Elaboración de una Propuesta Integral para la Implementación de una Infraestructura de Red Definida por Software (SDN) con Cisco ACI para la Empresa Seguridad Perimetral Henry Marín.

Alberto Bermúdez Blanco

Abstract: ***Seguridad Perimetral Henry Marín currently operates on a traditional network infrastructure characterized by manual configurations, limited segmentation, and the absence of a centralized control model. This approach has generated difficulties in scaling services, maintaining consistent policies, implementing granular security mechanisms, and responding efficiently to incidents. The objective of this study was to design an integral proposal for the implementation of a Software-Defined Network (SDN) infrastructure based on Cisco Application Centric Infrastructure (ACI), in order to modernize operations, strengthen internal security, and improve business continuity. The research, applied in nature and with a descriptive and propositional approach, used direct observation, technical review of the infrastructure, interviews with network personnel, and comparative analysis with standards such as ISO/IEC 27001, NIST CSF, and CIS Controls. The results revealed significant gaps in microsegmentation, traffic visibility, automation, and policy consistency. Based on this diagnosis, a technical proposal was developed integrating a Leaf–Spine physical architecture, a logical model built on tenants, VRFs, Bridge Domains, and Endpoint Groups, and microsegmentation and access control policies through Contracts. The adoption of Cisco ACI emerges as the most suitable solution to reduce operational complexity, eliminate repetitive manual configurations, enhance security through a Zero Trust approach, and enable scalable and standardized growth. The study concludes that transitioning to an SDN architecture with Cisco ACI represents a strategic step toward strengthening operational resilience and aligning network management with international best practices.***

Resumen: ***La empresa Seguridad Perimetral Henry Marín opera actualmente sobre una infraestructura de red tradicional basada en configuraciones manuales, segmentación limitada y ausencia de un modelo centralizado de control. Este enfoque ha generado dificultades para escalar servicios, mantener políticas consistentes, aplicar mecanismos de seguridad granular y responder de manera eficiente ante incidentes. El objetivo del estudio fue diseñar una propuesta integral para implementar una infraestructura de Red Definida por Software (SDN) basada en Cisco Application Centric Infrastructure (ACI), con el fin de modernizar la operación, fortalecer la seguridad interna y mejorar la continuidad del negocio. La investigación, de tipo aplicada y con un enfoque descriptivo y propositivo, utilizó observación directa, revisión técnica de la infraestructura, análisis comparativo con estándares como ISO/IEC 27001, NIST CSF y CIS Controls. Los resultados evidenciaron brechas relevantes en microsegmentación, visibilidad del tráfico, automatización y consistencia de políticas. A partir de este diagnóstico, se desarrolló una propuesta técnica que integra una arquitectura física Leaf and Spine, un modelo lógico basado en tenants, VRF, Bridge Domains y Endpoint Groups, y políticas de microsegmentación y control de acceso mediante Contracts. La adopción de Cisco ACI se presenta como la solución más adecuada para reducir la complejidad operativa, eliminar configuraciones manuales repetitivas, mejorar la seguridad mediante un enfoque Zero Trust y habilitar un crecimiento escalable y estandarizado. El estudio concluye que la transición hacia una arquitectura SDN con Cisco ACI constituye un paso estratégico para fortalecer la resiliencia operativa y alinear la gestión de la red con las mejores prácticas internacionales.***

Palabras Clave: Software-Defined Networking (SDN), Cisco ACI, microsegmentation, network security, Leaf–Spine architecture

I. INTRODUCCIÓN

La empresa Seguridad Perimetral Henry Marín mantiene su operación sobre una infraestructura de red tradicional basada en configuraciones manuales y dispositivos gestionados de forma independiente. Este modelo ha sido funcional en etapas iniciales, pero presenta limitaciones importantes frente a las necesidades actuales de escalabilidad, seguridad y continuidad operativa. La falta de automatización, la baja granularidad en la segmentación interna y la ausencia de un plano de control centralizado dificultan aplicar políticas consistentes, responder con eficiencia ante incidentes y garantizar una gestión estable conforme aumenta la demanda tecnológica.

El avance de las Redes Definidas por Software (SDN) ha transformado los modelos de administración de red al separar el plano de control del plano de datos, permitiendo una gestión centralizada y dinámica. En este contexto, Cisco Application Centric Infrastructure (ACI) se consolida como una alternativa robusta que combina

automatización, segmentación lógica mediante políticas y un modelo de operación orientado a las aplicaciones. La implementación de Cisco ACI permite mejorar la visibilidad del tráfico, reducir errores derivados de configuraciones manuales y fortalecer la seguridad mediante microsegmentación y control granular de flujos.

La necesidad de modernizar la arquitectura actual llevó al desarrollo de una propuesta técnica basada en SDN con Cisco ACI, orientada a mejorar la disponibilidad, la flexibilidad y la protección de los servicios críticos de la empresa. La introducción de este modelo busca alinear la infraestructura con estándares reconocidos internacionalmente, optimizar los procesos operativos y establecer una base tecnológica capaz de soportar el crecimiento futuro de la organización. Este estudio presenta el análisis del entorno actual y la propuesta integral que permite avanzar hacia una arquitectura de red más segura, escalable y eficiente.

II. Fundamentos conceptuales de SDN y Cisco ACI

1. ¿Por qué las Redes Definidas por Software (SDN) representan una mejora significativa frente a la infraestructura de red tradicional utilizada actualmente por la empresa?

La infraestructura de red tradicional de la empresa Seguridad Perimetral Henry Marín se basa en configuraciones manuales, dispositivos gestionados de forma independiente y una segmentación limitada, lo que genera dificultades para escalar, mantener políticas consistentes y responder de manera eficiente ante incidentes. En este modelo, el plano de control y el plano de datos operan de forma distribuida, lo cual incrementa la complejidad operativa y el riesgo de configuraciones inconsistentes.

Las Redes Definidas por Software (SDN) abordan estas limitaciones mediante la separación del plano de control y el plano de datos, centralizando la gestión a través de controladores que administran políticas y comportamientos de red de manera uniforme. Este enfoque permite automatizar tareas repetitivas, reducir errores asociados a configuraciones manuales y mejorar la capacidad de adaptación ante cambios operativos o de seguridad. La tesis evidencia que la empresa requiere mayor escalabilidad, visibilidad del tráfico y mecanismos de segmentación granular, aspectos que el enfoque SDN satisface mediante políticas centralizadas, abstracción de servicios y operación basada en la lógica de la aplicación.

En este contexto, la adopción de Cisco ACI, como implementación avanzada de SDN, representa una mejora significativa al introducir automatización, microsegmentación, control basado en políticas y una arquitectura eficiente Leaf–Spine que facilita el crecimiento, la resiliencia y la seguridad de la infraestructura.

Tabla 1: Diferencias redes SDN

Categoría	Tradicional	APIC
Gestión de la red	Configuración manual equipo por equipo.	Administración centralizada desde un controlador APIC.
Escalabilidad	Limitada, requiere configuración física y manual en cada dispositivo.	Alta, permite añadir recursos y servicios de forma automatizada y rápida.
Seguridad	Basada en dispositivos perimetrales y reglas locales.	Seguridad integrada mediante segmentación lógica (tenants, VRF, EPG) y políticas globales.
Tiempo de implementación	Elevado, con riesgo de errores humanos.	Reducido, gracias a la automatización y plantillas de configuración.
Flexibilidad	Cambios lentos y con impacto operativo.	Cambios dinámicos sin afectar la disponibilidad del servicio.

1.1 Evolución del modelo tradicional hacia las Redes Definidas por Software (SDN)

La infraestructura de red tradicional utilizada por la empresa Seguridad Perimetral Henry Marín se caracteriza por configuraciones manuales, dispositivos administrados de forma aislada y una dependencia directa del plano de control distribuido. Este modelo, aunque funcional en etapas iniciales, presenta limitaciones significativas en escalabilidad, seguridad y eficiencia operativa. La necesidad de aplicar cambios repetitivos en múltiples equipos incrementa el riesgo de inconsistencias, mientras que la segmentación limitada dificulta el aislamiento adecuado de servicios críticos.

Las Redes Definidas por Software (SDN) surgen como una respuesta a estas restricciones mediante la separación del plano de control y el plano de datos, permitiendo que las decisiones de enrutamiento, políticas y comportamiento de tráfico se centralicen en un controlador. Este enfoque aporta mayor coherencia en la administración, facilita la automatización de tareas y reduce la probabilidad de errores derivados de configuraciones manuales. Además, proporciona una visión integral del entorno, lo cual mejora la capacidad de análisis y respuesta ante incidentes. En el contexto de la

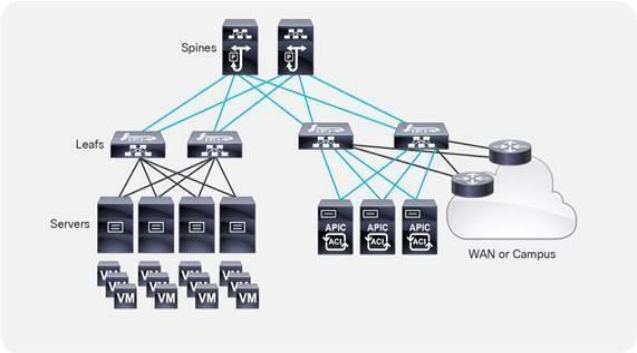
empresa, la adopción del enfoque SDN se alinea con la necesidad de modernizar la infraestructura para enfrentar mayores niveles de demanda, garantizar la continuidad del negocio y fortalecer la seguridad interna a través de un control más granular y dinámico.

1.2 Arquitectura Leaf and Spine como base estructural de Cisco ACI.

Cisco ACI adopta la arquitectura Leaf–Spine como fundamento estructural del fabric, permitiendo superar las limitaciones de los modelos jerárquicos tradicionales. En este diseño, todos los switches Leaf se conectan directamente a todos los switches Spine, asegurando trayectorias uniformes y predecibles para cualquier flujo de tráfico. Esto elimina la dependencia de capas intermedias y evita cuellos de botella que son comunes en infraestructuras tradicionales, donde la comunicación entre dispositivos puede requerir múltiples saltos o atravesar nodos saturados.

Esta arquitectura mejora la eficiencia operativa al ofrecer baja latencia, alto ancho de banda y capacidad de procesamiento paralelo. Además, su naturaleza modular permite escalar la red incorporando nuevos equipos Leaf o Spine sin necesidad de reconfigurar completamente la infraestructura existente. En la tesis se destaca que este modelo brinda mayor estabilidad y facilita la adopción de políticas centralizadas a través del controlador APIC, permitiendo que la automatización, la visibilidad del tráfico y la microsegmentación se integren de manera nativa en la operación diaria. De esta forma, el diseño Leaf and Spine no solo optimiza el rendimiento, sino que proporciona la base necesaria para implementar un entorno seguro, flexible y preparado para el crecimiento futuro de la organización.

Ilustración 1: Topologia SDN ACI



1.3 Modelo lógico de Cisco ACI: Tenants, VRF, Bridge Domains y Endpoint Group

El modelo lógico de Cisco ACI constituye uno de los componentes centrales de la propuesta técnica desarrollada en la tesis, ya que permite estructurar la red en capas lógicas que separan funciones, aislan servicios y aplican políticas de manera controlada y coherente. Este modelo supera las limitaciones de la red tradicional de la empresa, en la cual la segmentación es limitada y no existe un aislamiento eficiente entre servicios o flujos de datos. ACI introduce una organización basada en políticas y objetos abstractos que permiten un control detallado y automatizado del tráfico interno.

1.4 *Tenants como estructura de separación lógica*

Los Tenants constituyen la unidad lógica que agrupa configuraciones, políticas y recursos dentro del fabric. La tesis propone un esquema de tres Tenants: Producción, Administrativo y Seguridad, cada uno con su propio ámbito operativo. Esto permite separar responsabilidades, aislar funciones críticas y mejorar la gobernanza de políticas de red.

El uso de Tenants asegura que los cambios realizados en un entorno no afecten a otros, promoviendo prácticas de seguridad y mantenimiento más robustas.

1.5 VRF como mecanismo de aislamiento de enrutamiento

El documento especifica que cada Tenant contará con uno o más VRF (Virtual Routing and Forwarding) para separar completamente las tablas de enrutamiento. Esto evita que el tráfico entre ambientes se cruce, garantizando independencia total de rutas y protegiendo servicios sensibles como el Tenant de Seguridad .

Esta separación no es posible en la arquitectura tradicional utilizada por la empresa, lo que demuestra la ventaja del modelo propuesto.

1.6 Bridge Domains como contenedores de políticas de capa 2

Cada segmento de red se define como un Bridge Domain asociado a un VRF. Los BD permiten controlar ARP, flooding y gateways distribuidos, elementos esenciales para gestionar el comportamiento del tráfico interno y evitar la propagación indiscriminada dentro del dominio de capa 2 .

La segmentación mediante BD resuelve el problema identificado en el diagnóstico del capítulo 4, donde la red actual presenta dominios amplios de difícil control.

1.7 Endpoint Groups (EPG) como núcleo de la segmentación

Los EPG agrupan servidores, dispositivos o endpoints que comparten una función o rol. La tesis detalla ejemplos específicos como EPG-Web, EPG-BaseDatos, EPG-Aplicaciones, EPG-Usuarios, EPG-CCTV/IoT y EPG-Seguridad .

Los EPG permiten aplicar políticas individualizadas, incluso cuando los endpoints comparten la misma VLAN física, habilitando una microsegmentación profunda indispensable para eliminar movilidad lateral.

1.8 Contracts como mecanismo de control de acceso granular

Los Contracts determinan qué comunicación está permitida entre EPG. Reemplazan la complejidad de las ACL tradicionales y aplican el principio explícito de "nada se comunica si no se define".

La tesis además indica que los contratos restrictivos reducen la superficie de ataque al requerir definiciones explícitas para cada flujo permitido, lo cual fortalece el enfoque Zero Trust nativo de ACI.

III. DIAGNÓSTICO DE LA INFRAESTRUCTURA DE RED ACTUAL

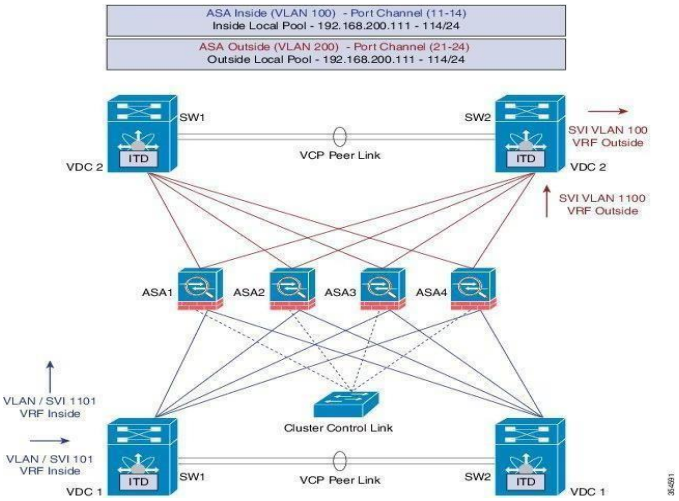
El análisis de la infraestructura de red existente en Seguridad Perimetral Henry Marín constituye un paso fundamental para determinar la viabilidad y pertinencia de la transición hacia una arquitectura basada en Cisco ACI. La tesis evidencia que la red actual opera bajo un modelo tradicional, donde las configuraciones manuales, la gestión distribuida y la falta de segmentación avanzada han generado limitaciones significativas en términos de seguridad, escalabilidad y eficiencia operativa. A partir de una revisión técnica exhaustiva, se identifican múltiples brechas que justifican la necesidad de modernizar la arquitectura tecnológica.

3 LIMITACIONES DEL MODELO TRADICIONAL UTILIZADO POR LA ORGANIZACIÓN

La infraestructura actual presenta una dependencia fuerte de configuraciones manuales realizadas dispositivo por dispositivo. Esto incrementa el riesgo de errores humanos, dificulta la estandarización de políticas y prolonga los tiempos de respuesta ante incidentes o cambios operativos. La ausencia de un plano de control centralizado obliga a que la administración se realice de forma aislada en cada equipo, generando inconsistencias, configuraciones heterogéneas y una complejidad creciente en la operación diaria.

Asimismo, el modelo tradicional dificulta la aplicación de medidas avanzadas de seguridad, ya que la segmentación se limita a VLANs amplias y estáticas sin mecanismos para controlar la movilidad lateral o aplicar políticas dinámicas basadas en roles. Esta limitación expone a la organización a riesgos mayores, especialmente en servicios críticos.

Ilustración 2: Topología red actual



3.1 Problemas de visibilidad, monitoreo y control del tráfico

El diagnóstico identifica que la empresa carece de herramientas avanzadas para visualizar el comportamiento del tráfico en tiempo real, analizar patrones anómalos o monitorear eventos dentro de la red con granularidad. La red tradicional opera con capacidades limitadas de telemetría, lo que dificulta la identificación temprana de incidentes y afecta la capacidad de realizar ajustes proactivos.

La falta de visibilidad integrada provoca que problemas operativos o de rendimiento sean detectados tardíamente y que las acciones correctivas dependan de procesos manuales de revisión, lo cual compromete la continuidad de los servicios.

3.2 Brechas de seguridad y exposición a amenazas internas

El análisis señala la ausencia de mecanismos adecuados de microsegmentación y control de acceso granular. La red tradicional mantiene dominios amplios, donde múltiples servicios comparten segmentos, aumentando la posibilidad de desplazamientos laterales no autorizados en caso de una intrusión.

Este escenario contrasta con las necesidades actuales de seguridad, donde se requieren controles más estrictos, segmentación dinámica y políticas basadas en identidad o función. La tesis identifica que esta falta de aislamiento interno incrementa la superficie de ataque y expone a la organización a incidentes que pueden comprometer la disponibilidad y la integridad de los servicios.

3.3 Restricciones de escalabilidad y crecimiento tecnológico

El diagnóstico también evidencia que la arquitectura existente no soporta adecuadamente el crecimiento de servicios, usuarios o cargas de trabajo. Cada nueva expansión implica configuraciones manuales complejas, ajustes en múltiples dispositivos y riesgo de interrupciones operativas.

La empresa requiere una infraestructura que permita: ampliaciones modulares, incorporación de nuevos servicios sin reconfiguraciones extensivas, automatización en el aprovisionamiento, mayor soporte para virtualización y cargas dinámicas.

El modelo actual no cumple con estos requerimientos, lo que limita la innovación y la modernización tecnológica.

Elemento	Definición	Función principal
Tenant	Unidad lógica que agrupa y aísla configuraciones de red, políticas y recursos dentro del fabric.	Segmentar la infraestructura para distintos clientes, áreas de negocio o entornos (producción, pruebas, desarrollo).
VRF (Virtual Routing and Forwarding)	Tabla de enrutamiento virtual que permite mantener rutas independientes dentro de un Tenant.	Garantizar separación de tráfico y rutas entre diferentes redes lógicas, evitando que se crucen o interfieran.
Bridge Domain (BD)	Segmento de capa 2 asociado a una o más subredes IP.	Controlar el dominio de broadcast y definir el alcance de comunicación en capa 2 dentro del fabric.
EPG (Endpoint Group)	Conjunto lógico de endpoints (servidores, VMs, dispositivos) que comparten las mismas políticas.	Facilitar la aplicación centralizada de políticas de seguridad, QoS y comunicación entre grupos de endpoints.
Contract	Conjunto de reglas que definen cómo pueden comunicarse dos EPG.	Establecer políticas de filtrado, control de tráfico y seguridad entre diferentes grupos de endpoints.
Filter	Lista de criterios (protocolos, puertos, direcciones) usada dentro de un Contract.	Definir condiciones específicas para permitir o denegar comunicación.
Application Profile	Contenedor lógico que agrupa EPGs y sus relaciones de comunicación.	Organizar de forma lógica los componentes de una aplicación y sus flujos de tráfico dentro del Tenant.

Tabla 2: Elementos Logicos

La Tabla 2 presenta un marco de referencia clave para identificar los elementos lógicos principales de una estructura de red definida por software:

3.4 Impacto operativo y limitaciones en la continuidad del negocio

La combinación de configuraciones manuales, visibilidad limitada y segmentación insuficiente afecta directamente la continuidad de operaciones. Los tiempos de resolución de incidentes son mayores, la recuperación ante fallos es más lenta y las tareas de mantenimiento requieren interrupciones prolongadas o ventanas de cambio más frecuentes.

Esto resulta especialmente crítico para los servicios de seguridad perimetral, donde la indisponibilidad o degradación de la red puede afectar la prestación de servicios esenciales. El diagnóstico concluye que la continuidad operativa requiere una arquitectura más resiliente, automatizada y alineada con mejores prácticas internacionales.

3.5 Ausencia de automatización y dependencia de procesos manuales

La tesis señala que uno de los mayores problemas en la red actual es la dependencia de configuraciones manuales, realizadas directamente en cada equipo. Esta condición genera:

- riesgo elevado de errores humanos,
- falta de uniformidad en políticas,
- imposibilidad de aplicar cambios masivos de manera controlada,
- retrasos en la respuesta operativa,
- limitaciones para mantener versiones de configuración homogéneas.

Además, la ausencia de automatización impide ejecutar tareas repetitivas como creación de VLAN, asignación de subredes, actualización de ACL o aprovisionamiento de servicios con tiempos previsibles. Esta situación afecta la estabilidad y reduce la eficiencia general del equipo técnico.

.

3.6 Inconsistencias en la aplicación de políticas y configuraciones

Al revisar los equipos, observé que existen diferencias notables entre políticas de seguridad, configuraciones de puertos, listas de acceso y parámetros operativos. Estas inconsistencias no son intencionales, sino producto del trabajo manual acumulado a lo largo del tiempo. Esta heterogeneidad compromete la confiabilidad de la red, dificulta auditorías internas y limita la capacidad de aplicar buenas prácticas de forma uniforme.

3.7 Limitaciones en la segmentación y aislamiento entre servicios

Constaté que múltiples servicios conviven dentro de los mismos segmentos, lo cual incrementa el riesgo de propagación de incidentes y dificulta aplicar controles basados en roles o funciones específicas. La falta de segmentación avanzada es uno de los aspectos más críticos identificados, ya que impide establecer límites claros entre aplicaciones, usuarios y dispositivos.

3.8 Dificultad para integrar nuevas tecnologías y ambientes virtualizados

La infraestructura actual no está diseñada para integrarse de manera eficiente con tecnologías modernas. Verifiqué que no existe soporte adecuado para ambientes virtualizados o dinámicos, ni para modelos híbridos que combinen múltiples entornos. La rigidez del modelo tradicional limita la incorporación de nuevas soluciones y debilita la capacidad de la organización para innovar.

IV. PROPUESTA TÉCNICA BASADA EN CISCO ACI

A partir del diagnóstico que desarrollé previamente, diseñé una propuesta técnica orientada a transformar la infraestructura de red tradicional de Seguridad Perimetral Henry Marín hacia un modelo definido por software basado en Cisco Application Centric Infrastructure (ACI). Esta solución responde directamente a las limitaciones identificadas, integrando automatización, segmentación avanzada, control mediante políticas y una arquitectura escalable que alinea la operación de red con mejores prácticas internacionales de ciberseguridad.
La propuesta que presento se estructura en dos dimensiones principales:

a) el diseño físico del fabric ACI (arquitectura Leaf–Spine), y
b) el modelo lógico basado en Tenants, VRF, Bridge Domains, Endpoint Groups y Contracts

.
Ambos componentes trabajan en conjunto para proporcionar una plataforma robusta, flexible y con la capacidad de soportar el crecimiento tecnológico de la organización.

4.1 Diseño físico del fabric: Arquitectura Leaf–Spine

La arquitectura física que propongo está conformada por una topología Leaf adn Spine, donde todos los switches Leaf se conectan directamente a todos los switches Spine. Este diseño garantiza rutas uniformes, baja latencia y una mayor tolerancia a fallos, ya que la comunicación entre cualquier par de dispositivos se realiza siempre mediante dos saltos predecibles.

Cada Leaf actúa como punto de acceso para servidores, firewalls, sistemas de seguridad y dispositivos de borde, mientras que los Spines funcionan como núcleo del fabric, conmutando el tráfico y manteniendo una conectividad estable y uniforme. Este enfoque permite escalabilidad horizontal: es posible agregar nuevos nodos sin afectar servicios ya desplegados, lo que resulta esencial para el crecimiento de la empresa.

Asimismo, el fabric se gestiona desde el clúster de controladores APIC, los cuales aplican políticas, distribuyen configuraciones y permiten automatizar procesos que antes se realizaban manualmente en cada dispositivo. Esto soluciona directamente la falta de estandarización y la dependencia operativa que identifiqué en la infraestructura actual.

4.2 Separación operativa mediante Tenants

En mi propuesta definí un esquema de Tenants que permite separar lógicamente los diferentes ambientes de operación. Cada Tenant agrupa políticas, servicios y configuraciones específicas, asegurando que las decisiones de seguridad y operación no se mezclen entre entornos.
Para cumplir con los requerimientos de la empresa estructuré tres Tenants principales:

- Tenant de Producción: destinado a los servicios esenciales.
- Tenant Administrativo: orientado a sistemas internos y de apoyo.
- Tenant de Seguridad: enfocado en cámaras, dispositivos de vigilancia y sistemas críticos.

Esta distribución mejora la gobernanza y el aislamiento, y soluciona la falta de segmentación avanzada identificada en la red actual.

4.3 Aislamiento de enrutamiento mediante VRF

Cada Tenant incluye uno o más VRF (Virtual Routing and Forwarding), lo cual garantiza separación total en el plano de enrutamiento. Este aislamiento impide que un servicio pueda comunicarse con otro sin autorización explícita, reduciendo la superficie de ataque y eliminando rutas innecesarias.

El uso de VRF es fundamental para evitar que los ambientes se crucen o que se generen dependencias no deseadas. Esto responde directamente a las brechas de seguridad que detecté en la infraestructura actual.

4.4 Estructura de segmento mediante Bridge Domains

Para administrar dominios de capa 2, definí Bridge Domains (BD) asociados a cada VRF. Cada BD agrupa subredes específicas y controla el comportamiento de tráfico interno, incluyendo ARP, flooding y gateways distribuidos.
En la infraestructura actual identifiqué que existen dominios amplios y poco controlados. Con los BD, cada segmento queda correctamente delimitado, permitiendo aislar servicios y mejorar la estabilidad operativa. Además, los BD facilitan la integración con gateways distribuidos propios de ACI, evitando cuellos de botella tradicionales.

4.5 Organización funcional mediante Endpoint Groups (EPG)

Los Endpoint Groups son el corazón del modelo lógico de ACI. En mi propuesta, cada servicio o grupo de dispositivos relevantes se organiza dentro de un EPG según su función y sus requisitos de seguridad.
Algunos de los EPG que definí son:

- EPG-Web
- EPG-Bases de Datos
- EPG-Aplicaciones
- EPG-Usuarios
- EPG-CCTV/IoT
- EPG-Seguridad

Esta estructura permite establecer políticas diferenciadas incluso dentro de la misma subred física, habilitando microsegmentación real y efectiva. Gracias a los EPG, un incidente en una aplicación no afecta a otros servicios, eliminando una de las principales vulnerabilidades del modelo tradicional.

4.6 Control explícito de comunicación mediante Contracts

Para definir qué flujos están permitidos entre EPG, utilicé Contracts, un mecanismo central de ACI que reemplaza las listas de acceso manuales. Los Contracts permiten establecer reglas basadas en protocolos, puertos y funciones específicas.
En mi diseño, los Contracts funcionan bajo el principio de "deny by default": ninguna comunicación está permitida si no se especifica. Esta filosofía soluciona la falta de controles explícitos que identifiqué en la red tradicional, y al mismo tiempo se alinea con estándares modernos de ciberseguridad como Zero Trust.

4.7 Automatización, telemetría y operación centralizada

Finalmente, la automatización nativa de ACI resuelve la dependencia de procesos manuales identificada en la infraestructura actual. La plataforma permite aprovisionar servicios desde APIC, implementar cambios masivos en minutos y aplicar políticas de manera centralizada.
Asimismo, la telemetría avanzada de ACI habilita monitoreo continuo, análisis de flujos, alertas en tiempo real y capacidad predictiva, elementos ausentes en la red actual y que fortalecen la continuidad del negocio.

V. PLAN DE IMPLEMENTACIÓN Y ALINEAMIENTO CON ESTÁNDARES DE CIBERSEGURIDAD

Con base en la propuesta técnica que presenté en la sección anterior, elaboré un plan de implementación estructurado que permite ejecutar la transición hacia Cisco ACI de forma ordenada, controlada y alineada con las mejores prácticas internacionales en materia de seguridad. Este plan se diseñó para minimizar riesgos operativos, garantizar la continuidad del negocio y asegurar que cada fase contribuya al fortalecimiento de la arquitectura tecnológica de Seguridad Perimetral Henry Marín.

El plan se organiza en etapas secuenciales que permiten validar cada avance antes de continuar con la siguiente fase, reduciendo el impacto de posibles fallos y facilitando la adopción progresiva del modelo definido por software.

5.1 Fase 1: Preparación y verificación de la infraestructura

En la primera fase defino todas las actividades necesarias para asegurar que el entorno físico y lógico esté listo para recibir el fabric ACI. Esto incluye la verificación del espacio en rack, energía redundante, compatibilidad con los enlaces ópticos, revisión del cableado y confirmación de que los equipos requeridos cumplen con las especificaciones técnicas establecidas.

También realizo la validación de versiones de software, licenciamiento y requisitos mínimos del clúster APIC para garantizar una puesta en marcha estable.

Durante esta etapa verifico las dependencias de la red actual, identificando segmentos críticos y rutas indispensables para planificar correctamente la migración sin afectar servicios esenciales.

5.2 Fase 2: Implementación inicial del fabric y configuración del clúster APIC

En esta fase realizo la instalación inicial del fabric Leaf–Spine. Conecto los enlaces entre los nodos Spine y los nodos Leaf, configuro los parámetros fundamentales del APIC y establezco la comunicación básica del tejido. Posteriormente, procedo con:

- La creación del fabric,
- La incorporación de cada equipo al clúster,
- La validación de la topología descubierta,
- Y la confirmación del correcto registro de todos los componentes.

Esta fase es crítica, ya que constituye el fundamento sobre el cual se desplegarán los Tenants, VRF, Bridge Domains y EPG definidos en la propuesta técnica.

5.3 Fase 3: Configuración del modelo lógico y creación de políticas

En esta etapa construyo la estructura lógica completa dentro del APIC. Esto incluye:

- La creación de los Tenants definidos en la propuesta,
- El aprovisionamiento de VRF,
- La configuración de Bridge Domains,
- La asignación de subredes,
- La creación de EPG para servicios, usuarios y sistemas de seguridad,
- Y la implementación de Contracts bajo el principio de “deny by default”.

El objetivo de esta fase es establecer la base del control de acceso y la segmentación granular que solucionará las brechas identificadas en el diagnóstico. Además, aquí preparo los mecanismos de microsegmentación y las políticas de comunicación explícita entre servicios.

5.4 Fase 4: Integración de servicios, migración y pruebas

Una vez que el modelo lógico está validado, inicio la integración de servicios:

- Conecto servidores y dispositivos a los puertos Leaf,
- Muevo cargas de forma gradual hacia los EPG correspondientes,
- Verifico flujos de tráfico por medio de pruebas controladas,
- Y ajusto los Contracts según los requerimientos específicos de cada servicio.

La migración se realiza de manera progresiva para evitar interrupciones. Cada servicio se prueba en condiciones reales antes de continuar con la siguiente carga. Este enfoque me permite garantizar estabilidad y corregir configuraciones con mínima afectación al negocio.

5.5 Fase 5: Verificación operativa, optimización y puesta en producción

Durante esta fase ejecuto pruebas finales de conectividad, rendimiento, redundancia y seguridad. Utilizo las herramientas de telemetría del APIC para identificar flujos anómalos, validar patrones de tráfico y optimizar políticas.

Una vez que todos los componentes han sido validados, procedo con la puesta en producción del fabric. Aquí documento configuraciones, preparo manuales operativos y elaboro lineamientos para la administración diaria de ACI, garantizando una transición ordenada para el equipo técnico.

5.6 Alineamiento con estándares de ciberseguridad: ISO 27001, NIST y CIS Controls

Durante la elaboración del plan confirmé que la arquitectura ACI se alinea naturalmente con marcos de ciberseguridad ampliamente utilizados. En particular:

- ISO/IEC 27001 se refleja en el control de acceso segmentado, la gestión centralizada de políticas y la capacidad de auditar cambios de forma estructurada.
- NIST Cybersecurity Framework se ve reforzado por la visibilidad del tráfico, la telemetría avanzada, la segmentación y los mecanismos de respuesta basados en políticas.
- CIS Controls encuentran cumplimiento en la microsegmentación, el inventario automatizado de activos (endpoints), la gestión de configuración y el monitoreo continuo.
- El enfoque Zero Trust se implementa mediante el modelo de EPG, Contracts explícitos y eliminación de comunicación no autorizada entre servicios.

Estos marcos fortalecen la postura de seguridad, asegurando que la infraestructura no solo mejore tecnológicamente, sino que también cumpla con lineamientos formales de protección de la información.

5.7 Beneficios operativos del plan de implementación

Al ejecutar este plan de manera ordenada, garantizo:

- Una migración controlada y sin interrupciones,

- Una reducción significativa de riesgos operativos,
- Una transición eficiente desde el modelo tradicional hacia sdn,
- Y una adopción real de mecanismos de seguridad modernos.

De esta forma aseguro que la implementación de Cisco ACI no solo responda a necesidades técnicas, sino también estratégicas para la continuidad y el crecimiento del negocio.

VI. Discusión

A partir del análisis realizado, confirmo que la transición hacia una arquitectura definida por software basada en Cisco ACI responde de forma directa y eficaz a las limitaciones identificadas en la infraestructura de red actual. La centralización del control mediante APIC y la automatización de procesos representan un avance significativo frente al modelo tradicional, caracterizado por configuraciones manuales y una alta probabilidad de inconsistencias operativas. Desde mi perspectiva, esta automatización no solo optimiza la gestión diaria, sino que también reduce riesgos asociados al error humano y mejora la disponibilidad del servicio.

En materia de seguridad, la microsegmentación mediante EPG y Contracts introduce un nivel de control que la red tradicional no puede ofrecer. El enfoque de comunicación explícitamente permitida se alinea con principios de Zero Trust y fortalece de manera sustancial la protección interna contra movimientos laterales y accesos no autorizados. Este cambio permite subsanar las brechas más críticas detectadas durante el diagnóstico inicial.

Asimismo, la arquitectura Leaf and Spine aporta una base sólida para escalar servicios sin la necesidad de reconfiguraciones complejas o interrupciones operativas. Considero que esta capacidad de crecimiento modular es esencial para garantizar que la red pueda adaptarse a las demandas futuras de la organización y a la incorporación de nuevas tecnologías.

Por otra parte, la integración de telemetría y monitoreo continuo en ACI habilita un modelo operativo más preventivo que reactivo, permitiéndome anticipar incidentes y tomar decisiones basadas en información precisa. Esta característica complementa la estrategia general de fortalecimiento de la seguridad y la eficiencia operativa.

En conjunto, los resultados obtenidos demuestran que la adopción de Cisco ACI no solo resuelve las limitaciones técnicas presentes, sino que transforma la infraestructura de red en un componente estratégico para la continuidad y modernización de los servicios institucionales.

VII. Conclusión

A partir del análisis que realicé sobre la infraestructura de red de Seguridad Perimetral Henry Marín, confirmo que el modelo tradicional presenta limitaciones significativas en automatización, seguridad, visibilidad y capacidad de crecimiento. Estas brechas representan riesgos operativos y estratégicos que afectan directamente la continuidad del negocio y la estabilidad de los servicios.

La propuesta técnica basada en Cisco ACI que desarrollé demuestra ser una alternativa sólida para superar estas limitaciones. La adopción de una arquitectura definida por software permite centralizar la administración, estandarizar políticas y reducir la dependencia de procesos manuales. La microsegmentación mediante EPG y Contracts fortalece la seguridad interna y habilita un enfoque alineado con Zero Trust, mientras que la arquitectura Leaf–Spine ofrece una base escalable y estable para soportar el crecimiento tecnológico futuro.

Asimismo, el plan de implementación por fases garantiza una transición ordenada y segura, minimizando interrupciones y permitiendo validar cada etapa antes de avanzar. La integración con estándares como ISO 27001, NIST y CIS Controls reafirma que la solución no solo es técnicamente viable, sino coherente con marcos internacionales de ciberseguridad.

En conjunto, concluyo que la adopción de Cisco ACI representa un avance estratégico para la organización, al modernizar la infraestructura, mejorar la postura de seguridad y aumentar la eficiencia operativa, posicionando a la red como un habilitador clave para la continuidad y el desarrollo institucional.

VIII Referencias

[1] Arias, F. (2012). *El proyecto de investigación: Introducción a la metodología científica* (6.ª ed.). Editorial Episteme.

[2] Bernal, C. A. (2010). *Metodología de la investigación: Administración, economía, humanidades y ciencias sociales* (3.ª ed.). Pearson Educación.

[3] Bernal, J. (2022). Clasificación de activos digitales en pymes de desarrollo software. *Revista Tecnológica*, 35(2), 45–60.

[4] Cisco. (2018). *Cisco ACI inter-VRF tenant route leaking design simplified*. https://community.cisco.com/t5/data-center-

and-cloud-blogs/cisco-aci-inter-vrf-tenant-route-leaking-design-simplified/ba-p/3820919

[5] Cisco. (2020). *Cisco Application Centric Infrastructure design guide.* https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-application-centric-infrastructure-design-guide.html

[6] Cisco. (2021). *Cisco Nexus 7000 Series Intelligent Traffic Director configuration guide.* https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/itd/configuration/guide/b-Cisco-Nexus-7000-Series-Intelligent-Traffic-Director-Configuration-Guide/m-itd-appendix.html

[7] Cisco. (2023a). *Data Center Application Centric Infrastructure (DCACI) training*. https://www.cisco.com/site/us/en/learn/training-certifications/training/courses/dcaci.html

[8] Cisco. (2023b). *Cisco ACI fundamentals*. https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/aci-fundamentals.html

[9] Cisco. (2023c). *Cisco ACI security best practices*. https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/application-policy-infrastructure-controller-apic/217427-cisco-aci-security-best-practices.html

[10] Cisco. (2023d). *Cisco ACI multi-site architecture*. https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-aci-multi-site-architecture.html

[11] Cisco. (2024). *Cisco ACI and zero trust security*. https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-744624.html



Alberto Bermudez Blanco

Cedula: 1-1722-0130,
beto.an.2498@gmail.com
Estudiante del postgrado de la Maestría Profesional en Ciberseguridad.
Universidad Internacional San Isidro Labrador, San José , Costa Rica, 2025