Seguridad arquitectural con LAN-*less*

Nombre Estudiante: Liliana del Rocío Mena Hernández
Master Interuniversitario en Seguridad de las Tecnologías de la Información y de las comunicaciones (MISTIC)
Seguridad Empresarial

Nombre Consultor: Amadeu Albós Raya

Nombre Profesor responsable de la asignatura: Víctor García Font

Centro: Universitat Oberta de Catalunya

Fecha entrega: 21 de junio de 2019

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Seguridad arquitectural con LAN-less*
Nombre del autor:	*Liliana del Rocío Mena Hernández*
Nombre del consultor/a:	*Amadeu Albós Raya*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2019
Titulación:	*Master Interuniversitario en Seguridad de las Tecnologías de la Información y de las comunicaciones (MISTIC)*
Área del Trabajo Final:	*Seguridad empresarial*
Idioma del trabajo:	*Español*
Palabras clave	Ciberseguridad, arquitectura de red, LAN-*less*, *Docker*

Resumen del Trabajo:

La presente investigación tiene como finalidad diseñar un modelo de arquitectura de seguridad para comunicación *on premise*-nube bajo el paradigma LAN-*less*, en una IES (Institución de Educación Superior), la cual fue sujeta a una serie de análisis y planteamientos necesarios para evidenciar posibles puntos vulnerables bajo el contexto de su arquitectura de seguridad actual y así justificar la implementación de un nuevo modelo de seguridad que abarque el paradigma LAN-*less*. Esta investigación se fundamenta en aspectos tanto teóricos como prácticos de la seguridad de la información, los cuales resultan ser altamente compatibles con el paradigma LAN-*less*, que consiste en la reducción del perímetro de seguridad de la red y los servicios de la IES sin comprometer la seguridad en la institución, y, a su vez, reduce el grado de complejidad de administración de los servicios que oferta la universidad. Sin lugar a dudas, una gran forma de mitigar riesgos y, además, de ofrecer a los administradores de red la simplicidad en el manejo y gestión de los diferentes servicios. El diseño propuesto en esta investigación también contempla la implementación de tecnología de contenedores *Docker*, lo que limita aún más el perímetro de seguridad de los servicios, y a su vez, potencia el rendimiento de éstos en función del hardware que actualmente posee la institución.

Palabras clave: Ciberseguridad, arquitectura de red, LAN-*less*, D*ocker*.

Abstract:

The purpose of this research is to design a security architecture model for premise-cloud communication under the LAN-less paradigm, in an Institution of higher education, which was subject to a series of analyses and approaches necessary to highlight possible vulnerable points under the context of its current security architecture and thus justify the implementation of a new security model that encompasses the LAN-less paradigm. This research is based on both theoretical and practical aspects of information security, which are highly compatible with the LAN-less paradigm, which consists of reducing the security perimeter of the network and services of the Institution of higher education without compromising the security of the institution, and at the same time, reduces the degree of complexity of administration of the services offered by the university. Without a doubt, a great way to mitigate risks and, in addition, to offer network administrators simplicity in the handling and management of the different services. The design proposed in this research also contemplates the implementation of Docker container technology, which further limits the perimeter of security of the services, and in turn, boosts the performance of these depending on the hardware currently owned by the institution.

Keywords: Cybersecurity, network architecture, LAN-less, Docker

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

En la actualidad la seguridad en redes y comunicaciones, es de vital importancia, ya que la función interrumpida de las aplicaciones informáticas puede llegar a causar graves problemas de pérdida de datos e incluso pérdidas económicas; es por esto que las empresas no pueden dejar de entregar sus servicios en ningún momento y se necesita contar con soluciones rápidas que ayuden a gestionar eficientemente las amenazas informáticas que podrían dañar la integridad de la información, haciendo que se afecten los servicios. Así mismo es imprescindible que las empresas cuenten con mecanismos que permitan mitigar los posibles ataques que puedan dañar la confiabilidad de la información o que causen daños en los servidores [1].

El acceso a internet en la institución educativa se realiza desde múltiples dispositivos y plataformas; a su vez permite el compartir, colaborar y acceder a información de acuerdo a las necesidades [2], por lo mismo la información que se maneja está expuesta a riesgos que pudieran afectar la confidencialidad, disponibilidad e integridad de la misma, es por esto que se ha visto la necesidad de diseñar un modelo de seguridad tomando como referencia el modelo LAN-*less*, que le permita a empresa (institución de educación superior), estar preparada para responder de forma eficiente, ante cualquier eventualidad que pudiera interrumpir el servicio y a su vez pueda ocasionar pérdida de la información.

Se pretende fundamentar teóricamente el modelo de arquitectura de seguridad bajo el paradigma LAN-*less*, para adecuar los mecanismos de seguridad que mejor se adapten al entorno de la empresa con respecto a la comunicación de los servicios tecnológicos *on premise*-nube. También a partir del diagnóstico de la situación actual se pueden determinar los riesgos más comunes que acechan a los sistemas informáticos de la empresa de acuerdo a sus características en este caso las instituciones de educación superior. Posteriormente se definirán los elementos que conforman el modelo de arquitectura de seguridad desde el paradigma LAN-*less* y en base a los mecanismos de seguridad aplicables al entorno específico.

Preguntas directrices

- **¿Cuál es la factibilidad de establecer un modelo de arquitectura de seguridad basada en el paradigma LAN-*less* para la comunicación de servicios tecnológicos on *premise*-nube?**

Para determinar la factibilidad indicada, se realizará una investigación profunda de cada elemento y procedimiento que integre la guía indicada, para ello se auscultarán otros modelos de arquitectura de seguridad en redes desde la tradicional como parte del estudio de la literatura.

- **¿Cómo el paradigma LAN-*less* mejora la comunicación *on premise*-nube en la red?**
De la revisión documental se determinará si el paradigma LAN-*less* incluye aspectos de mejora en la comunicación on *premise*-nube.

- **¿Cuáles son los modelos de despliegue de información en la nube?**
Se identificarán los diferentes tipos de modelos para desplegar información en la nube y se analizará el más acorde al caso de estudio.

- **¿Qué metodologías se utilizan para el diseño del modelo de arquitectura de seguridad?**
Realizando el análisis de la revisión de la literatura se podrá ir describiendo cada una de las metodologías para el diseño del modelo de arquitectura de seguridad encontradas, y explicando cada una de sus fases a detalle.

- **¿Cuáles son los procedimientos informáticos para generar el modelo de arquitectura de seguridad que permita comunicar servicios tecnológicos *on premise*-nube?**
Mediante la lectura y comparativa de información revisada en los textos investigados, se podrá ir identificando los procedimientos informáticos para la seguridad empresarial y que permitan generar el modelo de arquitectura de seguridad para comunicar servicios tecnológicos *on premise*-nube.

- **¿Cómo se describe el proceso que permite comunicar servicios tecnológicos *on premise*-nube a partir del modelo de arquitectura de seguridad LAN-*less*?**
La revisión documental específica sobre este tema y la experiencia previa del investigador, permitirá conocer y describir el proceso de comunicación de servicios tecnológicos *on premise*-nube a partir del modelo de arquitectura de seguridad LAN-*less*. La información que se registre será el resultado de la aplicación del proceso en el caso de estudio específico.

- **¿Cuál es el nivel de confianza para migrar o contratar servicios en la nube para la comunicación de servicios tecnológicos *on premise*-nube con una arquitectura segura?**
De la revisión bibliográfica se analizará el nivel de confianza para la comunicación de servicios tecnológicos *on premise*-nube que ofrece la empresa contratada para el caso de estudio.

- **¿Cuáles son las empresas más utilizadas para migrar servicios tecnológicos con una comunicación segura?**
Partiendo de la revisión de literatura se analizará las empresas utilizadas para migrar servicios tecnológicos con una comunicación segura, analizando a detalle la comunicación en el modelo de arquitectura segura propuesto bajo el paradigma LAN-*less*.

- **¿Cómo establecer el diseño del modelo de arquitectura de seguridad para comunicación *on premise*-nube bajo el paradigma LAN-*less* en una institución de educación superior?**

  En este caso se realizará una revisión y análisis exhaustivo de modelos arquitectura de seguridad y se determinará un modelo acorde a la realidad de la institución de educación superior y al contexto de la legislación ecuatoriana, basado principalmente en una comunicación segura en el caso de estudio.

1.2 Objetivos del Trabajo

1.2.1 Objetivo General

- Diseñar el modelo de arquitectura de seguridad para comunicación *on premise*-nube bajo el paradigma LAN-*less*, en una institución de educación superior.

1.2.2 Objetivos Específicos

- Fundamentar teóricamente los modelos de arquitectura de seguridad de la información para la identificación de elementos que los conforman.
- Analizar la seguridad del entorno actual de la empresa para el diagnóstico de riesgos informáticos.
- Definir el modelo de arquitectura de seguridad bajo el paradigma LAN-*less* que permita comunicar servicios tecnológicos *on premise* - nube.
- Diseñar los servicios actuales bajo la perspectiva LAN-less segura para la comunicación de servicios *on premise* con servicios en la nube.

1.3 Enfoque y método seguido

La metodología a seguir durante el desarrollo de la investigación se hará a partir de la definición del plan del trabajo.

Es decir, se parte de la descripción de los elementos participantes en el entorno de la investigación; se especifica la problemática a resolver; se definen los objetivos que permitirán el alcance de la investigación; se propone el diseño del sistema bajo el nuevo paradigma; se plantea la metodología a utilizar, se realiza un diagnóstico de la situación actual para determinar los riesgos que podrían surgir en el desarrollo investigativo, y se presenta un cronograma de actividades a cumplir en los tiempos establecidos para la investigación.

El enfoque de investigación a aplicarse es de tipo mixto, ya que a partir de la recopilación de información se analizan datos cuantitativos y cualitativos.

Además, en las empresas el modelo no es estático, sino que existe un proceso continuo para alinear las estrategias del negocio con las estrategias de SI/TI, de tal manera que se genere un impacto visible del uso adecuado de recursos. Para este caso las posibles estrategias a llevar a cabo son las estrategias de SI/TI, con un alineamiento de las estructuras de la organización y la cultura organizacional, en la institución de educación superior, bajo el paradigma LAN-*less*, estableciendo un alineamiento estratégico con cada proceso de gobierno, conocimiento y cultura de IT compartidos.

Se considera esta estrategia la más apropiada que permite en una empresa, diagnosticar el estado actual de los SI/TI y a partir de ello identificar la arquitectura tecnológica, procesos de gestión de TI desde el punto de vista estratégico que mejore aspectos de gobierno y toma de decisiones en la empresa.

1.4 Planificación del Trabajo

1.4.1 Descripción de las tareas

Las tareas a realizar estarán encaminadas al logro de los objetivos planteados al inicio del trabajo investigativo, las mismas se detallan a continuación:

Revisión del problema
A partir de las preguntas de investigación se define el problema a investigar, se tiene clara la importancia del tema y porque existe la necesidad de realizar la investigación en el contexto de la seguridad de la información y del modelo arquitectural LAN-*less*

Revisión de la literatura del tema
Es necesario realizar la revisión bibliográfica acerca de la arquitectura del modelo LAN-*less*, y del contexto relacionado a la seguridad de la información en dicho entorno, dicha revisión es la base para el desarrollo del estado del arte y para encontrar los referentes a nivel internacional, nacional y local.

Entorno de estudio
Se definen los objetivos, y a partir de estos y del título de la investigación se definen los apartados, temas y subtemas a desarrollarse en el transcurso de la investigación.

Planificación de trabajo
En el desarrollo de la investigación, se ha considerado elaborar un modelo LAN-*less* para la seguridad arquitectural de una institución de educación superior.

Se realiza un diagnóstico de la situación actual de la universidad para posteriormente mediante un análisis de riesgos establecer el modelo LAN-*less* acorde a las necesidades de la misma. Se está considerando a la universidad como una empresa para centrarse en el área de Seguridad empresarial. Es preciso indicar la importancia del estudio ya que el modelo es aplicable a otros contextos empresariales.

Se propone el diseño del sistema bajo el nuevo paradigma cuyas actividades a cumplirse están diseñadas para alcanzar el objetivo general que es: Diseñar un modelo LAN-*less* para la Seguridad arquitectural en una institución de educación superior.

A partir del análisis de la metodología del desarrollo con CISCO PDIOO (Planificación –Diseño – Implementación –Operación –Optimización), se proponen las fases para consecución de los objetivos.

1.4.2 Planificación del tiempo

A continuación, se presenta un diagrama de Gantt con la planificación temporal de las tareas:

Cronograma general de actividades:

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1		Plan de trabajo (PEC 1)	10 días	mié 20/02/19	mar 05/03/19	
7		Descripción del estudio (PEC 2)	20 días	mié 06/03/19	mar 02/04/19	1
11		Resultados del análisis (PEC 3)	20 días	mié 03/04/19	mar 30/04/19	7
14		Memoria Final (PEC 4)	27 días?	mié 01/05/19	mar 04/06/19	11
18		Presentación del Video	5 días	mié 05/06/19	mar 11/06/19	14
20		Defensa del TFM	5 días?	lun 17/06/19	vie 21/06/19	18

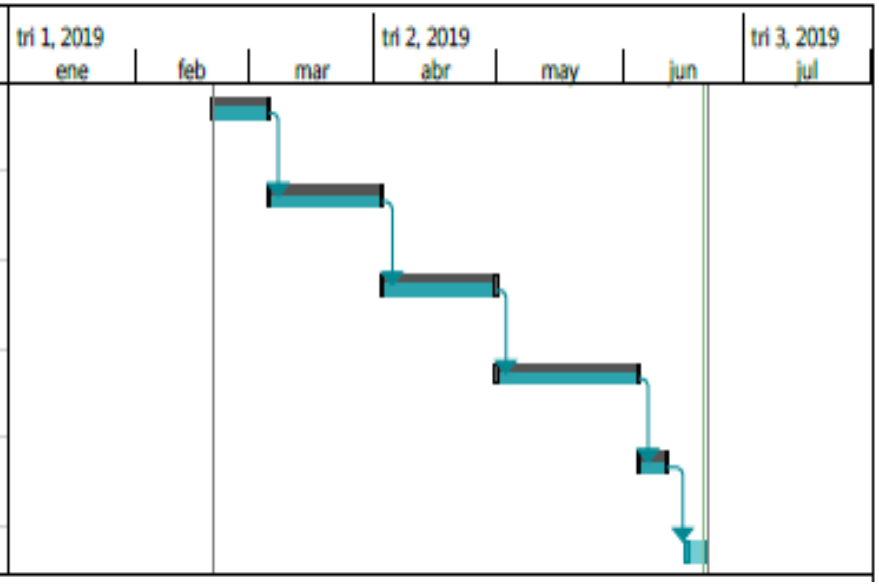

Ilustración 1: Hitos parciales de las PEC del TFM
Fuente: elaboración propia

Cronograma detallado de actividades:

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		**Plan de trabajo (PEC 1)**	**10 días**	**mié 20/02/19**	**mar 05/03/19**
2		Explicación del problema	2 días	mié 20/02/19	jue 21/02/19
3		Objetivos	2 días	vie 22/02/19	lun 25/02/19
4		Metodología	2 días	mar 26/02/19	mié 27/02/19
5		Tareas a realizar	2 días	jue 28/02/19	vie 01/03/19
6		Planificación temporal	2 días	lun 04/03/19	mar 05/03/19
7		**Descripción del estudio (PEC 2)**	**20 días**	**mié 06/03/19**	**mar 02/04/19**
8		Recolección y análisis de documentos sobre el tema de estudio.	7 días	mié 06/03/19	jue 14/03/19
9		Diagnóstico de la institución de educación superior.	7 días	vie 15/03/19	lun 25/03/19
10		Definición de la metodología.	6 días	mar 26/03/19	mar 02/04/19
11		**Resultados del análisis (PEC 3)**	**20 días**	**mié 03/04/19**	**mar 30/04/19**
12		Diseño de arquitectura de seguridad LAN-less para comunicar sistemas on premise con servicios en la nube.	10 días	mié 03/04/19	mar 16/04/19
13		Análisis de los resultados.	10 días	mié 17/04/19	mar 30/04/19
14		**Memoria Final (PEC 4)**	**27 días?**	**mié 01/05/19**	**mar 04/06/19**
15		Conclusiones y recomendaciones	18 días	mié 01/05/19	jue 23/05/19
16		Revisión de redacción y estilo de la memoria final.	7 días	vie 24/05/19	sáb 01/06/19
17		Check list del contenido de la memoria final.	2 días	lun 03/06/19	mar 04/06/19
18		**Presentación del Video**	**5 días**	**mié 05/06/19**	**mar 11/06/19**
19		Desarrollo del vídeo conforme a las especificaciones dadas.	5 días	mié 05/06/19	mar 11/06/19
20		**Defensa del TFM**	**5 días?**	**lun 17/06/19**	**vie 21/06/19**

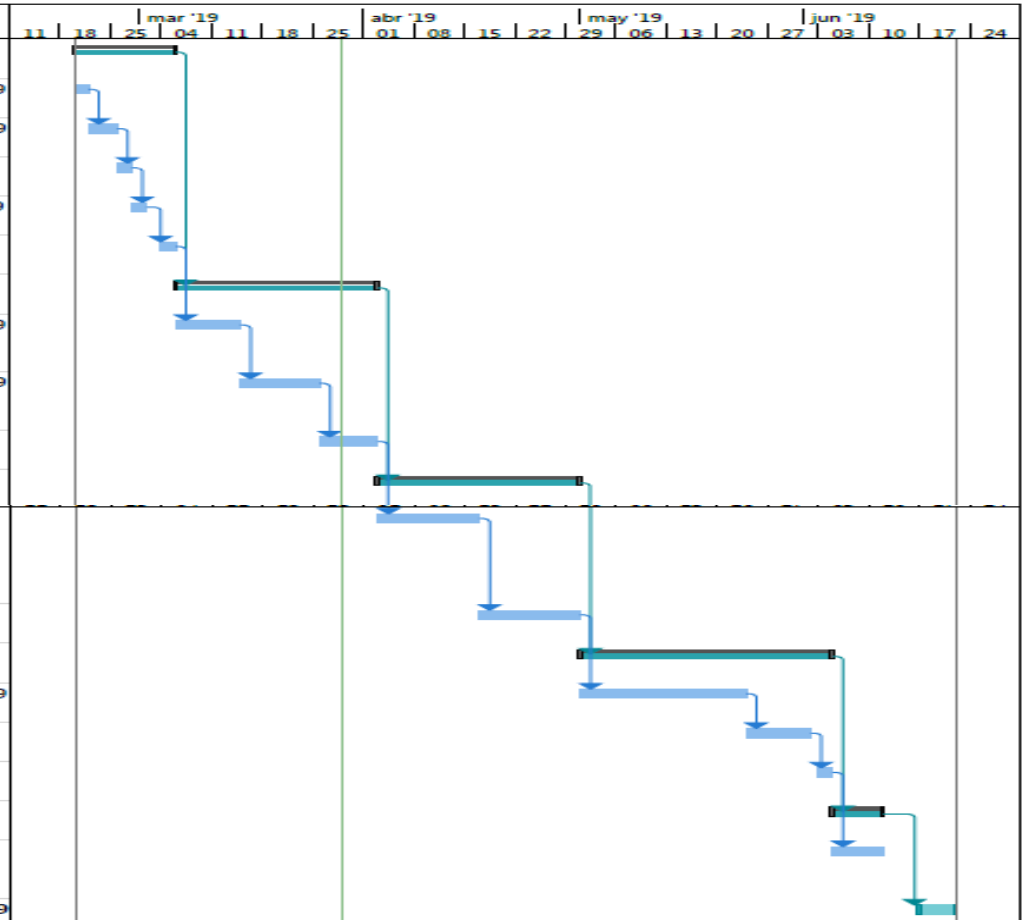

Ilustración 2: Planificación detallada de las tareas del TFM
Fuente: elaboración propia

1.4.3 Presupuesto del proyecto

El presupuesto que se estima para el proyecto es el siguiente:

Rubro	Valor
Materiales y suministros	100,00
Material bibliográfico	400,00
Transporte	0,00
Inversión parcial	500,00
Imprevistos	50,00
Total	550,00

1.5 Breve sumario de productos obtenidos

Los productos obtenidos al finalizar el proyecto son:

- **Plan de trabajo:** en este se señalan los hitos principales y planificación detallada de las tareas con fechas de inicio y fin, así como la duración y relación de las mismas.
- **Documento con la propuesta del diseño de seguridad arquitectural bajo el paradigma LAN-*less* en una institución de educación superior:** detalle de la propuesta planteada para la seguridad de la comunicación de los servicios *on premise* con los servicios en la nube.
- **Memoria final del proyecto:** el proyecto final con las conclusiones y recomendaciones de seguridad.
- **Presentación del proyecto**: contiene diseño de los servicios actuales de una institución de educación superior bajo la perspectiva LAN-*less* segura para la comunicación de servicios *on premise* con servicios en la nube
- **Video de presentación:** en el que se hará una presentación resumida del proyecto.

1.6 Breve descripción de los otros capítulos de la memoria

Una vez que se cuenta con el plan de trabajo, se realiza un estudio de la literatura donde se recopilan y analizan diferentes fuentes referentes a la temática y se describe la metodología a utilizar para la propuesta del diseño de seguridad bajo el paradigma LAN-*less*.

A continuación, se analiza la seguridad del entorno actual de la empresa para el diagnóstico de riesgos informáticos a nivel de la red de comunicación de servicios.

Después se realiza el análisis de los problemas de seguridad detectados en el proceso de comunicación, para a partir de aquí proceder a diseñar los servicios actuales de una institución de educación superior bajo la

perspectiva LAN-*less* segura para la comunicación de servicios *on premise* con servicios en la nube.

Luego se indican las conclusiones y recomendaciones del estudio, para la comunicación segura de los servicios.

En los últimos apartados se presentan: el glosario de términos, la bibliografía y los anexos.

2. Análisis y diseño teórico

En este punto del desarrollo del proyecto, se presenta un marco referencial a partir de la revisión de la literatura relacionada a varios aspectos de la seguridad empresarial y en torno al diseño del modelo de arquitectura con las medidas de seguridad bajo el paradigma LAN–*less*, para la comunicación entre servicios *on premise* y *cloud computing*. Describiendo la metodología aplicable, con un enfoque mixto, analizando también las características del proveedor de servicios en este caso Amazon y sus procesos técnicos, de seguridad con sus actores principales, los usuarios. Las normas y estándares internacionales, legislación ecuatoriana relacionadas al tema de estudio.

2.1 Seguridad de la información

Para el desarrollo de la investigación se hace necesario analizar información que podría servir de base, así en el estudio que propone Hernández et. al [3], se pone de manifiesto que el internet es una herramienta que promueve la conectividad pero no así la seguridad.

Según, la revista *Marketing 4 Ecommerce* [4], el internet en el mundo crece de un 53% de usuarios en el mundo en el 2018, apenas en estos pocos meses ya se cuenta con un 57% de usuarios interconectados, es decir más de la mitad de la población está en internet. Es por ello que hoy día es un tema central para todos los usuarios de equipos de cómputo, ya sean computadores de escritorio, dispositivos móviles, se usen en el hogar, en las escuelas o colegios, o en organizaciones, ya que su uso trae consigo el riesgo de que en algún momento puedan ser víctimas de un ataque informático.

Por otra parte, Reyes et. al [5], pone de manifiesto el *hackeo* de una página de la Universidad de Santa Elena y de igual manera concluye que tanto las pequeñas y medianas empresas no están exentas de que intrusos quieran acceder a páginas web para dañar la información o apoderarse de ella con fines maliciosos.

Todo sistema está expuesto a riesgos, estos pueden presentarse de forma interna o externa tales como: riesgos físicos, desastres naturales, alteraciones del entorno. Estos tipos de riesgos pueden ocasionar graves daños en los sistemas de información [6].

A pesar de los avances en el ámbito de la seguridad de la información, todavía hay mucho por hacer, y según Zambrano y Valencia [7], el creciente uso del internet promueve a la vez el desarrollo de proyectos de seguridad informática, con la finalidad de ayudar a prevenir y proteger el activo más preciado de las empresas, la información, garantizando la integridad y confiabilidad de la misma.

La seguridad de la información es un tema que presenta un amplio campo a desarrollar para la generación de proyectos con impacto social, es por esto que se desea realizar la presente investigación encaminada al diseño de un modelo de arquitectura de seguridad de la información bajo el paradigma LAN-*less*, para la comunicación de servicios *on premise* con servicios en la nube y aplicable a una institución de educación superior.

2.2 Arquitectura de seguridad de la información

La arquitectura de seguridad de la información, como lo manifiesta Abril [8], es la: "Organización lógica para los procesos, estructuras y acuerdos de una corporación que reflejan la integración y regulación de los requerimientos del modelo operacional de la misma".

La información con que cuenta la Institución de Educación Superior en estudio, es muy valiosa, por lo cual está expuesta a riesgos y en cualquier momento pudiera ser víctima de ataques que afecten la confidencialidad, integridad y disponibilidad de la misma.

Un modelo de arquitectura de seguridad de la información permite contar con un conjunto de controles de infraestructura para minimizar los riesgos que conlleva el tener libre acceso a la LAN y a los servicios *on premise* y nube, con los que cuenta la institución de educación superior, además la arquitectura apoya a las estrategias de la empresa [9].

2.3 Paradigma LAN-*less*

LAN-*less* equivale a pequeño perímetro de seguridad, es así como se considera a este paradigma que ha venido a revolucionar la comunicación de servicios *on premise*-nube.

Como lo manifiesta Scott [10] en su blog acerca de "*The Brave New LANless Future | MangoLassi*", si se habla de diseñar una LAN, hoy en día esto significa mucho más que una LAN local o tradicional, en las que se pueden ver una serie de factores que hacen la vida más difícil para todos los involucrados en aspectos de seguridad, ya que el perímetro de seguridad es enorme y abarca todos los dispositivos conectados a la red.

A diferencia de lo anterior el paradigma LAN-*less* proporciona una visión menos compleja en el entorno de seguridad, el perímetro de seguridad es pequeño ya que solo abarca los servicios de red. Si bien es cierto que cada dispositivo sigue siendo un riesgo para la seguridad, pero se puede considerar que ahora solo es un riesgo para la cantidad limitada de datos y servicios a los que tiene acceso un usuario en particular. Este paradigma genera a la vez varias cuestiones, sobre cómo estos servicios

que ahora se comparten en la nube de manera independiente se comunicarán y autentificarán de manera segura para la empresa.

2.4 Elementos que componen la arquitectura de seguridad de la información

La arquitectura de seguridad de la información, está conformada por los elementos que se muestran a continuación:

Ilustración 3. Modelo de arquitectura de seguridad de la información
Fuente: tomado de [11]

2.5 Normativas de seguridad

2.5.1 Normativas y estándares internacionales

Existen normativas internacionales y directrices que aportan notablemente con guías para el diseño del modelo de arquitectura de seguridad. Sin embargo, la particularidad legal y normativa en los diferentes países, permite una gran variabilidad para la aplicación específica de procedimientos metodológicos en la temática tratada.

En este estudio, bajo el paradigma LAN-*less*, para la comunicación de servicios tecnológicos *on premisse* con la nube, se toma como referencia los lineamientos de:

- Marco de Trabajo ITIL V3.- ITIL (*Information Technology Infrastructure Library*), conjunto de conceptos y mejores prácticas para la gestión de servicios informáticos.

- Estándares de seguridad ISO. - Es importante señalar que la Organización Internacional de Normalización (International Organization for Standardization, ISO), ha emitido normas que constituyen los estándares principales para resguardar y garantizar la integridad de la información alojada en la nube, del servicio ofrecido por empresas como Amazon Web Services (AWS), Google Cloud o Microsoft Azure, estas normas son: ISO/IEC 27000, 27001, 27005, 27017 y 27018

    - **ISO/IEC 27000.-** Conjunto de estándares que permiten tener un marco de Gestión de Seguridad de la Información.
    - **ISO/IEC 27001.-** Estándar para certificar los requisitos para implementar, mantener y mejorar la seguridad de la información.
    - **ISO/IEC 27005.-** Estándar internacional para la gestión de riesgos de seguridad de información.
    - **ISO/IEC 27017.-** Estándar que proporciona controles relativos a proveedores y clientes de servicios en la nube.
    - **ISO/IEC 27018.-** Estándar internacional sobre seguridad en la nube. Esta norma protege el derecho a la privacidad de la información de los usuarios y en cierta manera exige a las empresas proveedoras informar sobre el tratamiento que dan a los datos de los clientes.

- Normativa Legal vigente. - Estas normas ordenan y recomiendan mejores prácticas, por lo que es aconsejable que cualquier protocolo de actuación o normativa esté alineado con las mismas, [12], [13] y [14].

2.5.2 Legislación ecuatoriana

- Plan nacional de telecomunicaciones y tecnologías de información en el Ecuador 2016-2021.- El mismo que promueve el uso de las herramientas TIC, para el desarrollo económico y social del país, así como para mejorar la eficiencia, competencia y crecimientos del comercio electrónico; la sistematización de procesos en diferentes áreas como: educación, salud y justicia para el bienestar social.

- Normativa legal vigente en el Ecuador. - ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN – EGSI.
  - **Art. 1. –** "Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información".
  - **Art. 7.-** "Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 ". Gestión del Riesgo en la Seguridad de la Información.

2.6 Estado actual de la empresa

La IES en estudio, cuenta con el Departamento de TI que es el encargado de la gestión de los recursos tecnológicos que dispone la empresa.

Actualmente cuenta con servicio de aplicaciones en la nube proporcionadas por el proveedor Amazon, con una arquitectura con replicas en dos zonas: California y Europa.

En su estructura interna está conformado por: el Jefe de TI, Especialista de infraestructura, Especialista de software, y cuatro auxiliares

2.6.1 Sistema de interconectividad

La IES investigada, se encuentra conectada a la IES matriz o principal, que está ubicada en otra ciudad, el Centro de Datos de la Institución matriz, permite el acceso mediante IP pública al Servicio Financiero SAP, el resto de servicios como el académico, biblioteca, Moodle, en la Institución objeto de estudio, se manejan de manera independiente vía *web.*

La topología utilizada es una topología estrella que permite una comunicación entre los diferentes bloques que hay en la empresa.

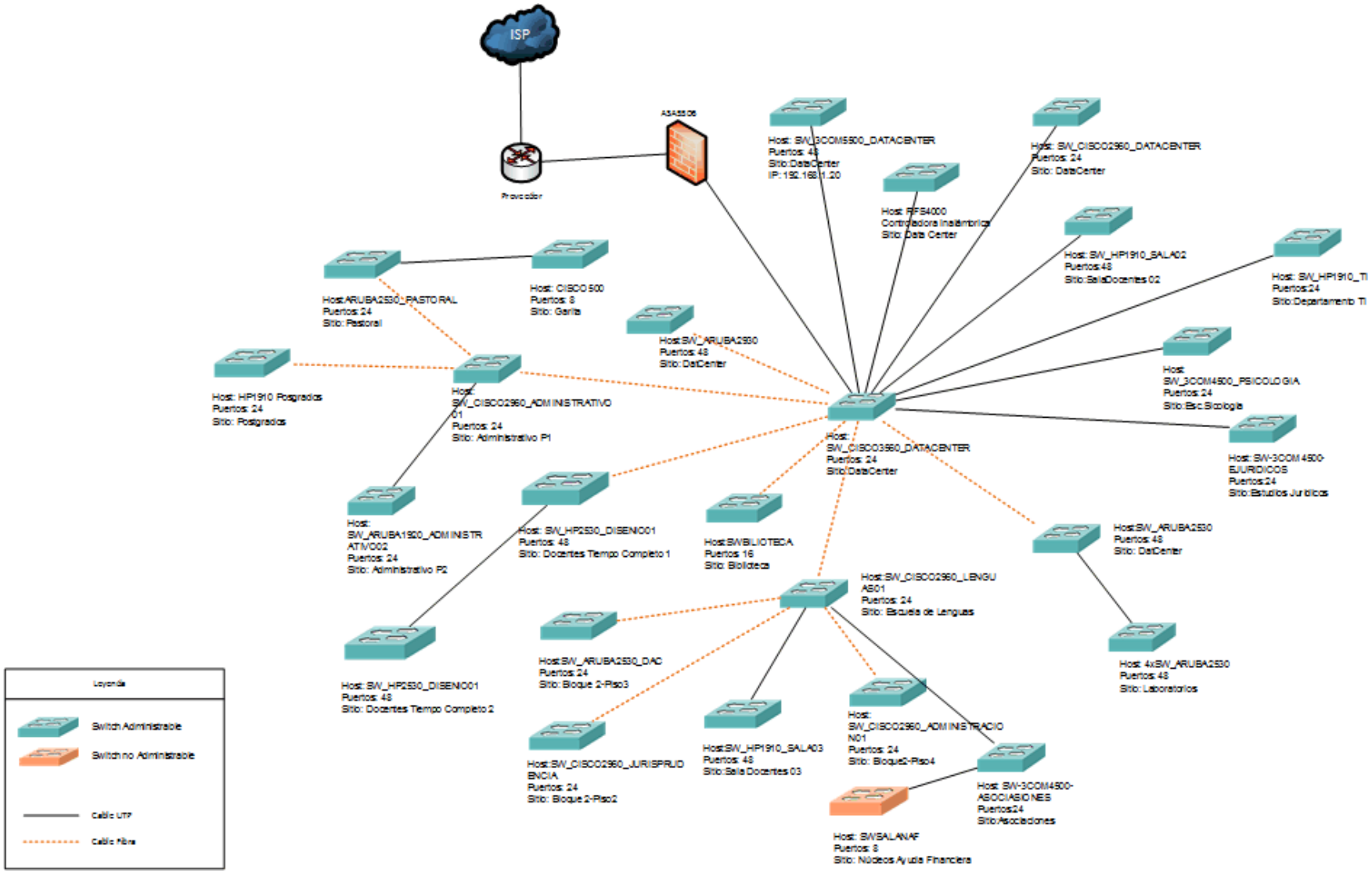

Ilustración 4. Interconectividad de la LAN de la IES
Fuente: (Departamento de TI de la IES, 2018)

2.6.2 Centro de Datos

El Departamento de TI cuenta con su Centro de Datos en el cuarto piso del bloque 1, bajo condiciones que cumplen con los requisitos establecidos en los estándares NTC – ISO/IES 27001 y 27002.

A continuación, se señalan los mecanismos de seguridad con que cuenta el Centro de Datos de la IES en estudio:

a) Acceso limitado con autenticación mediante tarjeta.
b) Ingreso solo personal autorizado: Jefe de TI y Especialista en infraestructura.
c) Sistema digital cámaras de monitoreo.
d) Sensores de temperatura y de humedad.
e) Condiciones ambientales entre 11,2° C y 21,8° C como máximo, siendo el promedio entre 18° C y 19° C.
f) Humedad 50%.
g) Detector de humo.
h) Controles de suministro de energía: conexión a tierra, UPS, pararrayos.

La distribución geográfica está en base al siguiente diagrama:

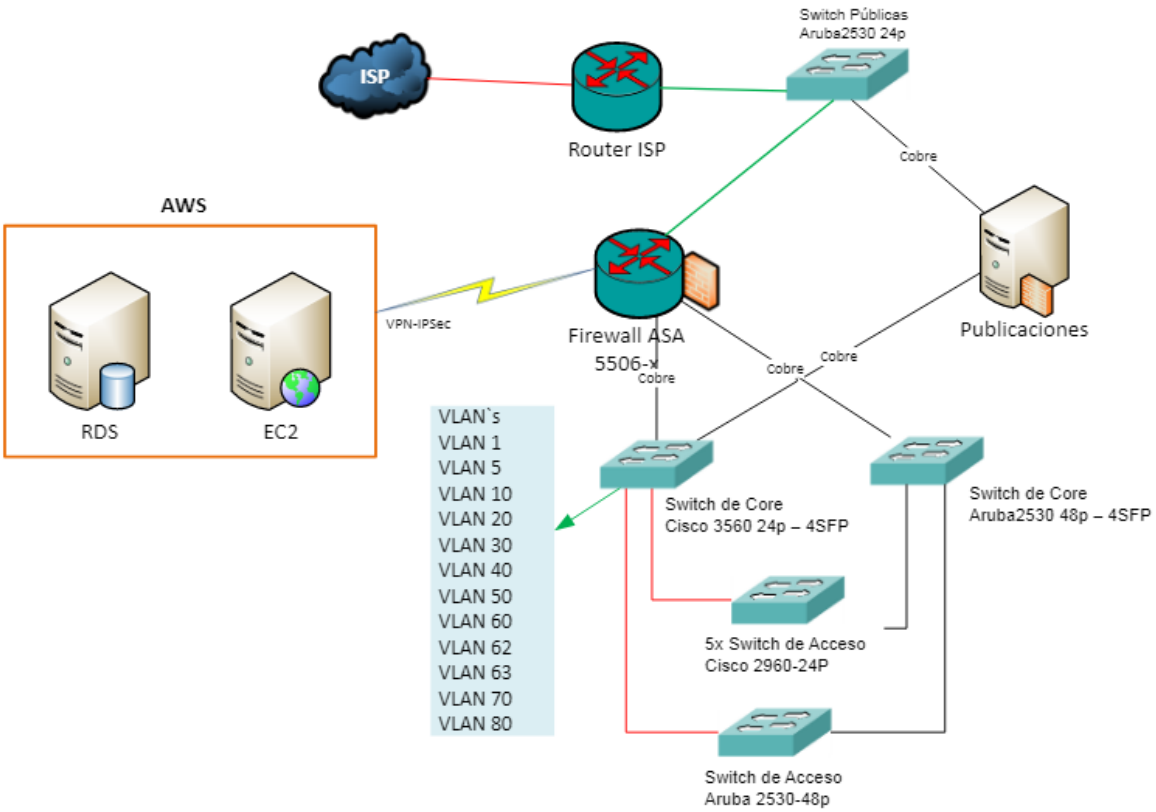

Ilustración 5. Diagrama de red *Data Center*
Fuente: (Departamento de TI de la IES, 2018)

2.6.3 Infraestructura de redes y ubicación geográfica

La red LAN de la empresa se distribuye con varias subredes para las diferentes escuelas, y cubículos donde están las PC de escritorio de los docentes, además se tiene acceso compartido de recursos como impresoras y escáneres.
Las aplicaciones de uso académico son: Académico que es un sistema de gestión de seguimiento de syllabus, reportes de tutorías y reportes de calificaciones. También está la plataforma de aulas virtuales Moodle 3.5 que se integra con el sistema Académico para el reporte de calificaciones.

Los estudiantes, docentes y visitantes tienen acceso a las redes inalámbricas mediante una clave general.

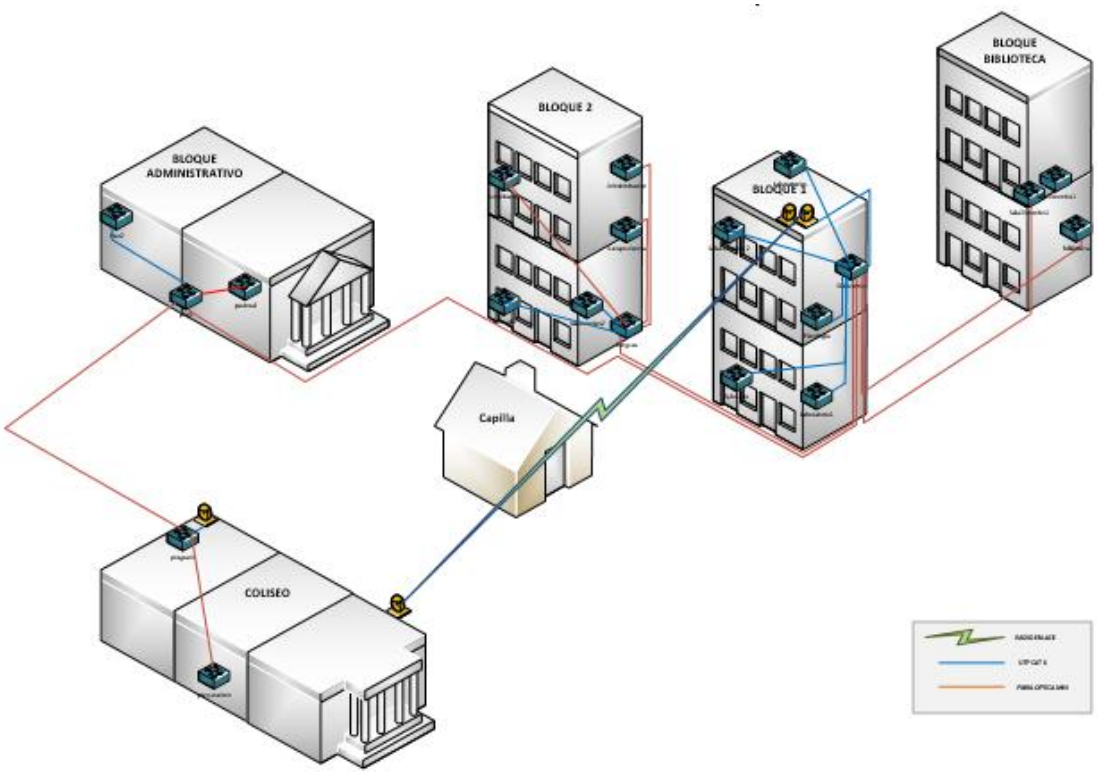

Ilustración 6. Ubicación geográfica e interconexión de bloques
Fuente: (Departamento de TI de la IES, 2018)

2.6.4 Servidores

En la empresa se cuenta con un servidor físico Nutanix SX-1065-G5, con 3 nodos cada uno con 7 TB dando un total de 21 TB de almacenamiento.

Además, hay 27 servidores virtuales, los mismos que tienen instalados los sistemas operativos: Windows 2008 R2, Linux Centos 7 y Server 2012.

Los servidores son monitoreados mediante el *software* VM*ware* 6,5 y el mismo es utilizado para la virtualización.

2.7 Esquema de seguridad de la información

La IES que se estudia, establece prioridades en cuanto a la seguridad de la información, con la finalidad de reducir riesgos, amenazas, y vulnerabilidades en la información que procesa la institución. Además, el esquema de seguridad tiene como base la normativa ISO/IEC 27002 para la gestión de la seguridad de la información.

En la empresa se han establecido políticas internas para el buen uso y manejo de la información, así como políticas de respaldos de la información en la web.

Se cuenta con un primer filtro que se realiza a través Equipo de respuesta a incidentes de seguridad o *Computer Incident Response Team* (CSIRT), este equipo pertenece a CEDIA la Red Nacional de Investigación y Educación Ecuatoriana.

CSIRT-CEDIA, apoya a los administradores en la gestión de la seguridad de la información, en la prevención de incidentes, tanto en lo técnico y organizacional. El servicio que brinda es recibir, atender y procesar los eventos de seguridad que ocurran en las redes del CSIRT-CEDIA.

En este primer filtro se previenen los ataques de *botnets*, que hoy en día son amenazas que están en crecimiento constante por el desarrollo que tiene el Internet de las Cosas (IoT). Esté filtro mediante notificaciones señala que tipo de amenazas se están produciendo y desde que IP se producen dichas *botnets*.

Provee asistencia en lo referente a aspectos como:

Servicios Reactivos:
Alertas y avisos
Manejo de Incidentes
Análisis de Incidentes
Respuesta a incidentes in-situ
Apoyo en respuesta a incidentes
Coordinación en respuesta a incidentes
Manejo de vulnerabilidades

Servicios Proactivos:
Vigilancia Tecnológica
Auditorías o evaluaciones de seguridad
Configuración y mantenimiento de Herramientas de Seguridad, Aplicaciones e Infraestructuras
Desarrollo de Herramientas de Seguridad
Servicios de Detección de Intrusos
Diseminación de Información relacionada con la Seguridad

Servicios de Gestión de la Calidad:
Consultorías de Seguridad
Concienciación sobre seguridad
Educación y entrenamiento en seguridad

En la siguiente ilustración se observa la estadística de la seguridad del reporte generado por el servicio CSIRT CEDIA; en el año 2017 es cuando más amenazas se presentaron, y en lo que va del presente año se puede ver que no se han identificado aún amenazas.

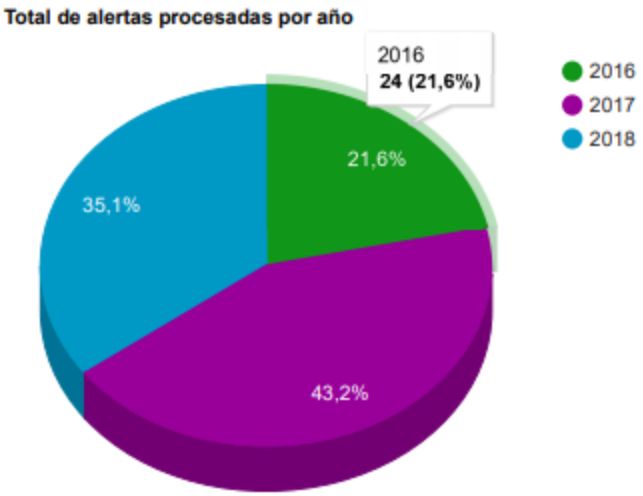

Ilustración 7. Alertas procesadas por año
Fuente: (Estadísticas de la IES) @ CSIRT CEDIA, 2019)

En el reporte con fecha 4 de abril del 2019, se presenta el total de alertas procesadas por tipo y año. Se puede contemplar que el tipo más común son incidentes por *sh-bots*.

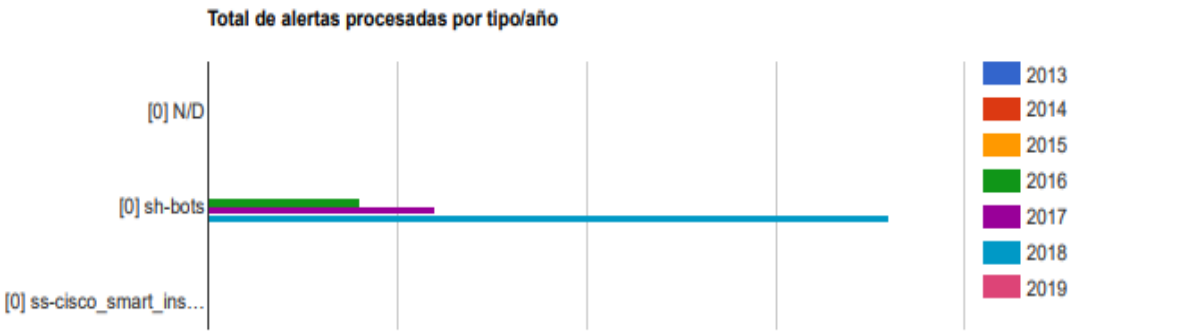

Ilustración 8. Alertas procesadas por tipo/año
Fuente: (Estadísticas de la IES @ CSIRT CEDIA, 2019)

2.7.1 Otras seguridades

Para prevenir incidentes, la empresa posee un sistema de seguridad perimetral con un *Firewall* perimetral, que bloquea las direcciones reportadas como amenazas al sistema de información.

Se mantiene el servicio de VPN IPSec de Amazon, para el control de aspectos de seguridad ya que por el momento se encuentra en proceso la migración de servicios a la nube.

Los servidores se manejan bajo los lineamientos y políticas para evitar ataques DoS o ataque de negación de servicio distribuido, también llamado DDoS de sus siglas *Distributed Denial of Service*.

Se tienen *switch* con enlaces redundantes y servidores con su propia encriptación.

Los equipos de escritorio tienen el antivirus *Kaspersky*, que tiene directivas de seguridad, controla *ransomware*, correo electrónico, proporciona así mismo estadísticas de los equipos con mayor número de infecciones.

2.8 Propuesta del diseño del modelo de seguridad bajo la perspectiva LAN-less

Para el diseño los servicios actuales bajo la perspectiva LAN-*less* segura para la comunicación de servicios *on premise* con servicios en la nube, se toman como referencia: el modelo de arquitectura de seguridad de la información propuesto por Killmeyer [11]; la metodología del desarrollo con CISCO; y las consideraciones de Scott Alan Miller, miembro técnico del NTG Lab con respecto al "*Brave New World of the LANless Future*", en las que se vislumbra a LAN-*less* no como futuro sino como presente, en que las empresas empiecen a mirar su red de área local como un dominio de seguridad, y dejar de lado el pensamiento centrado únicamente en LAN, como se señala en [10].

Considerando el contexto en el que se encuentra la presente investigación, se ha contemplado como referencia la Metodología CISCO por estar enfocada hacia el ciclo de vida de redes, permitiendo una visión para el diseño del modelo y su aplicabilidad durante el proceso de implementación del paradigma LAN-*less* en la IES objeto de estudio.

Esta metodología está conformada por seis fases y es conocida como PPDIOO (Preparación – Planificación – Diseño – Implementación – Operación – Optimización), [15].

A continuación, se detallan las fases del ciclo de vida de redes PPDIOO:

a) Preparación: Fase consistente en determinar el modelo de negocio para luego plantear un modelo de red de alto nivel.

b) Planificación: Fase encargada de realizar el levantamiento de toda la posible información de la red, revisando así su estado actual.

c) Diseño: En esta fase se presenta un diseño de la red fundamentado en el estado actual de la institución a realizarse, además el diseño propuesto debe ser sujeto a revisión junto con el cliente para mitigar fallas en el mismo.

d) Implementación: En esta fase la red es construida a partir del diseño propuesto en la fase anterior.

e) Operación: Es la fase donde la red es puesta en funcionamiento y sujeta a observaciones y monitoreo, garantizando así un correcto funcionamiento en la misma.

f) Optimización: En esta fase se solucionan los errores encontrados en la fase de operación, y de ser el caso, se plantea también un posible rediseño y si la red actual presenta muchos errores, es una fase de depuración.

Ilustración 9. Diagrama del ciclo de vida de la red según el modelo PPDIOO.
Fuente: tomado de [15]

A partir de lo referenciado y para dar seguimiento a la propuesta del diseño del modelo de seguridad de los servicios bajo la perspectiva LAN-*less* se proponen las siguientes fases:

Fase I: Identificación de los servicios actuales con los que cuenta la institución.

Fase II: Análisis de aquellos servicios que siguen un modelo centrados en LAN.

Fase III: Análisis de posibles vulnerabilidades y riesgos de estos servicios.

Fase IV: Diseño lógico de un modelo LAN-*less* que rompa esas zonas de confianza y permita asegurar los servicios.

Fase V: Análisis de la seguridad del diseño propuesto.

Fase VI: Análisis adicionales (*DevOps)*

2.9 Planteamiento del modelo de seguridad arquitectural implementando el paradigma LAN-*less* en la IES.

Para la contextualización de este caso en concreto, a continuación, se describen las fases para el planteamiento del modelo:

Fase I: Identificación de los servicios actuales con los que cuenta la institución.

Este aspecto puntualiza de manera sencilla los servicios con los que cuenta la IES, siendo estos los siguientes:

- Sistema Académico (Académico).
- Repositorio digital.
- Catálogo de servicios (Servicio de consulta web de libros).
- Sistema de reservas de laboratorio.
- SACI (Consultas, Financiero).
- SQUARENET (Consultas, Nómina).
- Controladora de dominio – Servicios de Active Directory
- Windows Azure..
- Página web.
- Moodle.

Fase II: Análisis de aquellos servicios que siguen un modelo centrados en LAN**.**

Los servicios que se presentan a continuación son aquellos que constan dentro del actual perímetro de seguridad de la IES

investigada, donde al ser este la red completa de la universidad, se asume que todos los *endpoints* o equipos clientes que interactúan con el mismo son realmente seguros y no posibles equipos hostiles a la red.

- Sistema Académico: Como anteriormente se lo menciona, este sistema se encarga del seguimiento del syllabus, reportes de tutorías, reportes de calificaciones, entre otros, al mismo tienen acceso tanto administrativos, docentes y estudiantes.
- Repositorio digital: Sistema encargado del almacenamiento y gestión de tesis, artículos publicados por docentes, acceden los docentes y administrador del servicio.
- Catálogo de servicios: Servicio de consulta web de libros.
- Sistema de Reservas de laboratorio: en este se realizan las reservas de salas y laboratorios por parte de los docentes.
- SACI: Software encargado del manejo financiero institucional (actualmente empleado solo para consultas).
- SQUARENET: Software encargado de realizar pagos y gestión del talento humano a nivel institucional (actualmente empleado solo para consultas).
- Controladora de dominio: Servicios de *Active Directory*, encargado de gestionar DNS, grupos de usuarios, permisos. Posee una réplica y a su vez se sincroniza con Windows Azure en la nube.

Cabe destacar que servicios tales como moodle, página *web* son sistemas almacenados en la nube con administración remota por parte del departamento de TI de la IES analizada.

Fase III: Análisis de posibles vulnerabilidades y riesgos de estos servicios

Para realizar una evaluación más objetiva, se han considerado los servicios como externos e internos, diferenciando así a aquellos servicios que también son públicos (*on premise*) de los que no lo son.

Servicios externos.

- Sistema Académico y repositorio digital: Son sistemas de uso público e interno, no poseen certificados *Secure Sockets Layer* (SSL), ni manejan ningún tipo de encriptación, cifrado u otra medida de seguridad en el *frontend*, por lo que en un modelo LAN-*centric* se tendrían que asegurar los dispositivos internos como externos que

interactúen con ellos, extendiendo así aún más el perímetro de seguridad de la red.

Servicios internos.

- Catálogo de servicios, SQUARNET, SACI, controladora de dominio y sistema de reservas de laboratorio: Son sistemas vulnerables a cualquier persona con acceso a las instalaciones de la universidad, debido a que se encuentran implementados bajo el modelo LAN–*centric* que asume que todos los dispositivos que interactúan con los servicios son seguros.

Fase IV: Diseño lógico de un modelo LAN-*less* que rompa esas zonas de confianza y permita asegurar los servicios.

Considerando la arquitectura de red con la que cuenta la IES en la actualidad, se propone un modelo de seguridad implementando el paradigma LAN-*less*, donde, los servidores se encuentren aislados físicamente de los equipos de red, siendo el *firewall* la única conexión y herramienta de gestión entre los servicios de la universidad y los equipos de red.

Este modelo estructural rescata el concepto de DMZ (*Demilitarized Zone)* y lo implementa junto con los demás servicios de la universidad, de tal manera que se tenga un segmento de red aislado exclusivo para ellos, facilitando así las tareas de aseguramiento y gestión de estos dispositivos y servicios, ofreciendo así a los usuarios finales exclusivamente los servicios y la información que estos requieren sin necesidad de que el usuario se entere de detalles técnicos por medio de su *endpoint* o la implementación del lado de la red (a través del *router*), de reglas de acceso a servicios poco eficientes en la red.

A continuación, se presentan gráficos del diseño lógico del modelo a manera de comparativa, considerando los modelos LAN-*centric* y LAN-*less*.

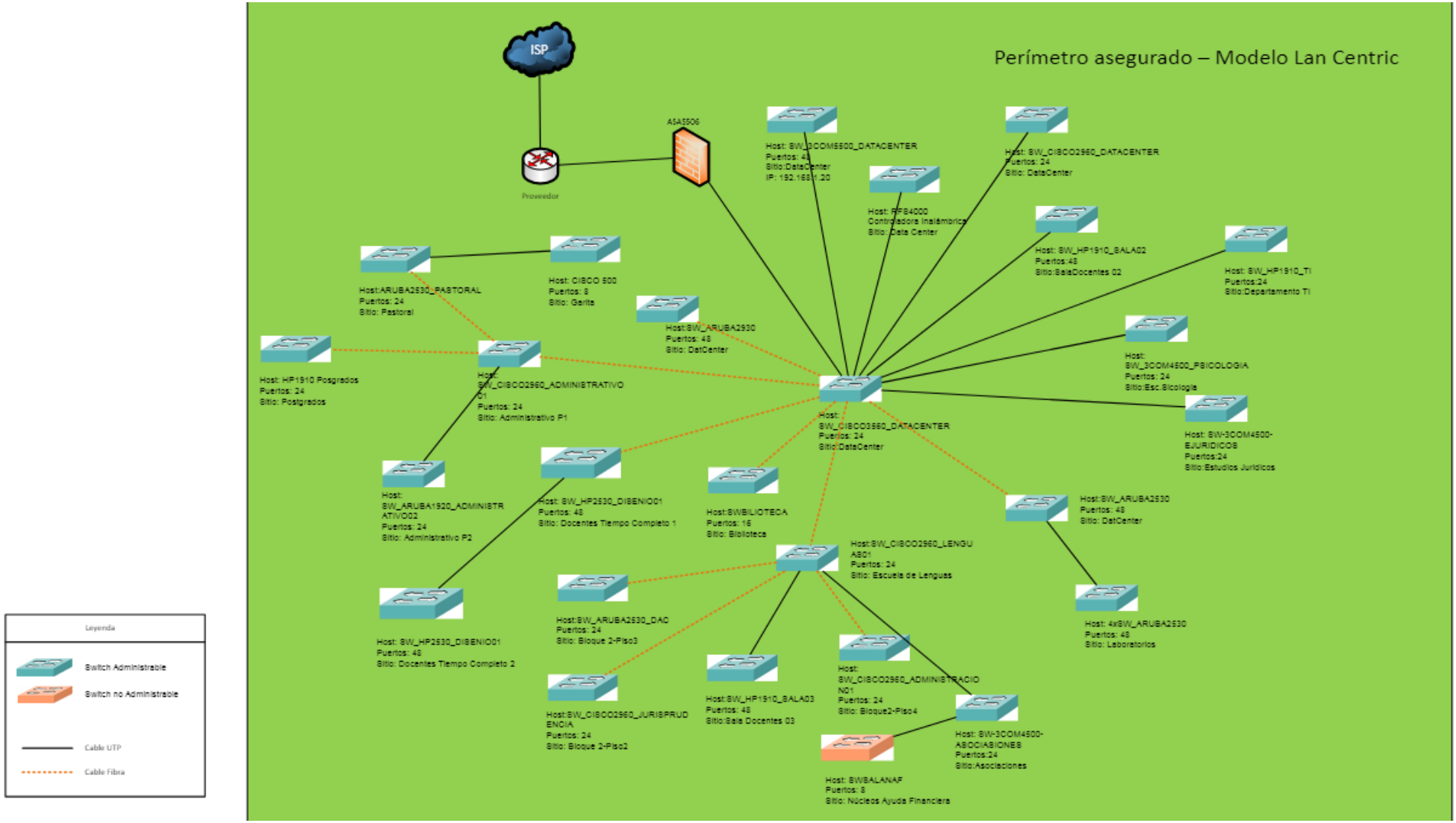

Ilustración 10. Diagrama lógico de red con el modelo LAN-*centric* (actual)
Fuente: elaboración propia a partir de (Departamento de TI de la IES, 2018)

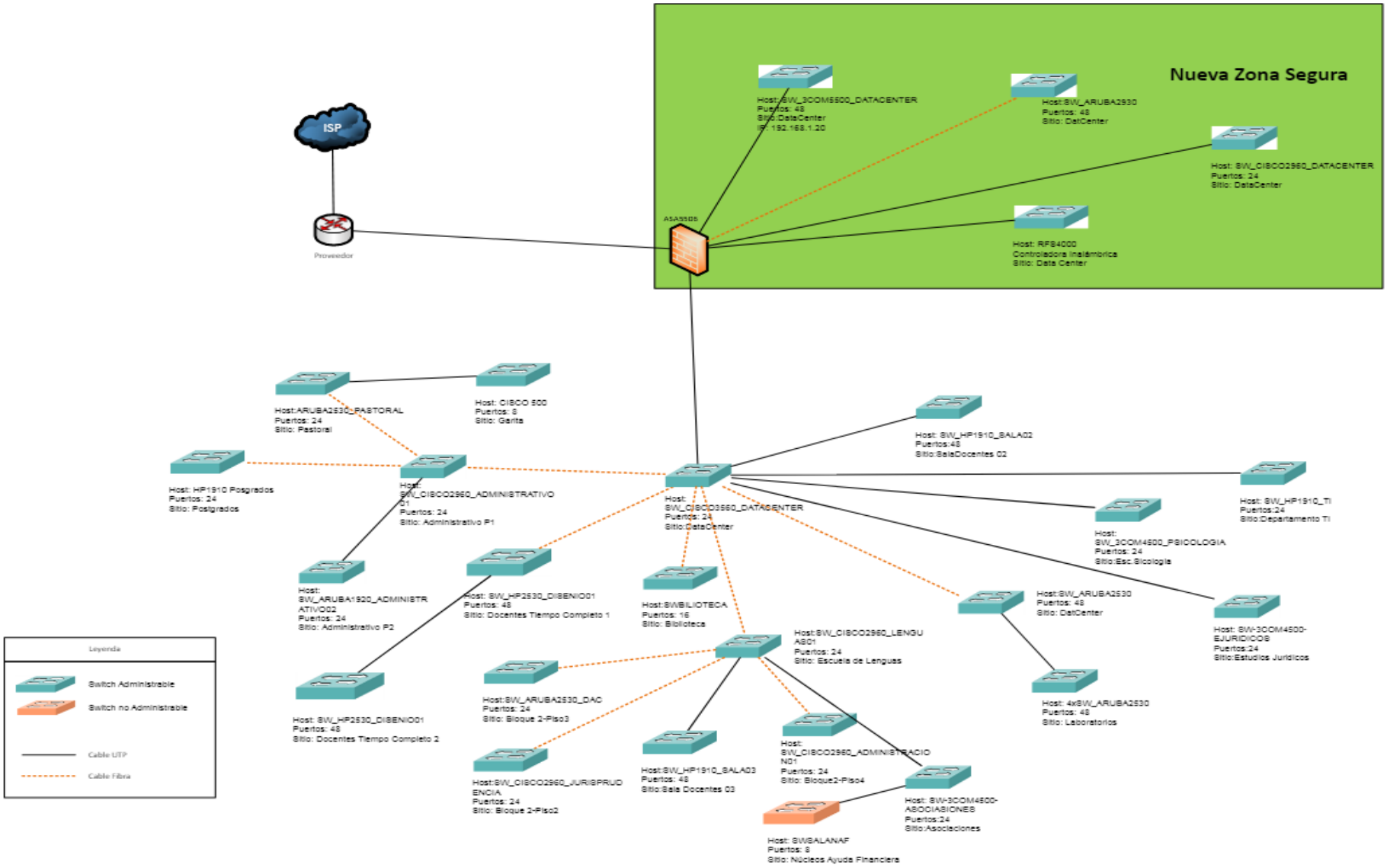

Ilustración 11. Diagrama lógico de red aplicando el modelo LAN-*less*.
Fuente: elaboración propia a partir de (Departamento de TI de la IES, 2018)

Esta propuesta contempla al *firewall* como principal gestor de Virtual LAN (VLAN) y reglas para administrar las *Virtual Memory System* (VMS) donde se encuentran asociados los servicios, mientras que las tareas de *Dynamic Host Configuration Protocol* (DHCP), enrutamiento, VLAN de oficinas, aulas, laboratorios y demás tareas de red seguirán siendo administradas por el *router* CISCO.

Fase V: Análisis de la seguridad del diseño propuesto.

El nuevo perímetro de seguridad de servicios de la IES en estudio, es de administración exclusiva del *firewall*, donde este, como principal y único actor, genera las VLAN y los permisos estrictamente necesarios para que los clientes administrados por el *router* CISCO sean capaces de consumir dichos servicios, de tal manera que estos no se vean involucrados de manera directa con el nuevo perímetro de seguridad que se plantea en este modelo, aislando así la red de los servidores.

De esta manera se logra limitar el perímetro de seguridad, asignando al firewall como principal y único partícipe de la seguridad de aquel nuevo segmento de red. Por su parte, en el lado de los clientes, los demás permisos y la red en general continúan siendo administrados por el *router* CISCO, mitigando así el impacto causado durante un hipotético proceso de migración al paradigma LAN-*less*.

Fase VI: Análisis adicionales (*DevOps)*

Considerando la solución para virtualización VM*ware* que posee la IES analizada, se propone además la implementación de *Docker* como principal gestor de aplicaciones y servicios, dando un gran salto en manejo de servicios TI, potenciando de esta forma la seguridad y el rendimiento en ejecución de estas aplicaciones, el modelo se representa gráficamente de la siguiente forma:

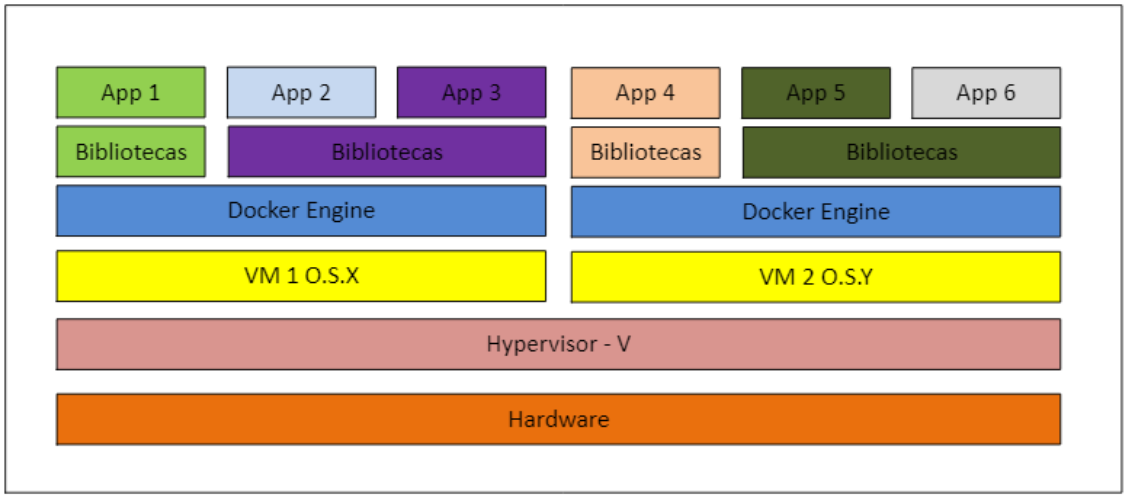

Ilustración 12 Arquitectura de aplicaciones implementando Docker junto con las ya existentes máquinas virtuales
Fuente: elaboración propia

Donde el *Hypervisor* – V es la solución para virtualizado VM*ware* que gestiona las diferentes máquinas virtuales, y a su vez, dentro de cada máquina virtual administrada por VM*ware* se tendrá un despliegue de contenedores ejecutando aplicaciones y diferentes servicios, de tal manera que se restrinja aún más el perímetro de seguridad de las aplicaciones y se optimice el rendimiento notoriamente de estas en función del *hardware* que actualmente se posee.

En adición a todo lo anteriormente mencionado, se sugiere que la administración del servidor a nivel de *Hypervisor* se de a través del uso de una única red y que sean las máquinas virtuales las que utilicen una o más VLAN (según los requerimientos del departamento de TI de la IES objeto de estudio).

En la red en general se recomienda el uso de reglas de *prerouting* según sea necesario, de tal manera que, a través del etiquetado de paquetes, se logre el redireccionamiento de determinadas redes a determinados servicios, de esta forma se ofrecen a los usuarios solamente los servicios que estos en verdad requieren.

3. Conclusiones

Sintetizando en función de la información recopilada de los modelos de arquitectura de red, los servicios *on premise* (aplicaciones locales), los servicios en la nube y, además, el análisis al que fue sujeta la red de la IES objeto de estudio, se puede afirmar que, la implementación de un modelo LAN-*less* es factible y altamente viable en el contexto en el que se encuentra actualmente la arquitectura de red y los servicios con los que cuenta la universidad.

Por medio de este postulado se logró llegar a las siguientes conclusiones:

Los modelos de seguridad de la información varían según acontecen las nuevas necesidades tecnológicas, a pesar de ello, el modelo LAN-*less* no busca saltarse lineamientos de los modelos de seguridad de la información tradicionales, en lugar de ello busca exactamente lo mismo, pero de forma más sencilla, limitando así el sector donde verdaderamente se deben enfocar los administradores de red y, por ende, mitigando así el riesgo de recibir cualquier tipo de ataque.

A criterio propio, el estado actual de la seguridad informática con la que cuenta la IES estudiada, brinda la seguridad tecnológica adecuada, sin embargo, bajo la perspectiva de este nuevo paradigma y considerando que el Ecuador en los últimos meses ha subido posiciones en el ranking de países que mayor número de ciberataques reciben, se plantea la implementación de un modelo LAN-*less* en la institución, ya que al reducir de forma considerable el perímetro de seguridad de los servicios como se ha planteado durante el desarrollo de esta investigación, se pretende mitigar otro tipo de riesgos, y dificultar aún más la explotación de posibles vulnerabilidades facilitando además la administración de redes y servicios.

El modelo de arquitectura de seguridad propuesto para el desarrollo de esta investigación consistió en aislar los servicios de la red en general, ubicándolos en un nuevo segmento de red situado detrás del *firewall*, de tal manera que dicho segmento de red se convierta en el nuevo perímetro de seguridad implementando el modelo LAN-*less*.

Para el caso práctico de la IES que cuenta con un *firewall*, y un *router* para administrar la red, el modelo LAN-less propuesto en esta investigación resulta altamente factible debido a que, al ser el propio *firewall* el encargado de la administración de este nuevo segmento de red, es el mismo quien también administra de forma directa los servicios *on premise*, vía IPSEC por ejemplo, asegurando la comunicación entre los servicios en la nube, los clientes y los servicios internos de la universidad.

Durante el desarrollo de esta investigación se pudo constatar que las estrategias empleadas para el cumplimiento de los objetivos fueron las correctas. La obtención del material bibliográfico necesario para la fundamentación teórica de esta investigación, el análisis al que fue sujeto la red de la IES objeto de estudio, la identificación de los servicios, luego identificar los puntos críticos para después plantear cómo estos serían migrados e implementados bajo el paradigma LAN-*less*, todos estos aspectos fueron concretados de forma exitosa, afirmando así el cumplimiento de la metodología y los objetivos de este proyecto investigativo.

Como recomendación final y a más de la implementación sugerida de tecnología de contenedores *Docker*, se propone también como trabajo futuro el uso de *kubernetes* como herramienta principal para el despliegue automatizado y fácil escalabilidad de todos los contenedores, siendo aún más seguro y eficiente el desempeño de aplicaciones dockerizadas en la institución.

4. Glosario

4.1 LAN (Local Area Network)

Red de área local, que desde sus inicios ha sido la base para la comunicación. - Redes pequeñas que se utilizan en empresas, formada por un conjunto de equipos conectados dentro de una misma área geográfica, para el autor Abril [8], las arquitecturas de área local se escogen con la finalidad de lograr la máxima eficacia del diseño de la red y alcanzar un mejor costo beneficio.

Las LAN en su desarrollo se enfocan bajo LAN-*less*, Travis [16], señala que dicha Lan-*less* es un paradigma que permite diseñar una red, bajo la concepción de menos red; Este paradigma reduce el perímetro de seguridad que es enorme en una LAN tradicional y abarca todos los dispositivos conectados a la red, hoy en día significa más que una LAN local, ya que al reducir el perímetro de seguridad ya solo abarca servicios de red.

4.2 Modelos de despliegue en la nube

Hoy en día se han extendido estos modelos de despliegue de la computación en la nube, así Pérez [17], los clasifica en: Público, Privado, Comunitario e Híbrido, cada uno con sus ventajas de aplicación.

En estos modelos se hace referencia también a términos como los que se señalan a continuación:

4.3 VPN (V*irtual Private Network*)

Las VPN como mecanismos de seguridad, no puede hacer que las conexiones en línea sean completamente anónimas, pero se pueden configurar con la finalidad de aumentar la privacidad y la seguridad de la información y así evitar la divulgación de información privada, las VPN permiten el acceso remoto autenticado mediante protocolos de túnel y técnicas de encriptación, que hacen que la comunicación sea fiable y con un nivel de seguridad de los datos que se envían en la red.

4.4 *Cloud Computing*

Paradigma que permite ofrecer servicios tecnológicos a través de la red, Internet. Pérez [17], señala las ventajas y desventajas de *cloud computing*, con la premisa de mejora continua de los servicios y la disponibilidad inmediata y el manejo de la seguridad punto clave para expandir su uso en las empresas y organizaciones, cuyos retos y oportunidades se fundamentan principalmente en la seguridad y privacidad de los datos [18]. La computación en nube se fundamenta en varios pilares [19]: SaaS (Software como Servicio), IaaS (Infraestructura como Servicio, PaaS (Plataforma como Servicio), virtualización y

almacenamiento, cada vez la informática es más potente y su consumo no tiene límites.

4.5 On premise

On premise quiere decir en la organización, los datos pueden existir en la organización o fuera de ella, puede ser en una nube privada, la organización cliente establece un entorno de virtualización en sus propios servidores, en cualquiera de sus propios centros de datos o en los de un proveedor de servicios [18].

4.6 Virtualización

Como manifiesta Pérez [17], se puede considerar a la virtualización como un modelo de gobierno directo, en la que el cliente de una nube privada, pasa a tener un alto grado de control sobre los aspectos físicos y lógicos de la seguridad de la infraestructura de la nube con la ventaja de que será más fácil para el cliente cumplir los estándares, políticas y regulación de la seguridad. En una nube privada, la organización cliente establece un entorno de virtualización en sus propios servidores, en cualquiera de sus propios centros de datos o en los de un proveedor de servicios.

4.7 Docker

Tecnología de código abierto para el despliegue automatizado de aplicaciones ejecutándose dentro de contenedores que brindan una capa adicional para virtualizado de diferentes sistemas operativos [20].

4.8 VM*ware*

Solución para virtualizado

4.9 Kubernetes

Tecnología de código abierto desarrollada para el despliegue, escalado y manejo de aplicaciones dockerizadas.

4.10 VLAN (*Virtual* LAN)

Red virtual, lógica e independiente de la red física.

4.11 Botnet

Las *botnets* son redes de computadores infectados por software malicioso controlados por un atacante de forma remota, usualmente son usados para la ejecución de ataques DDoS. El malware que infecta a los equipos suele ser comercializado por lo que a menudo el concepto de *botnet* tiende ser ligado un tipo de *malware* en específico, sin embargo, existen decenas de *botnets* disponibles en el mercado negro del ciberespacio [21].

5. Bibliografía

[1] «La importancia de la seguridad informática en las instituciones gubern». [En línea]. Disponible en: http://www.eumed.net/rev/caribe/2016/11/seguridad.html. [Accedido: 04-mar-2019].

[2] P. Marqués, «Los riesgos de Internet. Consejos para su uso seguro. Habilidades necesarias para utilizar internet.», p. 9.

[3] R. V. Roque Hernández, C. M. Juárez Ibarra, R. V. Roque Hernández, y C. M. Juárez Ibarra, «Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios», *PAAKAT Rev. Tecnol. Soc.*, vol. 8, n.º 14, 2018.

[4] «El número de usuarios de Internet en el mundo crece un 9,1% y alcanza los 4.388 millones (2019)», *Marketing 4 Ecommerce - Tu revista de marketing online para e-commerce*, 31-ene-2019. [En línea]. Disponible en: https://marketing4ecommerce.net/usuarios-internet-mundo/. [Accedido: 05-mar-2019].

[5] J. Reyes, C. Muñoz, y T. Guarda, «Seguridad Informática para Pequeñas y Medianas Empresas de la Provincia de Santa Elena», p. 10.

[6] E. De Luis, «Introducción a los fundamentos de la seguridad informática», *La seguridad para los menores en internet*. [En línea]. Disponible en: http://reader.digitalbooks.pro/book/preview/102400/id_ch_2. [Accedido: 26-mar-2019].

[7] S. M. Q. Zambrano y D. G. M. Valencia, «Seguridad en informática: consideraciones», *Dominio Las Cienc.*, vol. 3, n.º Extra 3, pp. 676-688, 2017.

[8] A. F. Abril, «Modelo de Arquitectura de Seguridad de la Información (MASI)», 2011.

[9] P. Saritama, «Diseño e implementación de un modelo de arquitectura de seguridad de la información para el área de infraestructura tecnológica del Cuerpo de Bomberos del Distrito Metropolitano de Quito.», Universidad Central del Ecuador, 2016.

[10] A. M. Scott, «The Brave New LANless Future», *MangoLassi.it*, 24-oct-2016. [En línea]. Disponible en: https://mangolassi.it/topic/11257/scott-alan-miller-the-brave-new-lanless-future. [Accedido: 01-mar-2019].

[11] J. Killmeyer, *Information Security Architecture: An Integrated Approach to Security in the Organization, Second Edition - PDF Free Download*. .

[12] «ISO 27018 La primera normativa para la privacidad en la nube». [En línea]. Disponible en: https://www.isotools.org/2017/03/23/iso-27018-la-primera-normativa-la-privacidad-la-nube/. [Accedido: 30-mar-2019].

[13] J. A. Nuñez, «Normas ISO de ciberseguridad en la nube». [En línea]. Disponible en: http://www.webdox.cl/blog/es/normas-iso-de-ciberseguridad-en-la-nube. [Accedido: 30-mar-2019].

[14] ISOTools, «La norma ISO 27001: Aspectos claves de su diseño e implantación», 2017. [En línea]. Disponible en: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf. [Accedido: 11-oct-2018].

[15] Network Direction, «Network Lifecycle», *Network Direction*. .

[16] D. Travis, «LANLess explained.», *MangoLassi*, 14-oct-2017. [En línea]. Disponible en: https://mangolassi.it/topic/15325/lanless-explained/5. [Accedido: 02-abr-2019].
[17] J. G. Pérez, «Calidad de servicios en la nube en combinación con el internet de las cosas: revisión sistemática de la literatura y modelo de calidad», Universidad de Cuenca, Cuenca, 2017.
[18] L. J. Aguilar, «Computación en la Nube e innovaciones tecnológicas», p. 22.
[19] J. T. Valdés, «Computo en la nube: instrumento y objeto del derecho», p. 13.
[20] Docker, «Enterprise Container Platform | Docker», *Docker, Sitio oficial*. [En línea]. Disponible en: https://www.docker.com/. [Accedido: 04-jun-2019].
[21] D. Fisher, «¿Qué es un botnet? – Kaspersky Daily | Blog oficial de Kaspersky», 25-abr-2018. [En línea]. Disponible en: https://www.kaspersky.es/blog/que-es-un-botnet/755/. [Accedido: 04-jun-2019].