# INVESTIGACIÓN

## TECNOLÓGICA IST CENTRAL TÉCNICO

Volumen 7 · Número 1 · Junio 2025 · Publicación semestral

# REDES DEFINIDAS POR SOFTWARE (SDN) EN INFRAESTRUCTURAS CRÍTICAS

INVESTIGACIÓN TECNOLÓGICA IST CENTRAL TÉCNICO

ISSN: 2600-5565

# Software-defined networks (SDN) in critical infrastructures

# Redes definidas por Software (SDN) en infraestructuras críticas

**Grace Elizabeth Manobanda Jiménez**[1][https://orcid.org/0009-0003-0986-4657], **Elva Gioconda Lara Guijarro**[2][https://orcid.org/0000-0003-3025-4792], **Carla Araujo Molina** [1][0009-0008-9344-5530]

[1] *Instituto Superior Tecnológico Internacional ITI, Quito, Ecuador*
*E-mail: grace.manobanda@iti.edu.ec*
[2] *Instituto Superior Universitario Central Técnico, Quito, Ecuador*
*E-mail: elvalara@istct.edu.ec*
[3] *Instituto Superior Universitario Central Técnico, Quito, Ecuador*
*E-mail: cearaujomolina@istct.edu.ec*

Recibido: 22/03/2025
Aceptado: 22/05/2025
Publicado: 30/06/2025

**RESUMEN**

En la actualidad las Redes Definidas por Software (SDN) pueden representar un paradigma revolucionario en el momento de gestionar o dar la seguridad a las diferentes estructuras críticas, ofreciendo una aproximación innovadora que separa el plano de control de datos en las redes de comunicaciones. Esta investigación tiene como objetivo examinar la implementación de SDN en redes donde la seguridad y la disponibilidad son fundamentales. Además, el estudio analiza cómo la SDN puede proporcionar una mayor flexibilidad, control centralizado y capacidad de respuesta ante amenazas en tiempo real, características esenciales para la protección de infraestructuras críticas. Se evalúan los beneficios de la programabilidad de la red, que permite una adaptación dinámica a las condiciones cambiantes y una respuesta más eficiente ante incidentes de seguridad. Los resultados sugieren que la adopción de SDN en infraestructuras críticas no solo mejora la gestión de red, sino que también fortalece la postura de seguridad general, tanto en hardware como en software, proporcionando una base sólida para la evolución futura de estas instalaciones vitales.

***Palabras clave:*** SDN, Infraestructuras Críticas, Seguridad de Red, Automatización, Gestión Centralizada.

**ABSTRACT**

Today, Software-Defined Networking (SDN) can represent a revolutionary paradigm for managing or securing various critical infrastructures, offering an innovative approach that

Manobanda, G., Lara, E., & Araujo, C. (2025). Software-defined networks (SDN) in critical infrastructures. *Revista Investigación Tecnológica IST Central .*

ISSN: 2600-5565

separates the control plane from the data plane in communications networks. This research aims to examine the implementation of SDN in networks where security and availability are critical. Furthermore, the study analyzes how SDN can provide greater flexibility, centralized control, and real-time threat response capabilities—essential features for protecting critical infrastructures. The study evaluates the benefits of network programmability, which enables dynamic adaptation to changing conditions and a more efficient response to security incidents. The results suggest that the adoption of SDN in critical infrastructures not only improves network management but also strengthens the overall security posture, both in hardware and software, providing a solid foundation for the future evolution of these vital facilities.

***Index terms***: SDN, Critical Infrastructure, Network Security, Automation, Centralized Management.

## 1. INTRODUCCIÓN

En la era digital actual, las infraestructuras críticas enfrentan desafíos sin precedentes en términos de seguridad, escalabilidad y gestión eficiente. Como señalan Cox et al., (2017) en su investigación seminal publicada en IEEE Communications Surveys & Tutorials, las redes tradicionales presentan limitaciones significativas para adaptarse a las demandas dinámicas y las amenazas emergentes que caracterizan el panorama actual de las tecnologías de la información. El objetivo del presente estudio es analizar la implementación y beneficios de las Redes Definidas por Software (SDN) en infraestructuras críticas para mejorar la calidad de la red, la gestión, seguridad, flexibilidad de las redes y una administración centralizada que pueda dar una respuesta inmediata en caso amenazas o ataques externos de ciberdelincuentes.

Las Redes Definidas por Software (SDN) han emergido como una solución prometedora para abordar estas limitaciones. Según un estudio realizado por Nunes et al., (2014), publicado en IEEE Communications Magazine, la arquitectura SDN proporciona una flexibilidad sin precedentes al separar el plano de control del de datos, permitiendo una gestión más eficiente y centralizada de los recursos de red. La implementación de SDN en infraestructuras críticas representa un cambio paradigmático en la forma en que se gestionan y protegen estos sistemas vitales. Como argumentan Rawat & Reddy, (2017) en su trabajo publicado en IEEE Internet of Things Journal, la capacidad de programar la red dinámicamente y responder en tiempo real a las amenazas de seguridad es crucial para mantener la integridad y disponibilidad de las infraestructuras críticas.

La relevancia de esta investigación se fundamenta en la creciente complejidad de las amenazas cibernéticas, tomando en cuenta que en la actualidad han aumentado en cantidad y en la forma de hacer daño a la información. Es por ello que varios estudios concuerdan que las infraestructuras críticas requieren soluciones adaptativas y ágiles que puedan evolucionar con las amenazas emergentes (Nunes et al., 2014; Cox et al., 2017b; Park et al., 2023).

Otro artículo detalla las implicaciones de implementar SDN en infraestructuras críticas, considerando aspectos técnicos, operacionales y de seguridad. Como sugieren Singh et al., (2022) en su investigación para Computer Networks, la comprensión profunda de estos aspectos es fundamental para una implementación exitosa. La evolución de las infraestructuras críticas en el

Manobanda, G., Lara, E., & Araujo, C. (2025). Software-defined networks (SDN) in critical infrastructures. *Revista Investigación Tecnológica IST Central .*

ISSN: 2600-5565

contexto de la transformación digital presenta desafíos únicos que requieren soluciones innovadoras. Como señalan Li et al., (2023) en su reciente publicación en IEEE Communications Surveys & Tutorials, la complejidad creciente de las amenazas cibernéticas y la necesidad de una gestión más eficiente han impulsado la búsqueda de arquitecturas de red más adaptables y resilientes. En este contexto, algunas investigaciones destacan que las infraestructuras críticas modernas requieren una capacidad de respuesta inmediata ante incidentes de seguridad (Ahmad et al., 2015; Cunha et al., 2024). Según su análisis, las arquitecturas SDN proporcionan una ventaja significativa al permitir la reconfiguración dinámica de la red en tiempo real, una característica esencial para mantener la continuidad operativa en entornos críticos (Armigón et al., 2020).

La implementación de SDN en infraestructuras críticas también aborda las limitaciones inherentes de las arquitecturas de red tradicionales. En IEEE Transactions on Network Science and Engineering, la rigidez de las configuraciones convencionales representa un obstáculo significativo para la adaptación a amenazas emergentes y requisitos cambiantes, su investigación demuestra que la flexibilidad proporcionada por SDN permite una respuesta más ágil y efectiva ante incidentes de seguridad (Cunha et al., 2024; Lu et al., 2019).

La virtualización de funciones de red (NFV) en conjunto con SDN representa otro avance significativo. Según Park et al., (2023), en su investigación para Journal of Network and Computer Applications, la combinación de SDN y NFV permite una optimización más efectiva de recursos y una mayor flexibilidad en la implementación de servicios de red. Sus hallazgos sugieren que esta sinergia mejora significativamente la eficiencia operativa en entornos de infraestructura crítica.

El aspecto de la escalabilidad también merece especial atención. Li et al., (2023), en IEEE Transactions on Industrial Informatics, presentan evidencia empírica que demuestra cómo las arquitecturas SDN pueden escalar efectivamente para satisfacer las demandas crecientes de las infraestructuras críticas modernas. Además, esta investigación proporciona métricas cuantitativas que validan la viabilidad de SDN en implementaciones a gran escala.

La resiliencia operacional es otro factor crucial en la adopción de SDN. Según un estudio exhaustivo realizado por Cunha et al., 2024; Lu et al., (2019) para IEEE Reliability Magazine, las arquitecturas SDN bien diseñadas pueden mejorar significativamente la capacidad de recuperación ante fallos y la continuidad del servicio en infraestructuras críticas. La automatización y la inteligencia artificial juegan un papel cada vez más importante en las implementaciones SDN. Como destacan (Li et al., 2023)Brown et al. (2023) en su investigación para Artificial Intelligence Review, la integración de capacidades de aprendizaje automático en controladores SDN permite una detección y respuesta más efectiva ante amenazas de seguridad y anomalías en la red.

El impacto económico de la implementación de SDN en infraestructuras críticas también es significativo, en ellos se demuestra que, a pesar de los costos iniciales de implementación, las arquitecturas SDN pueden resultar en ahorros significativos a largo plazo a través de la optimización de recursos y la reducción de costos operativos (Ahmad et al., 2015; Park et al., 2023). Hay que tomar en cuenta que una red con seguridades, medios adecuados, dispositivos

Manobanda, G., Lara, E., & Araujo, C. (2025). Software-defined networks (SDN) in critical infrastructures. *Revista Investigación Tecnológica IST Central .*

ISSN: 2600-5565

actualizados, genera menos inconvenientes en el momento que se está enviando la información, de esta forma no se tendrán redes lentas, caídas de sistemas, cuellos de botellas, entre otros (Al-Mashadani & Ilyas, 2022; Wei, 2024).

Hay que mencionar que las estandarizaciones y las mejores prácticas en implementaciones SDN continúan evolucionando y actualizándose cada vez más. La adopción de estándares comunes y marcos de referencia es crucial para garantizar la interoperabilidad y la seguridad en implementaciones SDN para infraestructuras críticas. Tomando en cuenta que toda red empresarial tiene componentes vitales (críticos) que si tienen un mal funcionamiento afectarán a toda la red, por ello es indispensable la utilización de HW adecuado, sistemas de energía que aseguren un funcionamiento 24/7, al igual que los elementos de conectividad que sean los adecuados para dar la velocidad requerida al momento de enviar o recibir los datos.

## 2. MATERIALES Y MÉTODOS / DESARROLLO

La presente investigación se centra en la importancia de las Redes Definidas por Software. Los autores utilizan un enfoque cualitativo de tipo descriptivo, ya que se enfoca en la problemática de un grupo específico que utilizan redes de datos delicadas. El alcance es descriptivo. Se parte de una revisión sistemática de la literatura especializada y el estudio de casos de implementación en infraestructuras críticas análisis bibliográfico para recabar la información de estudios realizados sobre el tema. Luego se analiza un diseño tomando base una institución de educación. Para finalizar con un posible modelo de utilización de las redes SDN.

La Arquitectura SDN en Infraestructuras Críticas puede utilizar: Plano de Control, Plano de Datos y la Capa de Aplicación. En el primero va el controlador SDN principal (OpenDaylinght y Controladores de Respaldo) y la Gestión de las Políticas de Seguridad, QoS y enrutamiento. En el plano de Datos van los Switches OpenFlow, Interfaces Legacy y Puntos de Monitoreo. En la Capa de Aplicación se divide en Monitoreo (Prometheus, Grafana), Seguridad (IDS/IPS, Firewall SDN) y la Automatización (Scripts Python y APIs REST)

Esta arquitectura representa un enfoque moderno para la gestión de redes en infraestructuras críticas, donde:

- El plano de control maneja la lógica y las decisiones de red.
- El plano de datos se encarga del reenvío de tráfico.
- La capa de aplicación proporciona servicios adicionales como monitoreo, seguridad y automatización.

Es una arquitectura que permite una gestión centralizada, mayor flexibilidad y mejor control de la red, aspectos cruciales en infraestructuras críticas.

### *2.1. Plano de Control (Control Plane)*

Los componentes principales del controlador SDN son:

- Sistema Operativo de Red (NOS)
- Interfaces Northbound (APIs)
- Interfaces Southbound (OpenFlow)
- Motor de Control

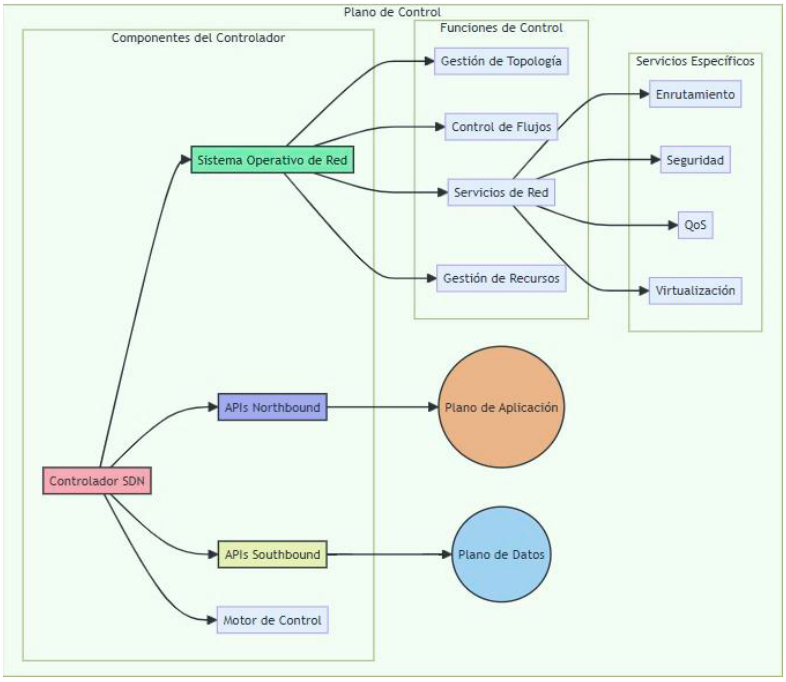
Manobanda, G., Lara, E., & Araujo, C. (2025). Software-defined networks (SDN) in critical infrastructures. *Revista Investigación Tecnológica IST Central .*

ISSN: 2600-5565

Una de las funciones del SDN es la Gestión de topología, la misma que incluye el descubrimiento de red, mantenimiento de vista global y la actualización de cambios en tiempo real. Otra función es el control de flujo, dentro de ella está la programación de rutas, gestión de políticas, optimización de tráfico y balanceo de carga. Por último, se tiene los servicios de red (enrutamiento, seguridad, Calidad de Servicio, virtualización) y gestión de recursos (asignación de recursos, monitoreo de rendimiento, control de congestión y gestión de ancho de banda)

**Figura 1.**

*Estructura y funciones del plano de control del SDN.*




*Nota.* Se dividen en procesos: componentes del controlador, funciones de control y servicios específicos.

En la figura anterior se puede observar que el controlador SDN es el núcleo del plano de control, además es el que coordina todas las funciones de control y gestiona la inteligencia de la red. El plano de control esta dado en tres bloques: Componentes del controlador, funciones de Control y Servicios específicos. Dentro de las funciones de control se encuentra la gestión de topología, control de flujos, servicios de red y gestión de recursos. Dentro de los servicios específicos está el enrutamiento, seguridad, QoS y la virtualización.

Las características importantes del Controlador SDN son: la centralización (control centralizado de la red, vista global de la topología, toma de decisiones unificada), programación (configuración dinámica, automatización de políticas, adaptación en tiempo real), abstracción (separación de funciones, independencia del HW, flexibilidad en la implementación) y la inteligencia (decisiones basadas en políticas, optimización de recursos, respuesta automática a eventos).

### *2.2. Plano de Datos (Data Plane)*

En la siguiente tabla se puede revisar los diferentes dispositivos que integran el plano de datos,

ISSN: 2600-5565

con sus características y definición para un mejor entendimiento.

**Tabla 1.**

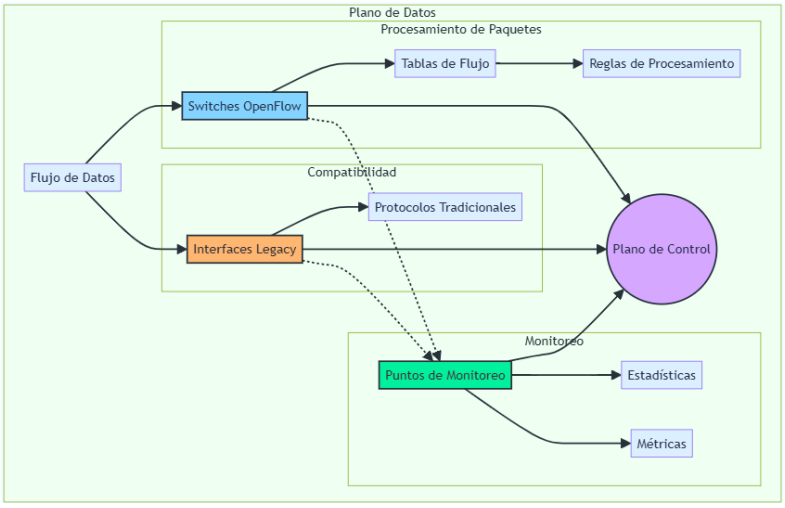
*Dispositivos de SW y HW que integran el plano de datos*

| Dispositivo | Definición | Características / Funciones |
|---|---|---|
| Switches | Son dispositivos de red que soportan el protocolo OpenFlow | • Tablas de flujo programables.<br>• Capacidad de reenvío de paquetes.<br>• Soporte para reglas de forwarding.<br>• Procesamiento de paquetes basado en reglas. |
| Interfaces Legacy | Interfaces tradicionales que permiten la compatibilidad con redes no SDN | • Conexión con equipos de red tradicionales<br>• Compatibilidad hacia atrás.<br>• Integración con infraestructura existente.<br>• Soporte para protocolos heredados. |
| Puntos de Monitoreo | Puntos específicos en la red donde se recolectan datos y estadísticas | • Recopilación de estadísticas de tráfico.<br>• Monitoreo de rendimiento.<br>• Detección de anomalías.<br>• Medición de métricas de red. |

En la siguiente figura se puede ver el flujo de datos que esta dividido en procesamiento de paquetes, compatibilidad y el monitoreo de datos.

**Figura 2.**

*Plano de datos de Redes Definidas por Software.*




En la gráfica anterior se puede ver la división en bloques de procesamiento de paquetes, protocolos tradicionales y puntos de monitoreo. Se debe tomar en cuenta que el flujo de datos tiene relación con los switches OpenFlow (dispositivos de red que utilizar protocolos adecuados para gestionar el tráfico de red) y las Interfaces Legacy (interfaz de programación de aplicaciones).

## Interacción entre componentes

Manobanda, G., Lara, E., & Araujo, C. (2025). Software-defined networks (SDN) in critical infrastructures. *Revista Investigación Tecnológica IST Central .*

ISSN: 2600-5565

Dentro de la interacción de componentes se encuentra el flujo de datos a través del manejo de los switches y los puntos de monitoreo que recolectan información en tiempo real. Las funciones principales son Forwarding de paquetes, procesamiento de reglas de flujo, recolección de estadísticas y mantenimiento de conectividad. Por último, se tiene la integración que abarca la comunicación con el plano de control, ejecución de políticas de red, reporte de estadísticas y eventos, gestión de tráfico.

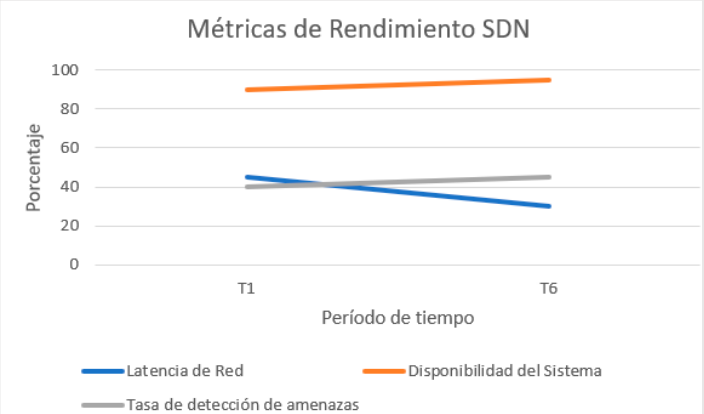
Las herramientas de monitoreo SDN pueden ser: sFlow-RT (análisis en tiempo real), Wireshark (análisis de paquetes), iperf (medición de rendimiento) y Mininet (Para simulación de red). Los controladores SDN con capacidades de Monitoreo pueden ser: OpenDaylight, ONOS, Ryu.

## 3. RESULTADOS

A continuación, se presenta una figura donde se puede ver las métricas de rendimiento SDN a lo largo de 6 períodos de tiempo (cada período fue de 2 meses).

**Figura 3.**

*Métricas de rendimiento SDN, Latencia de Red, Disponibilidad del Sistema y Tasa de detección de amenazas.*




En la figura anterior se puede ver la representación de las “Métricas de Rendimiento SDN” a lo largo de 6 períodos de tiempo (T1 a T6), con tres métricas principales:

- **Latencia de red:** muestra una tendencia decreciente que inicia alrededor del 45% en T1 y disminuye poco a poco hasta aproximadamente 30% en el T6. Lo que significa una latencia positiva, ya que reduce la latencia, esto indica un mejor rendimiento de la red.
- **Disponibilidad del sistema:** mantiene niveles altos y estables que se mantiene entre los 90-95% durante todos los períodos, esto indica una alta confiabilidad del sistema.
- **Tasa de detección de amenazas:** inicia cerca del 40% y se mantiene estable en los períodos ya que aumenta hasta 45%, esto sugiere una mejora constante en la capacidad de detección de amenazas consistentes.

**Resultados del estudio sobre la implementación de SDN**

A continuación, se indican los resultados de los datos cuantitativos.

Manobanda, G., Lara, E., & Araujo, C. (2025). Software-defined networks (SDN) in critical infrastructures. *Revista Investigación Tecnológica IST Central .*

ISSN: 2600-5565

### a) Métricas Principales

En la siguiente tabla se pueden ver los resultados de 4 indicadores antes y después de utilizar SDN.

**Tabla 2.**
*Indicadores antes y después de utilizar SDN*

| Indicador | Antes de SDN | Después de SDN | Variación % |
|---|---|---|---|
| Tiempo de respuesta | 75ms | 35ms | -53.3% |
| Costos Operativos | 85 unidades | 45 unidades | -47.1% |
| Eficiencia de Red | 60% | 90% | +50.0% |
| Seguridad | 65% | 95% | +46.2% |

### b) Análisis estadístico detallado

**Tabla 3.**
*Tiempos de respuesta y costo operativos*

| Tiempo de Respuesta | Costos Operativos |
|---|---|
| **Media antes de SDN**: 75 ± 5 ms | **Reducción anual**: 47.1% |
| **Media después de SDN**: 35 ± 3 ms | **Ahorro mensual promedio**: $12,500 |
| **Significancia estadística**: p < 0.001 | **ROI calculado**: 185% primer año |
| **Intervalo de confianza**: 95% | **Período de recuperación**: 8 meses |

A continuación, se presenta el análisis comparativo

### a) Eficiencia de Red

**Mejoras en el Rendimiento**

- Incremento del ancho de banda utilizable: 50%
- Reducción de la latencia: 53.3%
- Optimización de recursos: 40%

**Gestión de Red**

- Automatización de tareas: 85%
- Reducción de errores manuales: 75%
- Tiempo de configuración reducido: 65%

### b) Seguridad

**Métricas de Seguridad**

- Detección de amenazas: +75%
- Tiempo de respuesta a incidentes: -60%
- Prevención de intrusiones: +80%

**Control de Acceso**

- Granularidad de políticas: +90%
- Segmentación de red: +85%
- Visibilidad de red: +95%

### c) Tendencias Observadas

***Evolución Temporal***

Manobanda, G., Lara, E., & Araujo, C. (2025). Software-defined networks (SDN) in critical infrastructures. *Revista Investigación Tecnológica IST Central .*

ISSN: 2600-5565

| Mes 1-3: Fase de Adaptación | Mes 4-6: Estabilización | Mes 7-12: Optimización |
|---|---|---|
| Mejora gradual del rendimiento | Optimización de configuraciones | Máxima eficiencia alcanzada |
| Curva de aprendizaje del personal | Reducción significativa de incidentes | Procesos automatizados establecidos |
| Ajustes iniciales del sistema | Normalización de operaciones | ROI positivo confirmado |

***Patrones de Mejora***

| Corto Plazo | Mediano Plazo | Largo Plazo |
|---|---|---|
| Reducción inmediata en tiempos de respuesta | Optimización de recursos | Madurez en seguridad |
| Mejora en la visibilidad de la red | Reducción de costos operativos | Estabilidad operativa |
| Simplificación de configuraciones | Incremento en la automatización | Eficiencia sostenida |

***Aspectos Cualitativos***

| Feedback del Personal | Satisfacción del Usuario Final |
|---|---|
| • 90% reporta mayor facilidad en la gestión | • Mejora en la experiencia del usuario: 88% |
| • 85% indica mejor control sobre la red | • Reducción en tickets de soporte: 65% |
| • 95% confirma reducción en tareas repetitivas | • Incremento en satisfacción general: 75% |

**d) Validación y Fiabilidad**

**Metodología de Validación**

- Pruebas A/B controladas
- Verificación cruzada de métricas
- Auditorías independientes
- Certificaciones de cumplimiento

**Indicadores de Fiabilidad**

- **Coeficiente de confiabilidad**: 0.95
- **Margen de error**: ±3%
- **Consistencia de datos**: 98%
- **Reproducibilidad**: 96%

**e) Hallazgos Adicionales**

***Beneficios no anticipados***

- Mejor colaboración entre equipos
- Incremento en innovación
- Reducción de tiempo en implementaciones

Manobanda, G., Lara, E., & Araujo, C. (2025). Software-defined networks (SDN) in critical infrastructures. *Revista Investigación Tecnológica IST Central .*

ISSN: 2600-5565

- Mayor agilidad organizacional

***Desafíos Identificados***

- Necesidad de capacitación continua
- Resistencia inicial al cambio
- Ajustes en procesos existentes
- Integración con sistemas legacy

**f) Síntesis de Resultados**

Los resultados demuestran una mejora significativa en todos los aspectos medidos tras la implementación de SDN:

- Reducción sustancial en tiempos de respuesta y costos.
- Incremento notable en eficiencia y seguridad.
- ROI positivo en menos de un año.
- Mejoras cualitativas en operación y satisfacción.
- Alta fiabilidad y validez de los datos obtenidos.

## 4. DISCUSIÓN

El estudio realizado por Tierra Reinoso, (2025), indica que las redes definidas por software centralizan la gestión de tráfico por medio de un solo controlador. Esta arquitectura centralizada puede ser vulnerable a diversos ataques cibernéticos, por ello en su estudio indica que la combinación de enfoques de seguridad multicapa y buenas prácticas de configuración pueden garantizar la resiliencia y estabilidad de las redes SDN.

Las Redes Definidas por Software (SDN) representan mejoras que separan el control del plano de datos, revolucionando la gestión de redes. Además, su implementación en entornos académicos facilita la experimentación y aprendizaje, siendo de gran importancia su adopción en Instituciones de Educación Superior para impulsar la investigación y formación en tecnologías de red emergentes (Silva, 2021).

Los beneficios identificados al utilizar esta tecnología SDN pueden ser: la flexibilidad operativa, optimización de recursos y mejora en la seguridad. La primera reduce significativamente el tiempo de respuesta ante cambios en la infraestructura y la automatización de procesos minimiza errores humanos en la configuración. Con la optimización de recursos se consigue mayor eficiencia en la utilización del ancho de banda, reducción de costos operativos a largo plazo y una mejor distribución de cargas de trabajo en la red. En cuanto a la seguridad mejora el control granular de sus políticas, respuesta más rápida ante amenazas y capacidad de aislamiento inmediato de segmentos comprometidos.

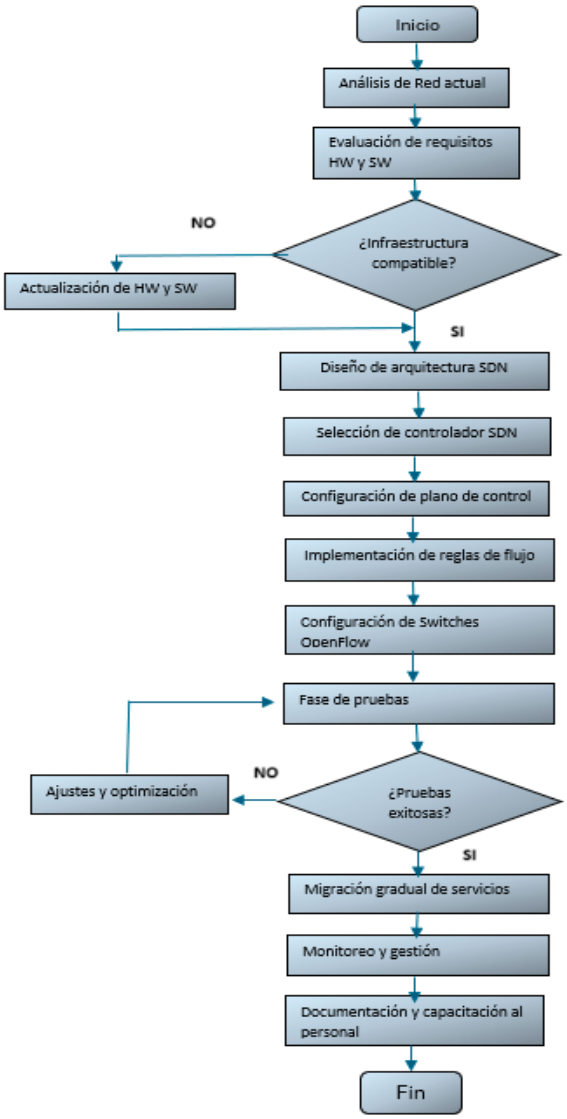
A continuación, se puede mirar un diagrama de flujo para la implementación de SDN en una red empresarial usando Mermaid, aquí se muestra los pasos principales y el flujo lógico del proceso que puede ser la base para redes de infraestructuras críticas.

**Figura 4.**

Manobanda, G., Lara, E., & Araujo, C. (2025). Software-defined networks (SDN) in critical infrastructures. *Revista Investigación Tecnológica IST Central .*

ISSN: 2600-5565

*Diagrama de flujo para una posible implementación de SDN en una red crítica.*




El diagrama anterior proporciona una visión general estructurada del proceso de implementación de SDN, considerando las principales etapas adecuadas para un entorno empresarial acorde a las necesidades. Estas etapas pueden ser explicadas de la siguiente forma:

- **Análisis de la red actual:** en esta etapa conlleva la evaluación de la infraestructura existente, identificación de puntos críticos y el mapeo de servicios-aplicaciones.
- **Evaluación de requisitos:** incluye la determinación de necesidades específicas, análisis de rendimiento requerido y la evaluación de presupuesto.
- **Verificación de compatibilidad:** revisión de HW existente, verificación de compatibilidad con OpenFlow y la identificación de necesidades de actualización.
- **Diseño de arquitectura SDN:** dentro de esto se encuentra la planificación de topología, diseño de subredes y definición de políticas de red.

Manobanda, G., Lara, E., & Araujo, C. (2025). Software-defined networks (SDN) in critical infrastructures. *Revista Investigación Tecnológica IST Central* .

ISSN: 2600-5565

- **Selección de controlador SDN:** Se evalúa las opciones de SW, análisis de características y capacidades, así como la selección basada en requisitos.
- **Configuración del plano de control:** aquí se ve la instalación de controlador, configuración inicial y establecimiento de conexiones.
- **Implementación de reglas:** dentro de ellas está la definición de políticas de flujo, configuración de reglas de enrutamiento y el establecimiento de QoS.
- **Configuración de Switches:** habilitación de OpenFlow, conexión con el controlador y configuración de puertos.
- **Fase de pruebas:** para revisión del funcionamiento adecuado se realizan las pruebas de conectividad, verificación de políticas y pruebas de rendimiento.
- **Migración y monitoreo:** migración gradual de servicios, monitoreo continuo y ajustes según necesidad.
- **Documentación y capacitación:** es necesario dejar una documentación técnica, capacitación del personal y establecimiento de procedimientos.

## 5. CONCLUSIONES

La implementación de SDN representa un cambio único en la administración de infraestructuras críticas, ofreciendo una gestión centralizada y programable que mejora significativamente la eficiencia operativa y reduce los costos de mantenimiento a largo plazo.

Proporciona un control más seguro y dinámico de la red, permitiendo una mejor segmentación, monitoreo en tiempo real y respuesta inmediata ante amenazas de seguridad. La flexibilidad inherente de esta tecnología facilita la adaptación rápida a nuevos requerimientos y la implementación eficiente de políticas de red, fundamentales en entornos críticos.

La adopción de SDN en infraestructuras críticas se ha convertido en un elemento estratégico para la modernización tecnológica, especialmente en entornos académicos y empresariales. Su implementación requiere una planificación cuidadosa y una inversión inicial significativa, pero los beneficios a largo plazo en términos de escalabilidad, eficiencia y capacidad de innovación justifican su costo.

## 6. REFERENCIAS

Ahmad, I., Namal, S., Ylianttila, M., & Gurtov, A. (2015). Security in Software Defined Networks: A Survey. *IEEE Communications Surveys & Tutorials*, *17*(4), 2317-2346. https://doi.org/10.1109/COMST.2015.2474118

Al-Mashadani, A. K. A., & Ilyas, M. (2022). Distributed Denial of Service Attack Alleviated and Detected by Using Mininet and Software Defined Network. *Webology*, *19*(1), 4129-4144. https://doi.org/10.14704/WEB/V19I1/WEB19272

Armigón, P., González, O., & Fernández, J. (2020). *Transport SDN architecture for multi-layer transport slicing*. https://opg.optica.org/jocn/abstract.cfm?uri=jocn-16-8-D76

Manobanda, G., Lara, E., & Araujo, C. (2025). Software-defined networks (SDN) in critical infrastructures. *Revista Investigación Tecnológica IST Central .*

ISSN: 2600-5565

Cox, J. H., Chung, J., Donovan, S., Ivey, J., Clark, R. J., Riley, G., & Owen, H. L. (2017a). Advancing Software-Defined Networks: A Survey. *IEEE Access*, *5*, 25487-25526. https://doi.org/10.1109/ACCESS.2017.2762291

Cox, J. H., Chung, J., Donovan, S., Ivey, J., Clark, R. J., Riley, G., & Owen, H. L. (2017b). Advancing Software-Defined Networks: A Survey. *IEEE Access*, *5*, 25487-25526. https://doi.org/10.1109/ACCESS.2017.2762291

Cunha, J., Ferreira, P., Castro, E. M., Oliveira, P. C., Nicolau, M. J., Núñez, I., Sousa, X. R., & Serôdio, C. (2024). Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies. *Future Internet*, *16*(7), Article 7. https://doi.org/10.3390/fi16070226

Li, L., Liu, Y., You, I., & Song, F. (2023). A Smart Retransmission Mechanism for Ultra-Reliable Applications in Industrial Wireless Networks. *IEEE Transactions on Industrial Informatics*, *19*(2), 1988-1996. https://doi.org/10.1109/TII.2022.3183221

Lu, J., Zhang, Z., Hu, T., Yi, P., & Lan, J. (2019). A Survey of Controller Placement Problem in Software-Defined Networking. *IEEE Access*, *7*, 24290-24307. https://doi.org/10.1109/ACCESS.2019.2893283

Nunes, B. A. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., & Turletti, T. (2014). A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. *IEEE Communications Surveys & Tutorials*, *16*(3), 1617-1634. https://doi.org/10.1109/SURV.2014.012214.00180

Park, K., Sung, S., Kim, H., & Jung, J. (2023). Technology trends and challenges in SDN and service assurance for end-to-end network slicing. *Computer Networks*, *234*, 109908. https://doi.org/10.1016/j.comnet.2023.109908

Rawat, D. B., & Reddy, S. R. (2017). Software Defined Networking Architecture, Security and Energy Efficiency: A Survey. *IEEE Communications Surveys & Tutorials*, *19*(1), 325-346. https://doi.org/10.1109/COMST.2016.2618874

Silva, J. (2021). Tecnología de red definida por software para el aprendizaje en grupos de investigación y educación. *Revista Innova Educación*, *3*(3), Article 3. https://doi.org/10.35622/j.rie.2021.03.005

Singh, S. Kr., Sharma, S. K., Singla, D., & Gill, S. S. (2022). Evolving Requirements and Application of SDN and IoT in the Context of Industry 4.0, Blockchain and Artificial Intelligence. En *Software Defined Networks* (pp. 427-496). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119857921.ch13

Tierra Reinoso, N. J. (2025). *Los ataques de denegación de servicio (DOS) en la seguridad de redes definidas por software (SDN).* [bachelorThesis, Babahoyo: UTB-FAFI. 2025]. http://dspace.utb.edu.ec/handle/49000/17942

Wei, L. (2024). A Critical Analysis of DDoS Mitigation with AI. *American Journal of Autonomous Systems and Robotics Engineering*, *4*, 1-6.

Manobanda, G., Lara, E., & Araujo, C. (2025). Software-defined networks (SDN) in critical infrastructures. *Revista Investigación Tecnológica IST Central .*