

TecnoLógicas
ISSN-p 0123-7799
ISSN-e 2256-5337
Vol. 23, No. 48, pp. 31-53
Mayo-agosto de 2020

Artículo de Investigación/Research Article

Modelo para la gestión de infraestructuras de tecnologías de la información

Model for Information Technology Infrastructures Management

Mónica Peña Casanova  ¹,
Caridad Anías Calderón ²

Recibido: 28 de julio de 2019
Aceptado: 09 de diciembre de 2019

Cómo citar / How to cite

M. Peña Casanova, Caridad Anías Calderón “Modelo para la gestión de infraestructuras de tecnologías de la información.”. *TecnoLógicas*, vol. 23, no. 48, pp. 31-53, 2020. <https://doi.org/10.22430/22565337.1449>

© Instituto Tecnológico Metropolitano
Este trabajo está licenciado bajo una
Licencia Internacional Creative
Commons Atribución (CC BY-NC-SA)



¹ PhD. en Ciencias Técnicas,, Facultad 2, Departamento de Programación y Sistemas Digitales, Universidad de las Ciencias Informáticas, La Habana-Cuba, monica@uci.cu

² PhD. en Ciencias Técnicas, Facultad de Ingeniería y Administración, Departamento de Ingeniería, Facultad de Telecomunicaciones, Departamento de Telemática, Universidad Tecnológica de La Habana, La Habana-Cuba, cache@tesla.cujae.edu.cu

Resumen

Entre los problemas actuales para la introducción de las tecnologías de la información en las organizaciones, se encuentran el desalineamiento y la complejidad existente entre las infraestructuras TI y las políticas del negocio provocadas por múltiples marcos de referencia con insuficiencias para su unificación, la heterogeneidad y dispersión en los elementos a gestionar y los modelos de gestión estandarizados con poca integración entre ellos e inexactitud en las soluciones de evaluación de impacto. En el presente trabajo, se desarrolla un modelo para la gestión de infraestructuras TI (MGITI) que contribuye a reducir la complejidad y el desalineamiento presentes en esta. Posee cinco componentes: marco integrado de procesos para la gestión de las TI, contextualizado a las necesidades de las organizaciones; diseño de políticas de TI a partir de la extrapolación de los métodos de diseño de arquitecturas de sistemas; dimensionamiento de la infraestructura subyacente necesaria para automatizar la gestión y cumplir las necesidades de calidad de servicio; ejecución de políticas en las infraestructuras subyacentes, con la propuesta de una modificación a la arquitectura de gestión basada en políticas; y, por último, evaluación de impacto, que contempla el impacto estratégico, estructural y social.

Palabras clave

Automatización de políticas, gestión de TI, alineamiento de TI, impacto de TI, infraestructura TI.

Abstract

Currently, organizations face problems in order to introduce new information technologies. They include the misalignment between and complexity of IT infrastructure and the business policies derived from different reference frameworks with insufficiencies for unification, the heterogeneity and dispersion of the elements to be managed, standardized management models with little integration with each other, and the inexactness of impact evaluation solutions. This paper presents an IT infrastructure management model that aims to reduce complexity and misalignment in management. It is divided into five components: (1) comprehensive framework for IT management adapted to organizational needs, (2) IT policy-making based on the extrapolation of system architecture design methods, (3) sizing of the underlying infrastructure necessary to automate management and meet service quality needs, (4) implementation of policies in the underlying infrastructures and proposing changes to the management architecture based on policies, and (5) impact evaluation including the strategic, structural, and social impact.

Keywords

Policy automatization, IT management, IT alignment, IT impact, IT infrastructure

1. INTRODUCCIÓN

El éxito de la introducción de las Tecnologías de la Información (TI) en las organizaciones está determinado por la gestión que se desarrolla de las mismas a través de la habilitación de un conjunto de sus capacidades, utilizando un grupo de facilitadores que forman parte de las prácticas de gestión [1]-[4].

Los administradores de TI se enfrentan al desafío de alinear (hacer converger, armonizar, integrar, enlazar, sincronizar, etc.) los objetivos y procesos de TI a los de las organizaciones, aplicar la mejora continua en los servicios que prestan, medir su eficacia y demostrar un retorno de la inversión que evidencie el impacto de las TI como habilitadores y conductores de los cambios en las organizaciones. Para lograr este alineamiento en entornos de determinada complejidad caracterizados por dispositivos heterogéneos y dispersos con cortos períodos de obsolescencia, múltiples servicios sometidos a variados requerimientos regulatorios y sus usuarios desde contextos diversos, la automatización de la gestión de infraestructuras TI se ha convertido en un imperativo [5]-[9].

Se ha ido superando un modelo de gestión puramente orientado al monitoreo y control del rendimiento de la infraestructura existente. En este, el área de las TI de las organizaciones se apoyaba para la ejecución de los procesos sin recibir retroalimentación con respecto al impacto de parte de un sector que considera la alineación a los objetivos del negocio. Sin embargo, varios estudios internacionales demuestran que el desalineamiento sigue siendo una problemática que urge solucionar en las organizaciones [6], [10]-[15].

Existen múltiples marcos de referencia, iniciativas y estándares de lo que resultan dificultades para su aplicación alineada a los diferentes escenarios de negocios, aspectos que obstaculizan su integración,

insuficiencias para la formulación de requisitos de las organizaciones como políticas de TI, y diversidad e inexactitud en la evaluación del impacto. La existencia de varios modelos para la gestión integrada complejiza la integración de estos, así como la representación de políticas de TI a ser ejecutadas en los diferentes dominios de gestión de las infraestructuras TI.

El presente trabajo propone un modelo que, utilizando estandarización, integración y automatización, debe contribuir a reducir la complejidad y el desalineamiento en la gestión de infraestructuras de las tecnologías de la información. En el mismo, se detallan los componentes del modelo.

2. DESCRIPCIÓN DE MARCOS DE REFERENCIA PARA GESTIÓN DE INFRAESTRUCTURAS TI

Se han publicado varias metodologías, estándares y guías de buenas prácticas que permiten la articulación entre personas, procesos y tecnología, con el objetivo de cumplir con los objetivos estratégicos y de operación en una organización. Además, incorporan gran cantidad de conocimientos acumulados a lo largo de muchos años en la explotación de infraestructuras TI en función de las organizaciones. Tales conocimientos se pueden utilizar como instrumentos para abordar tanto el gobierno como la gestión de TI, entre ellos: COBIT (por las siglas en inglés de Control Objectives for Information and Related Technology), ITIL (por las siglas en inglés Information Technology Infrastructure Library), las normas ISO 20000, ISO 27000, ISO 38500, CMMI (por las siglas en inglés de Capability Maturity Model Integration) y eTOM (por las siglas en inglés de enhanced Telecommunication Operations Map). Todas estas consensuadas y validadas a nivel internacional por más de 155 países [16], [17].

No obstante, seleccionar uno o varios marcos apropiados para la gestión y el gobierno de las TI no resulta sencillo, ya que algunos, como en el caso de COBIT, aunque abordan los dominios tanto de la gestión como del gobierno, hacen mayor hincapié en este último, incluido un modelo de madurez [18]. Otros modelos como ITIL se enfocan en la gestión y en la definición de los aspectos funcionales, atributos operacionales y de organización [19], [20].

Por su parte, ISO 38500 enuncia el gobierno de las TI, sus principios y actividades; otros marcos como la ISO 27000 se orientan en la gestión de la seguridad. Adicionalmente, la implementación de un marco de referencia requiere de una inversión previa en conocimientos e infraestructura [21]-[23].

La gran heterogeneidad de modelos y estándares existentes permite a las organizaciones seleccionar aquellos que se ajusten mejor a sus necesidades. Sin embargo, muchos de los marcos de referencia existentes se complementan, de ahí que la tendencia actual es a su integración, para garantizar la utilización de los mismos de manera eficiente [24], [25]. Estas soluciones de integración no incorporan la evaluación del impacto de tales prácticas en las organizaciones.

En la medida en que las infraestructuras TI han crecido en tamaño, complejidad y heterogeneidad, también ha crecido la necesidad de gestionarlas de manera integrada con el fin de hacer que sus características se puedan representar de forma estructurada y estandarizada.

Existen varios modelos de gestión que se han estandarizado, cada uno con su propio protocolo de comunicaciones y definición de información de gestión, utilizados en diferentes ámbitos. En razón a lo anterior, está presente el dilema de la integración de los modelos de gestión con vistas a tener un control holístico de la red y sus servicios. Una vía para lograrlo es la integración de los modelos de información.

Esta integración, unida a la automatización de la ejecución de políticas en las TI, debe permitir su comportamiento autónomo. Múltiples propuestas han surgido para lograr la integración de modelos de información pertenecientes a modelos de gestión estandarizados, pero las mismas no garantizan que se puedan ejecutar las políticas de la organización en las infraestructuras.

La mayor parte de las organizaciones operan utilizando una ventana de tiempo en la cual pueden realizarse los cambios en su infraestructura sin afectar el negocio.

La Gestión de Redes Basadas en Políticas (PBNM) permite hacer cambios en esa ventana de tiempo, pues facilita la automatización de tareas complejas y repetitivas; no obstante, está enfocada a la ejecución de políticas a nivel técnico y no tiene asociadas soluciones que faciliten el diseño de políticas de TI a partir de requisitos de las organizaciones [26].

Entre los modelos de información y datos más destacados se encuentran los correspondientes a los estándares SNMP (por las siglas en inglés de Simple Network Management Protocol), ampliamente utilizado en el ámbito de Internet, y OSI SM (por las siglas en inglés de Open Systems Interconnection-Systems Management), que es la base de muchos otros modelos de información y ha sido poco utilizado debido a su complejidad. Otros modelos de información de amplia aceptación son CIM (por las siglas en inglés de Commun Information Model), SID (por las siglas en inglés de Shared Information Data Model) y DEN-ng (por las siglas en inglés de Directory Enabled Network-next generation) [27]-[36]. Los modelos de información mencionados anteriormente han sido estandarizados por diferentes organismos encargados de esto [30], [37].

CIM se destaca por ser un modelo de gran integrabilidad, cosa que logra gracias a su gestor de objetos, CIMOM, que abarca no solamente modelos de gestión estandarizados, sino también algunos

propietarios [36]. Por otra parte, DEN-ng cuenta con gran capacidad para representar políticas, ya que precisa menos recursos para la ejecución de estas.

La representación de políticas mediante la tríada evento-condición-acción (ECA) empleada por DEN-ng faculta la inclusión, de forma explícita, de eventos que determinan cuándo deben evaluarse las políticas. Además, DEN-ng posibilita la representación del contexto del objeto gestionado, de ahí que ambos modelos, CIM y DEN-ng, brinden amplias capacidades para representar políticas en entornos de gestión integrados [38].

Según el grupo de trabajo del IETF (por las siglas en inglés Internet Engineering Task Force), un modelo de gestión basado en políticas incluye un contenedor o repositorio de políticas, un punto de decisión de políticas o servidor de políticas (PDP, por las siglas en inglés de Policy Decision Point) y uno o varios puntos de ejecución de políticas (PEP, por las siglas en inglés Policy Enforcement Point). En los PEP se aplican o ejecutan las políticas que

gobiernan los dispositivos físicos. El PDP revisa las políticas almacenadas en el contenedor de políticas y efectúa un proceso de toma de decisiones independientemente de las características de los dispositivos asociados a los PEP.

Son los PEP los encargados de traducir las políticas en operaciones o comandos específicos que puedan ser interpretados por la tecnología de los recursos por ellos gestionados. La Fig. 1 muestra una arquitectura general para un sistema PBNM, que sigue la filosofía cliente-servidor [39], [40].

El atributo más importante que ofrece la PBNM es cierta abstracción útil para manejar la brecha que existe entre las necesidades del negocio y las políticas de TI a este nivel y el funcionamiento de los elementos de red. Dichas políticas gobiernan el funcionamiento en tiempo real de la infraestructura y proporcionan un poderoso mecanismo para lograr cierto nivel de autonomía en la gestión alineada a las necesidades de la organización [37].

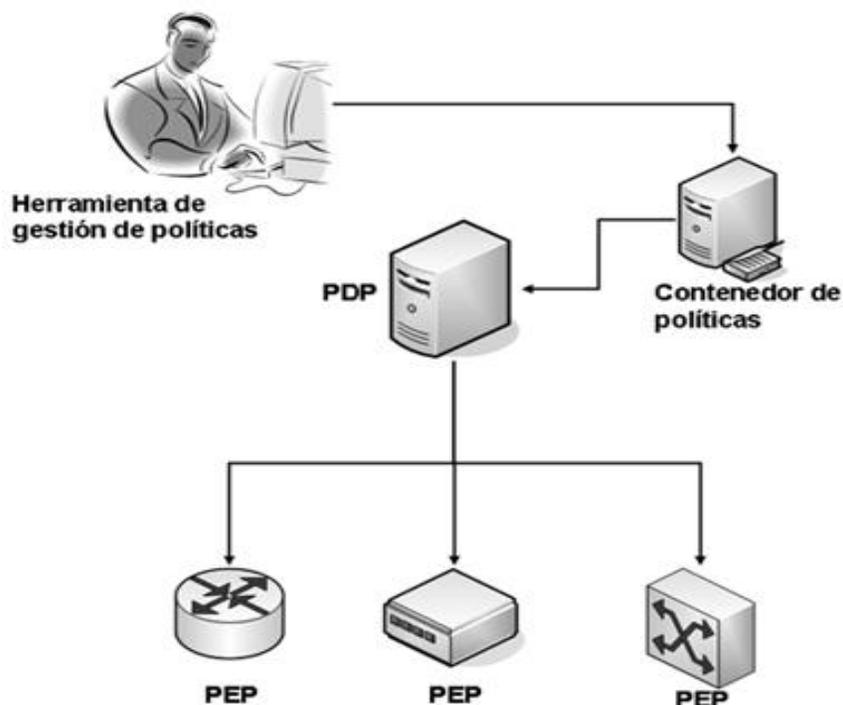


Fig. 1. Arquitectura PBNM propuesta por el IETF. Fuente: [40]

Para el funcionamiento alineado de PBNM, se requiere diseñar políticas a nivel de negocio y estratificarlas hasta las instancias que se ejecutarán en los PEP.

Por otra parte, al segmentar la gestión en dominios, PBNM posee dificultades para el tratamiento de conflictos entre las políticas que se aplican a las diferentes áreas de influencia. Además, cuando se emplea esta arquitectura, es muy importante ser cuidadosos en la selección de los modelos de información que se utilizarán, en aras de la predictibilidad, eficiencia y la operación sobre múltiples soluciones de gestión integrada, así como soluciones propietarias [38].

Adicionalmente, los métodos para la evaluación del impacto de los modelos de gestión o gobierno para las organizaciones son diversos. Algunos evalúan el impacto a nivel estratégico [4] y otros el alineamiento estructural [41]. También se han empleado modelos de madurez [42]-[44]. Además, existen modelos para evaluar el impacto de la implementación de los diferentes marcos de referencia [16], [45], [46]. Esta dispersión en la evaluación de impacto no permite tener medidas globales para

evaluar la gestión y el gobierno de las TI en las organizaciones en el ámbito estratégico, estructural y social.

3. PROPUESTA DE SOLUCIÓN

Como resultado de la necesidad de vencer la barrera de la diversidad de estructura, procesos y términos para la integración, alineamiento, disminución de la complejidad y aplicación pertinente en las organizaciones de los marcos de referencia, considerando las necesidades asociadas al monitoreo y control de las infraestructuras TI para tener un control holístico de las mismas mediante la automatización eficaz de políticas TI que se diseñen como resultado de la integración de marcos de referencia, y para corroborar la reducción de la complejidad y el incremento del alineamiento a través de la evaluación de impacto, se desarrolló el Modelo para la Gestión de Infraestructuras TI (MGITI). Su esquema general se muestra en la Fig. 2.

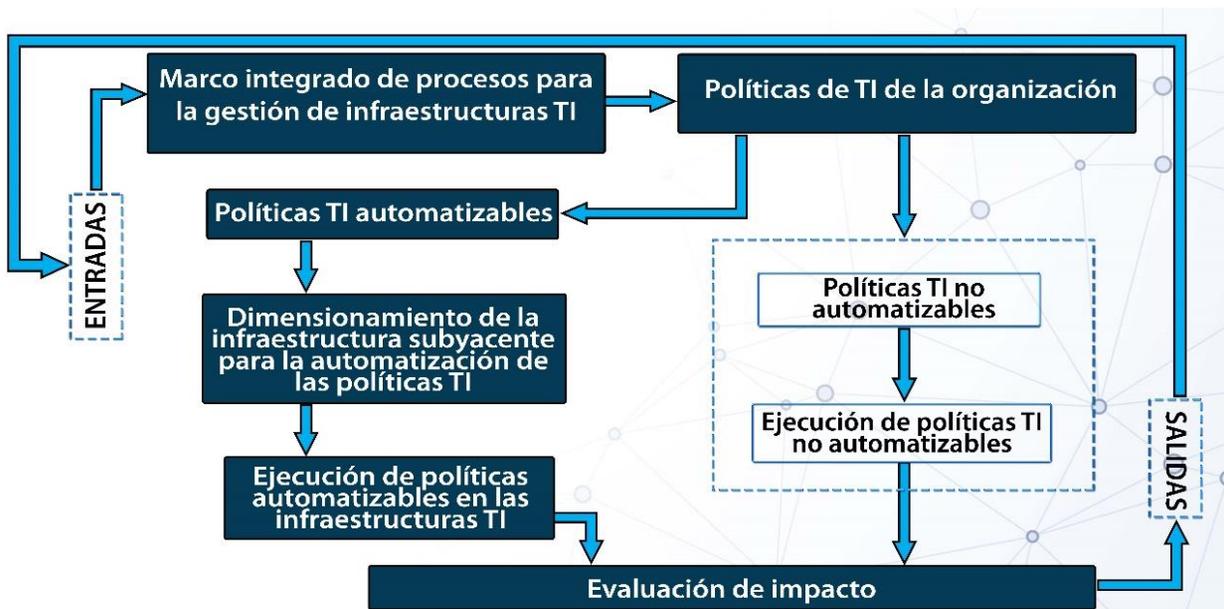


Fig. 2. Modelo para la Gestión de Infraestructuras TI. Fuente: elaboración propia.

El MGITI parte de la obtención de un marco integrado para la gestión de infraestructuras TI, el cual, unido a las políticas, estrategias y sistema organizativo establecidos por la organización, facilita el diseño de políticas de TI contextualizadas a las necesidades de las organizaciones. Estas políticas de TI se dividen en automatizables y no automatizables, en función de lo cual diseña y dimensiona la infraestructura necesaria para la automatización de la ejecución de políticas de TI. Las políticas de TI automatizables se ejecutan sobre las infraestructuras TI. Finalmente se evalúa el impacto del MGITI para la organización.

Durante la investigación realizada para el desarrollo del MGITI, se identificaron un conjunto de premisas consideradas necesarias para la aplicación exitosa de dicho modelo. Estas premisas se obtuvieron del análisis de los factores críticos establecidos por consenso en el uso de las infraestructuras TI en las organizaciones [47]; y los factores de fracaso en la implementación de marcos de referencia. Ellas son:

-La alta gerencia de las organizaciones debe conducir el empleo innovador de las

infraestructuras TI para soportar sus procesos, incrementar la eficiencia y generar nuevas formas de negocio.

-El personal que opera las TI debe estar familiarizado con los objetivos de la organización y estar calificado tanto para operar la tecnología instalada como para apoyar los procesos que se desarrollan en la organización.

-La infraestructura TI debe ser al menos la necesaria para ofrecer los niveles de servicio que necesita la organización.

-La organización debe incentivar la adopción de marcos de referencia tanto para la realización de sus procesos TI como para el gobierno y la gestión de las infraestructuras TI.

Seguidamente, se hace referencia a cada uno de los componentes del MGITI.

3.1 Marco integrado de procesos

Para la obtención del marco integrado de procesos contextualizados a la organización, primera componente del MGITI, útil para la gestión de la infraestructura TI, se propone el procedimiento que se muestra en la Fig. 3.

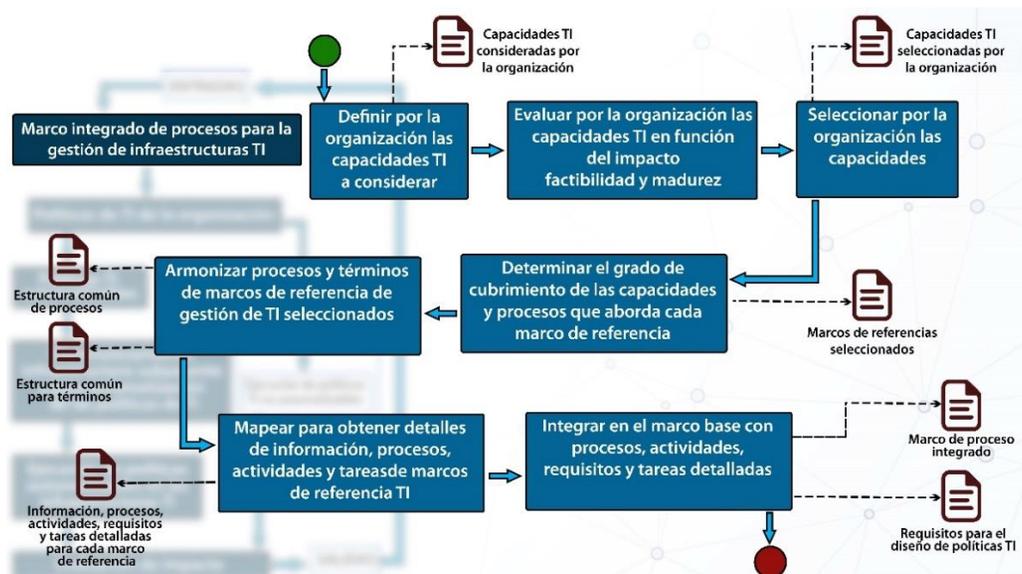


Fig. 3. Procedimiento para la obtención del marco integrado de procesos para la gestión de infraestructuras TI

Fuente: elaboración propia.

Como se puede apreciar en la Fig. 3, la obtención del marco integrado de procesos parte de la definición de las capacidades TI.

Se plantea en este que estas capacidades se obtienen a partir del análisis y síntesis de los catalizadores y factores críticos de éxito propuestos por COBIT v5, de las capacidades y recursos propuestos por ITIL v3, y de tener en cuenta los principales problemas en la adopción de marcos de referencia para la gestión de TI [22]. Se propone que algunas de las capacidades TI a considerar por una organización sean:

-Desarrollo tecnológico: tiene en cuenta el desarrollo del hardware y de las aplicaciones y de los servicios de TI en función de generar valor para la organización

-Sistema organizativo: incluye principios y políticas, estructura, relaciones y mecanismos de comunicación, así como flujos de información.

-Capacidad económica: considera los gastos de inversiones CAPEX (por las siglas en inglés de CAPital EXpenditures) y los gastos de operación OPEX (por las siglas en inglés de OPERating EXpense) para garantizar, entre otras cosas, la inversión y renovación tecnológica, el mantenimiento, escalamiento y operación de la infraestructura.

-Adopción de buenas prácticas y estándares en sus procesos y procedimientos de trabajo: facilita la formulación de políticas y procesos, así como el ordenamiento de los recursos humanos, el diseño de los flujos de información y la operación de los servicios, infraestructuras y aplicaciones. Contribuye al ordenamiento de las tareas de gestión y a la mitigación de riesgos asociados al empleo de las infraestructuras TI.

-Recursos humanos: con sus conocimientos contribuirán a potenciar la innovación y generar nuevos valores al negocio desde las TI. Estos podrán diseñar procesos más eficientes que reducirán la brecha temporal entre el momento que se

realiza la inversión en TI y que dicha impacte positivamente en la organización.

-Nivel de automatización de tareas de gestión de las TI: facilitan el monitoreo automatizado de parámetros de rendimiento de las infraestructuras TI, lo cual reduce el OPEX; el cumplimiento de los acuerdos de nivel de servicio (SLA por las siglas en inglés Service Level Agreement) pactados con otras áreas de la organización y la controlabilidad de la infraestructura TI.

Para la valoración de las capacidades a considerar por la organización, se recomienda que en las organizaciones se cree un comité de expertos que evalúe cada capacidad en función de tres criterios:

-Impacto: se refiere al efecto que tiene la capacidad en la organización.

-Factibilidad: considera si la organización cuenta con los conocimientos, recursos y autorizaciones para utilizar la capacidad evaluada.

-Madurez: tiene en cuenta el nivel de desarrollo de la capacidad en la organización.

Como los criterios a partir de los cuales se van a evaluar las capacidades son de tipo cualitativo, debe emplearse una escala ordinal, y para ello se propone la escala de Likert, que codifica de forma ordenada los valores de uno a cinco, donde cinco corresponde al valor máximo [48].

Se recomienda que, en la medida que los expertos evalúan las capacidades, se conformen tres matrices: I (impacto), F (factibilidad) y M (madurez) (ver las matrices representadas en (1), (2) y (3)), en las cuales se almacenen los valores asignados a las capacidades seleccionadas por cada experto. En dichas matrices, las filas (e) se corresponden con las capacidades a evaluar, y las columnas (j), con los expertos incorporados en las mismas. Cada elemento $I_{ej} \in I$, $I=(i_{ej})$ e (i_{ej}) corresponde con las evaluaciones asignadas por el experto a cada capacidad, evaluando el criterio impacto, (i_{ej}) ; $j=\overline{1,m}$;

$e=\overline{1,p}:m,p \in \aleph$ (ver (1)). Cada elemento $F_{ej} \in F$, $F=(f_{ej})$ y f_{ej} corresponde con las evaluaciones asignadas por el experto a cada capacidad, evaluando el criterio factibilidad (ver (2)); y cada elemento $m_{ej} \in M$, $M=(m_{ej})$ y m_{ej} corresponde con las evaluaciones asignadas por el experto a cada capacidad, evaluando el criterio madurez (véanse expresiones (1,2,3)).

$$I = \begin{bmatrix} i_{11} & \cdots & i_{1m} \\ \vdots & \ddots & \vdots \\ i_{p1} & \cdots & i_{pm} \end{bmatrix} \quad (1)$$

$$F = \begin{bmatrix} f_{11} & \cdots & f_{1m} \\ \vdots & \ddots & \vdots \\ f_{p1} & \cdots & f_{pm} \end{bmatrix} \quad (2)$$

$$M = \begin{bmatrix} m_{11} & \cdots & m_{1m} \\ \vdots & \ddots & \vdots \\ m_{p1} & \cdots & m_{pm} \end{bmatrix} \quad (3)$$

Dado que todas las capacidades analizadas están interrelacionadas, no se debe interpretar el resultado de estas por separado. Considerando que la dependencia entre las capacidades que se analizan varía de una organización a otra, en cada organización debe calcularse el coeficiente de correlación de Spearman, y evaluar que se encuentre por encima de 0,6 con el fin de validar la hipótesis de dependencia [49]. En caso de cumplirse lo anterior, se propone utilizar un método de análisis multivariado para la selección de las capacidades críticas a partir de la matriz obtenida. Específicamente, se plantea emplear el método de análisis de componentes principales, el cual permite reducir el número de variables y eliminar la varianza no compartida y la hecha por error, esta última asociada a sesgos en la toma de datos que podrían aparecer por cansancio de los expertos o por heterogeneidad en sus intereses [50].

Teniendo en cuenta que la cantidad de especialistas a consultar en cada organización no será grande (mayor de 200), se propone el empleo del método de Factorización de Ejes Principales para identificar las capacidades más significativas dentro de estas [51]. Con lo anterior, se obtienen las capacidades significativas con relación al impacto, la factibilidad y la madurez.

Seguidamente, a partir de las capacidades más significativas en cada organización, se preseleccionan los marcos de referencia para la gestión de infraestructuras TI a emplear, considerando los procesos que cubren los ámbitos y tipos de uso [52]. Debe realizarse un análisis a partir de la definición de procesos o tareas en cada marco de referencia de las capacidades por cada uno de los marcos de referencia preseleccionados, eligiendo aquellos que abordan con mayor nivel de profundidad las capacidades que deben institucionalizarse a partir de la asimilación de buenas prácticas para cada organización. Entre estos están los que tendrán mayor impacto, los que son más factibles de cambiar y los que tienen menor nivel de madurez. Además, debe seleccionarse un marco base para la integración, que debe ser el que trate la mayor cantidad de procesos que faciliten en control de las capacidades más significativas.

Una vez seleccionados los marcos de referencia a integrar y el marco base, se aplica el método propuesto por Calvache [53] para armonizar los mismos. Este proceder permite determinar los puntos en común tanto en los procesos que abordan, como en los términos que utilizan, eliminando las ambigüedades. De esta forma, el proceso de armonización permite obtener los procesos y términos comunes con diferentes marcos de referencia, así como la manera en que se abordan cada uno de los conceptos que se trabajan en los diferentes marcos de referencia

seleccionados. Se debe hacer y conservar una correspondencia entre los modelos iniciales y el armonizado, de manera que puedan asimilarse nuevos modelos o considerarse extensiones en los modelos empleados.

A continuación, se lleva a cabo un mapeo entre la información, procesos, actividades y tareas que abarca cada marco de referencia seleccionado a partir de la armonización, lo que permitirá determinar cuáles de estos aspectos se abordan con mayor nivel de detalle.

Finalmente, sobre un marco base seleccionado previo a la etapa de armonización se integran la información, procesos, actividades y tareas detallados como resultado del mapeo. Esto permite un mayor nivel de especificación de los elementos antes precisados, obteniéndose el marco integrado de procesos para la gestión de infraestructuras TI contextualizado a la organización. De la información, procesos, actividades y tareas que integran el marco integrado, se obtienen los requisitos para realizar el diseño de políticas de TI tal y como se detalla en el componente siguiente.

3.2 Componente de diseño de las políticas de TI de la organización

Para hacer el diseño de políticas de TI, se deben establecer los requisitos para las mismas a partir del marco integrado de procesos primeramente obtenido para la organización. Pudieran existir antecedentes de políticas de TI en la organización, en ese caso se debe realizar la verificación de la satisfacción de los requisitos definidos por las políticas existentes. En caso de no existir políticas de TI en la organización, es necesario realizar el diseño de estas.

Primeramente se deben definir las políticas de TI asociadas a los escenarios de despliegue de los servicios que ofrece la organización, considerando las buenas

prácticas [54]-[56], para el funcionamiento adecuado de los mismos.

Para el adecuado diseño de políticas TI se propone la confección de una lista de chequeo que contenga, por ejemplo: la infraestructura TI crítica para la organización, el nivel de preparación de los recursos humanos que interactúan con las infraestructuras TI, los elementos de configuración de cada servicio, así como de la infraestructura subyacente que lo soporta, la lista de alertas que se consideren y las respuestas ante las mismas, las principales métricas de rendimiento asociadas al cumplimiento de los SLA, las tareas comunes de gestión: salvadas, gestión de fallas, gestión de cambios, aprovisionamiento de servicios, creación y borrado de usuarios, así como los requisitos de calidad, asociados al negocio: sus estrategias y metas junto a las principales restricciones asociadas a los servicios, entre otros.

Para el diseño de políticas de TI, en este trabajo se plantea extrapolar los métodos de diseño basados en arquitecturas, específicamente, el método de diseño de arquitectura de software (ABD por las siglas en inglés de Architecture Based Design), aprovechando sus posibilidades para: trabajar de manera integrada la combinación de requerimientos de negocio, calidad y funcionales; garantizar completitud del sistema desde su diseño; facilitar la reutilización de conocimientos; permitir la representación de incumbencias transversales de determinados parámetros a través de la orientación a aspectos; y permitir mostrar patrones de interacción y responsabilidades.

Siguiendo con los pasos establecidos en el método ABD [57], [58], se propone realizar un proceso recursivo de descomposición de requisitos para el diseño de políticas. En cada paso de descomposición de los requisitos deben asignarse los niveles de responsabilidad, de autoridad y prever los recursos que sean

necesarios. Para cada requisito de calidad o asociado a las necesidades de la organización, deben asociarse las políticas de TI que le darán cumplimiento. Cada uno de estos requisitos deben pasar por una revisión de despliegue, de concurrencia y de lógica de funcionamiento. En la revisión de despliegue, se evaluará el lugar en que se ejecutarán las políticas, lo que permitirá segmentar el ámbito de las políticas en diferentes dominios de aplicación, según las necesidades de la organización, que podrían ser de hardware, software, aplicaciones, servicios, datos o personas.

En la de concurrencia se evalúa si el cumplimiento de la política de TI depende de otras políticas, por ejemplo, si el cumplimiento de las políticas asociadas al funcionamiento de un servicio depende del cumplimiento de las políticas de TI asociadas a la infraestructura subyacente de este. La revisión de la lógica de funcionamiento permitirá establecer relaciones de precedencia o de sucesión entre las políticas de TI diseñadas.

Además, para la descomposición de requisitos, es necesario considerar estratos, proponiéndose, para este caso, los niveles de negocio, sistema e instancia/dispositivo.

Realizar en cada uno de estos niveles la descomposición de requisitos permitirá la obtención de políticas de manera estratificada. Primeramente, se obtendrán las políticas a nivel de negocio, a continuación, se determinarán las políticas de sistema que se necesitan para cumplir con las anterior mencionadas. Finalmente, se diseñarán las políticas que se deben configurar a nivel de dispositivo/instancia con el mismo objetivo.

Como resultado de la aplicación del método ABD deben quedar documentadas un conjunto de vistas de las políticas: vista lógica, que debe incluir los roles y responsabilidades, tanto las funcionales como las asociadas a la calidad; vista de concurrencia o proceso, donde se documentan los flujos asociados a la ejecución de políticas, incluyendo los

mensajes que se transmiten y reciben, facilitando la identificación de las políticas que se ejecutan de manera concurrente; vista de despliegue, que incluye la infraestructura subyacente para el despliegue; y por último, la vista de implementación, en la que se detallan los casos de uso para la captura de los requisitos funcionales y los escenarios para los requisitos de calidad.

Adicionalmente, empleando el método ABD, es posible definir plantillas de políticas. Estas plantillas pueden reutilizarse para diferentes políticas y facilitan la solución de conflictos entre ellas. Se recomienda definir plantillas de políticas para: la atención a alarmas; la respuesta ante fallos; la configuración de servicios, elementos de software, de hardware o de red; la actualización, ya sea de sistemas operativos, de antivirus o de aplicaciones, y el monitoreo. En todas las plantillas de políticas deben incorporarse elementos de entrada/salida de datos que faciliten su empleo.

El empleo ABD permite agrupar las políticas de diferentes maneras: según la periodicidad, según los dominios a los que se aplican, asociadas a los atributos de calidad a los que responden, entre otras.

Los expertos a cargo de la aplicación del método ABD en las organizaciones podrán establecer el orden de acuerdo con los aspectos que decidan.

Una vez diseñadas las políticas estratificadas, se procede a identificar conflictos entre las mismas a través del método *Policy continuum* [59].

Finalmente, para la validación de las políticas diseñadas, se procede a la construcción del árbol de utilidad de estas, empleando el método ATAM, lo que permite verificar el cumplimiento de los atributos de calidad definidos. ATAM brinda una caracterización para varios atributos creada a partir del conocimiento existente en las comunidades de atributos de calidad, como rendimiento, capacidad de

ser modificable, disponibilidad, usabilidad y seguridad [60], [61].

El árbol de utilidad contiene escenarios que constan de mecanismos de arriba abajo para verificar el cumplimiento de las políticas diseñadas mediante reglas operacionales. Para la elaboración de los escenarios, se utilizan o los requisitos a partir de los cuales se diseñan las políticas de TI, o directamente las políticas de TI.

En cada escenario, se evalúa la interacción entre las políticas de TI diseñadas para identificar de manera temprana riesgos y puntos sensibles. En los escenarios modelados para cada una de las políticas de TI se determinan: estímulo externo, decisión arquitectónica y respuesta (tríada de evento-condición-acción).

Seguidamente, se realiza la priorización de cada escenario con base en dos dimensiones: importancia y grado de dificultad para ser realizado [60].

En función de esta valoración, se determina automatizar o no las políticas.

Las políticas de TI no son automatizables cuando este proceso resulta muy complejo y tiene poca importancia. Estas políticas de TI no automatizables se deben implementar de manera manual, lo que no es objeto de esta investigación.

3.3 Componente dimensionamiento de infraestructuras para automatización de políticas de TI

Para garantizar la automatización de la ejecución de políticas de TI, es necesario confirmar que se cuenta con la infraestructura necesaria, algo planteado en una de las premisas del MGITI, y contar con recursos de hardware y de conectividad adicionales en la infraestructura subyacente, para garantizar los parámetros de calidad de servicio definidos.

Se considera que la infraestructura subyacente para alcanzar los niveles de calidad de servicio deseados (I_{exp}) depende

de la infraestructura mínima necesaria para alcanzar los atributos de funcionamiento de la red (I_{FN}) y de la infraestructura necesaria para conseguir el nivel de confianza que se planifica en la red (I_{NC}).

Para determinar la infraestructura necesaria para tener un nivel de confianza en la red, debe modelarse la infraestructura subyacente capaz de enfrentar deficiencias temporales o permanentes en el funcionamiento de los servicios, así como la reconfiguración de estos. Resulta una buena práctica [62], [63] segmentar la función estadística $u(i,t)$ en períodos de tiempo T y comparar los resultados de la función estadística con predictores basados en datos históricos de funcionamiento seleccionando la función que más se adecúe a cada intervalo de tiempo. Es posible obtener tantas funciones $u(i,t)$ como intervalos estadísticos se tomen. De esta manera, para cada intervalo $[x, x+T]$ y cada máquina virtual soportando un servicio sobre un servidor físico, o para cada servicio soportado sobre una máquina física (i) se tiene para obtener I_{NC} las expresiones (4) y (5):

$$I_{FN} = \sum_{t=y}^{y+T} \sum_{i=1}^n u(i,t) \quad (4)$$

$$u(i,t) \rightarrow \bar{u}(i,t) + \check{u}(i,t) + e(i,t) \quad (5)$$

El cálculo de esta infraestructura subyacente está determinado por parámetros como, por ejemplo, la disponibilidad, seguridad y confiabilidad de los servicios establecidas en los acuerdos de nivel de servicio, cuya variación en el tiempo se modela a través de la función $u(i,t)$ descompuesta en (5).

En esta función, $\bar{u}(i,t)$ representa la tendencia de funcionamiento de los servicios y modela el comportamiento de un sistema, cuyos parámetros de

funcionamiento varían en el tiempo, dentro de umbrales establecidos en el régimen sin averías. Por su parte, $\tilde{u}(i,t)$, representa irregularidades con respecto a la tendencia de funcionamiento de los servicios y $e(i,t)$ representa errores o incertidumbre en el funcionamiento de estos. Todo esto se emplea para determinar la infraestructura necesaria para un nivel de confianza de la red [62], [64].

Para el cálculo de la infraestructura necesaria para alcanzar un nivel de confianza en la red (I_{NC}) es necesario realizar un mapeo de parámetros de calidad de servicio a métricas de rendimiento de las redes. Para ello se emplea una matriz de diseño MD_{ij} que considera la infraestructura necesaria para garantizar determinados requisitos funcionales [62], [64]. Dicha matriz se construye a partir del análisis histórico de los parámetros de rendimiento de la infraestructura subyacente, lo que permite la obtención de grupo de parámetros de diseño PDi para cada servicio (i) que utiliza cada cliente (j) bajo las restricciones que definen los requisitos funcionales para cada cliente (RF_j) [64]. A partir de los parámetros anteriores se determina la infraestructura necesaria para un nivel de confianza de la red I_{NC} (ver (6)), tal que $j = \overline{1,m}; i = \overline{1,p}; m, p \in \mathbb{N}$.

De esta forma es posible obtener la infraestructura requerida para alcanzar los niveles de calidad de servicio deseados I_{exp} (ver (7)).

$$I_{NC} = \sum_{i=1}^n MD_{ij} \delta PD_i \quad (6)$$

$$I_{exp} = I_{NC} \cup I_{FN} \quad (7)$$

Una vez obtenida la infraestructura subyacente necesaria para la prestación de servicios con los niveles de calidad diseñados (I_{exp}), es necesario, para automatizar la ejecución de políticas,

desplegar una infraestructura adicional que se ha denominado Infraestructura para la Automatización de Políticas (I_{AP}).

Esta infraestructura adicional se determina considerando los elementos necesarios para la automatización de políticas en una arquitectura PBNM, de ahí que se requiera determinar la infraestructura necesaria en los Puntos de Decisión de Políticas (I_{PDP}) y en los Puntos de Ejecución de Políticas (I_{PEP}).

Para I_{PEP} , se parte de evaluar las posibilidades de ejecución de políticas en estos, lo cual considera su capacidad para soportar los agentes y su nivel de autonomía. Adicionalmente, es preciso conocer la cantidad de PDP que se necesitan, pues algunos de estos pueden ser legados. Para el cálculo de I_{PDP} , debe considerarse la demanda de procesamiento que estos tendrán. En el caso de trabajar de manera autónoma, la demanda de procesamiento dependerá del mecanismo que se implemente para la toma de decisiones.

Es importante tener en cuenta que la planificación y organización de políticas debe realizarse, no solamente para establecer prioridades entre estas, sino, además, para implementar los PDP en el lugar óptimo de la infraestructura gestionada. En este sentido surge una relación de compromiso, pues mientras más PDP se desplieguen en la red, más se dispersa la toma de decisiones y se hace más certera la ejecución de políticas a bajo nivel, pero la evaluación del impacto de las políticas ejecutadas será más compleja, al igual que la detección de conflictos entre estas. Una práctica bastante extendida [65]-[67] es la definición de PDP según sus funciones: seguridad, calidad de servicios, etc., creando subsistemas de aplicación de políticas, los cuales se pueden segmentar basados en criterios funcionales y no funcionales.

También, para determinar la infraestructura necesaria para automatizar la ejecución de políticas, debe

considerarse la infraestructura que se requiere en el repositorio de políticas (I_{RP}), el cual depende de la capacidad de almacenamiento del gestor y la estructura de la base de datos que se utilizará para el almacenamiento de políticas y del modelo de información que se utilice para la representación de políticas.

Finalmente, el despliegue de la arquitectura de gestión basada en políticas implica el consumo de ancho de banda para el envío de políticas y para la verificación del funcionamiento de los elementos gestionados (BW_{PBNM}). A partir de lo anterior, se recoge en (8) cómo obtener la infraestructura necesaria para la automatización de políticas (I_{AP}).

$$I_{AP} = I_{PDPP} \cup I_{PDP} \cup I_{PEP} \cup I_{RP} \cup I_{CMDB} \cup BW_{PBNM} \quad (8)$$

3.4 Componente ejecución de políticas automatizables en las infraestructuras TI

Para la ejecución de políticas automatizadas en las infraestructuras TI, estableciendo un enlace entre la configuración de los elementos de la red y las necesidades de la organización, y permitiendo la detección y corrección de conflictos entre las políticas definidas, se propone una modificación a la arquitectura PBNM definida por la IETF, la cual se muestra en la Fig. 4.

Dicha modificación consiste en incorporar un Punto de Decisión de Políticas Principal (PDPP), el cual tiene una jerarquía superior y puede detectar y resolver conflictos entre políticas, según lo explicado en el componente diseño de políticas, forzando a los PDP a regresar a los PEP a un estado anterior, en el caso de que se manifieste una condición prevista, por ejemplo, la ocurrencia de un conflicto entre las políticas que se ejecutan en las capas jerárquicas inferiores.

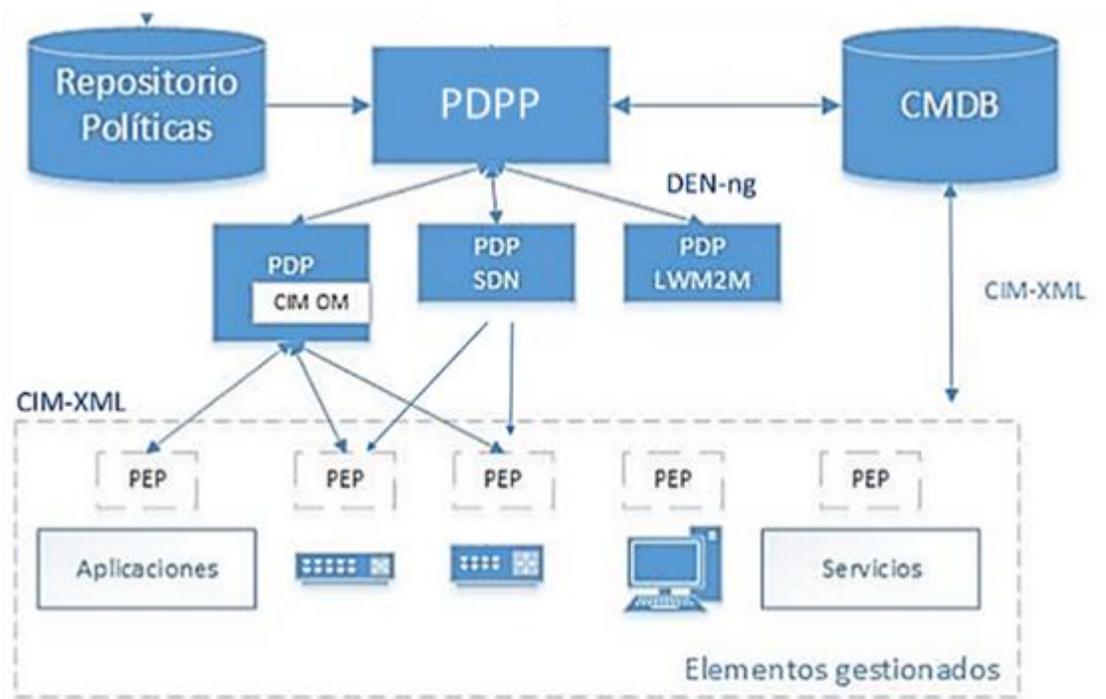


Fig. 4. Propuesta de modificación a la PBNM. Fuente: elaboración propia.

Además, el empleo de dos modelos de información, uno a alto nivel y otro a bajo nivel. Como modelo de información para la ejecución de políticas a alto nivel se propone DEN-ng en su versión 7 o superior, entre el PDPP y el PDP dada su capacidad para representar políticas empleando la triada evento-condición-acción que permite: identificar y resolver conflictos entre las políticas, trabajar con máquina de estado finito y abordar los contextos a partir de su expresividad semántica y conceder al sistema la posibilidad de determinar cuándo serán evaluadas las condiciones.

Este último elemento le otorga la misma capacidad de respuesta temprana, ya que no es necesario que las condiciones sean visibles para que se ejecuten las acciones.

Asimismo, hacer esto, garantiza mayor eficiencia en el funcionamiento de la arquitectura porque es posible definir eventos a partir de los cuales se evaluarán las condiciones, lo que implica no tener que invertir recursos computacionales y de ancho de banda adicionales para la evaluación periódica de las condiciones.

Para la ejecución de políticas a bajo nivel, se propone el empleo de CIM de la Fuerza de Tarea para la Gestión Distribuida (DMTF por las siglas en inglés de Distributed Management Task Force) como modelo de información entre los PDP y los PEP, el cual abarca gran cantidad de escenarios de gestión, y tipos de infraestructuras de redes y servicios. CIM permite la operación de la arquitectura tanto en soluciones de gestión integrada como propietaria, ya que es capaz de representar, con mayor integralidad, los diferentes ámbitos de gestión. Su gestor de objetos, CIMOM, se ha extendido hasta comprender los más importantes modelos de gestión estandarizados, así como modelos propietarios, y se han desarrollado extensiones para las nuevas tecnologías a gestionar, por ejemplo: las Redes Definidas por Software (SDN por las siglas en inglés de Software Defined Network), la Virtualización de las Funciones de Red (NFV

por las siglas en inglés de Network Functions Virtualization) y la nube [38], [68]. Se puede afirmar que, en general, todos los elementos que forman parte de la infraestructura de redes y servicios a gestionar soportan implementaciones de CIM. Debido a que, la mayor parte de los sistemas que implementa PBNM trabajan a bajo nivel, ejecutando políticas sobre los elementos gestionados, es preciso establecer un enlace entre la configuración de estos elementos y las necesidades de la organización.

También se incorpora a la arquitectura propuesta por el IETF, una base de datos de configuración (CMDB por las siglas en inglés de Configuration Management Database) donde se registran los atributos de cada instancia de configuración (CI, por las siglas en inglés de Configuration Instance) durante su ciclo de vida, las relaciones que la misma posee con otras instancias y los registros vinculados a cada una, por ejemplo, registros de incidentes, problemas o cambios. La CMDB se emplea para la evaluación de condiciones y registro de las modificaciones que se ejecuten como resultado de la ejecución de políticas en los PEP.

Para ejecutar las acciones de gestión se utiliza el PDP, especializado en tomar las decisiones de cuáles políticas se deben ejecutar y del procesamiento de las mismas, alineando de esta forma las necesidades del negocio con el comportamiento coherente de la infraestructura TI. Para este fin, el PDP transforma las políticas o reglas en representaciones operacionales aptas para ser interpretadas por PEP que se encuentran en los elementos gestionados.

Para ello, el PDP debe contar con un motor de inferencia y se basa, para la toma de decisiones, en la información contenida en la CMDB y en el Repositorio de Políticas [68].

Según recomienda el IETF, en el PDP debe existir una aplicación de gestión basada en políticas preferiblemente con interfaz web para el monitoreo y control de

los elementos que forman parte de la infraestructura que ejecuta las políticas.

Dicha aplicación debe permitir modelar las políticas que controlarán el sistema y verificar la no existencia de conflictos entre las políticas existentes, lo que se debe hacer en cada uno de los estratos. Las nuevas políticas de TI que no presentan conflictos con las precedentes se almacenan en el repositorio de políticas, el cual constituye una base de datos donde se registran todas las políticas a ejecutar.

En el PDPP ocurre el proceso de toma de decisiones de las políticas representadas con la triada evento-condición-acción.

La condición puede contener un conjunto de cláusulas que darán como resultado una condición simple, a partir de la cual puede evaluarse si esta se satisface consultando la CMDB. En el caso de que esté previsto que se ejecuten varias acciones, se establecerá el nivel de prioridad en función de la estrategia de ejecución de las mismas, que se define en el PDPP.

3.4 Componente estrategia de evaluación de impacto

El impacto de las TI en las organizaciones para incrementar la rentabilidad empresarial, elevar la productividad, mejorar los procesos que conducen a la elevación del desempeño organizacional y de los servicios, ha sido ampliamente tratado.

En función de la evaluación del impacto del MGITI en las organizaciones, en este trabajo se propone un conjunto de medidas agrupadas en las alineaciones establecidas en el Modelo de Alineación Estratégica SAM (por las siglas en inglés de Strategic Alignment Model) propuesto por [69], que consideran la alineación estratégica y estructural, a las que se incorpora posteriormente la alineación social.

Dentro de la alineación estratégica, se proponen en este trabajo, como medidas; la cantidad de requisitos de la organización; el nivel de formalización de procesos TI en la

organización, lo que se considera en el componente uno del modelo mediante la obtención del marco integrado de procesos para la gestión de TI contextualizado a las necesidades de cada organización; y la implementación de estándares que se encuentran tanto en el marco integrado como en el empleo de modelos de información y en la arquitectura PBNM modificada para la ejecución de políticas de TI automatizables en la infraestructura.

Para garantizar la alineación estructural, se propone el establecimiento de acuerdos de nivel de servicio entre el área de TI y otras áreas de procesos de la organización. Para realizar esto, se debe definir un conjunto de indicadores de calidad de servicio.

En la evaluación de la alineación social, se consideraron la calidad de comunicación, lenguaje común, entendimiento compartido y conocimiento de dominio compartido, y se agrega el nivel del compromiso de los usuarios de la TI [70]. Este aspecto se implementa a través de la asignación de responsabilidades para diseño de políticas en el proceso de estratificación de políticas; la formulación de políticas de TI a partir de requisitos de la organización y que contribuyen a la sistematización de conocimiento en políticas de TI automatizables y no automatizables.

La definición de políticas a nivel de negocio permite el entendimiento de estas por parte de la junta directiva de la organización. El establecimiento de SLA entre el área de TI y las diferentes áreas de procesos de la organización proporcionan un lenguaje común de comunicación entre estas.

Además, la formalización de políticas a nivel de negocio, de sistema y de instancia, permite la reutilización de las políticas de TI diseñadas en diferentes organizaciones compartiendo el repositorio de políticas; y el empleo CIM, como modelo de información entre los PDP y los PEP facilita que los administradores de TI solamente deban dominar los estándares del DMTF,

independientemente del proveedor de tecnología, lo cual impacta en la reducción del costo total de la propiedad en las organizaciones.

4. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

MGITI, se aplicó el mismo para el despliegue de la Plataforma Integral de Telecomunicaciones Unificadas, PLATEL 3.0.

Según establece el MGITI, para identificar las necesidades de cada una de las organizaciones en las que se realiza el despliegue, se indicó el empleo de marcos de referencia para el establecimiento de SLA en los clientes con el objetivo de alinear la implementación de la solución de comunicaciones unificadas que se comercializa a las necesidades de las organizaciones clientes, considerando sus capacidades.

De la integración de los diferentes marcos de referencia que incorporan metodologías para la aplicación de SLA en las organizaciones: COBIT 5, ITIL v3 y eTOM, se obtienen los procesos y métricas a

considerar, estas se deben alinear a las necesidades de las organizaciones a partir de las cinco fases que integran el ciclo de vida de los SLA y las siete funciones: diseño, negociación, aprovisionamiento, ejecución, monitoreo, evaluación y reporte.

Las funciones de monitoreo y de reporte del cumplimiento de los SLA permiten la verificación de las MRRS y la evaluación de impacto con la emisión de informes que reporten el cumplimiento de dichos SLA.

Como resultado del marco integrado para la gestión de los SLA para los servicios de comunicaciones unificadas que las empresas pueden extender para la gestión de sus infraestructuras TI de acuerdo con el desarrollo de sus capacidades, se obtienen las relaciones entre procesos, variables de control y requisitos que se muestra en la Tabla 1.

A partir de los requisitos obtenidos se diseñaron, empleando ABD, las políticas para la configuración de la plataforma en las diferentes organizaciones. Además, se obtuvieron un conjunto de políticas TI a través de la ampliación de los atributos en requisitos de calidad abstractos.

Tabla 1. Relación entre los procesos y los atributos de calidad para la implementación de PLATEL 3.0
Fuente: elaboración propia.

Procesos	Métricas	Atributo
Gestión de incidentes, problemas y fallas.	Tiempo entre pérdidas y remplazos de servicios.	Seguridad, disponibilidad
Gestión de configuración.	Tiempo para agregar un elemento de configuración en la CMDB.	Modificabilidad
Gestión de nivel de servicio.	Número de SLA. Violaciones a los SLA.	Rendimiento
Gestión de capacidad	MRRS	Rendimiento
Gestión de disponibilidad	Parámetros de QoS	Disponibilidad

El dimensionamiento de la infraestructura para la automatización de la ejecución de políticas y para lograr un nivel de servicio permitió la obtención de configuraciones prediseñadas para el despliegue de la arquitectura en función de las necesidades de las organizaciones. Para identificar cuál es la configuración que requiere cada organización, durante la fase de negociación se elicitaban requisitos funcionales como: cantidad de usuarios, cantidad de usuarios concurrentes, cantidad de servicios por usuarios y total de servicios, sistemas y aplicaciones de comunicaciones que abarca. Además, se determina si el despliegue de la arquitectura se realizará de forma centralizada o distribuida.

Para ejecutar las políticas que se diseñan, se incorporó a la arquitectura PLATEL 3.0 un subsistema de gestión. Este subsistema tiene la misión de llevar a cabo los dos modos de actuación de la gestión de red, o sea, monitorizar y controlar todos los elementos que conforman la plataforma de comunicaciones unificadas, esto de acuerdo con las políticas diseñadas. El mismo, presenta una arquitectura de PBNM empleando como base WEBM (PBNM-WEBM), proporcionando de esta forma una gestión integral de la red de comunicaciones unificadas. El empleo de CIM como modelo de información para la comunicación entre el PDP y los PEP resuelve el problema de la heterogeneidad de los elementos gestionados y reduce la complejidad en la operación del sistema. Además, se normalizó el modelo para enviar a los clientes reportes del cumplimiento de los SLA con el fin de lograr un mayor entendimiento por parte de estos.

Para automatizar las políticas diseñadas, se desplegó la arquitectura PBNM-WEBM para el monitoreo y control de la infraestructura que soporta el servicio de voz sobre IP (VoIP). Para garantizar el funcionamiento de dicho servicio, se monitoriza el porcentaje de usabilidad de la RAM, la CPU y del disco duro; el tráfico en

las tarjetas de red en el servidor, así como los principales parámetros de QoS para la VoIP [71]: la pérdida de paquetes, el jitter, la latencia, el estado de las extensiones, así como la cantidad de llamadas concurrentes y fallidas. Para facilitar el proceso de gestión se efectúa un control sobre cada uno de estos parámetros empleando políticas establecidas por el administrador de la red.

Esto tiene como objetivo lograr que los elementos y servicios que hospedan los servidores de telefonía IP tengan un comportamiento autónomo y se dimensionen en función de la demanda.

Además, se generan reportes en los cuales se muestra el comportamiento de los parámetros monitorizados durante un tiempo determinado (el intervalo es configurable).

Como se muestra en [72], para el despliegue del servicio de VoIP gestionado, se montó un servidor de base de datos PostgreSQL 9.4, con sistema operativo GNU/Linux, Nginx 1.4.6 y *framework* Django versión 1.7, se verificó que todos los terminales de VoIP eran gestionables y que los agentes tenían la infraestructura necesaria para su funcionamiento (todos eran PC Pentium 4 o superior con 512 Mb de memoria RAM). Para el punto de decisión de políticas, se determinó que era necesario un servidor con un Microprocesador de 2 núcleos, 4GB de memoria RAM, 250 Gb de memoria en el disco duro y una fuente de 800 W como mínimo para lograr el despliegue de la herramienta Zabbix, la cual tiene capacidad de ejecutar monitorización y control de elementos de hardware [73]; además funciona como PDP y como repositorio de políticas. Este servidor puede ser desplegado sobre máquinas virtuales o máquinas físicas, según se determine en la organización.

La comunicación entre los agentes y el punto de decisión de políticas se implementó a través del protocolo HTTP, verificándose que el ancho de banda disponible era suficiente. Además, los tiempos de sondeo se pudieron configurar

para no atentar con el correcto funcionamiento del servicio en el momento de establecimiento de llamadas.

La automatización de la gestión tuvo un gran impacto por cuanto permitió garantizar los parámetros de calidad de servicio de la organización. Se crearon varias máquinas virtuales configuradas para funcionar como servidores de VoIP.

Se pudo monitorear en el servidor que, si dicho programa sobrepasaba los umbrales de rendimiento definidos, o sea, 60 % de uso de la memoria RAM, 65 % de uso del CPU, más del 70 % de uso de las capacidades de red o más de 80 % de uso de la capacidad de almacenamiento, comenzaría a ser ejecutada como pos condición un script que creaba una máquina virtual para apoyar las peticiones de clientes. En adición, el servidor Zabbix notifica a los administradores del sistema sobre la acción ejecutada. Este proceso resulta transparente para el usuario final y permite que la plataforma PLATEL 3.0 funcione alineada a las necesidades de las organizaciones, a la vez que reduce la complejidad en su gestión.

5. CONCLUSIONES

La gestión de infraestructuras TI con impacto en las organizaciones requiere del empleo de múltiples marcos de referencia de manera integrada, unido a inmediatez y pertinencia en la respuesta, lo cual se consigue a través del diseño y automatización de política de TI. Dichas políticas necesitan de la integración de modelos de gestión, la definición de dominios de gestión y la solución de conflictos entre políticas para ejecutarse en entornos tecnológicos heterogéneos. Todo lo anterior provoca alta complejidad y desalineamiento entre las necesidades de las organizaciones y las TI.

El presente trabajo soluciona el problema científico mencionado mediante el desarrollo de un modelo para la gestión de

infraestructuras TI, que constituye el principal aporte de la investigación realizada, pues contribuye a reducir la complejidad y el desalineamiento de dichas infraestructuras. El modelo desarrollado considera los principales estándares y recomendaciones asociadas a la gestión de infraestructuras TI.

Otros aportes identificados dentro del modelo son: un marco integrado de procesos contextualizado a las necesidades de las organizaciones; el empleo de los métodos ABD y ATAM para la definición de políticas de TI y su estratificación, lo que facilita la alineación estratégica mediante el cumplimiento de requisitos en las organizaciones; modificaciones a la arquitectura de gestión basada en políticas, asociadas a estratificación de la toma de decisiones y a la selección de dos modelos de información que facilitan la integración de modelos de gestión estandarizados y propietarios, así como la solución de conflictos entre políticas; el establecimiento de medidas de evaluación de impacto en lo estratégico, lo estructural y lo social, lo que contribuye a evaluar la incidencia de cada componente del modelo; y el establecimiento de un procedimiento que orienta el empleo del MGITI y precisa los puntos de control sobre el funcionamiento del mismo, contribuyendo a su usabilidad.

6. REFERENCIAS

- [1] M. Bartnes Line, I. Anne Tøndel y M. G. Jaatun, "Current practices and challenges in industrial control organizations regarding information security incident management. Does size matter? Information security incident management in large and small industrial control organizations", *Int. J. Crit. Infrastruct. Prot.*, vol. 12, pp. 12-26, Mar. 2016. <https://doi.org/10.1016/j.ijcip.2015.12.003>
- [2] R. Wijesinghe, H. Scheepers y S. Mcloughlin, "Defining the optimal level of business benefits within IS/IT projects: Insights from benefit identification practices adopted in an IT Service Management (ITSM) project", en *Australasian Conference on Information Systems*, Adelaide, 2015. pp. 1-10. Disponible en: [URL](#)

- [3] P. H. de Souza Bermejo, A. O. Tonelli, A. L. Zambalde, P. A. dos Santos y L. Zuppo, "Evaluating IT Governance Practices and Business and IT Outcomes: A quantitative Exploratory Study in Brazilian Companies", *Procedia Technol.*, vol. 16, pp. 849-857, 2014. <https://doi.org/10.1016/j.protcv.2014.10.035>
- [4] J. Luftman, K. Lyytinen y T. ben Zvi, "Enhancing the measurement of information technology (IT) business alignment and its influence on company performance", *J. Inf. Technol.*, vol. 32, no.1. pp. 26-46, Mar. 2017. <https://doi.org/10.1057/jit.2015.23>
- [5] N. A. A. Bakar, S. Harihodin y N. Kama, "Assessment of Enterprise Architecture Implementation Capability and Priority in Public Sector Agency", *Procedia Comput. Sci.*, vol. 100, pp. 198-206, Oct. 2016. <https://doi.org/10.1016/j.procs.2016.09.141>
- [6] M. O. Alassafi, R. K. Hussain, G. Ghashgari, R. J. Walters y G. B. Wills, "Security in Organisations: Governance, Risks and Vulnerabilities in Moving to the Cloud", en *ES 2015. Lecture notes in computer science*, Springer: Cham, 2017. pp. 241-258. https://doi.org/10.1007/978-3-319-54380-2_11
- [7] L. V. Astakhova, "Evaluation Assurance Levels for Human Resource Security of an Information System", *Procedia Eng.*, vol. 129, pp. 635-639, 2015. <https://doi.org/10.1016/j.proeng.2015.12.083>
- [8] R. Chaparadza *et al.*, "Industry harmonization for Unified Standards on Autonomic Management; Control (AMC) of Networks and Services, SDN and NFV", en *2014 IEEE Globecom Workshops (GC Wkshps)*, Austin, 2014. , pp. 155-160. <https://doi.org/10.1109/GLOCOMW.2014.7063423>
- [9] A. F. Betancur-Pérez, J. J. Granada-Torres, y N. Guerrero-González, "Elastic networks of the future: benefits for the Colombian internal telecommunication network", *TecnoLógicas*, vol. 18, no. 34, pp. 125-136, 2015. <https://doi.org/10.22430/22565337.222>
- [10] T. Coltman, P. Tallon, R. Sharma y M. Queiroz, "Strategic IT alignment: twenty-five years on", *J. Inf. Technol.*, vol. 30, no. 2, pp. 91-100, Feb. 2015. <https://doi.org/10.1057/jit.2014.35>
- [11] J. R. Aranguren y S. R. Rabai, "Determinación del aumento de la productividad en empresas de tecnología al aplicar el Sistema de Gestión de la Calidad TL9000", (Trabajo de grado) Universidad Argentina de la Empresa, Facultad de ingeniería y ciencias exactas, Argentina, 2014. Disponible en: [URL](https://doi.org/10.1057/jit.2014.35)
- [12] J. E. Gerow, J. B. Thatcher y V. Grover, "Six types of IT-business strategic alignment: an investigation of the constructs and their measurement", *Eur. J. Inf. Syst.*, vol. 24, no. 5, pp. 465-491, Dec. 2015. <https://doi.org/10.1057/ejis.2014.6>
- [13] P. Cholda y P. Jaglarz, "Optimization/simulation-based risk mitigation in resilient green communication networks", *J. Netw. Comput. Appl.*, vol. 59, no. C. pp. 134-157, Jan. 2016. <https://doi.org/10.1016/j.jnca.2015.07.009>
- [14] H. Echeverry Díaz y C. P. Milanés Álvarez, "De la aplicabilidad de la gestión del riesgo a la reciente declaratoria de emergencia sanitaria de Bogotá", *Rev. Logos, Cienc. Tecnol.*, vol. 8, no. 2, pp. 132-144, 2017. Disponible en: [URL](https://doi.org/10.1016/j.jiproman.2015.03.016)
- [15] C. Marnewick, "Benefits of information system projects: The tale of two countries", *Int. J. Proj. Manag.*, vol. 34, no. 4, pp. 748-760, May. 2016. <https://doi.org/10.1016/j.jiproman.2015.03.016>
- [16] M. Mora, J. M. Gomez, R. V. O'Connor, M. Raisinghani, and O. Gelman, "An extensive review of IT service design in seven international ITSM processes frameworks: Part I", *Int. J. Inf. Technol. Syst. Approach*, vol. 7, no. 2, pp. 83-107, Oct. 2014. <http://dx.doi.org/10.4018/ijitsa.2014070105>
- [17] M. Mora, J. M. Gomez, R. V. O'Connor, M. Raisinghani, and O. Gelman, "An Extensive Review of IT Service Design in Seven International ITSM Processes Frameworks: Part II", *Int. J. Inf. Technol. Syst. Approach*, vol. 8, no. 1, pp. 69-90, Ene. 2015. <https://doi.org/10.4018/ijitsa.2015010104>
- [18] Y. Bartens, S. de Haes, Y. Lamoén, F. Schulte y S. Voss, "On the Way to a Minimum Baseline in IT Governance: Using Expert Views for Selective Implementation of COBIT 5", en *2015 48th Hawaii International Conference on System Sciences*, Kauai, 2015. <https://doi.org/10.1109/HICSS.2015.543>
- [19] M. D. L. Arévalo, "Implementation of standard international public entities ITIL 2011 infor a new change in the management of IT", *Sistémica*, no. 9, pp. 9-12, Feb. 2014. Disponible en: [URL](https://doi.org/10.1109/HICSS.2015.543)
- [20] J.-L. Baud, *preparación para la certificación ITIL Foundation V3: ITIL V3-2011: más de 400 preguntas-respuestas*. Ediciones ENI, 2015. Disponible en: [URL](https://doi.org/10.1109/HICSS.2015.543)

- [21] M. Panjwani, M. Jantti y J. Sormunen, "IT Service Management from a Perspective of Small and Medium Sized Companies", en *2016 10th International Conference on the Quality of Information and Communications Technology (QUATIC)*, Lisbon, 2016. pp. 210-215.
- [22] K. A. Melendez-Llave y A. E. Dávila-Ramón, "Problemas en la adopción de modelos de gestión de servicios de tecnologías de información. Una revisión sistemática de la literatura", *DYNA*, vol. 85, no. 204, pp. 215-222, Ene. 2018. <https://doi.org/10.15446/dyna.v85n204.57076>
- [23] R. McAdam, U. Bititci y B. Galbraith, "Technology alignment and business strategy: a performance measurement and Dynamic Capability perspective", *Int. J. Prod. Res.*, vol. 55, no. 23, pp. 7168-7186, Jul. 2017. <https://doi.org/10.1080/00207543.2017.1351633>
- [24] H. Ben Laadar, I. Cherti y M. Bahaj, "Alignment of IT Frameworks for Corporate Governance", en *Lecture Notes in Networks and Systems*, vol. 25. Springer: Cham, 2018. pp. 196-207. https://doi.org/10.1007/978-3-319-69137-4_18
- [25] Y. Kryftis, M. Grammatikou, D. Kalogeras y V. Maglaris, "Policy-Based Management for Federation of Virtualized Infrastructures", *J. Netw. Syst. Manag.*, vol. 25, pp. 229-252, Jun. 2017. <https://doi.org/10.1007/s10922-016-9390-z>
- [26] R. S. Moreira, R. S. Morla, L. P. C. Moreira y C. Soares, "A behavioral reflective architecture for managing the integration of personal ubicomp systems: automatic SNMP-based discovery and management of behavior context in smart-spaces", *Pers. Ubiquitous Comput.*, vol. 20, no. 2, pp. 229-243, Abr. 2016. <https://doi.org/10.1007/s00779-016-0901-4>
- [27] J. Jiang, X. L. Xu y N. Cao, "Research on Improved Physical Topology Discovery Based on SNMP", en *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, Guangzhou, 2017. pp. 219-222.
- [28] K. Wac, M. Cummings y J. Dey, "E2eUberIM: end-to-end service management framework for anything-as-a-service", *IEEE Commun. Mag.*, vol. 54, no. 3, pp. 54-60, Mar. 2016. <https://doi.org/10.1109/MCOM.2016.7432172>
- [29] D. Kontoudis y P. Fouliras, "A Survey of Models for Computer Networks Management", *Int. J. Comput. Networks Commun.*, vol. 6, no. 3, pp. 157-176, May 2014. <https://doi.org/10.5121/ijcnc.2014.6313>
- [30] A. McGibney, A. Esquiva Rodriguez y S. Rea, "Managing wireless sensor networks within IoT ecosystems", en *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, 2015. pp. 339-344. <https://doi.org/10.1109/WF-IoT.2015.7389077>
- [31] J. Strassner y W. W. Diab, "A semantic interoperability architecture for Internet of Things data sharing and computing", en *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Reston, 2016. pp. 609-614. <https://doi.org/10.1109/WF-IoT.2016.7845422>
- [32] E. Becerra-Orrala, "Implementación de monitoreo de red utilizando los Protocolos icmp y snmp" (trabajo de grado), Facultad de Electrónica y Telecomunicaciones, Universidad Estatal Península de Santa Elena, La libertad, 2016. Disponible en: <URL>
- [33] D. W. Kim, H.-D. Lee, C. W. de Silva y J.-W. Park, "Service-provider intelligent humanoid robot using TCP/IP and CORBA", *Int. J. Control. Autom. Syst.*, vol. 14, no. 2, pp. 608-615, Apr. 2016. <https://doi.org/10.1007/s12555-014-0441-5>
- [34] H. Guang-jun y L. Zheng-qiu, "Research on SLA information model based on SID", en *2015 10th International Conference on Computer Science & Education (ICCSE)*, Cambridge, 2015. pp. 991-994. <https://doi.org/10.1109/ICCSE.2015.7250396>
- [35] F. Estrada-Solano, A. Ordonez, L. Z. Granville y O. M. Caicedo Rendon, "A framework for SDN integrated management based on a CIM model and a vertical management plane", *Comput. Commun.*, vol. 102, pp. 150-164, Apr. 2017. <https://doi.org/10.1016/j.comcom.2016.08.006>
- [36] M. A. Khan, S. Peters, D. Sahinel, F. D. Pozo-Pardo, and X.-T. Dang, "Understanding autonomic network management: A look into the past, a solution for the future", *Comput. Commun.*, vol. 122, pp. 93-117, Jun. 2018. <https://doi.org/10.1016/j.comcom.2018.01.014>
- [37] M. Casanova y C. A. Calderón, "Empleo de modelos de información en arquitectura modificada para gestión de redes y servicios basada en políticas", *Rev. Ing. Electrónica, Automática y Comun.*, vol. 39, no. 3, pp. 77-89, Sep. 2018. Disponible en: <URL>
- [38] W. Liu *et al.*, "Policy-Based Management Framework for the Simplified Use of Policy Abstractions (SUPA)", Category: Informational, 8328. 2018. Disponible en: <URL>

- [39] A. Westerinen *et al.*, “Terminology for Policy-Based Management” Network Working Group, Request for Comments: 3198, 2001. <https://doi.org/10.17487/rfc3198>
- [40] A. Karpovsky y R. D. Galliers, “Aligning in Practice: From Current Cases to a New Agenda”, *J. Inf. Technol.*, vol. 30, no. 2, pp. 136-160, Jun. 2015. <https://doi.org/10.1057/jit.2014.34>
- [41] M. Curley, J. Kenneally, and M. Carcary, *IT Capability Maturity Framework™ (IT-CMFTM)*, 2nd edition. Van Haren, 2016. Disponible en: [URL](#)
- [42] C. G. Machado, E. Pinheiro de Lima, S. E. Gouvea da Costa, J. J. Angelis y R. A. Mattioda, “Framing maturity based on sustainable operations management principles”, *Int. J. Prod. Econ.*, vol. 190, pp. 3-21, Ago. 2017. <https://doi.org/10.1016/j.iipe.2017.01.020>
- [43] B. Trinkenreich, G. Santos y M. Perini Barcellos, “Metrics to Support IT Service Maturity Models. A Systematic Mapping Study”, en *Proceedings of the 17th International Conference on Enterprise Information Systems*, Barcelona, 2015. pp. 330-337. <https://doi.org/10.5220/0005376003300337>
- [44] D. da S. Avanzi, A. Foggiatto, V. A. dos Santos, F. Deschamps y E. de Freitas Rocha Loures, “A framework for interoperability assessment in crisis management”, *J. Ind. Inf. Integr.*, vol. 5, pp. 26-38, Mar. 2017. <https://doi.org/10.1016/j.jii.2017.02.004>
- [45] P. Malyzhenkov y M. Ivanova, “An Enterprise Architecture-Based Approach to the IT-Business Alignment: An Integration of SAM and TOGAF Framework”, en *Enterprise and Organizational Modeling and Simulation. EOMAS 2017. Lecture Notes in Business Information Processing*, Springer: Cham, 2017. pp. 159-173. https://doi.org/10.1007/978-3-319-68185-6_12
- [46] P. Pérez Lorences, “Procedimiento para mejorar la gestión de Tecnologías de la Información en el sector empresarial cubano”, Doctorado, Universidad Central “Marta Abreu” de Las Villas, Santa Clara, Cuba, 2014.
- [47] R. Bisquerra y N. Pérez-Escoda, “¿Pueden las escalas Likert aumentar en sensibilidad?”, *REIRE Rev. d'innovació i Recer. en Educ.*, vol. 8, no. 2, pp. 129-147, Jun. 2015. Disponible en: [URL](#)
- [48] M. M. Chiang Vega, I. I. Fuentealba Elgueta y R. A. Nova Cabrera, “Relación Entre Clima Organizacional y Engagement”, en *Dos Fundaciones Sociales, Sin Fines de Lucro, de la Región del Bio Bio*, *Cienc. Trab.*, vol. 19, no. 59, pp. 105-112, Ago. 2017. <https://doi.org/10.4067/S0718-24492017000200105>
- [49] P. Navarro, N. E. Ottone, C. Acevedo y M. Cantin, “Pruebas estadísticas utilizadas en revistas odontológicas de la red SciELO”, *Av. Odontostomatol.*, vol. 33, no. 1, pp. 25-32, 2017. Disponible en: [URL](#)
- [50] S. Lloret-Segura, A. Ferreres-Traver, A. Hernández-Baeza y I. Tomás-Marco, “El análisis factorial exploratorio de los ítems: una guía práctica, revisada y actualizada”, *An. Psicol.*, vol. 30, no. 3, Oct. 2014. <https://doi.org/10.6018/analesps.30.3.199361>
- [51] L. A. Acevedo-Bustacara, “Modelo TOC para la Solución de Problemas Puntuales en la Gestión de Información”, (Tesis de Maestría), Escuela Colombiana de Ingeniería Julio Garavito, Colombia, 2017. Disponible en: [URL](#)
- [52] C. J. P. Calvache, “A framework to support the harmonization between multiple models and standards” (tesis doctoral), Universidad de Castilla-La Mancha, Ciudad Real, 2012. Disponible en: [URL](#)
- [53] T. Hsu, *Hands-On Security in DevOps: Ensure continuous security, deployment, and delivery with DevSecOps*. Packt Publishing Ltd, 2018. Disponible en: [URL](#)
- [54] W. John *et al.*, “Service Provider DevOps”, *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 204-211, Ene. 2017. <https://doi.org/10.1109/MCOM.2017.1500803CM>
- [55] M. de la Cámara, F. J. Sáenz, J. A. Calvo-Manzano y M. Arcilla, “Security by design factors for developing and evaluating secure software”, en *2015 10th Iberian Conference on Information Systems and Technologies (CISTI)*, Aveiro, 2015. pp. 1-6. <https://doi.org/10.1109/CISTI.2015.7170500>
- [56] F. Bachmann, L. Bass, G. Chastek, P. Donohoe y F. Peruzzi, “The Architecture Based Design Method”. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Final rept. ADA375851, 2000. Disponible en: [URL](#)
- [57] A. Mavridou, E. Stachtari, S. Bliudze, A. Ivanov, P. Katsaros y J. Sifakis, “Architecture-based Design: A Satellite On-board Software Case Study”, Technical Report. EPFL-REPORT-221156, Oct. 2016. Disponible en: [URL](#)

- [58] S. Davy, B. Jennings y J. Strassner, “The policy continuum-Policy authoring and conflict analysis”, *Comput. Commun.*, vol. 31, no. 13, pp. 2981-2995, Ago. 2008. <https://doi.org/10.1016/j.comcom.2008.04.018>
- [59] R. Kazman, M. Klein y P. Clements, “ATAM: Method for Architecture Evaluation”, Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, Final rept. ADA382629. Ago. 2000. Disponible en: <URL>
- [60] N. Boucké, D. Weyns, K. Schelfhout y T. Holvoet, “Applying the ATAM to an Architecture for Decentralized Control of a Transportation System”, In: Hofmeister C., Crnkovic I., Reussner R. (eds) *Quality of Software Architectures. QoSA 2006. Lecture Notes in Computer Science*, vol 4214. 2006. pp. 180-198. https://doi.org/10.1007/11921998_16
- [61] W. Zheng *et al.*, “On dynamic performance estimation of fault-prone Infrastructure-as-a-Service clouds”, *Int. J. Distrib. Sens. Networks*, vol. 13, no. 7, Jul. 2017. <https://doi.org/10.1177/1550147717718514>
- [62] D. Bruneo, “A Stochastic Model to Investigate Data Center Performance and QoS in IaaS Cloud Computing Systems”, *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 560-569, Mar. 2014. <https://doi.org/10.1109/TPDS.2013.67>
- [63] H. J. Lee, M.-S. Kim, J. W.-K. Hong y G.-H. Lee, “QoS Parameters to Network Performance Metrics Mapping for SLA Monitoring”, *Rev. KNOM*, vol. 5, no. 2, pp. 42-53, 2003. Disponible en: <URL>
- [64] S.-Y. Kim, M.-E. Kim, K. Kim y J. Jang, “Information Model for Policy-Based Network Security Management”, Springer, Berlin, Heidelberg 2002. pp. 662-672. https://doi.org/10.1007/3-540-45803-4_60
- [65] J. C. Strassner, “Context-aware dynamic policy selection for load balancing behavior”, “Estados unidos, US9602380B2, Mar. 2017. Disponible en: <URL>
- [66] E. J. Scheid, C. C. Machado, R. L. dos Santos, A. E. Schaeffer-Filho y L. Z. Granville, “Policy-based dynamic service chaining in Network Functions Virtualization”, en *2016 IEEE Symposium on Computers and Communication (ISCC)*, Messina, 2016. pp. 340-345. <https://doi.org/10.1109/ISCC.2016.7543763>
- [67] K. S. Ibarra-Lancheros, G. Puerto-Leguizamón y C. Suárez-Fajardo, “Quality of service evaluation based on network slicing for software-defined 5G systems”, *TecnoLógicas*, vol. 21, no. 43, pp. 27-41, Sep. 2018. <https://doi.org/10.22430/22565337.1066>
- [68] M. P. Casanova, J. L. da Silva, O. F. Díaz y C. A. Calderón, “Sistema para detección y aislamiento de fallas”, *rev. Cuba. Ciencias informáticas*, vol. 12, no. 2, pp. 200-220, Apr. 2018. disponible en: <URL>
- [69] J. C. Henderson y H. Venkatraman, “Strategic alignment: Leveraging information technology for transforming organizations”, *IBM Syst. J.*, vol. 32, no. 1, pp. 472-484, 1993. <https://doi.org/10.1147/sj.382.0472>
- [70] D. S. Preston y E. Karahanna, “Antecedents of IS Strategic Alignment: A Nomological Network”, *Inf. Syst. Res.*, vol. 20, no. 2, pp. 159-179, Jun. 2009. <https://doi.org/10.1287/isre.1070.0159>
- [71] Frameworx Project, “TM Forum”, *GB988 TM Forum Metrics Definitions R18.5.1*, Apr. 2019. Disponible en: <URL>
- [72] M. P. Casanova y A. C. Caridad, “Procedimiento de dimensionamiento de infra-estructura empleando Gestión de Redes Basada en Políticas”, *Rev. Telemática*, vol. 18, no. 1, pp. 92-105, 2019. Disponible en: <URL>
- [73] R. Olups, *Zabbix 1.8 Network Monitoring: Monitor Your Network's Hardware, Servers, and Web Performance Effectively and Efficiently*. Packt Pub, 2010. Disponible en: <URL>

7. CONTRIBUCIÓN DE LOS AUTORES

¹ Diseño de la investigación, validación del procedimiento, análisis de los resultados y redacción de la versión final del artículo.

² Diseño de la investigación, análisis de los resultados y revisión crítica del artículo.