Atributos de calidad abstractos	31
2.2.4. Descripción de las vistas de la arquitectura	35
2.2.5. Salidas de la metodología	39
2.2.5.1. Estilo arquitectónico	39
2.2.5.2. Directrices de la arquitectura	39

2.2.5.3. Tabla de políticas estratificadas	40
2.3. Procedimiento para el desarrollo de la arquitectura	42
2.4. Arquitectura PBNM	42
2.4.1. Funcionamiento de la arquitectura tradicional con PBNM.....	44
2.5. Políticas a implementar en la arquitectura según sus necesidades.....	46
2.5.1. Estrategias de seguridad y calidad de servicio	47
2.6. Simulación	47
2.7. Conclusiones del Capítulo	48
Capítulo III Validación y pruebas de la arquitectura	49
3. Introducción	49
3.1. Aplicación del método de validación de la metodología mediante ATAM	49
3.2. Validación de la arquitectura implementada mediante Redes Petri	54
3.3. Escenario de evaluación de la arquitectura	56
3.4. Conclusiones del Capítulo	57
Conclusiones	58
Recomendaciones	59
Referencia Bibliográfica	60
Bibliografía	64
Anexos	68

Índice de Figuras

Figura 1: Evolución de la gestión de red (elaboración propia)	11
Figura 2: Ciclo de vida del diseño e implementación de un proyecto propuesto por la filosofía Top-Down	12
Figura 3: Análisis bibliométrico del PBNM(Según MSc. Mónica Peña Casanova).....	24
Figura 4: Modelo de estratificación de políticas.....	24
Figura 5: Problemas de las TI que ha padecido su organización (Mónica Peña Casanova, 2018)	25
Figura 6: Evaluación del impacto de la ejecución de políticas sobre las infraestructuras TI (Mónica Peña Casanova, 2018)	26
Figura 7: Fases de la metodología ABD (F. Bachmann y L. Bass, 2000)	28
Figura 8: Diagrama de caso de uso (elaboración propia).....	30
Figura 9: Vista lógica de la arquitectura (elaboración propia).....	35
Figura 10: Vista de concurrencia de políticas (elaboración propia).....	36
Figura 11: Desarrollo de las vistas (elaboración propia)	37
Figura 12: Diagrama de despliegue (elaboración propia)	38
Figura 13: Diagrama de secuencia (elaboración propia)	38
Figura 14: Estilo arquitectónico (elaboración propia)	39
Figura 15: Procedimiento de diseño de la arquitectura (elaboración propia).....	42
Figura 16: Gestión de red basada en políticas (PBNM) según el IETF.....	43
Figura 17: Arquitectura tradicional con PBNM (elaboración propia)	44
Figura 18: PDP secundario comunicación con los PEP (elaboración propia)	46
Figura 19: Imagen de la simulación.....	57

Índice de Tablas

Tabla 1: Políticas estratificadas (elaboración propia)	40
Tabla 2: Tabla de resultados de las métricas antes de aplicada la metodología (elaboración propia)	49
Tabla 3: Tabla de importancia del escenario según ATAM	50
Tabla 4: Tabla de dificultad del escenario según ATAM	50

Tabla 5:Tabla del valor del peso según ATAM	50
Tabla 6:Tabla de Importancia/Esfuerzo según ATAM.....	51
Tabla 7:Tabla de listado de escenario(elaboración propia)	51
Tabla 8:Tabla de cambio después de aplicada la metodología(elaboración propia).....	53
Tabla 9:Tabla de datos de la Red Petri(elaboración propia)	55

Introducción

Las infraestructuras de las tecnologías de la información (TI) facilitan a las organizaciones la mejora de sus procesos de negocio y la creación de nuevas formas de negocio a través de la habilitación de un grupo de capacidades de almacenamiento, procesamiento y conectividad que facilitan la distribución de información. Estas capacidades están desplegadas en entornos de alta complejidad son heterogéneas y se encuentran dispersas, de ahí que las TI tengan un rol importante en todo tipo de organizaciones, convirtiéndose en un elemento fundamental en la gestión de las organizaciones.

Según informe publicado por la consultora Gartner, una de las tendencias que marcarán la evolución de las TI, es el alineamiento de los servicios TI con los objetivos del negocio, minimizando de esta manera los costos y optimizando la calidad de dichos servicios. En este contexto, una alternativa que se ha generalizado es la gestión del equipamiento activo. (Ted Friedman, 2015)

La gestión del equipamiento de redes presenta dos modos de actuación: el monitoreo y el control. Existen múltiples herramientas para el monitoreo del equipamiento activo de redes y un conjunto de estándares para garantizar la gestión integrada en entornos heterogéneos. Para controlar y coordinar, de manera dinámica los elementos de red, tomando decisiones de forma automática a través de reglas, peticiones de usuarios o de servicios, se emplea la Gestión de red basada en políticas (PBNM). Según el grupo de trabajo de ingeniería de internet (IETF¹), un modelo de gestión basado en políticas, incluye un contenedor o repositorio de políticas, un punto de decisión de políticas o servidor de políticas (PDP²) y uno o varios puntos de ejecución de políticas (PEP³) donde se aplican o ejecutan las políticas y que gobiernan los dispositivos físicos. El agente PDP revisa las políticas almacenadas en el contenedor de políticas y efectúa un proceso de toma de decisiones. El PDP envía las decisiones tomadas, que son independientes de las características de los dispositivos a los PEP asociados, que se encargan de traducirlas en operaciones o comandos específicos que puedan ser interpretados por la tecnología concreta de los agentes que actúan en los recursos gestionados por dichos PEPs.

¹ Sigla correspondiente al término en inglés: Internet Engineering Task Force

² Sigla correspondiente al término en inglés: Policy Decision Point

³ Sigla correspondiente al término en inglés: Policy Execution Point

La implantación de políticas en la gestión del equipamiento activo a nivel mundial ha revolucionado la seguridad y calidad de los servicios, cumpliendo así con un mayor nivel de satisfacción en cuanto al avance dentro del mundo de la informática y las telecomunicaciones, dando a las grandes empresas a nivel mundial un mejor manejo de la seguridad de sus usuarios, habilitándolos para la ejecución de políticas de la organización sobre la infraestructura subyacente mediante el establecimiento de reglas para la gestión del equipamiento activo.

En Cuba el Ministerio de Comunicaciones (MINCOM) se encarga de velar por la seguridad de la información de los usuarios dentro de las redes, todo esto se protege con políticas específicas definidas según el lugar y las características de los equipos de trabajo. Tras el avance en las tecnologías el país se encuentra enfocado en la informatización de la sociedad para el cumplimiento de este objetivo, se planteó en el 7mo Congreso del PCC en el lineamiento 108. (Cuba, 2017)

“Política integral para el perfeccionamiento de la infraestructura de la informatización de la sociedad en Cuba” (Perfeccionamiento del Estado Socialista, sus sistemas y órganos de dirección); párrafo 109, que plantea: Están desarrolladas las tecnologías de la información, las comunicaciones y la automatización, de modo que contribuyen a una activa participación ciudadana -sobre todo de los jóvenes-; a la elevación del conocimiento, el nivel y calidad de vida; a la innovación, al perfeccionamiento del Estado, al desempeño de la economía nacional y de la esfera social.

Esta política integral lleva implícita la instrumentación de las políticas específicas y principios siguientes:

1. Instrumentar el Programa Nacional de Informatización, que integre y armonice por cada sector de la economía y a nivel territorial las principales prioridades del país a corto, mediano y largo plazos.
2. Desarrollar e implementar los servicios en línea entre las instituciones y hacia los ciudadanos, con prioridad en los trámites, la gestión del gobierno y el comercio electrónico.
3. Priorizar la informatización de los registros públicos del país.

4. Elaborar los planes para el desarrollo y uso de las TIC en cada sector de la economía y a nivel territorial, con prioridad en los sectores estratégicos del país. (Comunicaciones, 2017)

Bajo todas estas normas y otras establecidas por el MINCOM, organizaciones de Cuba se rigen para preservar los recursos informacionales que se distribuyen en sus redes y brindar calidad en el servicio, lo cual requiere la formación continua de los administradores de equipamiento activo debido a la vertiginosidad con que evoluciona esta tecnología. Miles de profesionales se han formado en estos últimos 15 años en las diferentes tecnologías. (Rodríguez, 2017)

Cuba se encuentra enfrascada en una estrategia dirigida por el presidente para impulsar la informatización de la sociedad, pero en la Universidad de las Ciencias Informáticas (UCI) que es un centro de alto prestigio en la formación de profesionales en la rama de la informática, existe un alto nivel de informatización de sus procesos y una alta dependencia de las infraestructuras TI, tanto para su desarrollo productivo como para la investigación, la extensión y la formación de los cursos de pregrado y posgrado (informáticas., 2019).

Por su alta demanda de las tecnologías cuenta con una infraestructura robusta y un amplio catálogo de servicios desplegados sobre ella, la cual debe ser gestionada, en especial el equipamiento. Rigiéndose por los estándares y políticas que debe presentar la arquitectura de red que tiene articulada la UCI.

En la infraestructura se hace necesario además garantizar la seguridad dentro de los puntos de acceso inalámbricos y la calidad del servicio de acuerdo con las necesidades de la organización, por lo que se debe monitorear los parámetros de funcionamiento de la red, así como los asociados al uso que hacen de esta los usuarios que se autentican y autorizan dentro de los servicios que posee la universidad. En su red se encuentran presente equipos de distintas tecnologías, estos se localizan en áreas distantes, tiene oportunidad de mejora en su gestión de funcionamiento y en su gestión de seguridad para proporcionar un buen balanceo de carga evitando así la congestión.

La infraestructura implementada no cuenta con mecanismos que faciliten la detección temprana de fallas, antes de que estas sean percibibles por los usuarios, así como el

control sobre los elementos de red que forman parte de la capa de acceso, por lo que se pierde el control de estos.

Dada la **problemática** descrita anteriormente y la necesidad de encontrar una solución para estas dificultades se plantea el siguiente **problema a resolver**:

Actualmente en la UCI, la gestión del equipamiento activo está limitada, provocando un escaso control sobre su funcionamiento.

Para dar solución a la problemática presentada se propone como **objeto de estudio** gestión del equipamiento activo de red.

El **campo de acción** se enmarca: en la gestión de red basada en políticas.

Se trazó como **objetivo general** de la investigación: Desarrollar una arquitectura capaz de enmarcar la gestión del equipamiento activo de red basado en políticas.

Las **preguntas científicas** que orientan y guían el proceso investigativo son:

- ¿Cómo se gestionan las infraestructuras de red, qué equipamiento forma parte de ellas?
- ¿Cómo se encuentra la gestión de red basada en políticas en cuanto a su aplicación en arquitecturas de red?
- ¿Cómo obtener las metodologías y herramientas para el montaje de una arquitectura de red?
- ¿Qué propuesta de solución se define para la modelación de la arquitectura?
- ¿Cómo se valida el correcto funcionamiento del procedimiento, la metodología y la arquitectura?

Para dar respuesta a mis preguntas y objetivo general se plantea el cumplimiento de las siguientes **tareas de la investigación**:

- Análisis del estado de las redes para un mayor conocimiento.
- Análisis de la gestión de redes basada en políticas para su utilización en la arquitectura.
- Selección de las metodologías y herramientas para la simulación de la arquitectura propuesta.

- Modelación de la arquitectura a montar para una correcta implementación de la misma.
- Evaluación de la arquitectura en un entorno de trabajo simulado para validar los resultados obtenidos.

La investigación está sustentada en los siguientes **métodos científicos**:

1. **Métodos teóricos:**

Histórico-Lógico para comprender a partir de la consulta de la bibliografía especializada en los temas de:

- El surgimiento y evolución de la gestión de redes.
- La aplicación de políticas en equipos de redes.
- Tecnologías para simular redes.

Analítico-Sintético para analizar y comprender la documentación relacionada con la implantación de políticas en equipos de redes.

Modelación para modelar los diferentes diagramas correspondientes al diseño de la arquitectura.

2. **Métodos empíricos:**

Entrevista para consultar a los especialistas en gestión de redes y servicios telemáticos, con el objetivo de obtener información que sustente la presente investigación.

Estructura del documento

Para una mejor comprensión de la investigación, el contenido del presente trabajo de diploma se encuentra estructurado en 3 capítulos, conclusiones, recomendaciones, bibliografía y anexos. Los contenidos a tratar en cada capítulo son:

Capítulo 1: Fundamentación teórica. Se abordan temas relacionados con la gestión de redes, los equipos activos en las redes, sobre las políticas y estándares. Descripción de las herramientas, metodología y tecnologías a utilizar en el desarrollo de la arquitectura. Estado del arte nacional e internacional sobre las diferentes tecnologías que aplican la gestión basada en políticas.

Capítulo 2: Diseño lógico y físico de la arquitectura. Se evidencia un procedimiento como guía para la planeación de la infraestructura de red. Se muestran los escenarios para redes cableadas e inalámbricas y se describe implementación de las políticas en el escenario simulado.

Capítulo 3: Validación al procedimiento y a la metodología utilizada. Se presenta la validación de la arquitectura simulada, se le aplican pruebas a los distintos escenarios simulados.

Capítulo I Fundamentación teórica

1. Introducción

En este capítulo se realiza un estudio de los conceptos y definiciones relacionados con el tema de la investigación, los cuales son abordados en su desarrollo. Incluye una profundización en la gestión del equipamiento activo de red y sus áreas funcionales, los componentes de redes, las iniciativas y estándares, así como los protocolos. Se hace referencia sobre los elementos del equipamiento activo y las tecnologías.

1.1. Conceptos Relacionados

Política: Según Strassner (Strassner, 2001) define política como un conjunto de reglas que se utilizan para gestionar y mantener el control de los cambios y/o el estado de uno o varios objetos gestionados.

Procedimiento: Según la ISO 9000 (9000, 2015) un procedimiento es una forma específica para llevar a cabo una actividad o un proceso.

Tecnología: Según (Cristina Leiceaga Abal, 2016) la tecnología se define como el conjunto de conocimientos y técnicas que, aplicados de forma lógica y ordenada, permiten al ser humano modificar su entorno material o virtual para satisfacer sus necesidades, esto es, un proceso combinado de pensamiento y acción con la finalidad de crear soluciones útiles.

Simulación: Según Thomas T. Gold Smith Jr. y Estle Ray Mann (Thomas T. Gold Smith Jr., 2014) la definen así: "Simulación es una técnica numérica para conducir experimentos en una computadora digital. Estos experimentos comprenden ciertos tipos de relaciones matemáticas y lógicas, las cuales son necesarias para describir el comportamiento y la estructura de sistemas complejos del mundo real a través de largos períodos de simulación.

1.2. Gestión de redes

Gestión de red: Es la planificación, organización, supervisión y control de los elementos que forman una red y del rango de capacidades suministradas para garantizar un nivel de servicio de acuerdo a un costo. Pretende optimizar la pertinencia, disponibilidad y rendimiento de las redes y capacidades suministradas e incrementar su efectividad

alcanzándose una mayor productividad en la institución y un aumento de la satisfacción de los usuarios. (Tejedor, 2005)

1.2.1. Elementos del sistema de gestión de red

Los elementos del sistema de gestión de red, bajo el **paradigma gestor-agente**, se clasifican en dos grupos: Según el autor Ramón Millán Tejedor (Tejedor, 2005) en la planificación y gestión de redes.

- Los **gestores** son los elementos del sistema de gestión que se interrelacionan con los operadores humanos y desencadenan acciones necesarias para llevar a cabo las tareas por invocadas por ellos.
- Los **agentes**, son los componentes del sistema de gestión invocados por el gestor o gestores de la red.

El principio de funcionamiento reside en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Habitualmente, los agentes mantienen en cada nodo gestionado información acerca del estado y las características de funcionamiento de un determinado recurso de la red. El gestor pide al agente, a través de un protocolo de gestión de red, que realice determinadas operaciones con estos datos de gestión, gracias a las cuales podrá conocer el estado del recurso y podrá influir en su comportamiento.

Cuando se produce alguna situación anómala en un recurso gestionado, los agentes, sin necesidad de ser invocados por el gestor, emiten los denominados eventos o notificaciones que son enviados a un gestor para que el sistema de gestión pueda actuar en consecuencia.

1.2.2. Áreas funcionales de la gestión de redes

Según el modelo de gestión ISO⁴ clasifica las tareas de los sistemas de gestión en cinco áreas funcionales. La tarea del encargado de gestionar una red empresarial será evaluar la plataforma de gestión a utilizar en cuanto a la medida en que dicha plataforma resuelva la problemática de gestión en cada una de estas áreas (Tejedor, 2005):

⁴ Sigla correspondiente al término en inglés: Open Systems Interconnection

Gestión de configuración

El objetivo de la gestión de configuración es obtener datos de la red y utilizarlos para incorporar, mantener y retirar los distintos componentes y recursos a integrar. Consiste en la realización de tres tareas fundamentales:

- Recolección automatizada de datos sobre el inventario y estado de la red, tales como versiones software y hardware de los distintos componentes.
- Cambio en la configuración de los recursos.
- Almacenamiento de los datos de configuración.

Gestión de rendimiento

La gestión de rendimiento tiene como objetivo principal el mantenimiento del nivel de servicio que la red ofrece a sus usuarios, asegurándose de que está operando de manera eficiente en todo momento. La gestión de rendimiento se basa en cuatro tareas:

- Recogida de datos o variables indicadoras de rendimiento, tales como el throughput⁵ de la red, los tiempos de respuesta o latencia, la utilización de la línea, etc.
- Análisis de los datos para determinar los niveles normales de rendimiento.
- Establecimiento de umbrales, como indicadores que fijan los niveles mínimos de rendimiento que pueden ser tolerados.
- Determinación de un sistema de procesamiento periódico de los datos de prestación de los distintos equipos, para su estudio continuado.

Gestión de contabilidad

La gestión de contabilidad tiene como misión la medida de parámetros de utilización de la red que permitan a su explotador preparar las correspondientes facturas a sus clientes. Entre las tareas que se deben realizar en esta área, están:

- Recolección de datos sobre la utilización de los recursos.
- Establecimiento de cuotas.

⁵ Significado: La tasa promedio de éxito en la entrega de un mensaje sobre un canal de comunicación. Este dato puede ser entregado sobre un enlace físico o lógico, o a través de un cierto nodo de la red.

- Cobro a los usuarios con las tarifas derivadas de la utilización de los recursos.

Gestión de fallos

La gestión de fallos tiene por objetivo fundamental la localización y recuperación de los problemas de la red. La gestión de fallos de red implica las siguientes tareas:

- Determinación de los síntomas del problema.
- Aislamiento del fallo.
- Resolución del fallo.
- Comprobación de la validez de la solución en todos los subsistemas importantes de la red.
- Almacenamiento de la detección y resolución del problema.

Gestión de seguridad

La misión de la gestión de seguridad es ofrecer mecanismos que faciliten el mantenimiento de políticas de seguridad (orientadas a la protección contra ataques de intrusos). Entre las funciones realizadas por los sistemas de gestión de seguridad, están:

- Identificación de recursos sensibles en la red, tales como ficheros o dispositivos de comunicaciones.
- Determinación de las relaciones entre los recursos sensibles de la red y los grupos de usuarios.
- Monitorización de los puntos de acceso a los recursos sensibles de red.
- Almacenamiento de los intentos de acceso no autorizados a estos recursos, para su posterior análisis.

1.2.3. Evolución de la gestión de redes

Las redes han creado las condiciones para el despliegue de servicios variados que demandan cada vez más prestaciones de conectividad, integrándolos a sus plataformas computacionales, es por ello que cada día, las redes evolucionan para poder satisfacer todas y cada una de las expectativas planteadas.

En ese sentido, la gestión de redes da un paso adelante sobre todos y cada uno de estos aspectos, los cuales han venido evolucionando a la par con cada uno de los diferentes servicios que proporcionan las redes de datos. (Chacín, 2010)

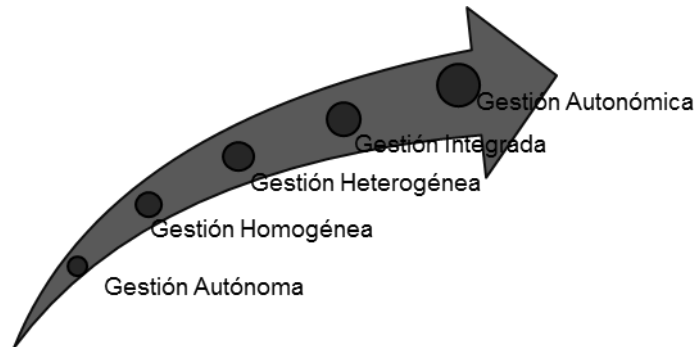


Figura 1: Evolución de la gestión de red (elaboración propia)

- Gestión Autónoma: Gestión local en cada nodo, alto costo de gestión, incompatibilidad.
- Gestión Homogénea: Un único nodo de gestión, redes de un mismo fabricante.
- Gestión Heterogénea: Poca eficiencia y efectividad. Cada fabricante con su solución de gestión: diferentes programas con las mismas funcionalidades, información en BD redundante y posiblemente inconsistente.
- Gestión Integrada: Protocolos para normalizar comunicaciones: SMTP, CMIS/CMIP. Normalizado el nombre y formato de respuesta de los elementos de red, normalizar la información. (IBM, 2011)
- Gestión Autónoma: Donde se alcanza la automatización completa de los procesos, que ellos ante fallas y errores sean capaces de dar su propia evaluación para así poder dictaminar una solución todo esto bajo estudios de IoT⁶ e inteligencia artificial.

⁶ Significado del término en inglés: Internet of things

1.2.4. Elementos generales de la Filosofía de diseño de redes Top-Down

La filosofía de diseño de redes Top-Down (Oppenheimer, 2011) tiene como objetivo lograr que el diseño elaborado satisfaga las metas y los requerimientos técnicos de la entidad cliente. Cada parte nueva es entonces redefinida, cada vez con mayor detalle, hasta que la especificación completa es lo suficientemente detallada para validar el modelo. Para lograrlo plantea cuatro fases definidas en un proceso iterativo y cíclico como muestra la siguiente figura:

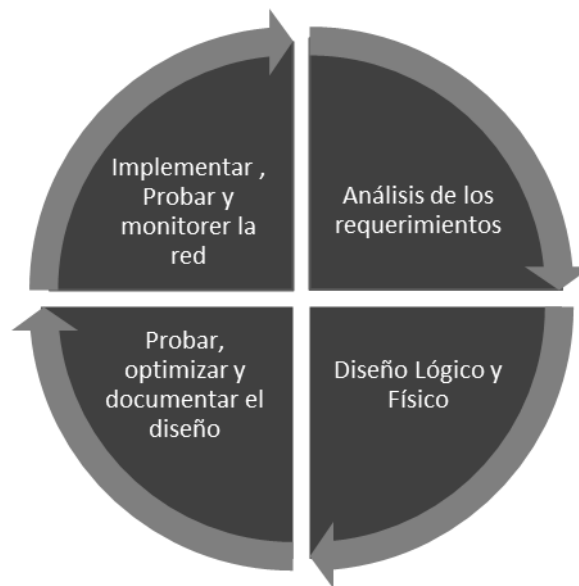


Figura 2: Ciclo de vida del diseño e implementación de un proyecto propuesto por la filosofía Top-Down

1.3. Componentes de la gestión integrada de redes

Los componentes de una red son los encargados de permitir la comunicación entre uno o varios equipos, estos tienen disímiles formas de trabajo y vías para la comunicación y son diferenciados en grupos según sus funciones en una red. En este trabajo se ha decidido solo hacer mención de los componentes que van a encontrarse en el diseño de la arquitectura, ver Anexo 1 las características de los componentes.

- **Tarjeta de red:** Es un componente que permite a la computadora comunicarse a través de una red. Este componente es frecuentemente incorporado en la placa en las computadoras actuales, pero también puede ser una tarjeta separada para su uso en una ranura PCI, o parte de una unidad externa que se conecte al

ordenador mediante un puerto USB. Las tarjetas de red se clasifican según operan en las redes cableadas o inalámbricas. Sin embargo, algunas tarjetas son compatibles con ambos tipos de redes. (Marugan, 2010)

- **Cableado de red:** Los cables de red son los medios físicos que se utilizan para transmitir información entre ordenadores. (Cisco, 2019)
- **Enrutadores de red:** Los enrutadores de red se utilizan para conectar redes, estos pueden conectar grupos de equipos que estén separados por una pared o por un océano. Los enrutadores de red modernos son en realidad la combinación de unidades que contienen un enrutador y un conmutador de red, además de otras funciones. (Cisco, 2019)

1.3.1. Aspectos esenciales para la gestión de equipamiento activo en las redes

Para la obtención de los aspectos esenciales que se necesitan gestionar en el equipamiento activo se debe saber que estos se llevan mayormente en un control que debe tener el administrador de red, o sea un inventario de los activos (software y hardware) para así poder tener registradas las amenazas, las oportunidades, las fortalezas y las debilidades con que cuenta la red.

El inventario lleva la medición de todos los elementos que influyen en la obtención de una red persistente dentro de una organización desde el presupuesto, las tecnologías con que cuenta, el centro donde va a ser montada la arquitectura y otros aspectos a medir por parte de los administradores de red.

1.3.2. Protocolos y estándares

Organización DMTF

DMTF⁷ es una organización industrial que desarrolla, mantiene y promueve estándares para la gestión de sistemas en entornos de TI empresariales. Estos estándares permiten la construcción de los componentes de infraestructura de gestión de sistemas de forma independiente de la plataforma y de neutralidad tecnológica. Mediante la creación de estándares abiertos de la industria, DMTF ayuda a habilitar la interoperabilidad de

⁷ Siglas correspondientes al término en inglés: Distributed Management Task Force

sistemas de gestión entre productos de TI de diferentes fabricantes o empresas. (IBM, 2018)

Iniciativas y estándares del DMTF

Entre los estándares de DMTF se incluyen: (IBM, 2018)

Common Information Model (CIM) :El esquema CIM es un esquema conceptual que define cómo los elementos gestionados en un entorno de TI (por ejemplo, ordenadores o redes de área de almacenamiento) se representan como un conjunto común de objetos y relaciones entre ellos. CIM es extensible para permitir ampliaciones específicas de productos para la definición común de estos elementos gestionados. CIM utiliza un modelo basado en UML para definir el esquema CIM. CIM es la base para la mayoría de los otros estándares DMTF.

Common Diagnostic Model (CDM): El esquema CDM es una parte del esquema CIM que define cómo los diagnósticos del sistema deben ser incorporados en la infraestructura de gestión.

Web-Based Enterprise Management (WBEM): Define protocolos para la interacción entre componentes de infraestructura de gestión de sistemas que implementan CIM, un concepto de perfiles de gestión de DMTF, que permite definir el comportamiento de los elementos definidos en el esquema CIM, el CIM Query Language (CQL) y otras especificaciones necesarias para la interoperabilidad de la infraestructura CIM.

Systems Management Architecture for Server Hardware (SMASH): Es una iniciativa de gestión de DMTF que incluye perfiles de gestión para la gestión de hardware de servidor. SMASH 2.0 permite WS-Management o SM-CLP (un protocolo de línea de comandos para interactuar con la infraestructura CIM). SM-CLP fue adoptado como un estándar internacional en agosto de 2011 por el Comité Técnico Mixto 1 (JTC 1) de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).

System Management BIOS (SMBIOS): Se define cómo la interfaz de la BIOS de los sistemas de arquitectura x86 es representada en CIM (y DMI).

Alert Standard Format (ASF): Se define el control remoto y las interfaces de alerta para entornos carentes de sistema operativo (por ejemplo, un controlador de la placa base de un PC).

Directory Enabled Network (DEN): Se define cómo los directorios LDAP pueden ser usados para proporcionar acceso a los elementos gestionados por CIM y define las asignaciones de CIM a LDAP para una parte del esquema CIM, entre otros.

Protocolo CIM/XML

Con el fin de optimizar su funcionamiento, los sistemas de energía eléctrica son controlados desde puestos remotos. Estos sistemas de gestión remotos están formados por distintas aplicaciones. Cada una de estas aplicaciones permite la realización de una funcionalidad de gestión determinada: cálculo de flujo de cargas óptimo, análisis de los eventos transitorios en la red, configuración de los sistemas de protecciones, gestión de activos, software SCADA⁸ para el control y supervisión de la red en tiempo real, etc.

A pesar de que cada aplicación se centra en una funcionalidad concreta, muchas de ellas, en ocasiones, comparten una misma información de entrada. Así, por ejemplo, la mayor parte de las aplicaciones de un sistema de gestión remoto deben importar la información acerca de la topología de la red eléctrica que van a gestionar. También puede ocurrir que la información de salida que genere una determinada aplicación tras haber realizado sus cálculos sirva como información de entrada para otra aplicación. Estas situaciones también se pueden dar entre aplicaciones de distintos sistemas de gestión. En definitiva, hay información relacionada con el sistema eléctrico que se repite en distintas aplicaciones de un mismo o de diferentes sistemas de gestión remotos. Ante este hecho, se podría optar por introducir varias veces esta información en el sistema. Sin embargo, esta opción no es nada eficiente, ya que supone un trabajo extra innecesario, aumenta las probabilidades de introducir la información erróneamente y, por tanto, puede dar lugar a incongruencias.

Por este motivo, lo más lógico es que exista un intercambio de información entre las aplicaciones de software de gestión de las redes eléctricas. El problema es que, en general, dichas aplicaciones son desarrolladas por distintos fabricantes y los esquemas de modelamiento de los datos son a discreción de los requerimientos la empresa. Esto implica que cada aplicación tiene su propia manera de organizar la información y cuenta con un formato propio para intercambiarla. De este modo, para cada dos aplicaciones que deban intercambiar información es necesario un convertidor de formato. La existencia de

⁸ Siglas correspondientes al término en inglés: Supervisory Control And Data Acquisition

convertidores incrementa el costo computacional y la complejidad de los sistemas de gestión de las redes eléctricas.

La definición de un modelo de información único para el intercambio de información basada en dicho modelo, reduce de manera considerable la complejidad y costo computacional de los sistemas de gestión remoto. Así, en un sistema de n aplicaciones, en el peor de los casos (si ninguna de las aplicaciones tuviese implantado el CIM), serían necesarios n convertidores de formato. Por el contrario, sin la intervención de CIM XML como un formato común de intercambio, se necesitarían $n(n-1)$ convertidores para la interacción entre las n aplicaciones. Minimizar la complejidad de los sistemas implica una mejoría en su funcionamiento y fiabilidad. (Optimal generator start-up strategy for bulk power system restoration., 2012)

1.4. Metodología a utilizar

Una arquitectura de referencia define la infraestructura común a todos los sistemas de un dominio en particular, componentes o subsistemas que incluyen y las interfaces que deben ofrecer dichos componentes o subsistemas (Shaw, 1994). Disponer de tal arquitectura facilita enormemente el desarrollo de nuevas aplicaciones dentro del dominio de solución en la cual se enmarca, pues permite por un lado la reutilización de modelos y componentes, y por otro ofrece un marco para el desarrollo de los mismos. Es un recurso que contiene un conjunto coherente de buenas prácticas arquitectónicas, para su empleo por todos los equipos de desarrollo de una organización, siendo una guía para la construcción de los productos en una línea de desarrollo de software y sistemas. Su utilización en empresas que presentan una organización en líneas de productos, es crucial, ya que permite potenciar la reutilización de alto nivel desde etapas tempranas del proceso, estableciendo buenas prácticas para el desarrollo de las soluciones para la cual está definido. (F. J. Ortiz Zaragoza, 2005)

En el presente trabajo no se trabaja directamente con requisitos funcionales, se hace uso de las políticas a implementar en una red como si fueran los requisitos a cumplir por un software, se realiza el estudio de varias metodologías que llevan interrelación con la filosofía Top Down lo que permite utilizar el término de requisito como política.

1.4.1. Metodología de ingeniería a utilizar siguiendo la filosofía Top Down

En este sentido existen diversos métodos para diseñar, documentar y evaluar las arquitecturas de red, entre los más destacados se pueden encontrar:

- **Lenguaje de Descripción de Arquitectura (ADL):** Proporciona un modelo explícito de componentes, conectores y sus respectivas configuraciones. Los ADLs permiten modelar una arquitectura mucho antes que se lleve a cabo la programación de las aplicaciones que la componen, analizar su adecuación, determinar sus puntos críticos y eventualmente simular su comportamiento (C. Billy Reynoso, 2004.). Estos lenguajes ocupan una parte importante del trabajo arquitectónico, sirven de soporte para el análisis y las decisiones tempranas del diseño, y son factibles en la construcción de herramientas que asistan en el proceso de desarrollo.
- **Lenguaje Unificado de Modelado (UML):** Es un lenguaje de modelado visual que se emplea para especificar, visualizar, construir y documentar los artefactos de un sistema de software (Larman, 2006). Se ha convertido en un estándar para los sistemas de software, gestionado por el Object Management Group (OMG). Su objetivo es lograr modelos que, además de escribir conciergo grado de formalismo tales sistemas, puedan ser entendidos por los clientes o usuarios de aquello que se modela. (J. Rumbaugh, 1998)
- **Diseño Guiado por Atributos (ADD):** Es una metodología que define los pasos que deben llevar a cabo para la construcción de la arquitectura de un sistema de información, desde la perspectiva de sus requerimientos no funcionales. Es un enfoque para definir una arquitectura de software en el cual el proceso de diseño está basado en los requerimientos de calidad del software. Se basa esencialmente en un ciclo del tipo "Planear, Realizar, Verificar". (P. Clements, F. Bachmann, L. Bass, D. Garlan, J. Ivers, R. Little, R. Nord, y J. Stafford, Addison-Wesley, , 2002)
- **Método de Diseño Basado en la Arquitectura (ABD):** Es un método de desarrollo en el que el diseño de arquitecturas se basa en los requisitos de calidad y que sigue una filosofía Top-Down a partir de una descomposición funcional del problema y una división del sistema en subsistemas más simples, eligiendo a cada paso el estilo arquitectónico más adecuado, en cada iteración del proceso de diseño, se realiza un proceso de evaluación para determinar si se cumplen los requisitos establecidos. (F. Bachmann y L. Bass, 2000)

- **Método de Análisis de Acuerdos de Arquitectura (ATAM):** Es un método de evaluación de arquitectura de software desarrollado e impulsado por el SEI, está inspirado entre áreas distintas, los estilos arquitectónicos, el análisis de atributos de calidad y el Método de Análisis de Arquitecturas de Software (SAAM). Es una técnica que permite analizar arquitecturas de software con el objetivo de validar requerimientos de atributos de calidad, su interacción (conocidos como tradeoffs), detectar problemas de manera temprana e identificar riesgos y puntos sensibles. Se concentra en la identificación de los estilos arquitectónicos o enfoques arquitectónicos utilizados sobre la base de la técnica de escenarios. El método comprende nueve pasos, agrupados en las fases presentación, investigación y análisis, pruebas e informes. (K. R., 2000)

1.4.1.1. Evaluación de la metodología a seguir

Teniendo en cuenta el análisis realizado sobre los métodos existentes para especificar, documentar y validar una arquitectura en la presente investigación para llevar a cabo la obtención de la arquitectura basada en PBNM, se seguirá una aproximación centrada en la arquitectura de red, como la que propone el método ABD. Esta decisión se fundamenta a partir del cotejo de los métodos existentes, donde se ha podido apreciar que para diseñar una arquitectura de referencia para un dominio específicos, hay que abordar las decisiones estratégicas de diseño arquitectónico al principio del ciclo de diseño, de forma que estas decisiones sean tenidas en cuenta más adelante en la fase de diseño detallado de la arquitectura. Precisamente ABD es el método adecuado puesto que establece un procedimiento especialmente enfocado al diseño de arquitecturas de referencia, sistemas de larga vida operativa. ABD tiene en cuenta la evaluación de la arquitectura que se está diseñando, incluyendo pequeñas validaciones a través de la metodología ATAM en su proceso de diseño.

1.5. Herramientas y métodos a utilizar

1.5.1. Herramientas de simulación de red

Para aplicar y evaluar la propuesta de arquitectura PBNM se emplea un software de simulación de redes, con una interfaz gráfica de usuario que admite la creación de una topología de red física que permite configurar y gestionar los dispositivos. Para la selección de esta herramienta de simulación se tienen en cuenta un conjunto de

soluciones de este tipo, cuyas características y funcionalidades se describen a continuación.

Packet Tracer

Packet Tracer es una herramienta gráfica de simulación de red desarrollada por Cisco que ofrece un entorno de simulación basado en el aprendizaje para diseñar y configurar soluciones sobre equipamiento de Cisco. (Cisco., 2019)

Esta herramienta ofrece una interfaz de usuario muy fácil de manejar con dos espacios de trabajo donde el usuario puede realizar las soluciones: el lógico y el físico. El espacio de trabajo lógico permite la creación de la topología de red, la configuración de los diferentes dispositivos de red, la interconexión del mismo mediante interfaces de varios tipos y el soporte de redes remotas multiusuario. Por su parte, el espacio de trabajo físico proporciona una visión general de la topología de red creada, la distribución del equipamiento físicamente, la estructura del cableado y la administración de cobertura inalámbrica. Además, Packet Tracer incluye un modo de simulación que permite el control y el análisis del tráfico de los paquetes en la red, así como de sus campos y los valores que contienen. (Cisco., 2019)

eNSP

eNSP (*Enterprise Network Simulation Platform*) es una herramienta de simulación de red libre, extensible y gráfica desarrollada por Huawei. Esta aplicación permite el despliegue de soluciones sobre equipamiento de Huawei en diferentes escenarios de red. (Co., Huawei Technologies, 2018)

eNSP proporciona una interfaz de usuario gráfica conveniente para simplificar las operaciones en una gestión de redes compleja y les permite a los usuarios ver los modelos de dispositivo y obtener ayuda en línea sobre configuración del equipamiento y documentación de dispositivos.

eNSP puede enlazar los adaptadores en red físicos para llevar a cabo la conexión entre los dispositivos simulados y los dispositivos reales, permitiendo una gestión de redes flexible. Cuenta también con soporte para Virtual Box lo que permite implementar nuevos servicios a través de nodos virtuales. En el modo del despliegue distribuido, el servidor del

eNSP se despliega en los múltiples servidores, formando una red compleja, y se asignan recursos en los servidores automáticamente.

eNSP en general, proporciona una plataforma de la simulación basada en redes que es fácil de usar y apoya las interfaces gráficas del usuario o GUI (*Graphic User Interface*, por sus siglas en inglés) extensibles. (Co., Huawei Technologies, 2018)

GNS3

GNS3 es un software de código abierto de simulación de red que permite diseñar topologías de redes complejas y poner en marcha simulaciones sobre ellas, tiene una interfaz gráfica intuitiva que permite la gestión de dispositivos a través de un motor de emulación denominado Dynamips que permite a los usuarios ejecutar imágenes binarias del IOS de Cisco Systems. Dynamips permite probar y experimentar las capacidades del IOS de Cisco, revisar configuraciones rápidas para luego utilizarlas en routers reales, y especifica configuraciones de hardware para routers virtuales específicos. (GNS3, 2018)

GNS3 se puede utilizar para experimentar con características o para comprobar configuraciones que necesitan ser desplegadas más adelante en dispositivos reales e incluye funcionalidades que permiten, por ejemplo, la conexión de la red virtual con redes reales y capturas de paquetes utilizando aplicación Wireshark provee administración vía comandos para listar los dispositivos, iniciar, detener, recargar, suspender, resumir, y conectar a las consolas de los routers virtuales. (GNS3, 2018)

OMNeT++

OMNeT++ es un software simulador de red enfocado al área académica y orientado a modelar y simular eventos discretos en redes de comunicaciones a través de la recreación de dichos eventos discretos por módulos orientados a objetos. OMNeT++ es una versión libre, de la versión comercial OMNEST desarrollado por Omnest Global, Inc. Esta herramienta se puede ejecutar perfectamente sobre sistemas operativos Windows y sobre algunas versiones de UNIX y Linux, usando varios compiladores de C++. (Sitio Oficial OMNeT++. , 2019)

Este simulador, utiliza el lenguaje de programación NED, que se basa en el lenguaje C++; como herramienta para modelar topologías de red; este lenguaje facilita la descripción modular de una red, es decir, un modelo en OMNeT++ se construye con módulos jerárquicos mediante el lenguaje NED, dichos módulos pueden contener estructuras

complejas de datos y tienen sus propios parámetros usados para personalizar el envío de paquetes a los destinos a través de rutas, compuertas y conexiones, componentes y especificaciones de la descripción de una red de comunicaciones.

Con el fin de facilitar el diseño de redes y la simulación de eventos sobre las mismas, OMNeT++, permite al usuario trabajar gráficamente empleando el editor del lenguaje NED (GNED). Este editor es la interfaz gráfica que permite crear, programar, configurar y simular redes de comunicaciones, sin necesidad de hacerlo utilizando la codificación del lenguaje NED. Las simulaciones en OMNeT++ pueden utilizar varias interfaces de usuario, dependiendo del propósito. La interfaz más avanzada permite visualizar el modelo, controlar la ejecución de la simulación y cambiar variables/objetos del modelo. Esto facilita la demostración del funcionamiento de un modelo. (Sitio Oficial OMNeT++. , 2019)

OMNeT++ es una herramienta multiplataforma gratuita solamente para propósitos académicos, lo que facilita su utilización en universidades y grupos de investigación. Sin embargo, para su uso en estos fines, tiene un alto grado de complejidad en su manejo ya que es necesario saber programar en lenguaje NED, pues el trabajo con el editor gráfico no permite acceder a todas las posibilidades de configuración.

1.5.1.1. Evaluación de las herramientas de simulación de red

Luego del análisis realizado a las herramientas anteriormente expuestas se decide trabajar con Cisco Packet Tracer al ser una herramienta que facilita trabajar en entornos de aprendizaje y no es de un nivel complejo para la simulación de la topología que se necesita montar siguiendo la arquitectura PBNM. Packet Tracer cuenta con los equipos necesarios para satisfacer los elementos que trae PBNM integrada y a su vez poder mostrar la gestión que se realiza con el equipamiento activo dentro de la red tradicional.

1.5.2. Lenguaje de Modelado

Para el desarrollo de los procesos de la simulación se empleó el lenguaje UML (Stevens Perdita, 2002), al ser un lenguaje de modelado para especificar o para describir métodos o procesos. En el caso de presente investigación se utiliza para evidenciar los artefactos generados dentro de la metodología seleccionada.

Este se generó en la herramienta Visual Paradigm en su versión 8.0 con el objetivo de obtener todos los artefactos necesarios.

1.5.3. Métodos para validar la simulación

Existen disímiles vías para validar una simulación de red, dentro de estas se encuentran métodos y herramientas que permiten dar justificación de lo simulado mediante las herramientas de trabajo. Para obtener la herramienta o el método para validar la simulación se realiza un análisis según sus características.

Redes Petri

Según los autores (Pedro Solana González, Margarita Alonso Martínez, Danile Perez González, 2010) , las Redes Petri se destacan como método formal de la especificación de proceso de negocios estructurados , por su semántica formal , por su modo de representación gráfica, por su expresividad y por las relevantes técnicas que ofrecen, estas técnicas modelan las transacciones (partes activas del proceso) y los estados de forma explícita de manera que los últimos son considerados elementos de primera clase, al contrario de otras técnicas de modelado, que se centran exclusivamente en las actividades. Por ende, esta técnica puede ser aplicada en los entornos simulados, al trabajar las necesidades de la red como las transacciones del negocio.

Policy Continuum

Según los autores (Steven Davy , Brendan Jennings , John Strassner , 2008), la política del continuo es un componente fundamental de cualquier aplicación de dirección política-basado para el autonómico conectando a una red de computadoras, pero aún no se tiene ninguna semántica operacional formal. Esta propone un modelo de política del continuo y el proceso de creación de política, que demuestran las propiedades importantes que pusieron un continuo aparte de un modelo de la política non-jerárquico.

Como la parte de creación del proceso de políticas, se presenta una política de conflicto y el análisis del algoritmo que las influencias, el modelo de información, haciéndolo aplicable a las aplicaciones arbitrarias y niveles del continuo. El acercamiento para el análisis de conflicto de política trae consigo analizar una política candidata (o recientemente creada o modificada) en una base par-sabia con las políticas ya

desplegadas y si se dan conflictos potenciales entre las políticas atrasadas el autor de la política debe aplicar el método. (Steven Davy , Brendan Jennings , John Strassner , 2008)

Es un algoritmo de dos fases que primeramente determina las relaciones entre el par de políticas y segundo aplica el modelo del conflicto específico para determinar si las políticas deben marcarse como potencialmente en conflicto y con las métricas propuestas se llega al completo análisis de si es válida la utilización de dichas políticas.

1.5.3.1. Evaluación de los métodos de validación de la simulación

Luego de lo antes descrito se decide trabajar con la Red Petri, ya que el método de Policy continuum es un método aún en desarrollo que aporta alta innovación y seguridad en cuanto a la validación de las redes, pero la Red Petri permite validar la calidad del procedimiento e integrarle las políticas que se obtienen de la salida de la metodología, este evalúa que la calidad del procedimiento cumpla con la necesitada en la infraestructura a articular.

1.6. Estado del arte

En el transcurso de los años y aún con el rápido avance de las telecomunicaciones se ve el desarrollo que están teniendo las nuevas tecnologías, según un análisis bibliométrico⁹ realizado por la MSc. Mónica Peña Casanova (ver figura 3) se puede identificar la vigencia del empleo del PBNM¹⁰ asociada a las nuevas tecnologías, utilizando palabras clave: PBM SDN, PBM Cloud, PBM NFV, PBM Datacenter, en varias de las más prestigiosas bases de datos internacionales en el período comprendido entre los años 2015 a 2018, el cual corrobora el empleo creciente de la Gestión Basada en Políticas en las nuevas tecnologías (Mónica Peña Casanova, 2018).

⁹ Concepto: Es el estudio bibliográfico de las tecnologías que lo aplican

¹⁰ Siglas correspondientes al término en inglés: Policy Based Network Management

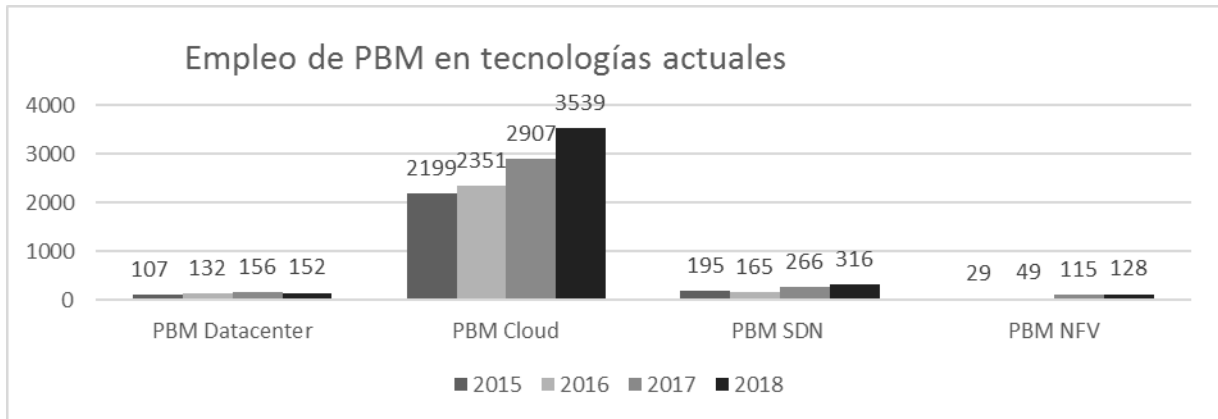


Figura 3: Análisis bibliométrico del PBNM (Según MSc. Mónica Peña Casanova)

En la figura 4 se pone en evidencia las vistas de la arquitectura PBNM, van hacer analizadas la evolución de todas las vistas para obtener sus avances dentro de la gestión de políticas en el equipamiento activo.

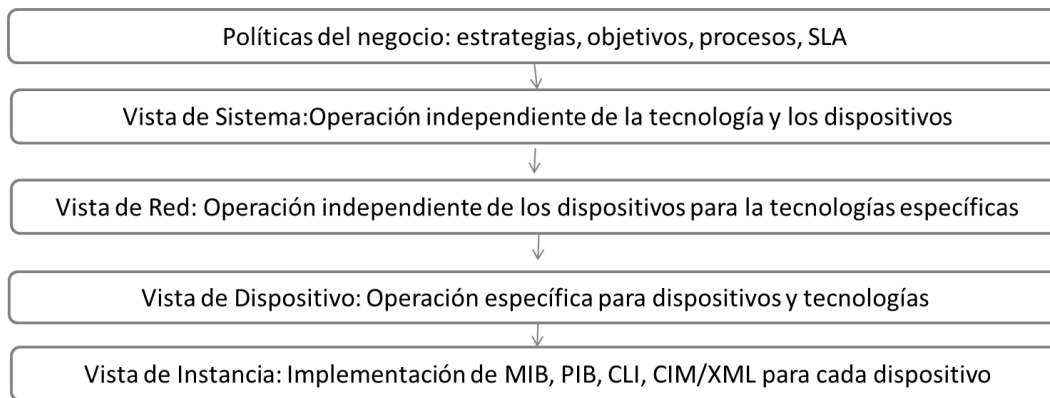


Figura 4: Modelo de estratificación de políticas.

Mientras que el incremento del uso de la arquitectura PBNM se muestra como evidencia en el Anexo 2 el cual es una encuesta realizada por la MSc. Mónica Peña Casanova, esta fue ejecutada a diferentes centros de Cuba a los cuales se les pidió que evidenciaran diferentes puntos:

- Problemas de las TI que ha padecido su organización.
- Las prácticas de gestión y gobierno de la organización.
- Evaluación del impacto de ejecución y políticas sobre su organización.
- Impacto dentro de los centros en cuanto al avance.
- Marcos de referencia para la gestión o gobiernos de las TI.

Los puntos anteriores son los factores principales para el uso de las arquitecturas en dependencia de las necesidades de los centros. En la figura 5 y 6 se evidencian algunos de los resultados obtenidos, ver los demás en el Anexo 3:

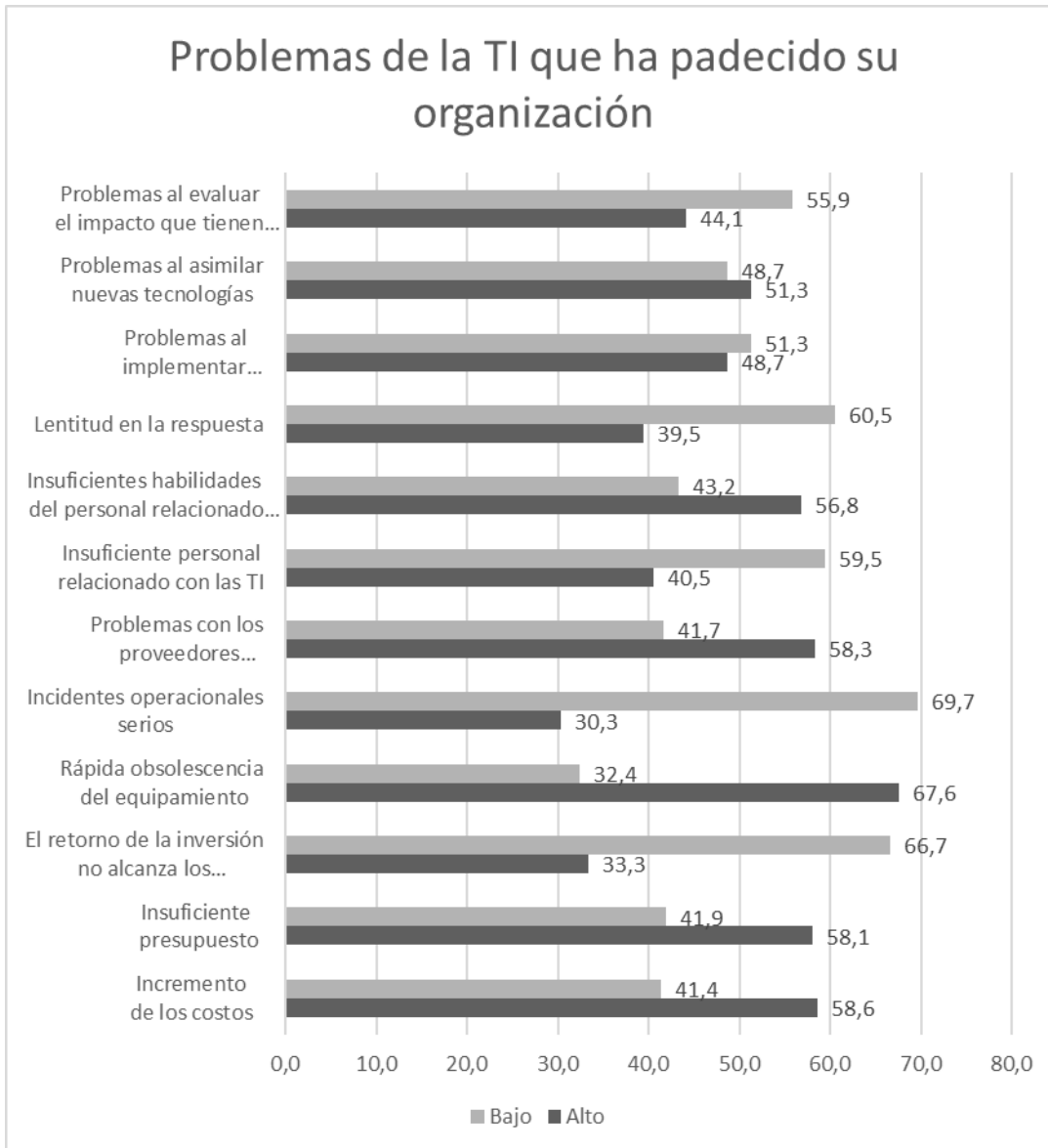


Figura 5: Problemas de las TI que ha padecido su organización (Mónica Peña Casanova, 2018)



Figura 6: Evaluación del impacto de la ejecución de políticas sobre las infraestructuras TI (Mónica Peña Casanova, 2018)

1.7. Conclusiones del Capítulo

Luego de haber analizado el marco teórico de la investigación se ha podido arribar a las siguientes conclusiones:

En el análisis del contexto actual de las Tecnologías de la Información y las Comunicaciones se comprueba que existen deficiencias en las redes de telecomunicaciones actuales, que hacen necesaria la integración entre distintas tecnologías para la satisfacción de las necesidades reales de usuarios y negocios. El análisis de la arquitectura PBNM evidencia que esta se puede integrar a nuevas tecnologías y permite mejorar significativamente tanto la capacidad de gestión y control, como la escalabilidad y agilidad de una red de información. El estudio PBNM demuestra que esta permite en redes tradicionales la automatización de los recursos en la red reduciendo tiempo, costos, y problemas asociados con la configuración de los dispositivos.

Capítulo II Diseño lógico y físico de la arquitectura

2. Introducción

En el capítulo se propone un procedimiento para diseñar lógicamente y físicamente la arquitectura de la red a montar, basado principalmente en la filosofía de diseño Top-Down, así como el análisis de las políticas a integrar en la arquitectura. La comprensión de cada una de las fases que componen el método resulta de vital importancia para su correcta implementación en la práctica, por esta razón en el presente capítulo se realizará un análisis exhaustivo de cada fase planteada.

2.1. Fase de diagnóstico del negocio y propuesta para el diseño de la arquitectura

Luego de un diagnóstico realizado al negocio se detectó que presenta:

- Heterogeneidad
- Dispersión en la red
- Oportunidad de mejora en su gestión de funcionamiento.
- Oportunidad de mejora en su gestión de seguridad.

Teniendo en cuenta el diagnóstico realizado y los disímiles tipos de características que existen para mejorar una red, el presente trabajo va a regirse por los elementos y tareas de las cuatro fases de diseño de la filosofía Top-Down, presenta el comportamiento de un proceso cíclico e iterativo lo que permite el trabajo siguiendo la metodología ABD.

2.2. Propuesta de la metodología

Para este trabajo de tesis se hace uso del método ABD (ver figura 7), no para proponer una arquitectura de un sistema concreto sino para llevar a cabo una arquitectura de red que sirva de guía para el desarrollo de este tipo de soluciones en el centro. Para ello se seguirán el conjunto de pasos que propone el método ABD.

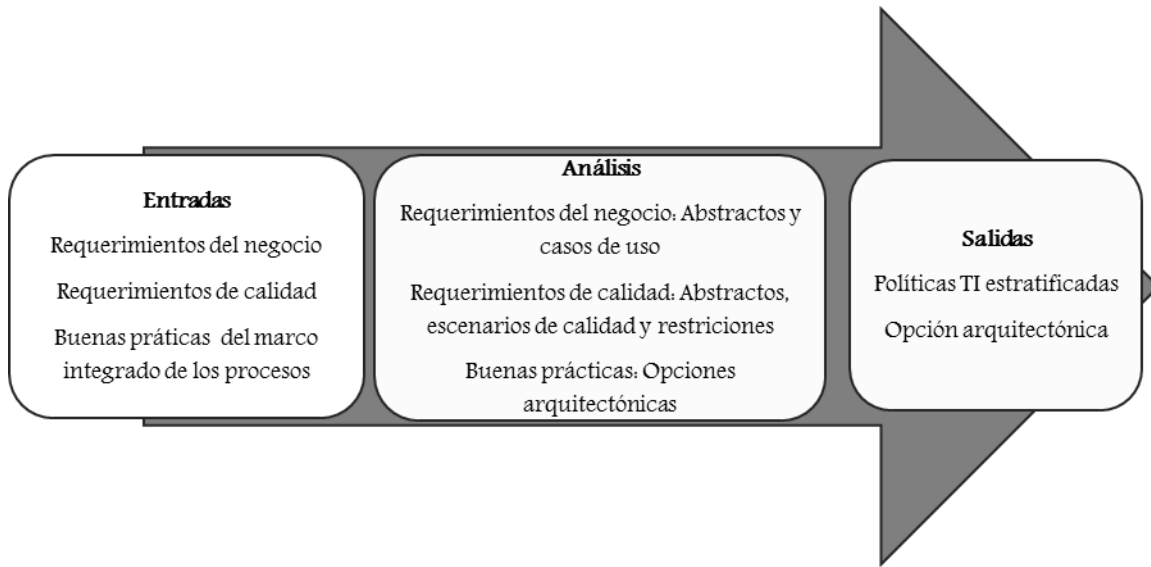


Figura 7: Fases de la metodología ABD (F. Bachmann y L. Bass, 2000)

2.2.1. Factores del negocio

2.2.1.1. Mercado potencial

Las soluciones de gestión de clientes constituyen una forma de mantener monitorizadas y controladas las tecnologías informáticas presentes en las organizaciones. Debido a la variedad de equipos de conexión presentes en las organizaciones, es necesario tener un método efectivo para el control y extracción de datos de las mismas, que a su vez sea personalizable para cada una. En el caso específico de la Universidad de las Ciencias Informáticas, existen muchos centros productivos, laboratorios de docencia, oficinas y otros lugares que poseen PEP que necesitan ser gestionados de forma remota por uno o varios PDP.

2.2.1.2. Objetivos del negocio

La UCI, como centro docente productor que dirige la formación a distancia, genera un conjunto importante de objetos de aprendizaje, así como productos y servicios informáticos. Su modelo de desarrollo de software, se encuentra certificado con la norma CMMI Nivel 2 lo que implica el almacenamiento de un conjunto de elementos que conforman los expedientes de proyectos. Por otra parte, el proceso de formación de pregrado u postgrado también se encuentra certificado, lo que implica un uso intensivo de su infraestructura TI y el almacenamiento de una cantidad importante de evidencias. Por

todo lo anterior, los servicios desplegados demandan una alta conectividad y disponibilidad por lo que el trabajo con los equipos que integran la infraestructura de la UCI llevan una forma distinta de monitoreo y control.

2.2.2. Requerimientos del negocio

Como una de las entradas del método se obtuvieron todos los requisitos funcionales del negocio, los cuales se tratan como políticas de la red que se va a desplegar.

Siguiendo las consideraciones de la organización de investigación industrial Gartner (Garnet, 2019), para la arquitectura PBNM.

Revisión automatizada y Aprobación (Automated Review & Approval)

- Monitoreo y control del equipamiento de la red.

Administración de Contenido (Content Management)

- Inventario de software y hardware.

Captura de Conocimiento (Knowledge Capture)

- Salvas de las configuraciones de los equipos ante caídas o fallas.

Creación de políticas (Policy Creation)

- Políticas de QoS.
- Políticas de Seguridad.

Formación de políticas (Policy Training)

- Formación de las políticas para mantener los servicios.
- Formación de políticas para dar mantenimiento a los equipos.

Las funciones anteriormente expuestas permiten identificar las características que debe cumplir cualquier arquitectura PBNM. Dentro de cada una de ellas se evidencian las políticas (Requisitos Funcionales) que se implementaron en la simulación.

2.2.2.1. Diagrama de Caso de uso del sistema

En el siguiente diagrama se muestran los casos de uso del sistema en específico son las políticas a aplicar en la arquitectura a articular:

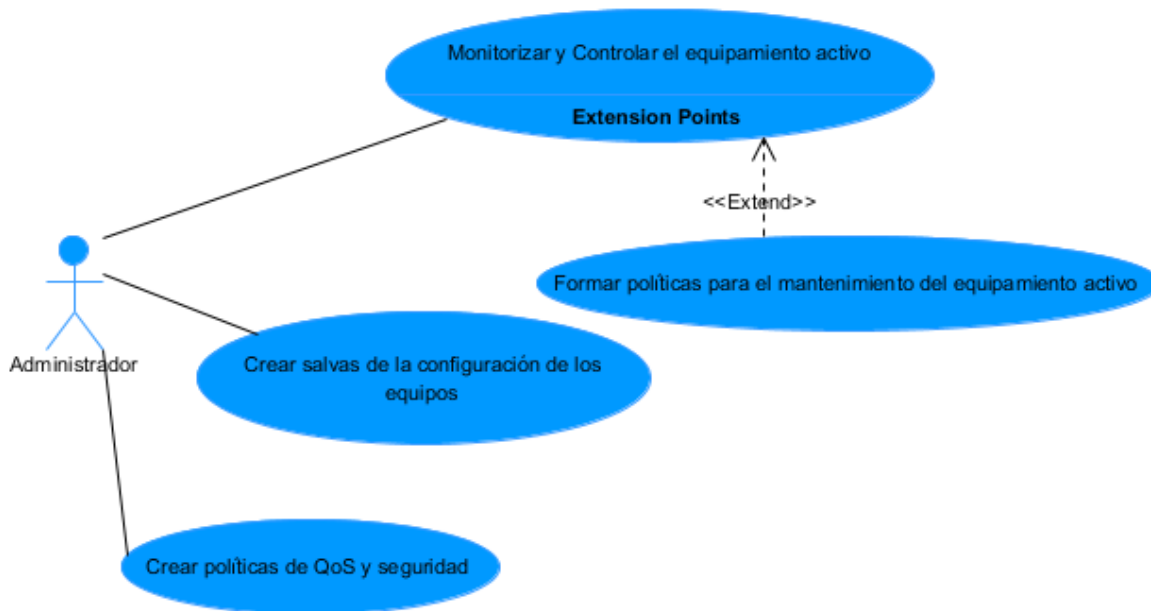


Figura 8: Diagrama de caso de uso (elaboración propia)

2.2.2.2. Requisitos funcionales abstractos

Los requisitos funcionales suelen estar más ligados a los sistemas que a la arquitectura, puesto que expresan cuales deben ser las funcionalidades que se le exige a un sistema concreto. No obstante, como los requisitos funcionales suelen ser muy numerosos, pueden ser organizados en diferentes niveles de abstracción, siendo concretados en las funcionalidades de un sistema; en este caso son las funcionalidades de la red. En consecuencia, se proponen una lista de requisitos funcionales abstractos que pueden brindar la mayoría de las soluciones de red:

- Gestión de seguridad.
- Gestión de configuraciones.
- Gestión de inventario.
- Gestión de usuarios y control de acceso.
- Gestión de disponibilidad de recursos.

2.2.3. Atributos de calidad abstractos

2.2.3.1. Aspectos del negocio y objetivo de la organización

Para dar cumplimiento a sus principales servicios, la organización necesita dar acatamiento a los requisitos siguientes:

- Reservar ancho de banda y calidad de servicio para eventos virtuales.
- Ofertar servicios de videoconferencia para profesores aspirantes con tutores extranjeros.
- Habilitar matrícula a través de una plataforma de teleformación.
- Establecer SLA¹¹ entre las áreas de TI y el resto de las áreas de proceso de la universidad.
- Se establecen y monitorean niveles de calidad de servicio.

2.2.3.2. Aspectos de modificabilidad

La modificabilidad, no es más que la capacidad de realizar cambios en la arquitectura de una manera rápida y eficiente. Se debe establecer una relación de compromiso entre el costo de construcción y el costo de cambio. Este atributo es decisivo para la presente investigación ya que uno de los objetivos para lograr capacidad de reacción en función de las necesidades de la organización, es reducir el tiempo de respuestas, costo y complejidad de crear y mantener actualizadas las políticas TI que se desean aplicar y la arquitectura para la ejecución de las mismas. Se puede agrupar en los aspectos relacionados con la extensibilidad, portabilidad, reestructurabilidad, reusabilidad, interoperabilidad y mantenibilidad que presenta un componente o solución en la arquitectura a desarrollar, centrándose en los siguientes aspectos de interés:

- Probabilidad del cambio.
- Magnitud y dimensión.
- Costo del cambio.
- Complejidad del cambio.
- Conservación del conocimiento de la solución.

¹¹ Siglas correspondientes al término en inglés: *Service Level Agreement*

- Confiabilidad del cambio.

Teniendo en cuenta lo anteriormente planteado, la arquitectura debe satisfacer los siguientes requisitos:

- Asegurar que un componente con responsabilidades comunes (alta cohesión de responsabilidades) no tengan que depender demasiado de componentes con distintas responsabilidades (bajo acoplamiento entre componentes).
- Proveer integración entre los componentes mediante interfaces abstractas, con el objetivo de poder sustituir un componente por otro, con la menor cantidad de cambios posibles.
- Proveer componentes reutilizables de forma tal que puedan ser empleados por otras soluciones.

2.2.3.3. Aspecto de seguridad

La seguridad expresa cual es el nivel de compromiso que la arquitectura debe tener con sus clientes, al ejecutar una funcionalidad específica dentro de ciertas restricciones de velocidad, precisión, entre otras; así como en qué grado utiliza eficientemente los recursos. La seguridad está muy relacionada con los demás atributos de calidad, por eso es vital tener una balanza entre todos los parámetros, de forma tal que no se contradigan unos y otros, logrando establecer una medida promedio entre todos. Su análisis se establece en cada uno de los componentes y en la arquitectura en general teniendo en cuenta los aspectos:

- Cifrar el contenido enviado a través de la red.
- Comprobación de la autoría de la información enviada.
- Poseer un registro de los cambios realizados.
- Poseer un mecanismo de control de acceso por roles.

Dada las particularidades del dominio, la seguridad sólo puede caracterizarse con alto grado de abstracción, ya que en dependencia de cada una de las funciones que caracterizan a los gestores de clientes será la calidad de su seguridad y de la información recibida de los equipamientos en la red organizacional. Teniendo en cuenta lo anteriormente planteado la arquitectura debe satisfacer los siguientes requisitos:

- Establecer límites de tamaño y cantidad de los paquetes enviados en las subredes.
- Proporcionar mecanismos para establecer múltiples conexiones seguras en los equipos monitorizados.
- Optimizar los procesos realizados para ser ejecutados en el menor tiempo posible.

2.2.3.4. Aspecto de disponibilidad

La disponibilidad recoge los aspectos que garantizan la probabilidad de que la solución esté operativa en un período de tiempo determinado. Por el momento es suficiente con caracterizar la disponibilidad mediante la identificación de los servicios o funciones más críticas de los sistemas, y enumerar las estrategias y mecanismos que debe proporcionar la arquitectura para que dichos servicios estén disponibles y muestren un comportamiento fiable. En general, dichas estrategias y mecanismos se basan en aplicar diversas formas de redundancia homogénea o heterogénea. Los aspectos a destacar de este atributo son:

- Tiempo de recuperación.
- Disponibilidad de los datos.
- Trabajo de manera remota.

Por lo antes expuesto la arquitectura debe proveer los siguientes requisitos:

- Proveer mecanismos de control remoto.
- Proveer mecanismos de almacenamiento y respaldo de los datos.
- Proporcionar mecanismos de recuperación ante fallos.
- Proveer la disponibilidad de los servicios brindados todos los días a toda hora.

2.2.3.5. Aspecto de verificabilidad

Es el grado de facilidad que tiene un sistema para ser probado en su completitud, mediante pruebas de unidad, integración, aceptación, regresión, entre otras. Hace referencia a la facilidad con la cual el software puede ser construido para posteriormente encontrar defectos o problemas directamente probando sus componentes. Por lo antes expuesto la arquitectura debe proporcionar los siguientes requisitos:

- Proveer componentes o software especializado que permitan monitorizar el comportamiento de los componentes durante su ejecución.

- Proveer métricas que permiten monitorizar el funcionamiento en cuanto a envío y recibo de paquetes.
- Proveer métricas que monitoricen la calidad de los servicios implementados en la red.

2.2.4. Restricciones

- El sistema debe funcionar 24 horas, los 7 días de la semana y los 365 días del año. (Disponibilidad)
- La integración entre los diferentes dominios que lo conforman haciendo uso de CIM/XML y su extensión DEN_ng. (Seguridad)
- Se debe brindar la solución de conflictos en las políticas de TI que se ejecuten en cada dominio. (Seguridad)

2.2.5. Estrategias arquitectónicas

Teniendo en cuenta las consideraciones para las arquitecturas de red, los factores del negocio, los requerimientos funcionales, las directrices, los atributos de calidad y las restricciones, se han seleccionado un conjunto de disposiciones arquitectónicas las cuales garantizan el éxito de la arquitectura.

- Encapsulamiento basado en el modelo común de información (CIM / XML).
- Control de acceso basado en roles.
- Arquitectura de repositorios.
- Uso de protocolos de transmisión seguros.
- Arquitectura basada en la puesta en marcha por ficheros de configuración.

2.2.5.1. Conductores arquitectónicos

Los conductores de la arquitectura son los que permiten la implementación de las políticas de negocio en las diferentes soluciones técnicas a través de la estratificación de políticas, además facilitará la creación de políticas en el PDPP que permitan la interacción de varios dominios de gestión de políticas, para tener un control holístico de la infraestructura desplegada. En este caso se propone el empleo del modelo DEN-ng para coordinar la comunicación entre los PDP de los diferentes dominios de gestión y el PDPP, aprovechando la definición de políticas con la tríada evento-condición- acción.

2.2.6. Descripción de las vistas de la arquitectura

En cuanto a las vistas en esta metodología se expresan como sistemas y subsistemas de red, los cuales encierran los procesos que se interconectan para la obtención del producto. Dando al cliente una breve vista de cómo se debe ejecutar el producto.

Vista Lógica

En la vista lógica de la arquitectura se evidencia el sistema, en el caso de este trabajo se evidencian la necesidad del negocio y dentro de esta las cinco entradas (páginas de servicios) y las políticas (subsistemas del servicio) a establecer en la red.

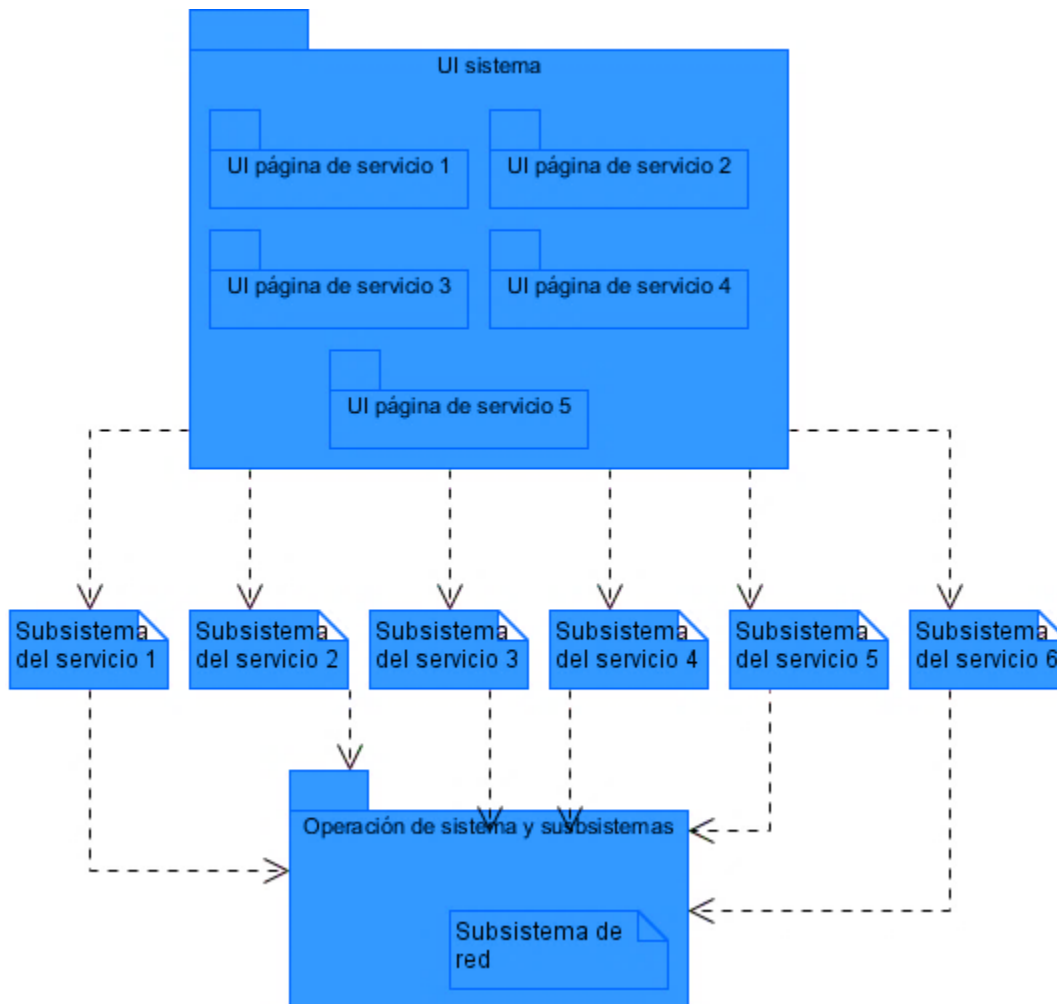


Figura 9: Vista lógica de la arquitectura (elaboración propia)

Vista de Concurrencia

En esta se evidencian todos los servicios en cuanto a su inicialización, su tiempo de servicio y de diagnóstico.

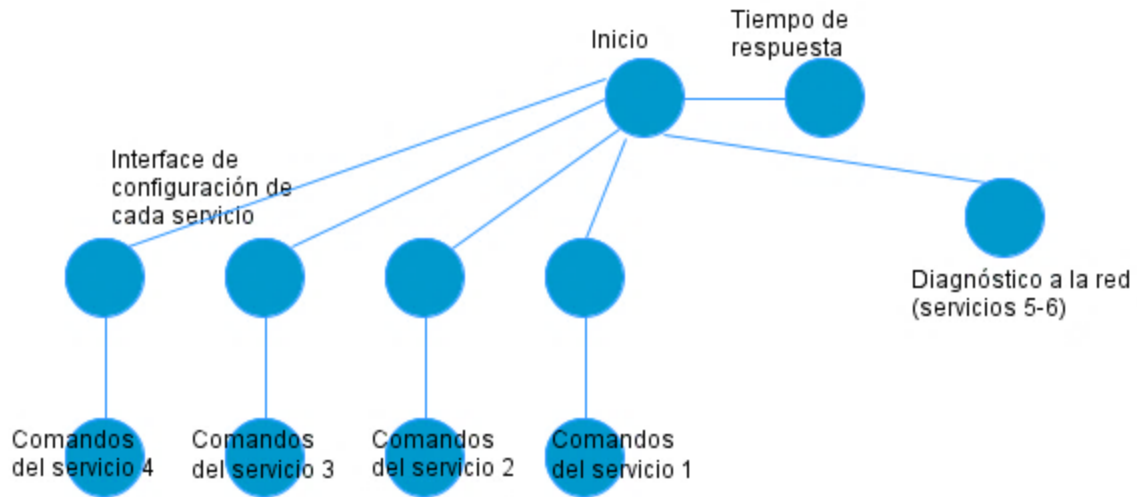


Figura 10: Vista de concurrencia de políticas (elaboración propia)

Desarrollo de las vistas

En el desarrollo de las vistas la notación de un diamante representa una unidad de despliegue y la notación de una línea con los rectángulos sobre él representa una configuración del proceso (la política).

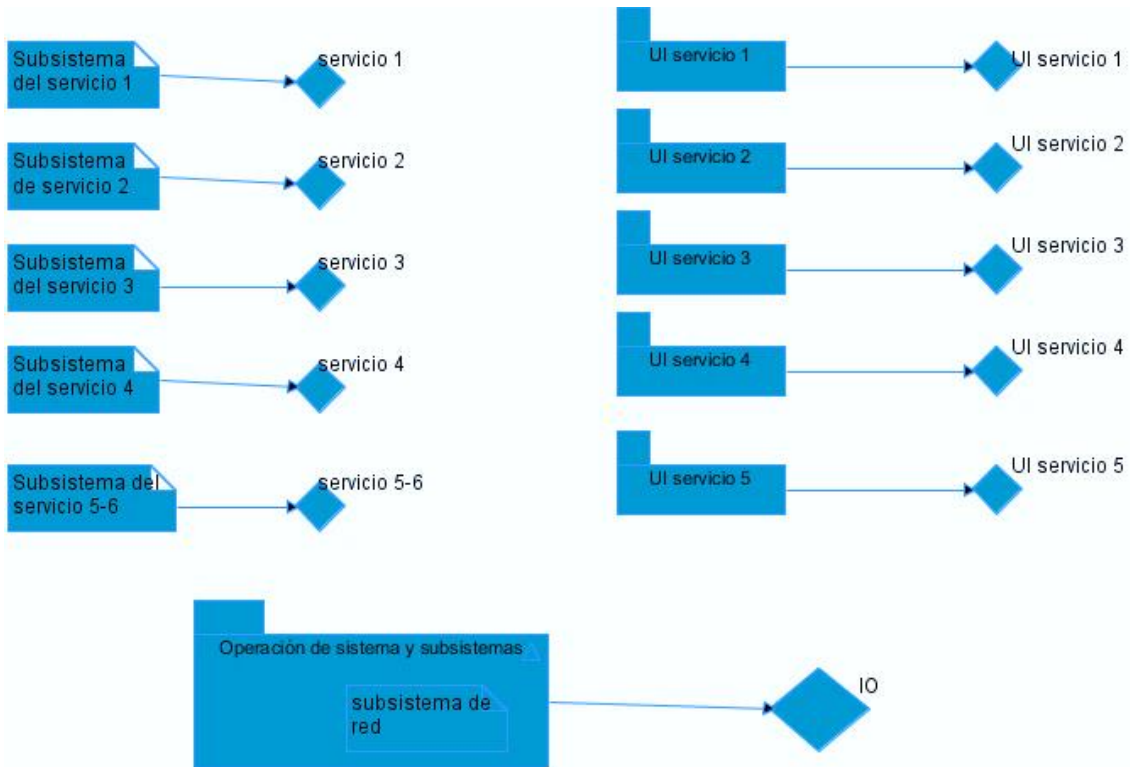


Figura 11: Desarrollo de las vistas (elaboración propia)

Diagrama de despliegue

Este diagrama consiste en desplegar en distintos nodos los componentes de la arquitectura. Mostrando el tipo de dependencia, los servidores, entre otras.

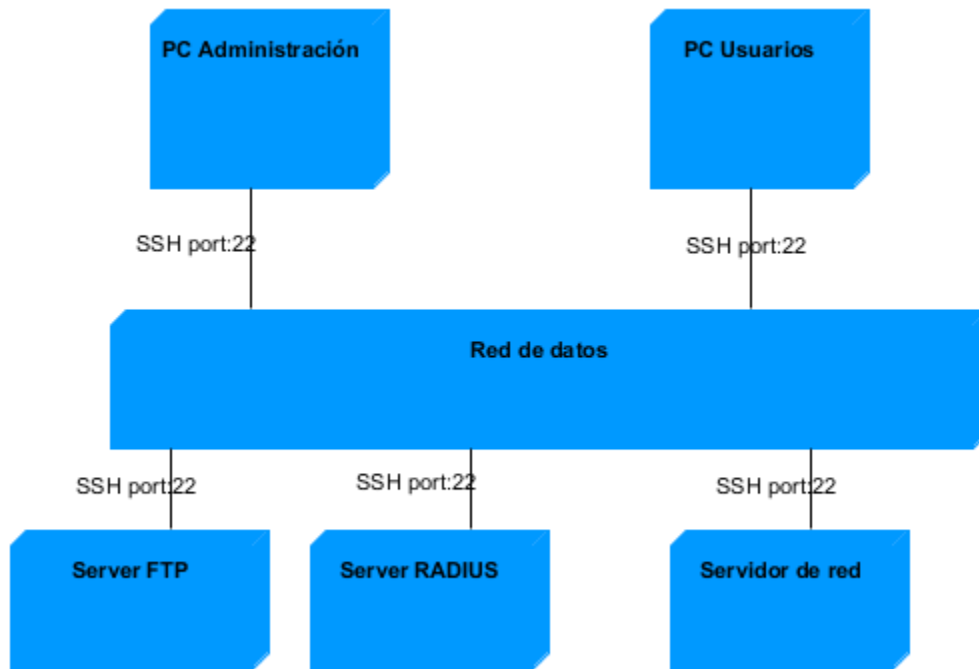


Figura 12: Diagrama de despliegue (elaboración propia)

Diagrama de secuencia

Este diagrama muestra el hilo conductor de cómo debe funcionar el negocio, también demuestra en que momento en específico se hace uso de la metodología.

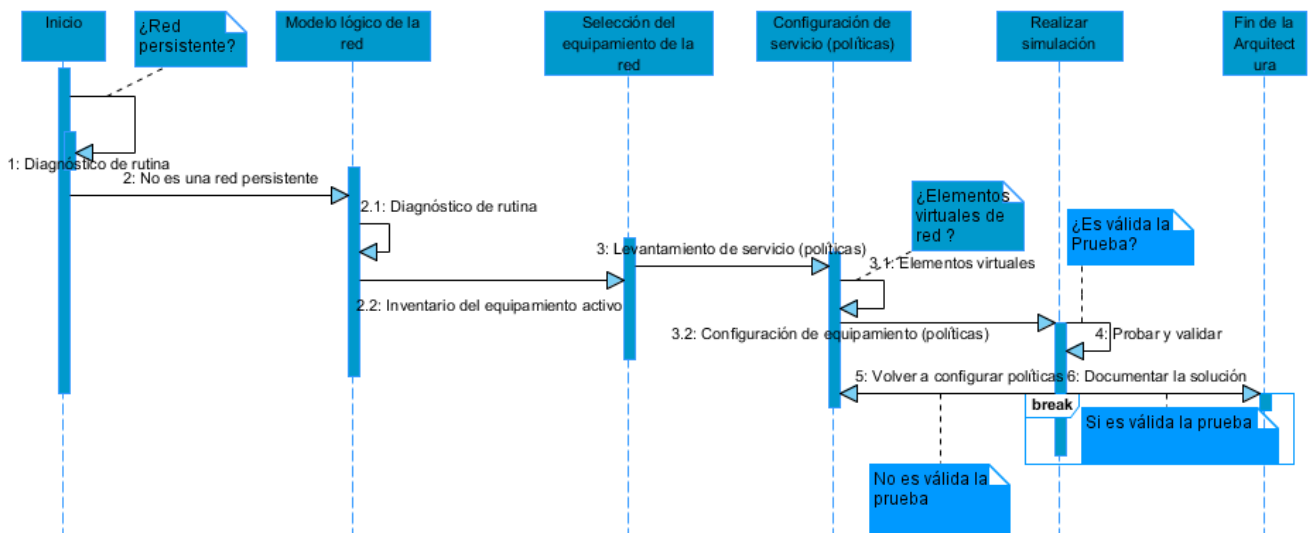


Figura 13: Diagrama de secuencia (elaboración propia)

2.2.7. Salidas de la metodología

2.2.7.1. Estilo arquitectónico

Los estilos arquitectónicos son un conjunto de descripciones de patrones e interacciones, algunos ejemplos de estos componentes, para el caso del dominio de red son: seguridad, parcheo, configuraciones, control remoto, inventarios, entre otros. En función de los estilos arquitectónicos identificados, se realiza la descomposición en elementos de diseño en el dominio de red para el diseño de políticas de TI.

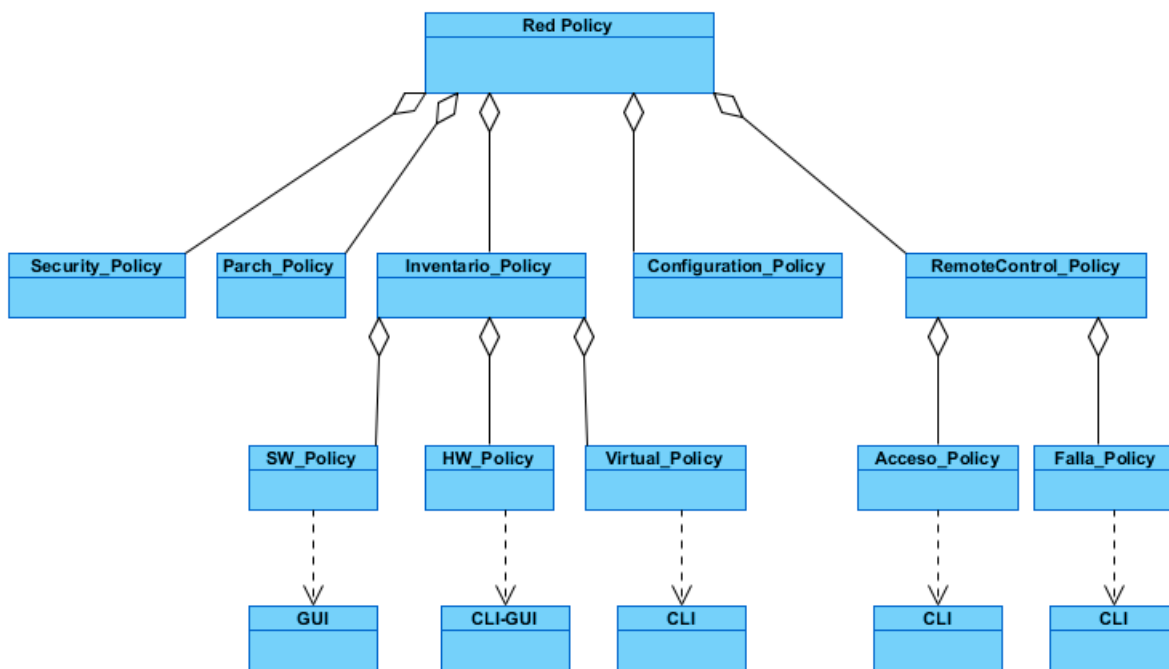


Figura 14: Estilo arquitectónico (elaboración propia)

2.2.7.2. Directrices de la arquitectura

Durante el análisis del dominio de solución y el apartado anterior, se determinaron una serie de requisitos los cuales guían y condicionan la arquitectura que se propone para el diseño de políticas de TI, estos requerimientos que, son críticos, para el éxito de un sistema se denominan "Directrices de la Arquitectura", ya que define la forma del diseño que debe seguir la solución. Las directrices son la combinación de requisitos funcionales, de calidad y negocio que modelan la arquitectura y su cumplimiento permitirá un diseño satisfactorio de las políticas (Felix Bachmann, Len Bass, Gary Chasteck, 2000). Para la

arquitectura objeto de este trabajo se proponen las siguientes directrices, clasificadas en categorías, según el atributo de calidad al que corresponden.

- Patrones de interacción con elementos de la infraestructura: configuración de los equipos.
- Patrones de cómo cada elemento interactúa ante determinados eventos: respuesta ante alarmas de fallos, manejo de errores en las configuraciones.
- Capacidad de reutilización de patrones en el diseño de políticas: si un usuario tiene calidad de servicio o una PC, todos los paquetes asociados a todos los servicios que intercambie esa PC se tratan en los equipos con prioridad.

2.2.7.3. Tabla de políticas estratificadas

Tabla 1: Políticas estratificadas (elaboración propia)

Política TI de negocio	Política TI de sistema	Política TI de red
Requisitos asociados a la calidad		
Modificabilidad		
Asegurar que un componente con responsabilidades comunes (alta cohesión de responsabilidades) no tengan que depender demasiado de componentes con distintas responsabilidades (bajo acoplamiento entre componentes).	Diseño y despliegue de la arquitectura basada en dominios con un PDPP que coordine la interconexión entre dominios.	Diseño de políticas en el dominio de red. Diseño de políticas en el dominio de servicios. Diseño de políticas en el dominio de infraestructura subyacente física y virtualizada.
Evitar modificar demasiados módulos al aparecer algún cambio.	Definir estados finitos de funcionamiento en cada dominio.	
Proveer integración entre los componentes mediante interfaces abstractas, con el objetivo de poder sustituir un componente por otro, con la menor cantidad de cambios posibles.	Coordinar el funcionamiento interdominio a través de la representación de políticas en DEN-ng y la ejecución de las mismas en los PDPP.	
Proveer componentes reutilizables de forma tal que puedan ser empleados por otras soluciones.	Creación de repositorios de configuración.	
Verificabilidad		

Proveer mecanismos de separación de interfaz e implementación, y el uso de componentes específicos para la realización de pruebas.	Segmentación en dominios de gestión.	Definir políticas a nivel de dominio de gestión y solucionar conflictos desde el PDPP.
Proveer componentes o software especializado que permitan monitorizar el comportamiento de los componentes durante su ejecución.	Definición de eventos que permitan la detección temprana de fallas	
Disponibilidad		
Proveer mecanismos de almacenamiento y respaldo de los datos.	Crear mecanismos de salva de configuración	
	Crear mecanismos de salvas incrementales	
	Crear mecanismos de salvas totales	
Proporcionar mecanismos de recuperación ante fallos.	Crear mecanismos de respaldo	
Proveer la disponibilidad de los servicios brindados todos los días a toda hora.		
Seguridad		
Cifrar el contenido enviado a través de la red.		
Comprobación de la autoría de la información enviada.	Despliegue de firma digital.	
Almacenamiento y copias de seguridad de los datos.		
Poseer un registro de los cambios realizados.	Sistema de logs.	
Poseer un mecanismo de control de acceso por roles.		
Rendimiento		
Establecer límites de tamaño y cantidad de los paquetes enviados en las subredes.		
Proporcionar mecanismos para establecer múltiples conexiones en los equipos monitorizados.		
Optimizar los procesos realizados para ser ejecutados en el menor tiempo posible.		

2.3. Procedimiento para el desarrollo de la arquitectura

Para el desarrollo de este procedimiento se utilizó el visual paradigm en su versión 8.0, con el objetivo de poder mostrar el seguimiento de cada tarea y sus pautas. En el Anexo 4 se muestran las interrogantes realizada en una entrevista a los trabajadores del Nodo Central para poder desarrollar los patrones a seguir para la obtención del presupuesto y los equipos a utilizar en la simulación y la topología más adecuada. En el desarrollo del procedimiento se aplica la filosofía top Down solo que la 2 y 3 fase se realizan juntas.

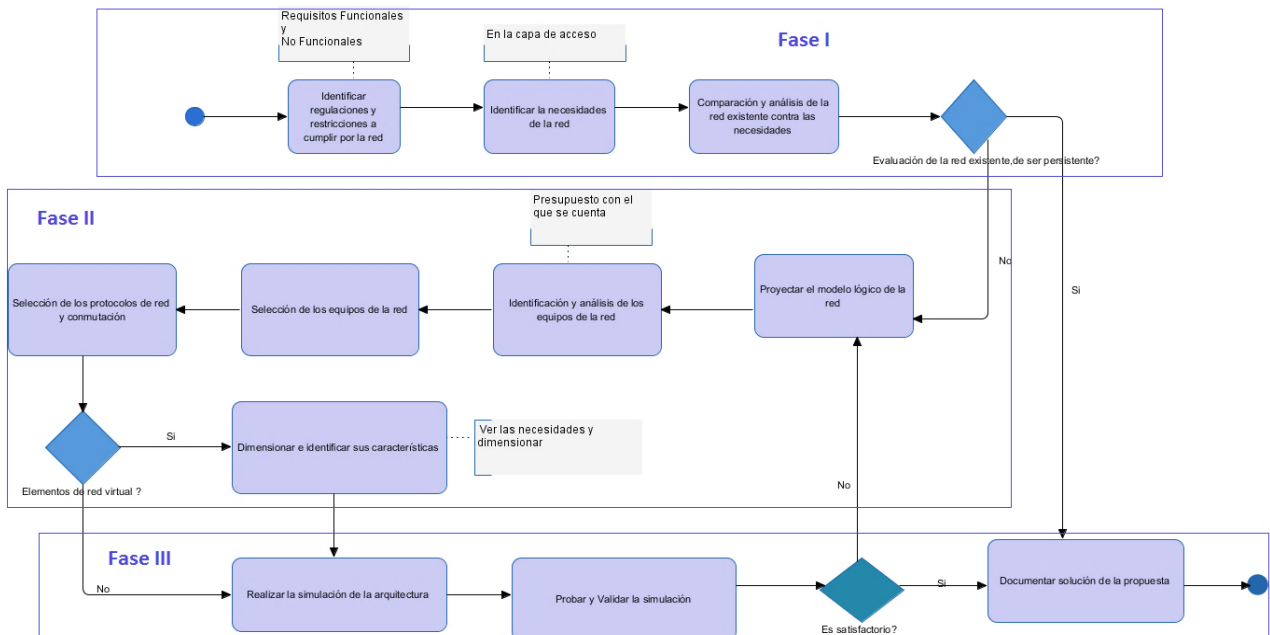


Figura 15: Procedimiento de diseño de la arquitectura (elaboración propia)

2.4. Arquitectura PBNM

La arquitectura tradicional a implementar en esta investigación se encuentra planteada sobre la notación PBNM o gestión de red basada en políticas, es una de las tareas de gestión que evita a los administradores de red la configuración y manipulación de los elementos de la red manualmente a través de interfaces de control, proceso propenso a errores y que consume tiempo. PBNM en una organización permite la automatización de los recursos en la red para ofrecer un servicio rápido y con calidad, lo cual significa una mejor posición en el mercado y, por tanto, un mayor volumen de negocio que los competidores. (Anías Calderón, 2018) Este modelo se encuentra certificado por el Grupo

de Trabajo de Ingeniería de Internet o IETF¹², IETF (IETF, 2018) es una organización internacional abierta sin fines de lucro de normalización y estandarización que regula las propuestas de estándares de Internet conocidos como RFC¹³.

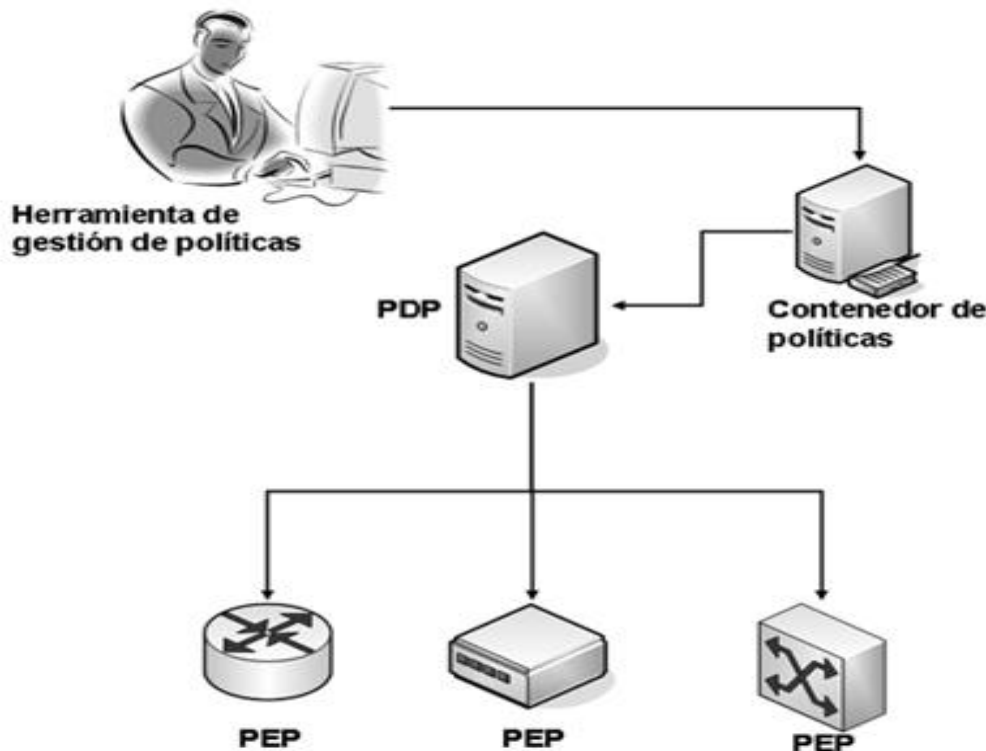


Figura 16: Gestión de red basada en políticas (PBNM) según el IETF

En esta arquitectura se identifican los elementos siguientes (Engineering, 2018):

- Herramienta de gestión de políticas: Herramienta que ayuda a los administradores a crear políticas que se van a ejecutar en las redes.
- Contenedor de políticas: Entidad que almacena las políticas, las cuales pueden ser almacenadas utilizando un modelo estándar, un repositorio de políticas, un directorio LDAP o una base de datos relacional dependiendo de la implementación.
- PEP: Entidad donde las políticas son aplicadas.

¹² Según el término correspondiente en inglés: Internet Engineering Task Force

¹³ Según el término correspondiente en inglés: Request for Comments

- PDP: Entidad en donde se evalúan las políticas que posteriormente se ejecutan en el PEP.

Según el modelo anterior de la arquitectura PBNM la autora se basa para el diseño de su arquitectura con PBNM, como se muestra en la Figura 17:

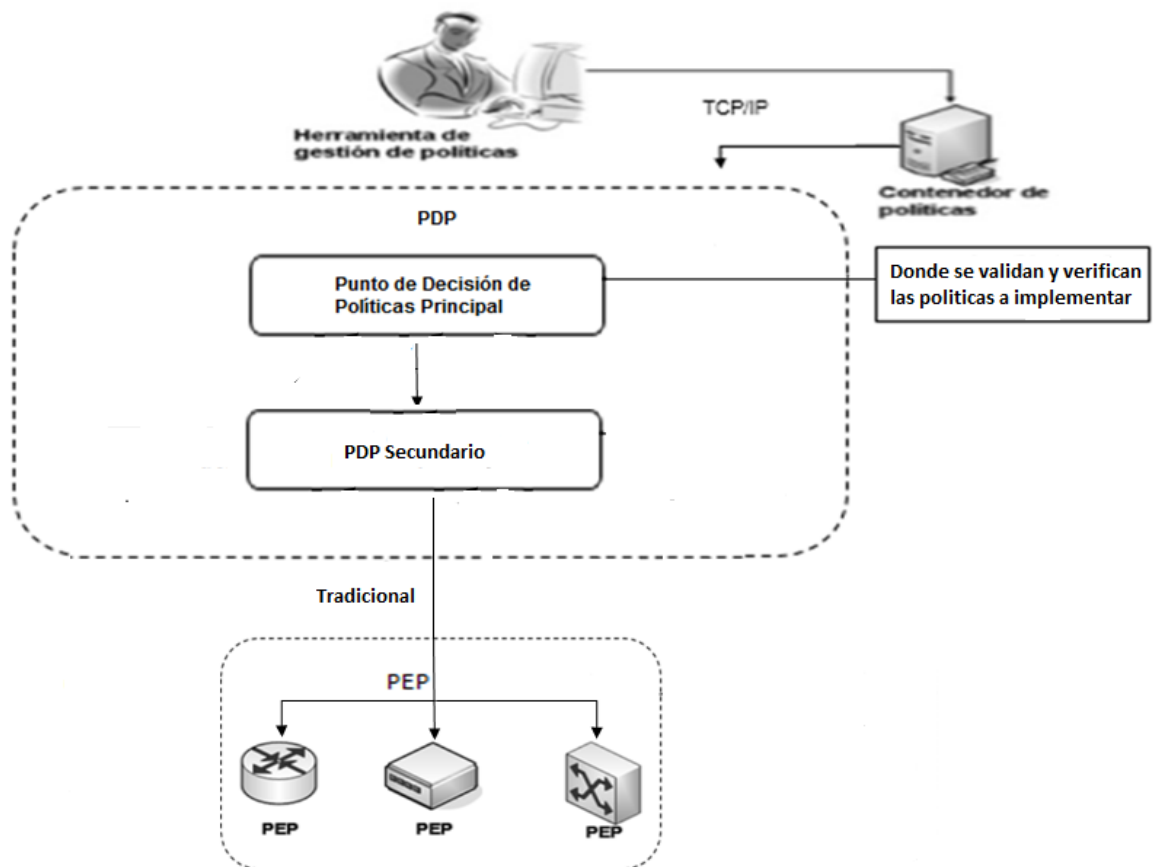


Figura 17: Arquitectura tradicional con PBNM (elaboración propia)

2.4.1. Funcionamiento de la arquitectura tradicional con PBNM

En esta arquitectura se tienen todos los componentes que conforman la arquitectura PBNM también las políticas que se establecen en una arquitectura, con el fin de conseguir la automatización y el desarrollo de la red UCI en aras de una evolución en la gestión del equipamiento activo.

En cuanto al PDP permite integrar los componentes de la red aunque sea una red heterogénea, se utilizan dos PDP que serían para:

Un PDP secundario que controla la ejecución de políticas en la red tradicional y un PDP principal que gestiona la ejecución de políticas entre las entidades que manejan el tráfico de la red.

2.4.1.1. Punto de decisión de políticas principal

El PDP principal es el componente de la arquitectura encargado de gestionar la ejecución de políticas que permiten la comunicación entre los diferentes tipos de redes al tener una red heterogénea. El PDP principal evalúa y aplica en las entidades pertinentes las políticas almacenadas en la herramienta de gestión de políticas que permiten la interoperabilidad entre la red.

El PDP principal obtiene estas reglas a través de consultas al contenedor de políticas. Estas políticas implementadas representan tanto las necesidades de la organización como las del cliente definidas mediante Acuerdos de Nivel de Servicio y constituyen las reglas que controlan el tráfico de información y la interacción entre el equipamiento de red.

Este componente constituye la entidad que incluye la validación y la lógica de detección de conflictos de las políticas del PDP secundario. Este puede interactuar con el PDP secundario mediante protocolos como SNMP, COPS, solo que en este caso es a través del protocolo DMTF con CIM/XML. Permite un control centralizado sobre los dispositivos.

2.4.1.2. Punto de decisión de políticas secundario

El PDP secundario, por su parte, constituye la entidad que de forma nativa gestiona la ejecución de políticas en el equipamiento de red tradicional. Este componente interactúa con el PDP principal y con los PEP a través de protocolos de gestión como DEN-ng¹⁴, con CIM/XML, tal y como se describe en la Figura 18:

¹⁴ Concepto: DEN surge como una extensión para directorios de CIM con elementos de X.500. Es un estándar que define cómo construir y almacenar información sobre usuarios, aplicaciones y datos en un directorio central autoritativo, distribuido e inteligente.

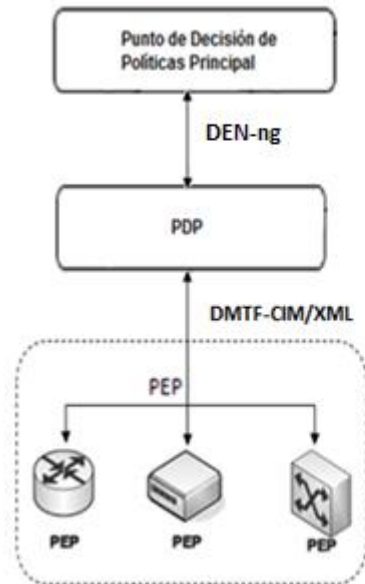


Figura 18: PDP secundario comunicación con los PEP (elaboración propia)

El PDP secundario evalúa y aplica las políticas en los PEP de la red tradicional, que, a través de un agente, recogen y almacenan información de administración, la cual es puesta a disposición de una herramienta de monitorización que la supervisa y controla. Esta información es la que permite la validación de las políticas almacenadas en el repositorio de políticas.

2.5. Políticas a implementar en la arquitectura según sus necesidades

Para cumplir las necesidades del negocio se hace necesario aplicar calidad de servicio, también la contabilidad de los servicios y su nivel de seguridad para identificar quien tiene acceso a determinados sitios, la seguridad en escenarios de fallos de los servicios eléctricos, como a la vulnerabilidad por ataques en la red, por todo esto y lo descrito en la situación problemática se aplican estas políticas:

Para Calidad de servicio (QoS):

- Modelo priorizado de servicios diferenciados o DiffServ: Se trata de marcar paquetes según un tipo de servicio deseado. Los routers y switch's de la red usan por lo general estrategias de encolado del tráfico para priorizar el tráfico atendiendo a dicha marca en el paquete. (Rejón, 2016)

Para la contabilidad y seguridad según su categoría:

- Servidor RADIUS: El RADIUS es un protocolo cliente/servidor. El cliente RADIUS es típicamente un NAS y el servidor de RADIUS es generalmente un proceso de daemon que se ejecuta en UNIX o una máquina del Windows NT. El cliente pasa la información del usuario a los servidores RADIUS designados. Los servidores de RADIUS reciben las peticiones de conexión del usuario, autentican al usuario, y después devuelven la información de la configuración necesaria para que el cliente entregue el servicio al usuario. Un servidor RADIUS puede funcionar como cliente proxy para otros servidores RADIUS u otro tipo de servidores de autenticación, como también lleva la contabilidad y la autoridad según el usuario. (Cisco., 2019)

Para la seguridad ante fallos:

- Protocolo de transferencia de archivos o TFTP¹⁵ : El protocolo de transferencia de archivos es un protocolo simple para transferir archivos, y por lo tanto fue nombrado el protocolo de transferencia de archivos trivial o TFTP. Se ha implementado en la parte superior del protocolo de usuario de Internet Datagrama (UDP o Datagram) ya su vez permite la creación de salvas de configuración. (Sollins, 2018)

2.5.1. Estrategias de seguridad y calidad de servicio

Se aplica seguridad por puerto en conjunto con el protocolo AAA que es empleado por el servidor Radius para mantener la seguridad de los usuarios y de los equipos gestionados.

La QoS se trabaja con el DiffServ (Cisco., 2019) para la calidad, por ser el protocolo que trabajar con el servidor RADIUS que se tiene en funcionamiento mediante el DSCP¹⁶.

2.6. Simulación**Gestión de la configuración en la red tradicional**

En este paso se configuran los equipos de gestión de la red y se mantiene un registro de los tiempos de uso de la red, de los servidores, de las máquinas conectadas y de otros

¹⁵ Según el término correspondiente en inglés: File Transfer Protocol

¹⁶ Según el término correspondiente en inglés: Differentiated Services Code Point

dispositivos. La mayoría de los sistemas de red actuales disponen de aplicaciones de control de inventario que puede utilizarse para obtener la información necesaria para resolver determinados problemas en la red.

Al integrarle a esta red la arquitectura PBNM se hace factible la gestión del equipamiento activo al poder trabajar a través de políticas que se encuentran almacenadas para dar un mejor funcionamiento a la red, dichas políticas son puestas en uso sin tener que aumentar el costo de la red ni comprometer su funcionamiento.

Segmentación de la red

La segmentación de la red se realiza a través de la creación de redes lógicas independientes dentro de una red física, también denominadas VLANs, que permiten la administración de diferentes segmentos lógicos de una red de área local y reducen el tamaño del dominio de difusión. Esto permite verificar la funcionalidad del protocolo VTP en cuanto a sus propiedades en los switch's Multilayer mediante la adición de una VLAN experimental la cual no se despliega a en los demás equipos si no es creada en el switch servidor.

2.7. Conclusiones del Capítulo

Una vez estudiado los elementos asociados a la gestión basada en políticas, como elemento base de la arquitectura PBNM, y a la propuesta de arquitectura tradicional se puede arribar a las siguientes conclusiones:

La descripción del procedimiento para integrar la arquitectura PBNM con la tradicional constituye una metodología para aplicar la arquitectura propuesta en un escenario de red simulado. La modelación de la propuesta de arquitectura permite ver que en una misma red pueden coexistir distintas tecnologías unidas por las políticas establecidas gracias a la arquitectura PBNM con el equipamiento en una red tradicional.

Capítulo III Validación y pruebas de la arquitectura

3. Introducción

Un elemento indispensable en el logro de una investigación científica lo constituye el proceso de validación. Por ello en el presente capítulo se presentan la validación realizada a la metodología ABD mediante el método ATAM y los resultados obtenidos de la aplicación de la técnica para cada atributo de calidad. También se valida el nivel de alcance del procedimiento realizado mediante la técnica de Red Petri la cual demuestra el nivel de confiabilidad del procedimiento. Mientras que la simulación de una arquitectura de red con características similares a la que se corresponde montar para la gestión del equipamiento activo basado en políticas se evidencia que si es posible la realización de este tipo de arquitecturas en cualquier negocio.

3.1. Aplicación del método de validación de la metodología mediante ATAM

Actualmente la UCI cuenta en su escenario de red con disímiles dificultades, se aplicó una entrevista a 4 especialistas (ver Anexo 5) los cuales a partir de sus propias experiencias evaluaron el comportamiento que presentaban las soluciones sobre la base de los atributos de calidad que presenta una arquitectura de software de acuerdo a los autores del libro "Software Architecture in Practice" (Bass, Clements y Kazman , 2003), llegando a las conclusiones que se muestran en la tabla 2: Tabla de resultados de las métricas antes de aplicada la metodología.

Tabla 2: Tabla de resultados de las métricas antes de aplicada la metodología (elaboración propia)

Atributo	Estado
Disponibilidad	80%
Seguridad	85%
Modificabilidad	80%

Verificabilidad	70%
------------------------	-----

Con los datos obtenidos se procede a la construcción del árbol de utilidad de la arquitectura propuesta, aplicada al dominio de red. El árbol de utilidad contiene los escenarios que ponen a prueba a la arquitectura PBNM modificada. Se construyó con el objetivo de verificar el cumplimiento de los atributos de calidad definidos, generados como consecuencia de la priorización de los requerimientos específicos de los atributos de calidad observados como escenarios en la metodología ABD. Teniendo en cuenta la priorización de cada escenario en base a dos dimensiones (D1, D2):

3.1.1.1. Dimensiones

D1: Importancia del escenario en relación al éxito del sistema, el cual emplea para su valoración los criterios mostrados en la tabla 3: Tabla de Importancia del escenario:

Tabla 3: Tabla de importancia del escenario según ATAM

Importancia	Descripción	Valor
Baja (B)	Importancia casi nula para el éxito del sistema	1
Media (M)	Importancia media para el éxito del sistema	2
Alta (A)	Importancia alta para el éxito del sistema	3

D2: Grado de dificultad que posee el escenario para ser realizado por la arquitectura, según la estimación del arquitecto: Ver tabla 4: Tabla de dificultad del escenario.

Tabla 4: Tabla de dificultad del escenario según ATAM

Dificultad	Descripción	Valor
Bajo (B)	Esfuerzo bajo para cumplir el escenario	1
Medio (M)	Esfuerzo medio para cumplir el escenario	2
Alto (A)	Esfuerzo alto para cumplir el escenario	3

3.1.1.2. Relación Importancia/ Esfuerzo

La tabla 5 demuestra los valores en rango en cuanto a los datos para medir el esfuerzo/importancia.

Tabla 5: Tabla del valor del peso según ATAM

Peso	Valor	Color

Baja	1 o 2	Gris claro
Media	3 o 4	Gris medio
Alta	Mayor a 6	Gris oscuro

Tabla 6 evidencia Importancia/Esfuerzo de los atributos que se miden para obtener el cambio luego del análisis.

Tabla 6: Tabla de Importancia/Esfuerzo según ATAM

Importancia/Esfuerzo	Bajo	Medio	Alta
Baja	1	2	3
Media	2	4	6
Alta	3	6	9

3.1.1.3. Listado de escenarios

El listado de escenarios se obtuvo a partir de los criterios propuestos por Gartner para seleccionar los mejores escenarios en cuanto a la gestión de red, la revisión automatizada y aprobación, la administración de contenido, la captura de conocimiento, la creación de políticas y la formación de políticas. En función de las carencias de la red actual, se diseñaron los escenarios siguientes ver en la tabla 7 (ver descripción de escenarios en el Anexo 6):

Tabla 7: Tabla de listado de escenario (elaboración propia)

No	Atributo / sub-característica	Escenario	Evaluación	Puntaje	Impacto (%)
1	Disponibilidad	Proveer mecanismos de almacenamiento y respaldo de los	A/M	6,4	95%

		datos.			
2	Disponibilidad	Proporcionar mecanismos de recuperación ante fallos.	A/M	6,4	95%
3	Disponibilidad	Proveer la disponibilidad de los servicios brindados todos los días a toda hora.	A/A	9,9	100%
4	Disponibilidad	Crear mecanismos de salvallas totales	M/M	4,4	80%
5	Seguridad	Cifrar el contenido enviado a través de la red.	A/M	6,4	95%
6	Seguridad	Comprobación de la autoría de la información enviada.	M/B	2,1	85%
7	Seguridad	Poseer un registro de los cambios realizados.	M/B	2,1	78%
8	Seguridad	Poseer un mecanismo de control de acceso por roles.	A/M	6,4	95%
9	Modificabilidad	Asegurar que un componente con responsabilidades comunes (alta cohesión de responsabilidades) no tengan que depender demasiado de componentes con distintas responsabilidades (bajo acoplamiento entre componentes).	M/M	4,4	90%
10	Modificabilidad	Diseño de políticas en el dominio de infraestructura subyacente física y virtualizada.	M/A	4,6	95%
11	Modificabilidad	Proveer integración entre los componentes mediante interfaces abstractas, con el objetivo de poder sustituir un componente por otro, con la menor cantidad de cambios posibles, con una copia de seguridad, guardada en un repositorio de contingencia o localmente.	M/B	2,1	80%
12	Verificabilidad	Proveer componentes o software especializado que permitan monitorizar el comportamiento de los componentes durante su ejecución.	M/M	4,4	90%
13	Verificabilidad	Proveer mecanismos de separación de interfaz e implementación, y el uso de componentes específicos para la realización de pruebas.	B/M	1,2	75%
14	Verificabilidad	Segmentación en dominios de	A/M	6,4	90%

		gestión.			
--	--	----------	--	--	--

Mientras que el peso relativo es obtenido a partir de la fórmula:

$$Pre_i = Pe_i / \sum_{i=0}^n Pe_i$$

Donde:

Pre= Peso relativo del escenario

Pe= Peso del Escenario

Tomando en cuenta los pesos relativos definido en cada uno de los escenarios y el porcentaje de impacto en el soporte de la arquitectura, se procede a calcular el valor que presenta cada uno de los atributos de calidad, posibilitando de esta forma comparar el porcentaje antes y después del empleo de la arquitectura propuesta ver cálculos en el Anexo 7.

3.1.1.4. Evidencia del cambio después de aplicada la metodología

En la siguiente tabla se demuestran los cambios luego de aplicada la metodología, donde se puede ver la variabilidad en cuanto al por ciento en cada uno de los atributos: Ver Tabla 8 de cambio después de aplicada la metodología.

Tabla 8: Tabla de cambio después de aplicada la metodología (elaboración propia)

Atributos	Antes	Después
Disponibilidad	80%	95%
Seguridad	85%	87%
Modificabilidad	80%	84%
Verificabilidad	70%	83%

3.2. Validación de la arquitectura implementada mediante Redes Petri

Con el objetivo de obtener de antemano una valoración de la lógica del comportamiento del procedimiento que se propone para la gestión del equipamiento activo de redes en un entorno simulado, verificando que no existen condiciones que limiten parcial o totalmente su ejecución, se utiliza un método cuantitativo, denominado Redes de Petri (RdP) (Gutiérrez, 2013). Las RdP es uno de los métodos más utilizados para la investigación de redes complejas, utilizadas inicialmente para el análisis de algoritmos en la computación paralela, que se ha extrapolado para la modelación de procesos productivos complejos y resultan válidas para evaluar su efectividad y facilitar su futura aplicación.

La construcción de la RdP correspondiente al procedimiento que se elaboró para la simulación, se comenzó con la traducción de las acciones, pasos, tareas, etapas o fases de este, a lugares, medios y recursos necesarios para la ejecución de cada una de las actividades, así como de las condiciones, resultado de la ejecución del procedimiento, mediante nodos tipo lugar; los eventos, procesos y actividades se representan por nodos del tipo transición. Los nodos y transiciones son unidos a través de arcos que representan las secuencias lógicas del procedimiento y sirven para comprobar la capacidad del mismo de ejecutarse total y parcialmente, y, por consiguiente, su flexibilidad y robustez. También se definen un conjunto de operadores para representar la evaluación de condiciones dentro del procedimiento (Distéfano, 2011). Auxiliada por la herramienta WoPeD se ejecutó la RdP planteada comprobándose que es realizable alcanzar el marcado final definido, a través de una secuencia de disparos de los nodos tipo “transición” que activaron los correspondientes nodos tipo “lugar”

Las fortalezas de las RdP estriban en sus propiedades, las que se dividen en dos áreas: las estructurales o estáticas, que validan la consistencia lógica del procedimiento modelado y dinámicas del comportamiento. La Tabla 9 muestra las propiedades resultantes del diseño por medio de las RdP del procedimiento. Las propiedades estructurales del procedimiento cuantifican la cantidad de nodos tipo “lugar”, nodos tipo “transición”, operadores y arcos, y la inexistencia de operadores usados erróneamente y violaciones de libre elección, lo que valida la consistencia lógica del procedimiento ya que no se imponen condiciones restricciones adicionales en su ejecución.

El análisis de robustez manifiesta lugares únicos tanto de inicio como de fin; así como el total de componentes conectados y fuertemente conectados. Lo cual significa que no se ha incorporado ninguna fase innecesaria dentro del procedimiento y que el orden que se ha planteado a las mismas es correcto. Las redes diseñadas son limitadas, así lo demuestra la inexistencia de lugares no acotados, por lo que las condiciones y los recursos son limitados, como sucede en la realidad, además la inexistencia de transiciones “muertas”, y “no vivas” garantiza la inexistencia de bloqueos en su ejecución, lo que permite verificar la vivacidad de las redes elaboradas. Esto significa que las salidas de cada uno de los componentes del modelo, operacionalizados en el procedimiento son suficientes para alcanzar las salidas esperadas a partir de las entradas definidas. El análisis del procedimiento para la simulación mediante RdP, como se observa en la Tabla 9 demuestra que este presenta condiciones adecuadas para su implementación siempre y cuando se cuente con los recursos necesarios y se cumplan las premisas.

Tabla de datos de la red Petri

Tabla 9: Tabla de datos de la Red Petri (elaboración propia)

Tipo de análisis	Elementos analizados	Fase
Análisis estructural	Nodos tipo lugar	13
	Nodos tipo transición	9
	Operadores	4
	Arcos	24
	Operadores usados erróneamente	0
	Violaciones de libre elección	0

Robustez	Lugar inicial	1
	Lugar final	1
	Componentes conectados	22
	Componentes fuertemente conectados	22
	Lugares no acotados (boundness)	0
	Transiciones muertas (dead- lock)	0
	Transiciones no vivas (non-live transitions)	0

Desde el punto de vista estructural, la tabla presenta las principales métricas de la red confeccionada (cantidad de nodos tipo lugar y tipo transición, cantidad de operadores y cantidad de arcos), y la inexistencia de operadores de uso erróneo y violaciones de libre elección¹⁷. Esta última comprobación garantiza que la propia dinámica de ejecución no agrega o impone condiciones o restricciones adicionales, lo cual valida la consistencia lógica del procedimiento general, así como sus procedimientos específicos.

3.3. Escenario de evaluación de la arquitectura

Para un mejor entendimiento de la propuesta de arquitectura a implementar se describen sus funcionalidades y características a través de un escenario de simulación. La configuración de dicho escenario es realizada en la herramienta de simulación Cisco Packet Trace. La figura 19 muestra la arquitectura simulada y permite ver los equipos utilizados en esta.

¹⁷ Definición: Esta condición implica que siempre que un nodo tipo lugar esté marcado y posea más de una transición de salida, es posible elegir la transición que se “disparará” independientemente del resto del marcado.

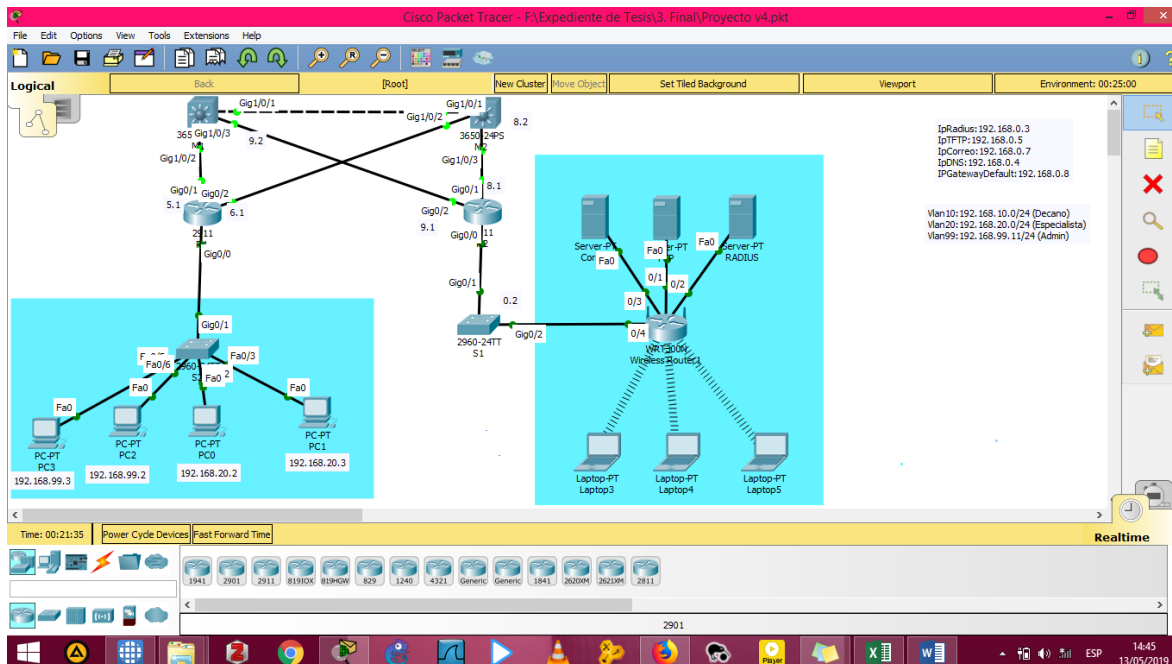


Figura 19: Imagen de la simulación

En este escenario se identifican los elementos que componen la arquitectura tradicional con PBNM que describe cada uno de los dispositivos (ver Anexo 8) que contiene el escenario y la función que realizan como parte la arquitectura propuesta.

3.4. Conclusiones del Capítulo

El método de evaluación de arquitectura ATAM y grupo focal demuestran el impacto positivo de la arquitectura en los atributos de calidad. Lo cual indica como el diseño de la arquitectura contribuye a elevar los atributos de calidad de la solución, haciendo uso de la gestión del equipamiento activo.

Mientras el método de validación de red Petri enmarca la validez del procedimiento a seguir en cuanto al análisis para el diseño de una arquitectura de red en cualquier negocio que desee promover la automaticidad dentro de la gestión de su equipamiento activo al establecer políticas.

La simulación de una arquitectura de red con estas características permite validar que si es posible la utilización de políticas en cuanto a la calidad, seguridad y automaticidad del proceso en red, un mejor monitoreo y control del equipamiento activo.

Conclusiones

El estudio de redes tradicionales integradas con la gestión basada en políticas (PBNM) demuestra que esta tecnología introduce una nueva etapa en el desarrollo de las redes, al mejorar significativamente la capacidad de gestión y control del equipamiento de una red.

La modelación del procedimiento constituye un esquema para simular un entorno de red tradicional integrado utilizando la gestión basada en políticas como elemento que permite la interoperabilidad entre las distintas tecnologías.

La arquitectura simulada constituye una guía metodológica para aplicar la propuesta en un escenario de red real, evidenciando la posibilidad de obtener mejor seguridad y calidad en las redes actuales.

La validación del procedimiento y la arquitectura demuestra que se puede incorporar en cualquier red permitiendo a las entidades mejorar su gestión de recursos informáticos al construir redes altamente escalables y flexibles.

Recomendaciones

Debido a los resultados de la investigación efectuada y a la experiencia adquirida durante la realización de este trabajo, se exponen las siguientes recomendaciones:

- Despliegue de la arquitectura en una infraestructura de red más amplia.
- Puesta en funcionamiento de una base de datos a la que se le envíen de forma automática las salvas realizadas de los equipos, para así mantener las políticas de una forma seguras.

Referencia Bibliográfica

9000, ISO. 2015. diferencia-proceso-procedimiento. *ISO 9000*. [En línea] 2015. <https://www.nueva-iso-9001-2015.com/2016/01/iso-9001-2015-diferencia-proceso-procedimiento/>.

ACM. 2014. Computing Carrers and Degrees. [En línea] 2014.

affiliates., Cisco and/or its. 2018 . The Cisco Community. [En línea] 2018 .

Alvarez Moraga, Sebastián Andrés y Gonzalez Valenzuela, Agustín José. [online]. 2005. Estudio y configuración de calidad de servicio para protocolos IPV4 e IPV6 en una red de fibra óptica. *Estudio y configuración de calidad de servicio para protocolos IPV4 e IPV6 en una red de fibra óptica*. [En línea] Rev. Fac. Ing. - Univ. Tarapacá, [online]. 2005. <http://dx.doi.org/>.

Anías Calderón, Caridad, Villariño Bolaño, Luis A. and Preciado Velasco, Jorge E. 2018. Gestión de Red Basada en Políticas. s.l. : <http://www.bibliociencias.cu/gsd/collect/eventos/import/>., 2018.

Arquitectura de Referencia para Unidades de Control de Robots de Servicio Teleoperados. **Zaragoza, F. J. Ortiz. 2005.** 2005. Cartagena.

Basalo, Antonio. Introducción a Angular.

Bass, Clements y Kazman . 2003. *Software Architecture in Practice*. 2003.

Bass, F. Bachmann y L. 2000. The architecture based design method. Carnegie Mellon University : CMU/SEI-200-TR-001, 2000.

Baykal, Yildirim, Karabacak. 2016. 2016.

Bunge, Mario. 2014. Ciencia, técnica y desarrollo. . 2014.

Casanova, Mónica Peña. 2018. 2018.

Castellano, Oscar. 2006. Red Petri. 2006.

Chachín, Rafael Belloso. 2010. Planificación y Gestión de redes. 2010.

Cisco., The Comunity. 2019. Implementación de políticas de calidad del servicio (QoS) con DSCP. [En línea] 2019.

—. **2019.** The Comunity Cisco. *Implementación de políticas de calidad del servicio (QoS) con DSCP*. . [En línea] 2019.

Co., Huawei Technologies. 2018. Sitio Oficial eNSP. [En línea] 2018. <http://enterprise.huawei.com/cn/>.

Cristina Leiceaga Abal, Angel Luis Hernandez Hernandez. 2016. Tecnología, Investigación y Desarrollo (I+D). [aut. libro] Cristina Leiceaga Abal. *Economía de Empresas*. 2016.

- Cuba, Partido Comunista de. 2017.** Lineamientos del PCC (PCC). [En línea] 2017.
- Distéfano, M., Pérez, S. 2011.** Desarrollo de sistemas concurrentes de control en tiempo real modelados con redes petri. 2011.
- Engineering, Task Internet. 2018.** Sitio oficial IETF. *nternet Engineering Task Force*. [En línea] 2018. <http://www.ietf.org..>
- F. J. Ortiz Zaragoza. 2005.** Arquitectura de Referencia para Unidades de Control de Robots de Servicio Teleoperados. Cartagena : s.n., 2005.
- foundation, Open networking. 2012. Software-defined networking: [En línea] abril de . 2012.** The new norm for networks. [En línea] 2012. opennetworking.org.
- Gillmeister, Brenner y. 2014.** 2014.
- GNS3, Sitio Oficial. 2018.** [En línea] 2018. <http://www.gns3.net/>.
- GNS3, Sitio Oficial. 2018.** GNS3. [En línea] 2018. <http://www.gns3.net>.
- Gutiérrez, H., Muñoz, Á. G. 2013.** Generación de diagramas ladder mediante el uso de redes de Petri difusas. 2013.
- . **2013.** Generación de diagramas ladder mediante el uso de redes de Petri difusas. 2013.
- Hernández, Garófalo. 2005.** 2005.
- IBM. 2018.** Organización de desarrollo de estándares (DMTF). [En línea] 2018. [http://www.dmtf.org/..](http://www.dmtf.org/)
- . **2018.** Sitio Oficial IBM. [En línea] 2018.
- . **2011.** The IBM Autonomic Computing Initiative. [En línea] 2011. [http://www.ibm.com/autonomic/..](http://www.ibm.com/autonomic/)
- IETF, Internet Engineering Task Force. 2018.** Sitio oficial IETF. [En línea] 2018. <http://www.ietf.org..>
- informáticas., Universidad de las ciencias. 2019.** Universidad de las ciencias informáticas. [En línea] 2019. [Citado el: 2 de noviembre de 2018.] <https://www.uci.cu/>.
- J. Rumbaugh, I. Jacobson, y G. Booch, Addison Wesley. 1998.** El lenguaje unificado de modelado. [En línea] 1998.
- K. R., M. Klein, y P. Clemens. 2000.** Method for architecture evaluations. s.l. : CMU/SEI-2000-TR-004, 2000.
- Larman, C. 2006.** UML y Patrones. 2006.
- Li et, al. 2016.** 2016.

librosweb.es. [En línea] www.librosweb.es.

Mann, Thomas T. Gold Smith Jr. y Estle Ray. 2013. 2013.

Margarita Alonso Martínez, Danile Perez González Pedro Solana González. 2010. Análisis y modelado con redes Workflow del procesos de tratamiento de experinecia. Redes Petri. 2010.

Marugan, Juan. 2010. Diseño de infraestructura de red y soporte informático. s.l. : ScienceDirect, 2010.

Mendillo, Vicencio. 2013. Cursos de Gestión de redes y servicios. 2013.

Oppenheimer, P. 2011. Top-Down Network Design. . Indianapolis: Cisco Press : 3a ed., 2011.

P. Clements, F. Bachmann, L. Bass, D. Garlan, J. Ivers, R. Little, R. Nord, y J. Stafford, Addison-Wesley,. 2002. Documenting Software Architectures. 2002.

Páez, Nicolás. 2014. Construcción de software: una mirada ágil. 2014.

Pedro Solana González, Margarita Alonso Martínez, Danile Perez González,. 2010. Redes Petri. 2010.

postgresql.org. [En línea] www.postgresql.org.es.

Pressman. 2010. 2010.

Reinoso, Billy. 2004. “Introducción a la arquitectura de software” . 2004.

Rolando Alfredo Hernández León, Sayda Coello González. 2014. *EL PROCESO DE INVESTIGACIÓN CIENTÍFICA (2 EDICIÓN)*. La Habana : Editorial Universitaria, 2014. ISBN 978-959- 16-1557-2.

Rouse. 2018. 2018.

Sánchez, Jorge. 2013. Introducción al JavaScript. 2013.

Sevilla. 2016. 2016.

Shaw, G. D. y M. 1994. “An introduction to software architecture” . 1994.

Sitio Oficial OMNeT++ . 2019. OMNeT++. [En línea] 2019. <http://www.omnetpp.org>.

Sollins, K. 2018. THE TFTP PROTOCOL. [En línea] 2018. <https://tools.ietf.org/html/rfc1350>..

Sommerville. 2017. 2017.

Steven Davy, Brendan Jennings , John Strassner. 2008. The policy continuum.Policy authoring and conflict analysis. . Schaumburg, Illinois : All rights reserved, 2008.

—. **2008.** The policy continuum–Policy authoring and conflict analysis. 2008.

Stevens Perdita, Rob Pooley, Addison Wesley. 2002. Utilización de UML en Ingeniería del Software con Objetos y Componentes. . 2002.

Strassner, J. 2001. *Terminology for Policy-Based Management*. 2001. RFC 3198.

sun.com. [En línea] (<http://www.sun.com/suntrademarks/>).

Ted Friedman, Eric Thoo. 2015. Magic quadrant for data integration tools. [En línea] 2015.

Ted Friedman, Eric Thoo. 2015.. Magic quadrant for data integration tools. . 2015.

Tejedor, Ramón Jesús Millián. 2005. Gestión de redes. [aut. libro] Ramón Jesús Millián Tejedor, David Roldán Martínez José Manuel Huidobro Moya. *Tecnologías de las telecomunicaciones*. México : s.n., 2005.

Thomas T. Gold Smith Jr., Estle Ray Mann. 2014. 2014.

Wei, S., L. Chen-Ching and Z. Li. 2012. Optimal generator start-up strategy for bulk power system restoration. 2012.

Wei, S., L. Chen-Ching and Z. Li. 2012. Optimal generator start-up strategy for bulk power system restoration. 2012.

XETID. online. XETID. [En línea] online. www.xetid.cu.

Zhang, Liam. 2010. Named Data Networking (ndn) project. [En línea] 2010.

Bibliografía

OMNeT++. [Online]. Sitio Oficial OMNeT++. *Sitio Oficial OMNeT++*. [En línea] [Online] <http://www.omnetpp.org>.

Alvarez Moraga, Sebastián Andrés y Gonzalez Valenzuela, Agustín José. [online]. 2005. Estudio y configuración de calidad de servicio para protocolos IPV4 e IPV6 en una red de fibra óptica. *Estudio y configuración de calidad de servicio para protocolos IPV4 e IPV6 en una red de fibra óptica*. [En línea] Rev. Fac. Ing. - Univ. Tarapacá, [online]. 2005. <http://dx.doi.org/>.

Anías Calderón, Caridad, Villariño Bolaño, Luis A. and Preciado Velasco, Jorge E. [Online]. Gestión de Red Basada en Políticas. [En línea] [Online]. http://www.bibliociencias.cu/gsd/collect/eventos/import/Gestión_Red_politicas.pdf.

Bunge, Mario. 2014. Ciencia, técnica y desarrollo. *Ciencia, técnica y desarrollo*. 2014.

C. Billy Reynoso. 2004.. “Introducción a la arquitectura de software”. [aut. libro] Billy Reinoso. 2004.

Castellano, Oscar. 2006. *Red Petris*. 2006.

Chacín, Dr. Rafael Belloso. 2010. Planificación y gestión de red. Venezuela, Maracaibo: s.n., 2010.

Cisco and/or its affiliates. 2018 (Online). The Cisco Community. [En línea] 2018 (Online).

Co., Huawei Technologies. [Online]. Sitio Oficial eNSP. *Sitio Oficial eNSP*. [En línea] [Online]. <http://enterprise.huawei.com/cn/>.

Cuba, Partido Comunista de. 2017. Lineamientos del PCC. *Granma*. 2017.

Distéfano, M., Pérez, S. 2011. *Desarrollo de sistemas concurrentes de control en tiempo real modelados con redes petri*. 2011.

Empleo de modelos de información en arquitectura modificada para gestión de redes y servicios basada en políticas. **Mónica Peña Casanova, Caridad Anías Calderón.** 2018. s.l.: RIELAC, p. 77-89 Septiembre – Diciembre, 2018, Vol. Vol. XXXIX 3/2018. ISSN: 1815-59.

- F. Bachmann y L. Bass, 2000.** *“The architecture based design method,”*. s.l. : Carnegie Mellon University, 2000. CMU/SEI-200-TR-001.
- F. J. Ortiz Zaragoza, Tesis Doctoral . 2005.** *Arquitectura de Referencia para Unidades de Control de Robots de Servicio Teleoperados.* Cartagena : s.n., 2005.
- Felix Bachmann, Len Bass, Gary Chasteck. 2000.** The architecture based design method. 2000.
- Force., Internet Engineering Task. [Online] .** Sitio oficial IETF. Internet Engineering Task Force. *IETF.* [En línea] [Online] . <http://www.ietf.org>.
- foundation, Open networking. 2012.** Software-defined networking: The new norm for networks. [En línea] abril de 2012. opennetworking.org.
- Garnet. 2019.** Best Policy Management Software. *Capterra.* [En línea] 2019.
- GNS3., Sitio Oficial. [Online] .** GNS3. *GNS3.* [En línea] [Online] . <http://www.gns3.net/>.
- Gutiérrez, H., Muñoz, Á. G. 2013.** *Generación de diagramas ladder mediante el uso de redes de Petri difusas.* . 2013.
- Hed, Harried. 2003.** Ethernet network, The Atrium. Chichester, England : s.n., 2003.
- IBM. 2018.** Organización de desarrollo de estándares (DMTF). *Organización de desarrollo de estándares (DMTF).* [En línea] 2018. [Citado el: 14 de 11 de 2018.] <http://www.dmtf.org/>.
- IEEE. 2009.** IEEE Architecture Working Group. [En línea] 2009.
- ISO/IEC. 2018.** *Information technology - Service management - Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1.* s.l. : ISO/IEC TR 20000-3, 2018.
- J. Rumbaugh, I. Jacobson, y G. Booch, Addison Wesley. 1998.** El lenguaje unificado de modelado. 1998.
- James Carlson, Addison Wesley. 2000.** *“PPP Design Implementation and •James Carlson PPP Design, Implementation, and Debugging”*. 2000. 2nd Edition.
- Jose Marin, Antonio Barbaro. 1999.** *Gestión de red.* s.l.: Universidad Politecnica de Cataluña, 1999.

K. R., M. Klein, y P. Clemens, 2000. "Atam sm: Method for architecture evaluation," s.l.: Carnegie Mellon University, 2000. CMU/SEI-2000-TR-004.

Kruchten, P. 1995. "The 4+1 View Model of Architecture". s.l. : IEEE Software, 1995.

Larman, C. 2006. UML. [aut. libro] Prentice Hall. *UML y Patrones*. s.l. : 2 ed, 2006.

2008. *Marcas Murrillo* . 2008.

Marugan, Juan. 2010. Diseño de infraestructura de red y soporte informático. s.l. : ScienceDirect, 2010.

Mendillo, Vicencio. 2013. *Cursos de Gestión de redes y servicios*. . 2013.

Mitra, Ananda. Digital Games: Computers at Play.

Mónica Peña Casanova, Caridad Anías Calderón. 2018. Empleo de modelos de información en arquitectura modificada para gestión de redes y servicios basada en políticas. La Habana,Cuba : s.n., 2018.

Oppenheimer, P. 2011. *Top-Down Network Design*. s.l. : Indianapolis: Cisco Press, 2011. 3a ed.

Optimal generator start-up strategy for bulk power system restoration. **Wei, S., L. Chen-Ching and Z. Li. 2012.** 2012.

P. Clements, F. Bachmann, L. Bass, D. Garlan, J. Ivers, R. Little, R. Nord, y J. Stafford, Addison-Wesley, . 2002. *Documenting Software Architectures*. 2002.

Pedro Solana González,Margarita Alonso Martínez,Danile Perez González. 2010. Redes Petri. [aut. libro] Margarita Alonso Martínez,Danile Perez González Pedro Solana González. *Análisis y modelado con redes Workflow del procesos de tratamiento de experinecias operativas*. 2010.

Rejón, Javier. 2016. Cisco Comunity. [En línea] 11 de marzo de 2016.

RFC-Editors. [Online]. [En línea] [Online]. <http://www.rfc-editor.org>..

Rolando Alfredo Hernández León, Sayda Coello González. 2014. *EL PROCESO DE INVESTIGACIÓN CIENTÍFICA (2 EDICIÓN)*. La Habana : Editorial Universitaria, 2014. ISBN 978-959- 16-1557-2.

Shaw, G. D. y M. 1994. “An introduction to software architecture” . “*An introduction to software architecture*” . [En línea] Enero de 1994.

Sollins, K. 1992. THE TFTP PROTOCOL. *THE TFTP PROTOCOL*. [En línea] 1992.
<https://tools.ietf.org/html/rfc1350>.

Steven Davy , Brendan Jennings , John Strassner . 2008. The policy continuum. [aut. libro] Brendan Jennings , John Strassner Steven Davy. *The policy continuum–Policy authoring and conflict analysis*. Schaumburg, Illinois : Elsevier B.V. All rights reserved, 2008.

Stevens Perdita, Rob Pooley, Addison Wesley. 2002. *Utilización de UML en Ingeniería del Software con Objetos y Componentes*. 2002.

Ted Friedman, Eric Thoo. 2015. “Magic quadrant for data integration tools.”. “*Magic quadrant for data integration tools*”. 2015.

Tejedor, Ramón Jesús Millán. 1999. *Gestión de Redes*. s.l.: Prensa Tecnica.SA, 2013.

The Comunity Cisco. Online. Implementación de políticas de calidad del servicio (QoS) con DSCP. [En línea] Online.

Undestanding capitalism. **Edwards, Samuel Bowless y Richard. 2016.** 2016.

2018. Universidad de las ciencias informáticas. *Universidad de las ciencias informáticas*. [En línea] UCI, 2 de noviembre de 2018. <https://www.uci.cu/>.

Wireshark., Sitio Oficial. [Online] . Wireshark. *Wireshark*. [En línea] [Online] .
<http://www.wireshark.org..>

Zhang, Liam. 2010. Named Data Networking (ndn) project. . *Named Data Networking (ndn) project*. . s.l. : Palo Alto : XeroxPaloAltoResearchCenter-PARC, 2010.

Anexos

Anexo 1

Tarjetas de red (Cisco, 2019) la siguiente tabla muestra los distintos tipos y sus características:

Tipos	Características
Tarjetas Inalámbricas	<ul style="list-style-type: none"> ➤ Estas tarjetas se conectan mediante señales de frecuencia específicas a otro dispositivo que sirva como concentrador de estas conexiones ➤ Elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red. ➤ Incrementan la productividad y eficiencia en las empresas donde está instalada.
Tarjetas Ethernet	<ul style="list-style-type: none"> ➤ La mayoría de tarjetas incluyen un zócalo para un PROM (Memoria programada de solo lectura, FIGURA 7.0). ➤ Esta alternativa tiene la ventaja de rebajar costos y aumentar la seguridad de acceso a la red, ya que los usuarios no pueden efectuar copias de los archivos importantes.
ARCNET	<ul style="list-style-type: none"> ➤ Las tarjetas para red ARCNET utilizaban principalmente conectores BNC y/o RJ-45.
Token Ring	<ul style="list-style-type: none"> ➤ Baja velocidad y elevado costo respecto de Ethernet. ➤ Tenían un conector DB-9. También se utilizó el conector RJ-45 para las NICs (tarjetas de redes) y los MAUs (Múltiple Access Unit- Unidad de

	múltiple acceso que era el núcleo de una red Token Ring).
Tarjetas de fibra óptica	<ul style="list-style-type: none"> ➤ Alta velocidad en la transmisión de los datos, así como en la confiabilidad y seguridad. ➤ Las señales se dan mediante impulsos de luz que hacen posible la transmisión de los datos a una mayor distancia, las tarjetas de fibra son más fáciles de configurar que las normales ya que solo se colocan y ya están en funcionamiento su uso está destinado a grandes estaciones, así como a concentradores de redes backbone ➤ Los conectores de las tarjetas son especiales en donde se ingresa el cable de fibra óptica monomodo o multimodo de una o dos vías según el diseño de la red,

Cables de red (Cisco, 2019) la siguiente tabla muestra los distintos tipos y características:

Tipos	Características
	<p>El par trenzado es un tipo de cableado de cobre que se utiliza para las comunicaciones telefónicas y la mayoría de las redes Ethernet.</p> <p>El par está trenzado para proporcionar protección contra crosstalk, que es el ruido generado por pares de hilos adyacentes en el cable. Los pares de hilos de cobre están envueltos en un aislamiento de plástico con codificación de color y trenzados entre sí. Un revestimiento exterior protege los paquetes de pares trenzados.</p> <p>Existen dos tipos básicos de cables de par trenzado:</p> <p>Par trenzado no blindado (UTP): Cable que tiene dos o cuatro pares de hilos. Este tipo de cable cuenta sólo con el efecto de cancelación producido</p>

	<p>por los pares trenzados de hilos que limita la degradación de la señal que causa la interfaz electromagnética (EMI) y la interferencia de radiofrecuencia (RFI).</p> <p>Par trenzado blindado (STP): Cada par de hilos está envuelto en un papel metálico para aislar mejor los hilos del ruido. Los cuatro pares de hilos están envueltos juntos en una trenza o papel metálico. El cableado STP reduce el ruido eléctrico desde el interior del cable. Asimismo, reduce la EMI y la RFI desde el exterior del cable.</p>
Cable coaxial	<p>El cable coaxial es un cable con núcleo de cobre envuelto en un blindaje grueso. Se utiliza para conectar computadoras en una red.</p> <p>Existen diversos tipos de cable coaxial:</p> <p>Thicknet o 10BASE5: Cable coaxial que se utilizaba en redes y funcionaba a 10 megabits por segundo con una longitud máxima de 500 m.</p> <p>Thinnet 10BASE2: Cable coaxial que se utilizaba en redes y funcionaba a 10 megabits por segundo con una longitud máxima de 185 m.</p> <p>RG-59: El más comúnmente utilizado para la televisión por cable en los Estados Unidos.</p> <p>RG-6: Cable de mayor calidad que RG-59, con más ancho de banda y menos propensión a interferencia.</p>
Cable de fibra óptica	<p>Tiene una o más fibras ópticas envueltas en un revestimiento. Debido a que está hecho de cristal, el cable de fibra óptica no se ve afectado por la interferencia electromagnética ni por la interferencia de radiofrecuencia.</p> <p>Los dos tipos de cable de fibra óptica de cristal son:</p> <p>Multimodo: Cable que tiene un núcleo más grueso que el cable monomodo. Es más fácil de realizar, puede usar fuentes de luz (LED) más simples y funciona bien en distancias de hasta unos pocos kilómetros.</p> <p>Monomodo: Cable que tiene un núcleo muy delgado. Es más difícil de</p>

realizar, usa láser como fuente de luz y puede transmitir señales a docenas de kilómetros con facilidad.
--

Enrutadores de red (Cisco, 2019) la siguiente tabla muestra sus características:

Tipo	Características
Router	<p>Interpretan las direcciones lógicas de la capa 3 en lugar de las direcciones MAC como hacen los switch's.</p> <p>Son capaces de cambiar el formato de la trama, ya que operan en un nivel superior a la misma.</p> <p>Poseen un elevado nivel de inteligencia y pueden manejar distintos protocolos previamente establecidos.</p> <p>Proporcionan seguridad a la red puesto que se pueden configurar para restringir los accesos a esta mediante filtrado.</p> <p>Reducen la congestión de la red aislando el tráfico y los dominios de colisión en las distintas subredes que conectan. Por ejemplo, un router TCP/IP puede filtrar los paquetes que le llegan utilizando las máscaras IP.</p>

Anexo 2

Encuesta realizada a centros sobre el desarrollo de las TI

Las infraestructuras relacionadas con las Tecnologías de la información (TI) han dejado de ser recursos de soporte a los procesos de las organizaciones para convertirse en activos estratégicos por cuanto les permiten mejorar los procesos de negocio, reducir los costos y crear productos y servicios innovadores. Existen un conjunto de marcos de referencia que se basan en buenas prácticas sobre cómo organizar la gestión y el gobierno de las infraestructuras TI.

La presente encuesta forma parte de una investigación para evaluar el nivel de implementación de estos marcos de referencia en el país. Analice con atención cada pregunta, cuidando además de la exactitud y veracidad de sus respuestas.

Gracias de antemano por su cooperación.

Escala: 1- 2 - 3 - 4 - 5 - 6 - 7 (7 es el valor que representa mayor impacto)

1. Marque con una X el rol que desempeña con respecto a las TI:

47 personas de 33 organismos diferentes

___ Usuario__ Decisor o directivo ___ Administrador

2. Evalúe su experiencia o nivel de conocimiento asociado a la gestión o gobierno de las infraestructuras y servicios TI de acuerdo con la escala anterior _____

3. ¿Cuál de los problemas relacionados con las TI ha padecido su organización en los últimos años? (Evalúe todos los que aplican)

	Escala						
	1	2	3	4	5	6	7
Incremento de los costos							
Insuficiente presupuesto destinado al mantenimiento de las TI							
El retorno de la inversión no alcanza los valores esperados							
Rápida obsolescencia del equipamiento, antes de poder renovarlo							
Incidentes operacionales serios							
Problemas con los proveedores de servicios TI							
Insuficiente personal relacionado con las TI							
Insuficientes habilidades del personal relacionado con las TI							
Lentitud en la respuesta a las necesidades de la organización							
Problemas al implementar nuevos sistemas							
Problemas al asimilar nuevas tecnologías							
Problemas al evaluar el impacto que tienen TI en la organización							
Ninguno							

Otras. ¿Cuáles?

Problemas con los mecanismos del país para la asignación de recursos

Rápida obsolescencia del equipamiento antes de poder renovarlo

"Falta de intercambio con áreas de TI de otras empresas de telecomunicaciones que permitan evaluar in situ las aplicaciones y plataformas implementadas. Dificultades con el acceso a información a algunos sitios importantes por la política de bloqueo contra Cuba, por ejemplo, el TM Fórum"

4. ¿Qué prácticas implementa su organización relacionadas con la gestión y el gobierno de las TI? (Evalúe todos los que aplican)

	Escala						
	1	2	3	4	5	6	7
Monitoreo del rendimiento de las infraestructuras TI							
Definición y monitoreo de métricas de calidad de servicio							
Definición y gestión de los procesos de TI							
Establecimiento de las políticas de TI							
Implementación de las políticas de la organización en las TI							
Ninguna							

Otras. ¿Cuáles?

Lentitud en la aprobación de las políticas definidas

Gestión de incidencias reportadas por usuarios

5. Sobre la evaluación del impacto de la ejecución de políticas sobre las infraestructuras TI en la organización.

	Escala						
	1	2	3	4	5	6	7
Considero importante evaluar el impacto							
Considero importante facilitar la evaluación del impacto							
Considero que el cumplimiento de acuerdos de nivel de servicio facilitan la evaluación del impacto							
Considero que la satisfacción de necesidades facilita la evaluación del impacto							
Considero que la medición de indicadores de calidad de servicio facilitan la evaluación del impacto							
Considero que la evaluación de la calidad de experiencia facilita la evaluación del impacto							

6. ¿Cómo se comportan en su organización los siguientes aspectos?

	Escala						
	1	2	3	4	5	6	7
Satisfacción con los servicios que brinda el área de TI de su organización.							
Alineamiento de las TI con los procesos claves de su organización.							

Información que tienen los técnicos de TI sobre los procesos de su organización.								
Infraestructura TI en función de lo que necesita su organización								
Utilización de marcos de referencia que incorpore mejores prácticas para la gestión o gobierno de las TI en la organización que usted dirige.								
NOTA: Por favor solo continúe de ser positiva su respuesta anterior.								
Seleccione cuál o cuáles marcos de referencia para la gestión o gobierno de las TI utilizan en la organización que usted dirige.								
COBIT								
ITIL								
TIA 942								
ISO 27000/ ISO 17799								
ISO 38500								
Frameworkx (eTOM, TAM)								
MOF								
CMMI								
TOGAF								
Zachman								
ISO 20000								
IT-CMF								
Acuerdos de Nivel de Servicio (SLA)								
Gestión de Redes Basadas en Política (PBNM)								
Iniciativas y estándares del DMTF								
Otros. ¿Cuáles?								
Facilidad para la contextualización de la gestión de redes y servicios para cada organización. ¿Cuál?								
Necesidad de integración de marcos de referencia para garantizar su uso eficiente								
Inclusión de guía que facilitara su implementación								
¿Cuánto tiempo le llevó como promedio implementarlo y asimilarlo?	0 - 6 meses							
	6 meses - 1 año							
	1 año -18 meses							
	18 meses - 2 años							
	Más de 2 años							
Impacto que ha tenido para su organización								
Empleo de métricas para evaluar impacto de las TI para la organización								
Inclusión de algún modelo de información que lleve las políticas a las tecnologías. ¿Cuál?								

7. ¿Cuáles han sido los resultados más importantes de la implementación de un marco de referencia relacionado con la gestión o el gobierno de las TI en su organización?

	Escala
--	--------

	1	2	3	4	5	6	7
Impacto en la gestión del conocimiento asociado a las TI							
Reducción de los costos de las TI							
Dimensionamiento adecuado de la infraestructuras TI							
Reducción de los riesgos asociados a las TI							
Optimización de la infraestructura							
Consolidación del portafolio de servicios							
Consolidación del portafolio de sistemas informáticos							
Redefinición de Acuerdos de Nivel de Servicio con los proveedores de tecnología							
Redefinición de los Acuerdos de Nivel de Servicio con el negocio, mejora en el cumplimiento de sus necesidades							
Inversiones en TI que provocaron reducción de los costos del negocio							
Optimización de los recursos humanos asociados a la operación de las TI							
Capacidad de evaluar el impacto económico de las TI en el sector que trabaja							
Inmediatez para responder a las necesidades de la organización							
Ejecución de las políticas asociadas al negocio en la infraestructura							

Otras. ¿Cuáles?

Anexo 3

Prácticas de gestión y gobierno



Gráfico 1: Prácticas de gestión y gobierno

Marcos de referencias según políticas y estándares utilizados en centros en Cuba

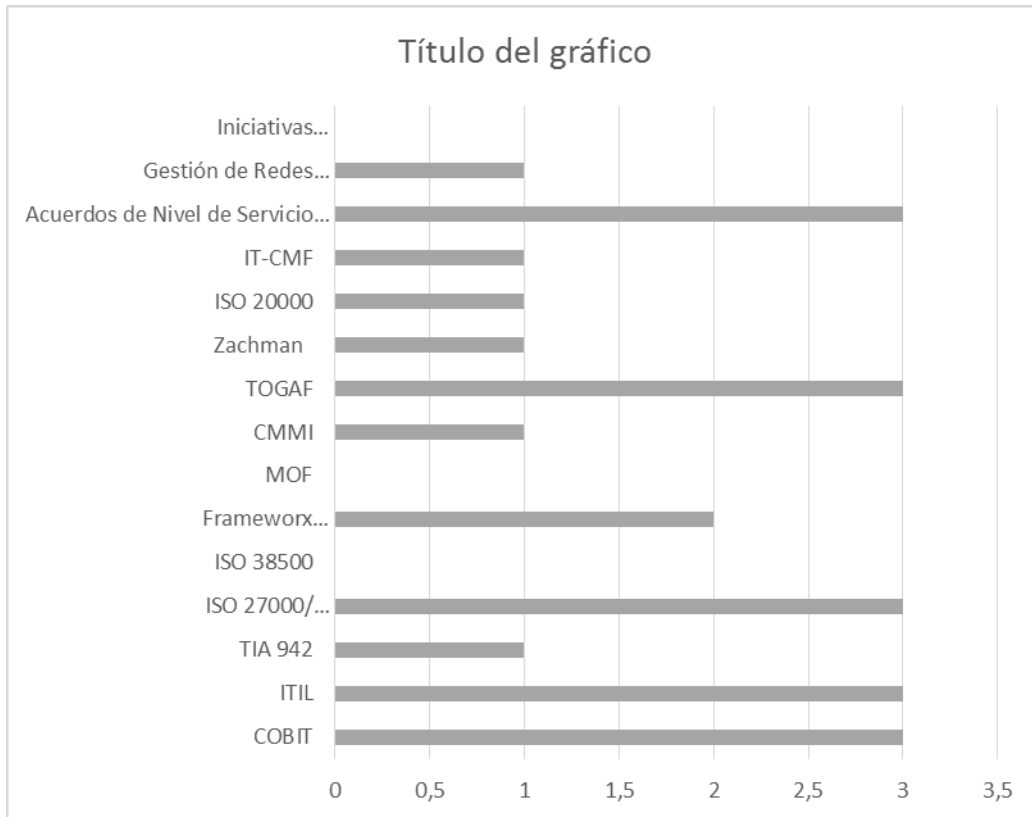


Gráfico 2: Referencias según políticas y estándares

Anexo 4

Entrevista realizada a los administradores de redes de la UCI

La siguiente entrevista es de modo profesional con el fin de recoger la información necesaria para realizar los cambios pertinentes en la arquitectura que se debe montar en la UCI al realizar una simulación para el desarrollo de una tesis de grado, velando a su vez por los costos, la integridad de los datos que maneja el centro, la privacidad de los usuarios y no realizar ninguna afectación a su actual arquitectura.

Gracias de antemano por su cooperación

1. ¿Cuál es la topología actual que presenta la red de la universidad?
 Anillo Estrella Malla Árbol
2. Qué tipo de cableado está presente en la red.

Ethernet Par trenzado Coaxial Fibra monomodo Fibra Multimodo
 UTP STP

3. ¿Qué equipos de interconexión están presente en el diseño UCI?

Router Switch L2 Switch L3 Puntos de acceso inalámbricos Router inalámbricos

4. El equipamiento utilizado es de proveedores como:

CISCO Huawei

Otros: _____

¿Qué clasificación de tiers utilizan en este centro de datos para mantener la fiabilidad y disponibilidad?

- Tier I: Centro de datos Básico
- Tier II: Centro de datos Redundante
- Tier III: Centro de datos Concurrentemente Mantenibles
- Tier IV: Centro de datos Tolerantes a Fallos

5. ¿Qué software de gestión utilizan actualmente? Creen que sea el más apropiado.

Sí

No justifique _____

Dentro de estas políticas ¿Cuáles se encuentran actualmente en funcionamiento en la UCI? Mencione las políticas que cree que deban estar actualmente implementadas para garantizar mejor seguridad y calidad.

- Políticas de autenticación, autorización y contabilidad mediante servidores Radius
- Políticas de gestión de salvas ante fallos eléctricos
- Políticas para calidad de servicio mediante ACL

Anexo 5

Entrevista a 4 modeladores en cuanto al análisis en porciento, con respecto a la disponibilidad, seguridad, modificabilidad y verificabilidad de la arquitectura de red actual en la UCI.

¿Qué porcentaje le dan ustedes a la disponibilidad que presenta la red actual de la UCI debido a su forma de gestión y por qué?

¿Qué porcentaje le proporcionan a la seguridad que tiene la red de la UCI y por qué?

¿Qué porcentaje le proporcionan a la modificabilidad de los servicios y equipos con que cuenta y brinda la red actual de la UCI?

¿Qué porcentaje le dan al software de verificabilidad con que cuentan actualmente en la UCI para manejar los servicios y gestionar los equipos de red?

Rol de Administración	Especialistas	Años de graduados	Años de ejercer	Categoría	Especialidad
	1	15	5	Ing. CCNA	Cibernética
	2	16	8	MSc. CCNA	Teleinformática
	3	16	16	Ing. CCNA	Teleinformática
	4	16	8	Ing. CCNA	Teleinformática

Anexo 6

Descripción de escenarios de ATAM

Escenario 1: Proveer mecanismos de almacenamiento y respaldo de los datos.

- **Atributo:** disponibilidad
- **Entorno:** ejecución normal
- **Estímulo:** salvas a través de un server TFTP
- **Respuesta:** mantiene configuraciones guardadas
- **Decisión Arquitectónica:**
 - Arquitectura basada server de salvas

Escenario 2: Proporcionar mecanismos de recuperación ante fallos.

- **Atributo:** disponibilidad
- **Entorno:** ejecución normal
- **Estímulo:** ocurre una caída de algún equipo en la red
- **Respuesta:** se informa de la caída y se levanta el servicio debido a las salvas en un TFTP
- **Decisión Arquitectónica:**
 - Arquitectura con un mecanismo centralizado de gestión de fallas
 - Arquitectura basada en eventos
 - Arquitectura de tiempo real

Escenario 3: Proveer la disponibilidad de los servicios brindados todos los días a toda hora.

- **Atributo:** disponibilidad
- **Entorno:** ejecución normal
- **Estímulo:** ocurre un fallo eléctrico durante la ejecución
- **Respuesta:** luego de encendido el servidor, se vuelve a ejecutar el sistema en un corto período de recuperación.
- **Decisión Arquitectónica:**
 - Basada en la puesta en marcha por ficheros de configuración

Escenario 4: Crear mecanismos de salvas totales

- **Atributo:** disponibilidad
- **Entorno:** momento de descanso de los equipos
- **Estímulo:** al asignar un momento de descanso a cada equipo
- **Respuesta:** se realizan salvas de su configuración completa
- **Decisión Arquitectónica:** Arquitectura centralizada

Escenario 5: Cifrar el contenido enviado a través de la red.

- **Atributo:** seguridad
- **Entorno:** ejecución normal

- **Estímulo:** solicitud seguridad en cuanto a los paquetes enviados
- **Respuesta:** se cifra el contenido de los paquetes para mayor seguridad en su envío
 - **Decisión Arquitectónica:** Uso de protocolos de transmisión seguro

Escenario 6: Comprobación de la autoría de la información enviada.

- **Atributo:** seguridad
- **Entorno:** ejecución normal
- **Estímulo:** seguridad en cuanto a la información recibida.
- **Respuesta:** se ve dominio de donde fue enviada la información.
 - **Decisión Arquitectónica:** Uso de protocolos de transmisión seguros

Escenario 7: Poseer un registro de los cambios realizados.

- **Atributo:** seguridad
- **Entorno:** ejecución normal
- **Estímulo:** pérdida de la configuración de un equipo
- **Respuesta:** al tener salvadas de configuración se pueden volver a levantar los cambios
- **Decisión Arquitectónica:**
 - Implementación de firmas digitales

Escenario 8: Asegurar que un componente con responsabilidades comunes (alta cohesión de responsabilidades) no tengan que depender demasiado de componentes con distintas responsabilidades (bajo acoplamiento entre componentes).

- **Atributo:** modificabilidad
- **Entorno:** ejecución normal
- **Estímulo:** dependencia de un repo en cuanto a su conexión con un server
- **Respuesta:** se requiere de los permisos para acceder a determinado repo
- **Decisión Arquitectónica:**
 - Arquitectura de repositorios

Escenario 9: Diseño de políticas en el dominio de infraestructura subyacente física y virtualizada.

- **Atributo:** modificabilidad
- **Entorno:** elaboración de políticas de red
- **Estímulo:** se crea una política nueva para las redes virtuales
- **Respuesta:**
- **Decisión Arquitectónica:**
 - Patrón de implementación de políticas basado en VLAN

Escenario 10: Proveer integración entre los componentes mediante interfaces abstractas, con el objetivo de poder sustituir un componente por otro, con la menor cantidad de cambios posibles, con una copia de seguridad, guardada en un repositorio de contingencia o localmente.

- **Atributo:** modificabilidad
- **Entorno:** ejecución normal
- **Estímulo:** se realiza cambio de equipos de red
- **Respuesta:** se ejecutan cambios en su configuración de acuerdo con el equipo
- **Decisión Arquitectónica:**
 - Mecanismo de configuración de equipos

Escenario 11: Proveer componentes o software especializado que permitan monitorizar el comportamiento de los componentes durante su ejecución.

- **Atributo:** verificabilidad
- **Entorno:** ejecución normal
- **Estímulo:** no se puede monitorizar un equipo
- **Respuesta:** se monitoriza el comportamiento de los equipos mientras estén en funcionamiento
- **Decisión Arquitectónica:**
 - Software de monitoreo

Escenario 12: Proveer mecanismos de separación de interfaz e implementación, y el uso de componentes específicos para la realización de pruebas.

- **Atributo:** verificabilidad
- **Entorno:** ejecución normal
- **Estímulo:** configuración mediante consola
- **Respuesta:** puesta en marchas de las políticas mediante su implementación
- **Decisión Arquitectónica:**
 - Implementación de las políticas mediante CLI

Escenario 13: Segmentación en dominios de gestión

- **Atributo:** verificabilidad
- **Entorno:** ejecución normal
- **Estímulo:** segmentación de los dominios por seguridad
- **Respuesta:** se obtiene seguridad por dominios luego de su segmentación
- **Decisión Arquitectónica:** Segmentación para verificar la seguridad

Anexo 7

Fórmula para la obtención de los valores de los criterios:

$$Pre_i = p_{e_i} / \sum_{i=0}^n p_{e_i}$$

Cálculo de Disponibilidad

$$\text{Disponibilidad} = 0.285*(95/100) + 0.285*(95/100) + 0.285*(100/100) + 0.142*(90/100) = 0.9543$$

Cálculo de Seguridad

$$\text{Seguridad} = 0.285*(95/100) + 0.285*(85/100) + 0.285*(78/100) + 0.142*(95/100) = 0.8702$$

Cálculo de Modificabilidad

$$\text{Modificabilidad} = 0.285*(90/100) + 0.285*(95/100) + 0.4*(80/100) = 0.84725$$

Cálculo de verificabilidad

$$\text{Verificabilidad} = 0.285*(90/100) + 0.285*(75/100) + 0.4*(90/100) = 0.83025$$

Anexo 8

Detalles de partes de la simulación

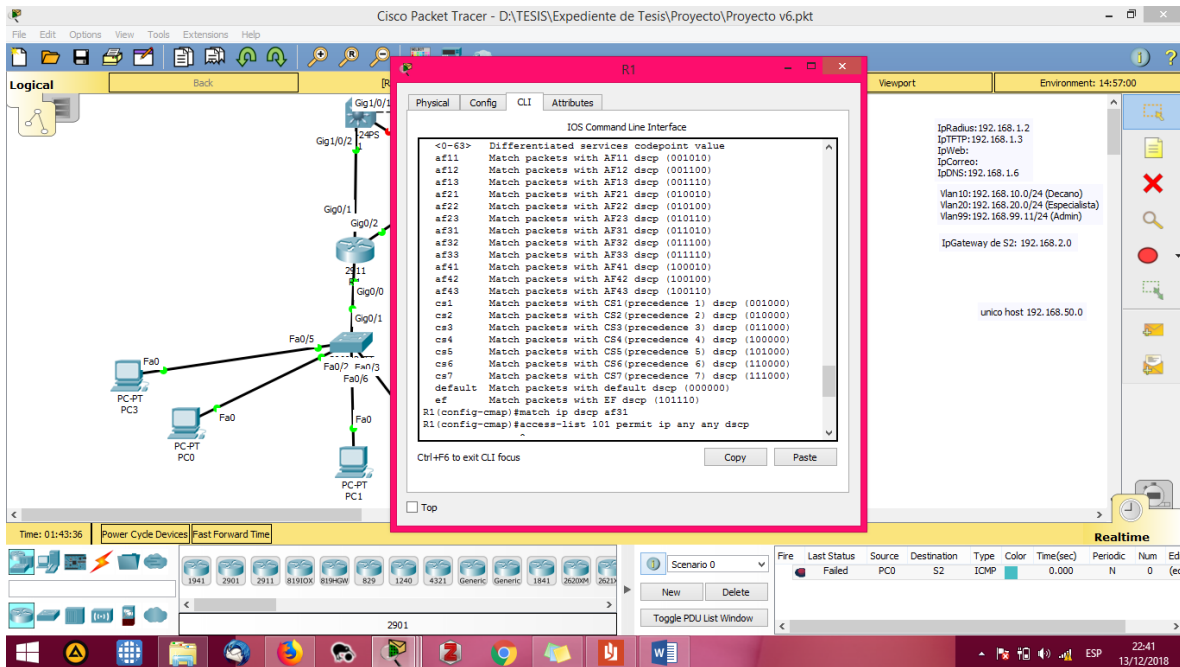


Imagen 1: Calidad mediante ACL (elaboración propia)

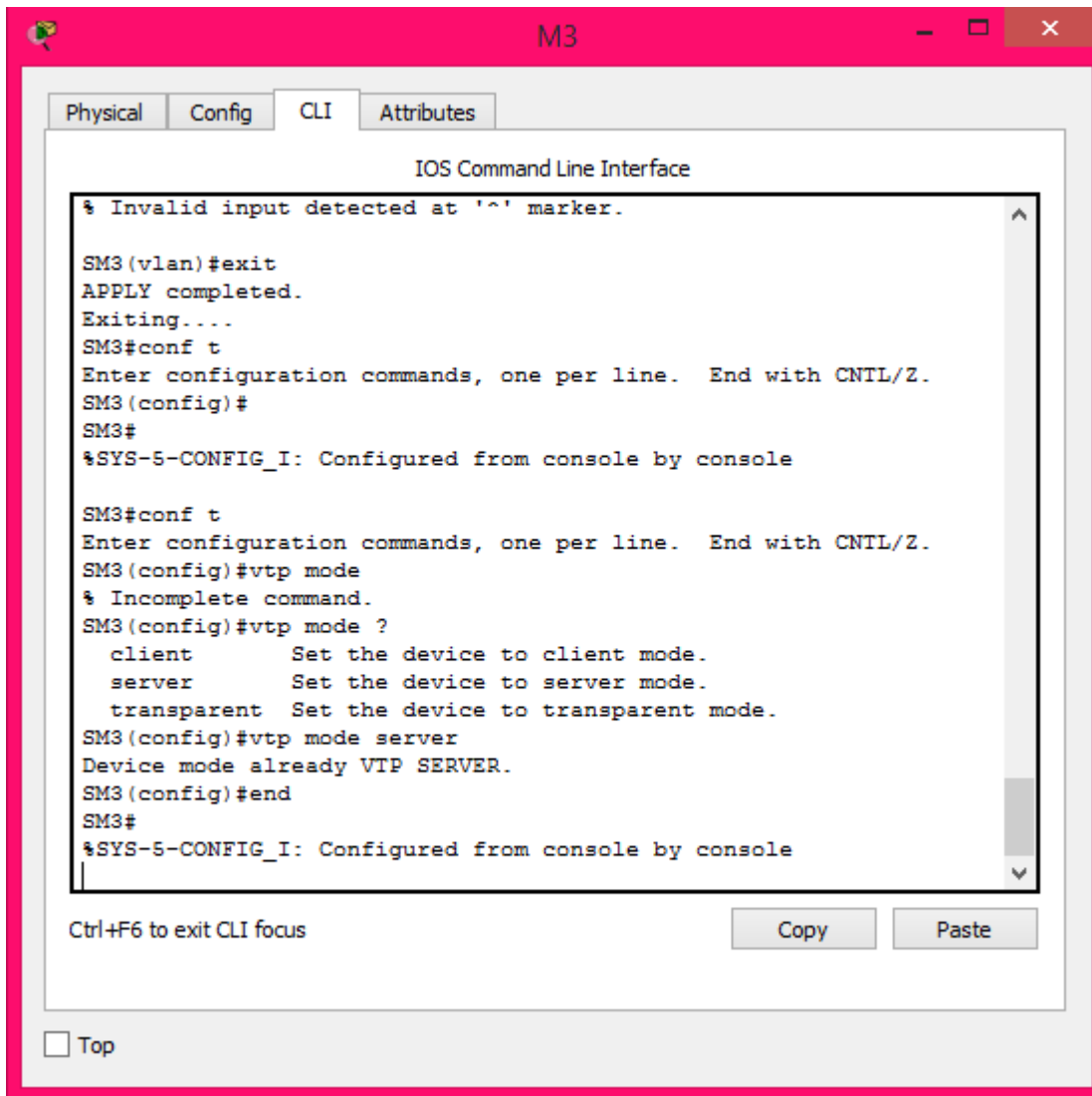


Imagen 2: Configuración del VTP (elaboración propia)

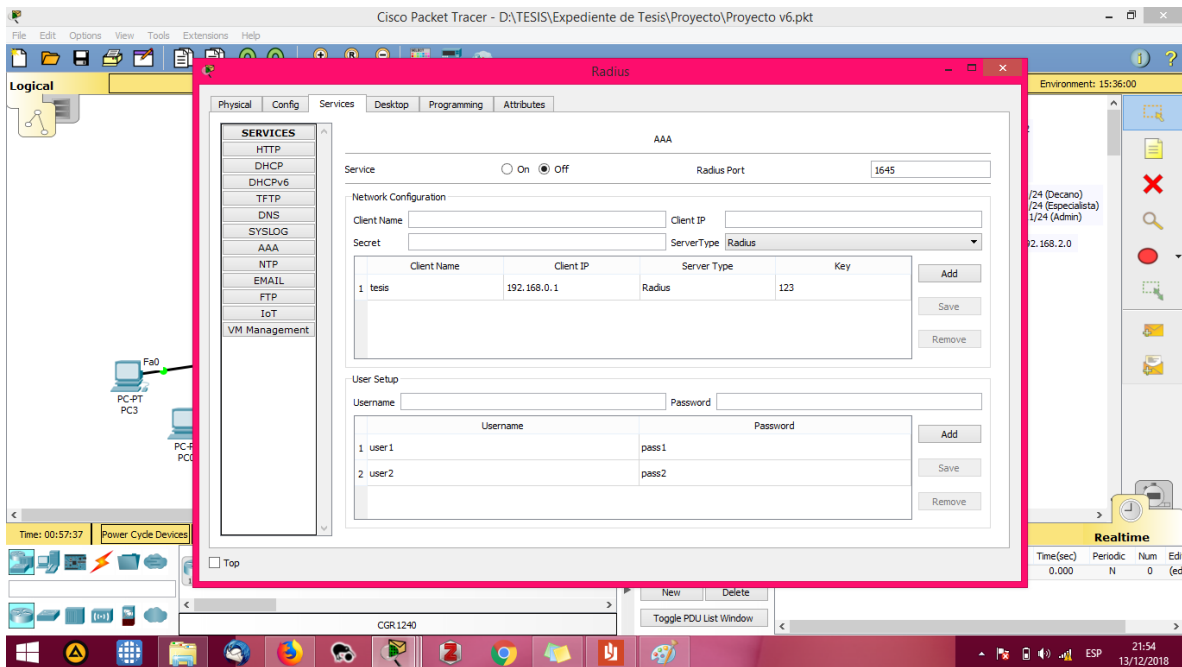


Imagen 3: Configuración del server RADIUS (elaboración propia)