Reporte sobre tendencias globales en redes 2020

Contenido

Introducción: Estado de las redes para la era digital 4

La evolución del rol de la red de TI 7
Tendencias globales que dan forma a la nueva red 9
- Globalización 9
- La transformación del negocio digital 9
- La automatización de las empresas 10
- La resiliencia operativa y empresarial 10
- Sustentabilidad 10

Tendencias tecnológicas que impulsan la evolución de la red 11
- El panorama de las aplicaciones en evolución 11
- IoT (Internet de las Cosas) 12
- IA 13
- Movilidad 13
- Seguridad 14
- Experiencias inmersivas 14

La necesidad de un nuevo tipo de red 16
- Los expertos de Cisco imaginan la arquitectura de la red emergente 17
- El estado de la arquitectura de red 19

Tendencias en tecnologías de redes 20

Automatización de la red a escala 23
- Redes definidas por software: apenas el comienzo 25
- Redes basadas en intención: cerrar el bucle 25
- Virtualización de las funciones de la red 27
- La programabilidad como la base de la red 27

Tendencias en tecnologías de redes (continuación)

Controladores de IBN de plataforma abierta: procesos de TI y la integración con el negocio 28

Alineación de garantía y políticas entre dominios: del cliente a la carga de trabajo 29

Aseguramiento habilitado por IA 30

¿Qué significan AI, ML y MR? 31

La complejidad de las redes impulsa la adopción de la IA 32

¿Cómo se aplican ML y MR en un contexto de red? 34

Estado actual y futuro de la IA para el aseguramiento de la red 34

Consideraciones para seguir adelante con la IA 36

Redes para datos y aplicaciones en entornos multinube 37

El impacto en la red de cambiar los modelos de aplicaciones 39

Optimización de la conectividad de usuario a multinube 41

Networking para un centro de datos en cualquier lugar 45

Consideraciones para diseñar la red para un entorno multinube 48

Acceso de red e inalámbrico 49

Ofrecer una agradable experiencia de usuario móvil 51

Preparación de TI para el éxito inalámbrico 53

Estado actual y futuro de la preparación para el acceso a la red 53

Consideraciones para habilitar el acceso y la conexión inalámbrica para la era digital 55

El rol cambiante de la seguridad de la red 56

Desafíos con la seguridad de la red 59

Abordaje de los desafíos de seguridad con una red inteligente 61

Estado actual y futuro de la seguridad de la red 64

Tendencias en las operaciones de red 65

Estado actual y futuro de las operaciones de la red 69

La manera en que los avances en la red están cambiando las operaciones de red 69

- Integración de las operaciones de red en el proceso de la TI 69
- Alineación completa entre TI y la intención de negocio 71
- Automatización para reducir la complejidad de las operaciones de red 72
- Gestión de problemas e incidentes preventiva versus reactiva 72
- Incorporación de la conectividad de la tecnología operativa a las operaciones de red 73

Presentación de un marco de operaciones de red de última generación 73

- Administración del ciclo de vida 74
- Administración de políticas 75
- Administración del aseguramiento 76

Predicciones sobre el futuro de las operaciones de red para 2025 77

Tendencias en los profesionales de redes 78

Preparación para el cambio de los conjuntos de habilidades de red 82

- Las mayores brechas de habilidades en tecnología de la información 82
- Las mayores brechas de habilidades de redes 83
- Creciente necesidad de habilidades sociales y laborales 84
- Los roles cruzados más importantes del futuro 84

Nuevos roles para los estrategas de redes 85

- El estratega del futuro: entrega de valor más allá de la red 85

Nuevos roles para los profesionales de redes 87

- Los ingenieros de redes del futuro: entrega de valor más allá de la conectividad 87

Líderes de TI: tomar medidas para cubrir las carencias de habilidades en redes 88

- Líderes: Consideren estas recomendaciones para construir el equipo de la red del futuro: 90

Introducción: Estado de las redes para la era digital

Resumen de la sección

Aportes clave

- Las tendencias como la globalización, la transformación digital, la automatización y la resiliencia del negocio, además de la sustentabilidad, están dando forma a los requisitos necesarios para lograr un nuevo tipo de red.
- El cambiante panorama tecnológico: modelos emergentes nativos de la nube, Internet de las Cosas, inteligencia artificial (IA), dispositivos móviles, amenazas de ciberseguridad y aplicaciones inmersivas, está afectando drásticamente las arquitecturas y operaciones de redes de TI.
- La enorme escala, complejidad y naturaleza dinámica de estas demandas superan la capacidad de los operadores humanos por sí solos.
- Las nuevas redes utilizan tecnologías emergentes como la IA (Inteligencia Artificial), el aprendizaje automático y la automatización para simplificar y proteger las operaciones, permitir una rápida adaptabilidad y aumentar la toma de decisiones de las personas.

Tendencias empresariales y tecnológicas globales que están dando forma a la nueva red

700M	50%	14.6B	42%	53%	12X
de contenedores alojados en el borde para el año 2021[1]	de las cargas de trabajo fuera del centro de datos empresarial para el 2021[2]	de dispositivos de IoT para el año 2022[3]	de crecimiento anual del tráfico móvil empresarial, de 2017 a 2022[3]	de ataques de ciberseguridad ocasionan más de US$500,000 en daños[4]	de aumento en el tráfico de AR/VR (Realidad Aumentada/ Realidad Virtual) para 2022[3]

Resumen de la sección (continuación)

Orientación esencial

- Los líderes de TI y los estrategas de redes deben impulsar un enfoque paso a paso para hacer evolucionar cada uno de sus dominios de red a un modelo basado en controladores, lo cual desarrolla tecnologías de IA y automatización.
- Los líderes de TI deben crear un plan de negocios y de tecnología que se alinee con las prioridades del negocio y abarque la arquitectura, la tecnología, las operaciones y el talento.
- Los estrategas y los profesionales de redes deben identificar las opciones de carrera y desarrollo que les darán los conjuntos de habilidades que se necesitan para liderar esta transformación de las redes y mejorar su valor.

Principal predicción

"Para 2025, los equipos de redes de vanguardia contarán con redes basadas en intención que operen en todos los dominios: campus, sucursal, WAN, centro de datos, nube, proveedor de servicios y seguridad. Sus redes tendrán la capacidad para comprender los requisitos de negocio y de las aplicaciones, y traducirlos en políticas de red y seguridad. La agilidad mejorará drásticamente a través de la automatización inteligente de la red, y las redes funcionarán con un potente bucle de retroalimentación que proporcionará supervisión, seguridad y optimización de manera continua. La red basada en intención garantizará que los servicios empresariales se entreguen y estén protegidos de manera continua en toda la red. Estos avances darán lugar a importantes beneficios para las organizaciones y también para la sociedad en general".

– John Apostolopoulos, CTO de Redes Empresariales, Cisco

Introducción: Estado de las redes para la era digital

En una serie de memorandos escritos en 1962, J. C. R. Licklider, Director de la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de los Estados Unidos, propuso una “red informática intergaláctica” en la que las computadoras de todo el mundo estuvieran interconectadas con el objetivo de proporcionar acceso rápido a los datos y los programas desde cualquier lugar.[5]

Unos pocos años después, en 1965, Leonard Kleinrock, Lawrence Roberts y Thomas Merrill utilizaron líneas telefónicas para conectar cuatro computadoras entre sí: crearon así la primera red de área amplia, así como los comienzos de Internet.[6]

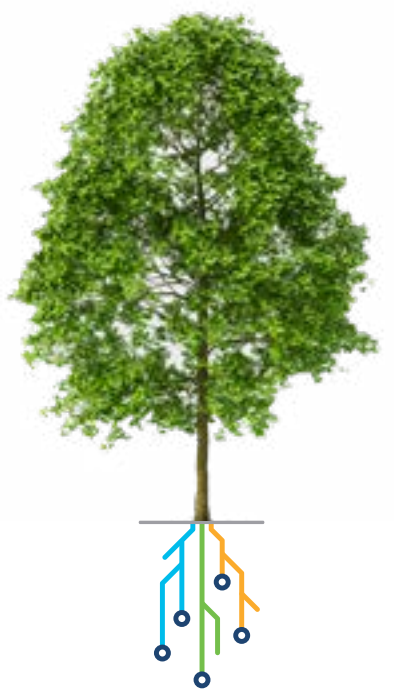
Más de 50 años después, la visión original de Licklider sigue siendo la misma, ya que la red sigue conectando a los consumidores globales de información y servicios con aplicaciones y fuentes de datos.

Por supuesto que todo lo demás ha cambiado.

La evolución del rol de la red de TI

El mundo actual, impulsado por el crecimiento exponencial del rendimiento de la tecnología, se ha vuelto cada vez más conectado, digitalizado, distribuido y diverso. Con cada "cosa" con el poder de procesar datos, los modelos informáticos están listos para convertirse en mucho más distribuidos y conectados en red. Y a medida que se le agregan dispositivos y usuarios, el valor y la importancia de la red, medida por la ley de Metcalfe, continúan su crecimiento exponencial.

El negocio digital continúa impulsando las innovaciones en red. IDC calcula que habrá 48,900 millones de dispositivos conectados y en uso en todo el mundo para el año 2023.[7] Y el *Pronóstico de VNI Completo de Cisco 2018* pronostica que la cantidad promedio de datos consumidos a través de una red será de casi 60 GB por computadora personal al mes.[3]

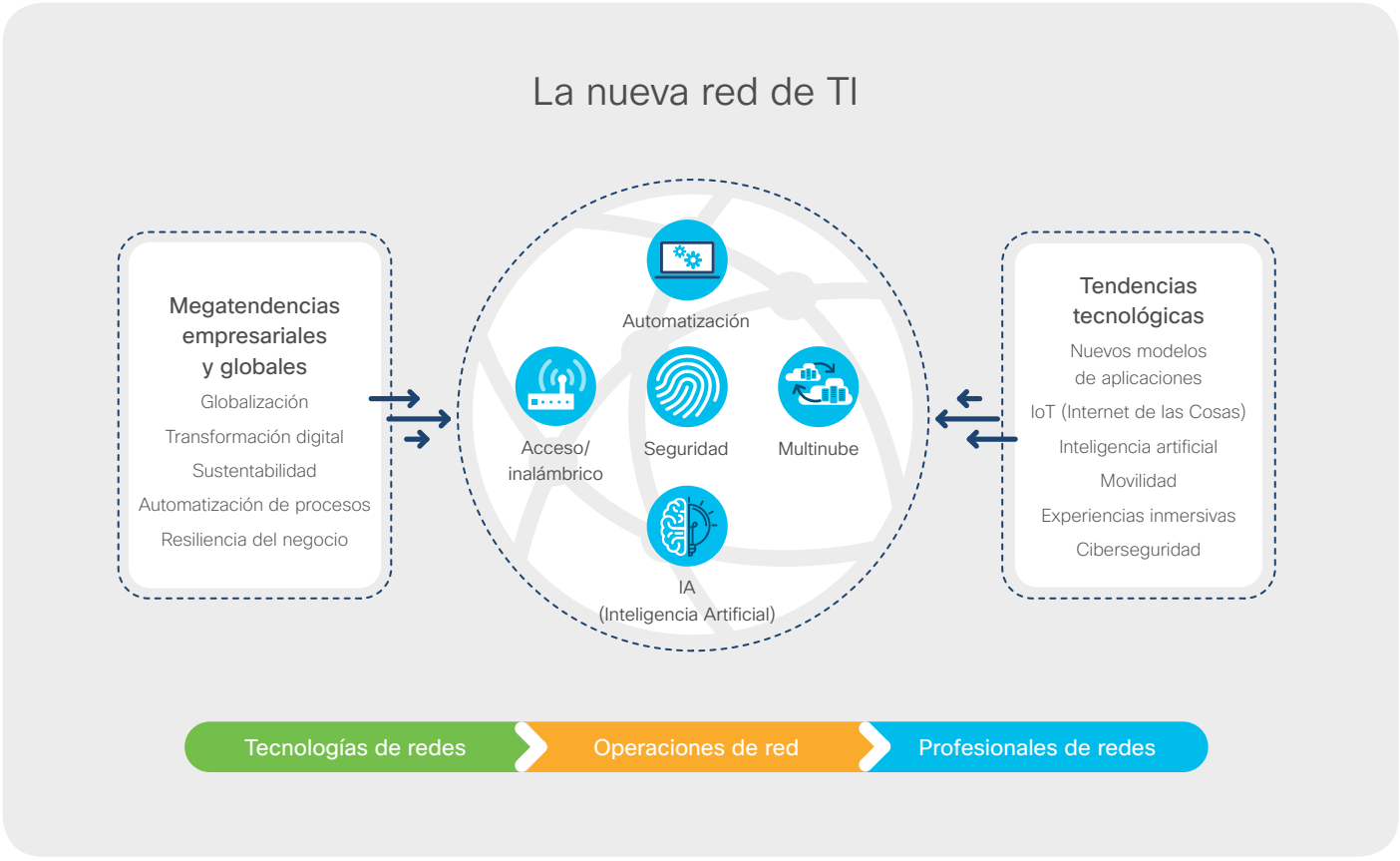


No es de extrañar que, dado este crecimiento incesante, descubramos que los equipos de TI están llegando a un punto en el que la gran escala y complejidad de las redes están superando su capacidad para administrarlas y protegerlas de modo eficaz. Lo que se necesita ahora son nuevos sistemas que combinen tecnologías como el aprendizaje automático, el razonamiento automático y la automatización para simplificar las operaciones y aumentar la toma de decisiones de las personas.

Actualmente nos encontramos en el umbral de una nueva era de las redes, donde la TI puede romper con las formas tradicionales de desarrollar y operar redes, y adoptar un futuro impulsado por tecnologías que pueden resolver estos desafíos de maneras tremendamente nuevas.

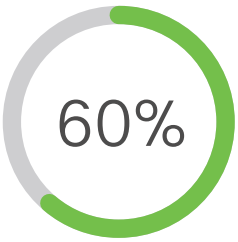
Antes de examinar las tendencias emergentes de la tecnología en redes, las operaciones y el talento que constituyen la base de esta nueva red, analicemos brevemente las tendencias empresariales y tecnológicas globales que impulsan su evolución.

Figura 1: Tendencias empresariales y tecnológicas globales que están dando forma a la nueva red



Tendencias globales que dan forma a la nueva red

Una serie de tendencias globales y empresariales están dando forma al rol que desempeña la red en una organización. Comprender estas tendencias puede ayudar a los líderes de TI a prepararse mejor para las expectativas cada vez mayores que los líderes empresariales tienen con respecto a la red.



Según Gartner, para el año 2023, más del 60% de las empresas considerará al networking como el núcleo de sus estrategias digitales y como un facilitador estratégico, frente a menos del 20% en la actualidad.[8]

Una breve mirada a algunas de estas megatendencias globales revela las demandas que probablemente tendrán hacia la red.

Globalización

Según el Foro Económico Mundial, estamos ingresando a una nueva era de globalización impulsada por la tecnología digital, denominada "Globalización 4.0". En esta era, los bienes y servicios *digitales*, posibilitados por las capacidades digitales y la inteligencia artificial constituyen las principales exportaciones.[9]

Impacto de la red

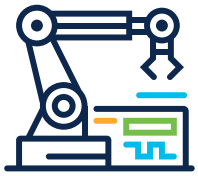
A medida que las conexiones entre sistemas, personas, procesos, ubicaciones y dispositivos se vuelven más distribuidas y complejas, el valor económico de la red para la organización aumentará, al tiempo que proteger y administrar la red se volverán tareas más estratégicas y más difíciles.

La transformación del negocio digital

Cada vez más empresas utilizan tecnologías digitales como la analítica, la movilidad, las soluciones en la nube y el Internet de las Cosas (IoT) como la base para la transformación de sus negocios. Según el informe IMD y Cisco *Digital Vortex de 2019*, el 88% de los ejecutivos cree que la disrupción digital tendrá un impacto importante o transformador sobre sus industrias, en comparación con solo el 27% en 2015.[10]

Impacto de la red

La imprevisibilidad inherente del negocio requiere una red que pueda adaptarse rápidamente a los requisitos en evolución con el objetivo de poder habilitar nuevos servicios, procesos y modelos.



La automatización de las empresas

El uso de la automatización y la robótica en los próximos años seguirá aumentando a medida que las empresas busquen mejorar la calidad, la productividad de la fuerza de trabajo, la satisfacción del cliente, etc. El Capgemini Research Institute predice que la adopción a gran escala de la automatización podría resultar en ahorros de costos de hasta US$471 mil millones hacia el año 2022 en los sectores automotriz, de venta minorista, de servicios públicos y de manufactura.[11]

Impacto de la red

Debido a que el tiempo es un factor crítico en la automatización de los procesos, la red debe garantizar que los paquetes se entreguen de manera confiable y oportuna.

La resiliencia operativa y empresarial

Debido a la globalización y la transformación digital, las organizaciones actuales dependen de una red cada vez más compleja de tecnologías, sistemas, procesos, cadenas de suministro e infraestructura. Una resiliencia empresarial eficaz requiere evaluar de manera continua y proactiva los riesgos operativos, establecer y auditar los planes de contingencia y administrar la capacitación de respuesta ante incidentes.

Impacto de la red

Una arquitectura de red ágil, resiliente y segura es fundamental para proteger a los empleados, clientes y socios de negocio, además de ser esencial para recuperar los datos y restablecer rápidamente los servicios y el acceso.

Sustentabilidad

A medida que nuestro mundo se vuelve más interconectado, las organizaciones se enfrentan al desafío de crecer con sustentabilidad medioambiental. Además de las métricas estándar, las organizaciones serán juzgadas en relación a lo eficiente que sean a la hora de reducir las emisiones de gases de efecto invernadero, preservar la biodiversidad y los recursos naturales, y diseñar productos para minimizar o reciclar los desechos.

Impacto de la red

Las redes avanzadas ofrecen la promesa de mayores eficiencias en prácticamente todos los aspectos del negocio, desde el consumo de energía hasta el uso de recursos y la reducción de emisiones.

Tendencias tecnológicas que impulsan la evolución de la red

En este momento, una serie de tendencias emergentes están cambiando drásticamente el panorama de la TI. Un vistazo más de cerca a algunas de estas tendencias clave revela el impacto que podrían tener en la red empresarial.

El panorama de las aplicaciones en evolución

Las aplicaciones y los datos, por supuesto, están en el corazón del negocio digital. Además, la forma en que las aplicaciones son desarrolladas, alojadas y consumidas cambia constantemente para satisfacer las nuevas necesidades empresariales.

Estas son algunas de las formas en que las aplicaciones están evolucionando y, de alguna manera, reinventando la red:

Las aplicaciones y los datos salen de las instalaciones: Las aplicaciones y los datos se están modularizando en microservicios y trasladando a múltiples nubes públicas. En algunos casos, también se distribuyen al borde de la red. Y cada vez se consumen más a partir de múltiples proveedores de software como servicio (SaaS).

Las aplicaciones son modulares y están distribuidas en diferentes entornos: En muchos casos, las aplicaciones monolíticas se están disolviendo en microservicios interconectados que se entregan a través de una variedad de cargas de trabajo virtuales y físicas, incluidos los contenedores, en toda la empresa.

Según el Uptime Institute, para el año 2021 la mitad de todas las cargas de trabajo se ejecutarán fuera del centro de datos empresarial, ya sea en infraestructuras de centros de datos, en la nube o en el borde de la red. [2]

Las aplicaciones se crean de manera continua y veloz: Para las aplicaciones desarrolladas y alojadas localmente, la TI debe acelerar la creación y entrega de sus propios servicios de infraestructura para satisfacer las necesidades de las aplicaciones y los usuarios; todo ello al tiempo que controla los costos operativos.

Las aplicaciones están migrando de física a virtual, a contenedores, a "sin servidor": El aumento de los contenedores deja expuestos los paradigmas de diseño e implementación

de aplicaciones a una disrupción mucho más masiva, es decir, arquitecturas sin servidor, lo que está obligando a las organizaciones a volver a analizar la manera de crear aplicaciones, el papel de la infraestructura y el diseño de los procesos operativos.

Se estima que, para el año 2021, las instancias de contenedores instalados y en uso superarán los 3,500 millones, con más del 20% de ellos en ejecución en ubicaciones distribuidas que sirven cargas de trabajo de IoT y del borde de red.[1]

Impacto en la red

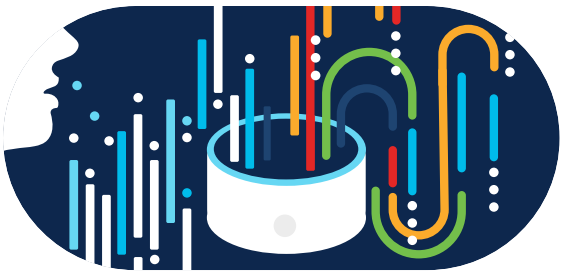
Con el surgimiento de aplicaciones y microservicios a lo largo de todos los dominios, la red debería ser vista más como un conjunto creciente de "clústeres de terminales nerviosas" interconectados y situados donde residen los datos, los cuales podrían estar en cualquier lugar a lo largo del continuo de la nube-borde. La nueva red debe tener la capacidad de conectarse de forma segura dentro y entre estos "clústeres de terminales nerviosas" interconectados, así como también comprender básicamente cómo funcionan estos nuevos modelos de aplicaciones y ampliar dinámicamente las políticas de aplicaciones a través de toda la red y hasta cualquier lugar donde haya aplicaciones alojadas.

IoT (Internet de las cosas)

El auge del uso de dispositivos de IoT, aplicaciones y datos adjuntos está impulsando la creación de nuevos modelos de cómputo distribuido que consisten en niveles exponencialmente mayores de escala y complejidad. Según la "Herramienta de Información Destacada del Pronóstico de VNI" de Cisco, para el año 2022 los dispositivos de máquina a máquina (M2M) representarán el 51% (14,600 millones) de todos los dispositivos conectados en red de todo el mundo.[12]

Impacto en la red

Además de proporcionar conectividad y seguridad para una gama increíblemente diversa de dispositivos de IoT, los administradores de red tendrán que idear formas escalables y eficientes de, automáticamente, identificar, clasificar, aplicar políticas y supervisarlas para garantizar el correcto funcionamiento sin afectar ni comprometer otros servicios que se ejecuten en la red.



IA (Inteligencia Artificial)

La aparición de aplicaciones impulsadas por la IA para uso tanto para empresas como para consumidores está dando lugar a un mundo completamente nuevo de dispositivos conectados, inteligentes y automatizados que se están implementando en todas partes.

Impacto en la red

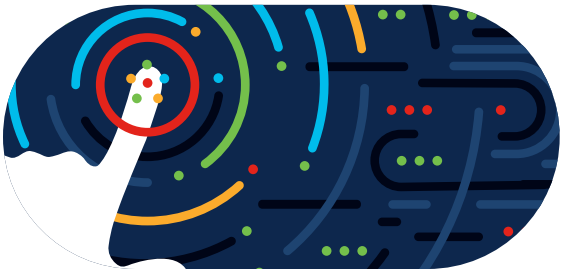
Para liberar todo el potencial de la IA en los negocios, se debe realizar más procesamiento informático y tomas de decisiones más cerca del borde de red. Según el rendimiento, la capacidad, la privacidad e incluso las consideraciones sobre costos, la colocación del procesamiento y datos de la IA podrá oscilar desde la nube hasta los centros de datos locales y el borde de la red.

Movilidad

Según la “Herramienta de Información Destacada del Pronóstico de VNI” de Cisco, el tráfico global de datos móviles de empresas se multiplicará por seis de 2017 a 2022, a una tasa de crecimiento anual del 42%.[12] Los usuarios móviles empresariales seguirán exigiendo conectividad inmediata y de alto rendimiento en cualquier lugar, en cualquier momento y en cualquier dispositivo a través de redes Wi-Fi y redes públicas 4G y 5G. Al mismo tiempo, los dispositivos de IoT inalámbricos se volverán cada vez más omnipresentes en todos los aspectos de nuestras vidas.

Impacto en la red

Los empleados que acceden a las aplicaciones en la nube desde dispositivos corporativos y privados desde fuera de la red están creando una falta de visibilidad y control que los administradores de red y de seguridad no han abordado. Y una oleada de dispositivos de IoT se sumará a los requisitos de las redes inalámbricas en cuestiones de escala, diferentes patrones de tráfico y seguridad.



Seguridad

Las amenazas a la ciberseguridad son cada vez más sofisticadas y peligrosas en toda una superficie de ataque más amplia que ya no está contenida dentro de perímetros bien definidos y defendidos. En particular, a medida que las cargas de trabajo salen de las instalaciones, existe el peligro de que la TI pierda visibilidad.

Impacto en la red

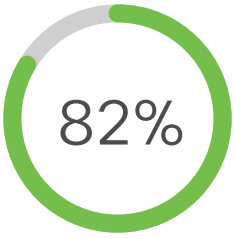
Si bien la red continuará siendo un poderoso aliado en la identificación y contención de amenazas, las operaciones de red y seguridad deben compartir datos e integrar herramientas y flujos de trabajo para combatir mejor el continuo aumento de la cantidad y la sofisticación de los ataques. Además, la red puede ampliar el alcance de TI a entornos en la nube para ayudar a proteger las aplicaciones y los datos incluso cuando no están directamente bajo su control.

Experiencias inmersivas

El aumento del uso de videos y la aparición de la realidad virtual y la realidad aumentada (VR y AR, por sus siglas en inglés) para mejorar la colaboración, la capacitación, la productividad y las experiencias de trabajo remoto exigirán cada vez más a las redes de las organizaciones.

Impacto en la red

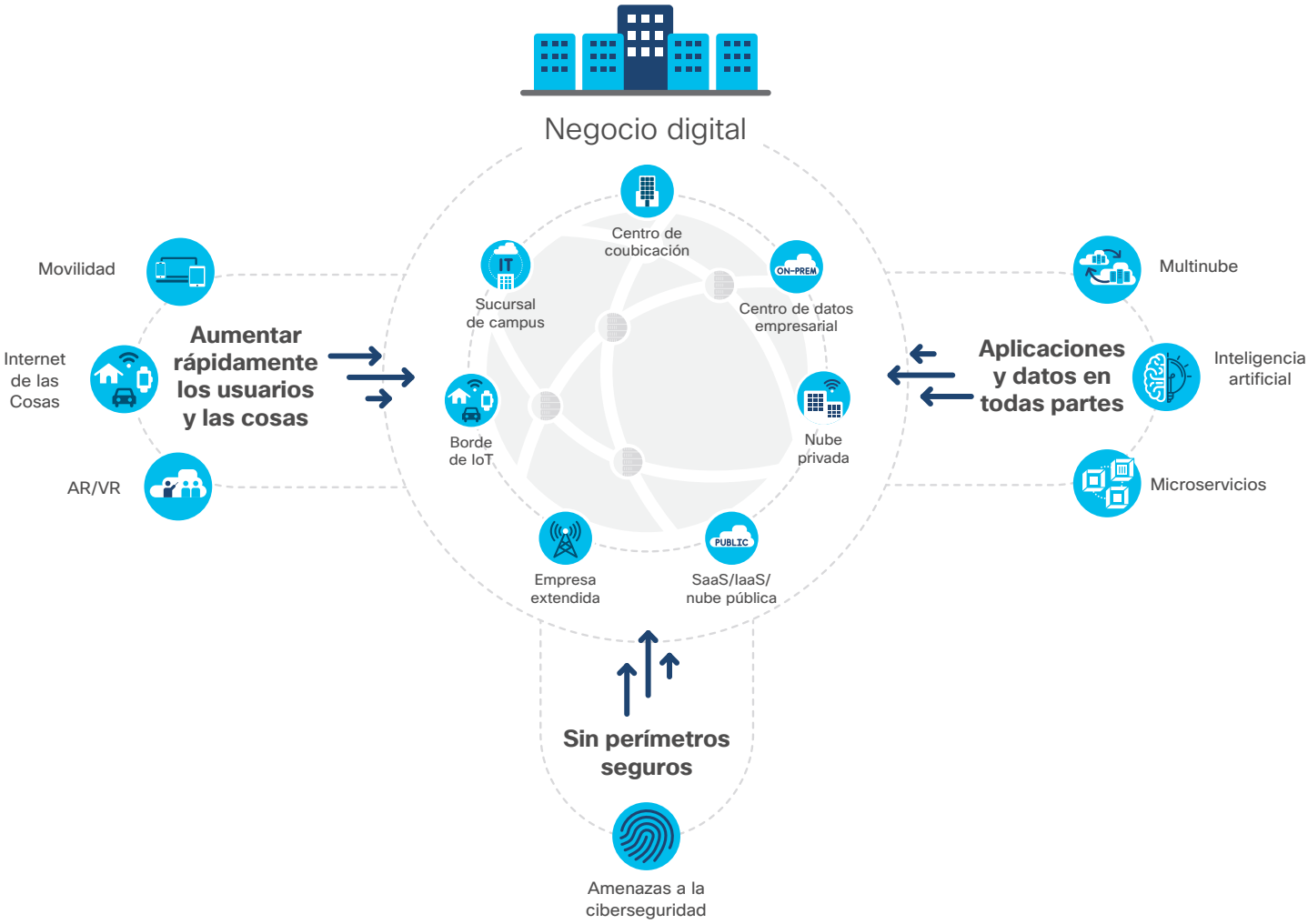
La red deberá proporcionar el ancho de banda de extremo a extremo, las comunicaciones de baja latencia y los controles de rendimiento dinámico necesarios para habilitar dichas experiencias inmersivas.



Para el año 2022, los videos de Internet representarán el 82% de todo el tráfico del Internet empresarial, el tráfico de VR/AR se multiplicará por doce y el tráfico de videovigilancia de Internet se multiplicará por siete.[13]

Este panorama tecnológico dinámico no solo es una realidad para todas las organizaciones y sus clientes, sino que también es el motor de la economía digital. Por lo tanto, no es de extrañar que la TI esté sintiendo la presión de abordar todas estas tendencias con las estrategias de tecnología de redes adecuadas, los modelos de operaciones y el talento.

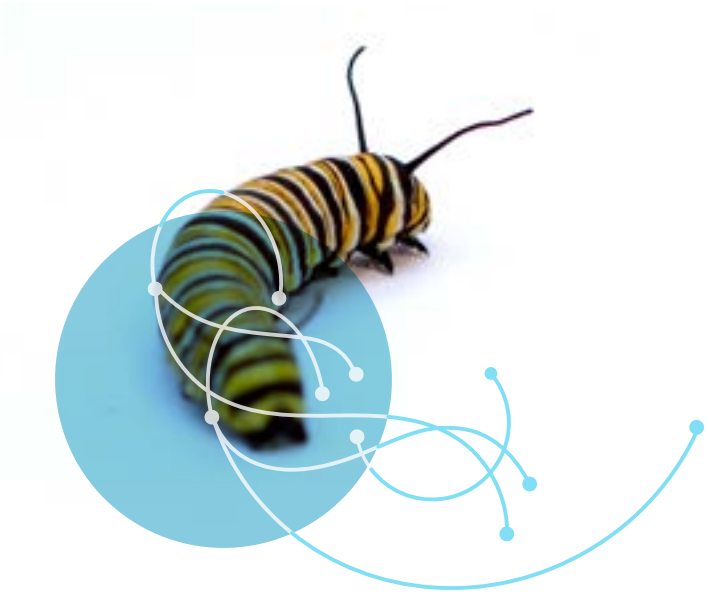
Figura 2: Tecnologías que impulsan las nuevas demandas de la red



La necesidad de un nuevo tipo de red

En este entorno cada vez más exigente, existe una necesidad crítica de que los líderes de la TI migren a un enfoque radicalmente nuevo para las redes.

Para que una organización florezca en la economía digital, la red debe tener la capacidad de adaptarse rápidamente a los cambiantes requisitos empresariales. La red debe admitir un conjunto cada vez más diverso y cambiante de usuarios, dispositivos, aplicaciones y servicios. Debe incorporar este conjunto diverso de dispositivos de forma fluida y segura y, a la vez, ofrecer la experiencia de usuario y aplicación deseada.



También debe garantizar un acceso rápido y seguro a y entre cargas de trabajo dondequiera que residan. Y para que la red funcione de manera óptima, todo esto debe lograrse de extremo a extremo entre usuarios, dispositivos, aplicaciones y servicios en cada dominio de red: campus, sucursales, redes remotas/domésticas, WAN, proveedores de servicios, dispositivos móviles, centros de datos, nubes híbridas y múltiples nubes.

Esto significa que las organizaciones necesitan una arquitectura nueva e integrada para cada dominio de red; que sea personalizada para satisfacer las necesidades específicas de ese dominio y que proporcione una manera de comunicarse y aplicar políticas coherentes en todos los dominios.

Figura 3: Cuatro objetivos principales para la nueva red

Alinearse con el negocio	Quitar la complejidad	Garantizar el rendimiento	Reducir el riesgo
• Habilitar nuevas iniciativas empresariales digitales • Alinear dinámicamente con las cambiantes necesidades de las aplicaciones	• Simplificar las operaciones de TI frente a las crecientes demandas • Permitir que la TI centre los recursos en la creación de valor para el negocio	• Satisfacer de manera coherente los requisitos de experiencia del usuario y rendimiento del servicio • Evitar las interrupciones de red	• Prevenir o contener las amenazas a la seguridad antes de que causen daños • Respetar los requisitos regulatorios y de cumplimiento

Los expertos de Cisco imaginan la arquitectura de la red emergente.

La mayoría de las redes actuales aún no están listas para satisfacer las demandas de esta era digital emergente. En nuestra *Encuesta sobre tendencias de redes a nivel global 2019*, encontramos que si bien el 39% de los líderes de la TI creen que sus redes están muy bien alineadas para satisfacer las demandas del negocio digital, solo el 19% de los estrategas de redes creen lo mismo.[14]

Aun así, existe una razón para ser optimista. John Apostolopoulos, CTO de Cisco para Redes Empresariales, anticipa una transición relativamente corta de las infraestructuras en gran medida rígidas y operadas manualmente a las arquitecturas más ágiles y basadas en software que pueden "adaptarse continuamente para satisfacer las cambiantes demandas de las aplicaciones y los servicios de los que depende la organización".

> "Las redes funcionarán como un sistema con niveles crecientes de autonomía, al tener en cuenta su propio estado, el estado dinámico de todos los usuarios y las aplicaciones, además de la amplia gama de opciones posibles".
>
> – Ravi Chandrasekaran, Vicepresidente Senior de Ingeniería, Redes Empresariales de Cisco

¿Cómo será esta arquitectura de red emergente? De acuerdo con Ravi Chandrasekaran, Vicepresidente Senior de Ingeniería, Redes Empresariales de Cisco: "Las redes funcionarán como un sistema con niveles crecientes de autonomía, al tener en cuenta su propio estado, el estado dinámico de todos los usuarios y las aplicaciones, además de la amplia gama de opciones posibles".

Observamos que si bien el 39% de los líderes de la TI creen que sus redes están muy bien alineadas para satisfacer las demandas del negocio digital, solo el 19% de los estrategas de redes creen lo mismo.[14]

La clave para lograr este estado más autónomo será la IA, que ayudará a los equipos de TI a responder rápidamente a las cambiantes condiciones de la red, ya sea que esto signifique cambiar automáticamente las rutas de tráfico, solicitar más ancho de banda, requerir un cambio de política o incluso rechazar una nueva solicitud de servicio.

Con el tiempo, al aprovechar la inteligencia y la automatización de todo el sistema, la red se volverá completamente transparente para el usuario. Simplemente estará allí, ofreciendo conectividad segura a los servicios que la necesitan, en el nivel requerido, en todas partes y en todo momento.

Si bien Apostolopoulos admite que todavía hay un largo camino por recorrer antes de que las redes tengan toda la inteligencia y potencia que

necesitan para cumplir con esta promesa, cree que los avances técnicos necesarios para reunir el aseguramiento de servicios habilitados para IA, la automatización basada en controladores, el procesamiento de lenguajes naturales y las mejoras significativas en la seguridad de la red están en marcha.

Caso de uso para la nueva red

En el año 2025, una red empresarial de vanguardia podrá tomar un requerimiento comunicado en un lenguaje natural desde cualquier línea de negocios y traducirlo automáticamente a un conjunto de políticas y acciones automatizadas que garantizarán que la necesidad del negocio se satisfaga continuamente a través de la red; todo sin afectar ningún otro servicio existente. Una red con estos tipos de capacidades es lo que comúnmente se conoce como una red basada en intención.

Así es como podría verse un caso de uso hipotético para una red basada en intención.

Descripción general: Una organización desea utilizar sensores ópticos de IoT inalámbricos para admitir una innovación empresarial que se entrega a través de una aplicación de realidad aumentada. Así es como la necesidad y la intención del negocio se traducirían en una acción de red.

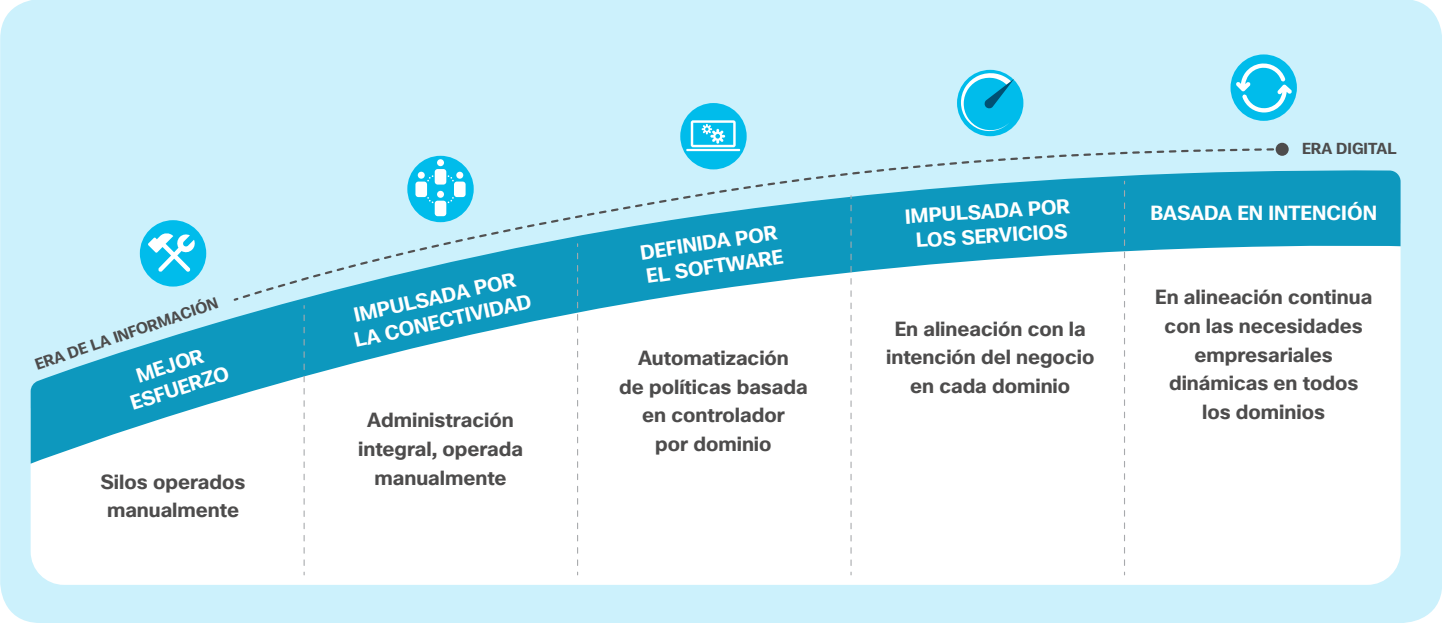
Figura 4: Caso de uso para la nueva red

El estado de la arquitectura de red

¿Dónde se encuentran las organizaciones hoy en día en su camino hacia una red más avanzada que pueda satisfacer las demandas de la era digital? El modelo de preparación de red digital de Cisco proporciona un modelo de madurez estándar de cinco etapas para ayudar a las organizaciones de TI a evaluar su nivel actual de preparación de la red y ayudarlas a planificar dónde deben estar en el futuro.

El modelo se puede aplicar en varias categorías de preparación de la red, como arquitectura, acceso, WAN, aseguramiento, seguridad de red, etc.

Figura 5: Modelo de preparación de red digital de Cisco



Reporte sobre tendencias globales en redes 2020

Tendencias en tecnologías de redes

Cinco tecnologías que están dando forma a la nueva red

En este preciso momento, una serie de importantes desarrollos tecnológicos de redes se están fusionando para sentar las bases de un nuevo modelo de red. Los avances en cinco áreas tecnológicas en particular (**automatización, IA, redes multinube, redes inalámbricas** y **seguridad de red**) prometen impulsar la mayor ola de transformación de redes vista en décadas. Estas tecnologías apoyarán las necesidades del mercado de aumentar la escala, la agilidad y la seguridad y, al hacerlo, permitirán las tendencias emergentes que están cambiando el mundo tal como lo conocemos.

5

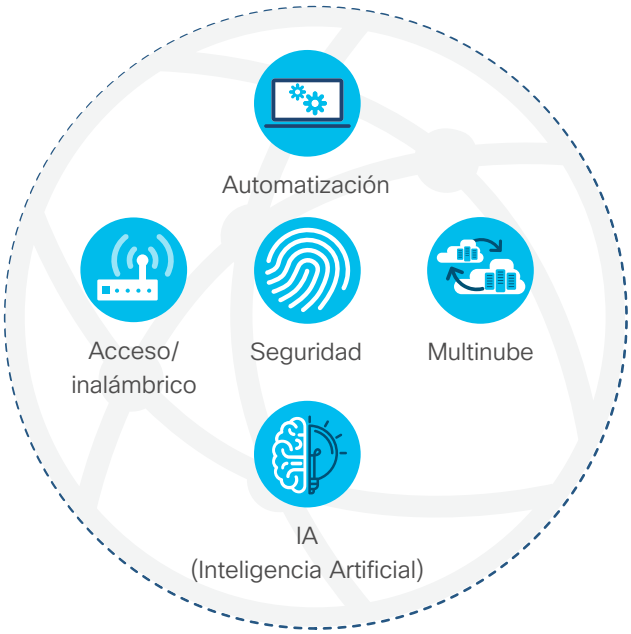
Áreas de tecnología

- Automatización
- IA (Inteligencia Artificial)
- Networking multinube
- Inalámbrico
- Seguridad de red

"Las organizaciones de todo el mundo se dan cuenta de la necesidad de transformarse digitalmente para mantenerse a la par del mercado y satisfacer las demandas de empleados, socios, clientes e integrantes", dice Brandon Butler, Analista Senior de Investigación de IDC, Redes Empresariales. "Los líderes de TI también se dan cuenta de que sin una red más robusta, segura y ágil, la transformación digital de su organización está en riesgo, lo cual estimula la refactorización simultánea de múltiples aspectos de sus redes".

Una mirada más en detalle al estado de cada una de estas áreas tecnológicas proporciona información sobre cómo están reinventando la red, su estado de adopción actual y los cambios que podemos esperar en un futuro próximo.

Figura 6: Cinco tecnologías que dan forma a la transformación de la red



Automatización de la red a escala

Resumen de la sección

Aportes clave

- Juntos, las redes definidas por el software (Software-Defined Networking, SDN), las redes basadas en intención (Intent-Based Networking, IBN), la virtualización de redes, la programabilidad y los controladores de redes de plataforma abierta están haciendo que la alineación automatizada de los servicios de red con las necesidades del negocio y los procesos de TI sea una realidad.
- La IBN aumenta las capacidades de automatización de la SDN con la capacidad de traducir la intención en políticas, recopilar datos, proporcionar visibilidad, corregir problemas y asegurar que las políticas en verdad estén logrando sus objetivos.
- El objetivo de la IBN es aplicar y asegurar continuamente los requisitos de rendimiento del servicio, las políticas de seguridad y cumplimiento, además de los procesos de las operaciones de TI en toda la red.
- Las interfaces de programación de aplicaciones (API) en un controlador de plataforma abierta le permiten al controlador integrar e intercambiar información con servicios de red y TI adyacentes, otros dominios de TI, aplicaciones empresariales e infraestructura heterogénea.

Principales hallazgos

- Según los líderes de la TI, la automatización de la red (25%), SDN (23%) e IBN (16%) son algunas de las tecnologías que tendrán más impacto en las redes durante los próximos cinco años.
- El 27% de los líderes de TI identificó al aislamiento de diseño y enfoque operativo en los dominios de acceso, WAN, centro de datos, nube y seguridad como un obstáculo para la adopción de tecnologías de red avanzadas.
- El 34% de los líderes de TI identificó a la mejor coordinación e integración de la red con otros equipos de TI como un área importante para mejorar.
- Aunque en la actualidad solo el 4% de los líderes de TI y estrategas de redes clasifican a su red como basada en intención, el 35% planea pasar a una red basada en intención dentro de los próximos dos años.

Resumen de la sección (continuación)

Orientación esencial

- Los líderes de TI deben evaluar la preparación de sus redes para entregar servicios de red al ritmo de las demandas empresariales.
- Analice crear una hoja de ruta que ofrezca una estrategia de red de bucle cerrado basada en intención en todos los dominios de red y a pasos incrementales para que cada uno ofrezca el mejor ROI a la organización.
- Identifique y priorice los procesos de TI y las aplicaciones empresariales que se beneficiarán más de la integración con un controlador de red de plataforma abierta.

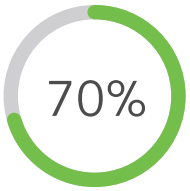
Principal predicción

"La visión largamente asumida de la aplicación de una política basada en intención de extremo a extremo comenzará a ser una realidad hacia el año 2025. Los equipos de redes podrán automatizar las políticas de segmentación dinámica y optimización de servicios a escala en todos los dominios (acceso, WAN, centro de datos, multinube, IoT) desde el cliente hasta la aplicación y entre las cargas de trabajo distribuidas".

– Ronnie Ray, Vicepresidente de Experiencia del Cliente de Redes Empresariales, Cisco

Automatización de la red a escala

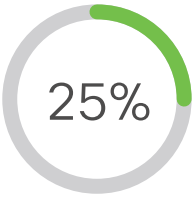
La automatización de la red, por supuesto, es el proceso de automatizar la configuración, administración, pruebas, implementación y operación de dispositivos físicos y virtuales dentro de una red. Incluso la optimización de la red en sí misma se puede automatizar para crear mejoras continuas del servicio.



Según Gartner: "Aproximadamente el 70% de las tareas de red del centro de datos se realizan manualmente, lo que aumenta el tiempo, el costo y la probabilidad de errores y reduce la flexibilidad".[15]

La automatización puede mejorar la disponibilidad de la red y aliviar a los equipos de operaciones de red (NetOps) en cuanto a las tareas diarias que consumen mucho tiempo. Por lo tanto, no es de sorprender que cuando se les preguntó sobre qué tecnologías tendrían el mayor impacto en las redes durante los próximos cinco años, el 25% de los líderes de TI apuntaron a la automatización de la red.[14]

Las innovaciones en las áreas de SDN, IBN, virtualización, programabilidad y controladores de plataforma abierta están haciendo que la automatización sea una realidad para las redes actuales.



El 25% de los líderes de TI cree que la automatización tendrá el mayor impacto en las redes durante los próximos cinco años.[14]

Redes definidas por software: apenas el comienzo

Durante los últimos años, la SDN significó a un gran paso hacia la habilitación de la automatización en toda la red. La SDN les permite a los equipos de redes administrar las redes como sistemas integrales, al hacer que la gestión sea más eficiente y flexible al separar los planos de control y de reenvío.

Como resultado, el plano de control se puede programar de forma directa. Abstrae la infraestructura y los dispositivos subyacentes de los servicios de redes y las aplicaciones. La inteligencia de la red se centraliza lógicamente a través de controladores SDN programables.

Al principio la SDN se introdujo para simplificar los entornos de los centros de datos complejos que necesitaban admitir migraciones de cargas de trabajo dinámicas portátiles y tráfico de servidor a servidor. Los mismos principios están subyacentes en el acceso definido por el software (SD-Access), que ayuda a proteger el acceso de usuarios y dispositivos de manera más eficaz, y la WAN definida por software (SD-WAN), que puede habilitar mejores experiencias de los usuarios que acceden a las aplicaciones y los servicios en la nube.

Redes basadas en intención: cerrar el bucle

El objetivo principal de los equipos de redes es entregar, de manera continua, rendimiento y protección de aplicaciones y servicios para el negocio. Así que mientras que la SDN ofrece avances importantes en automatización, esto es solo una parte de la solución. Las organizaciones también necesitan supervisión y optimización continuas de la red para admitir modelos de negocios cada vez más dinámicos e impulsados digitalmente.

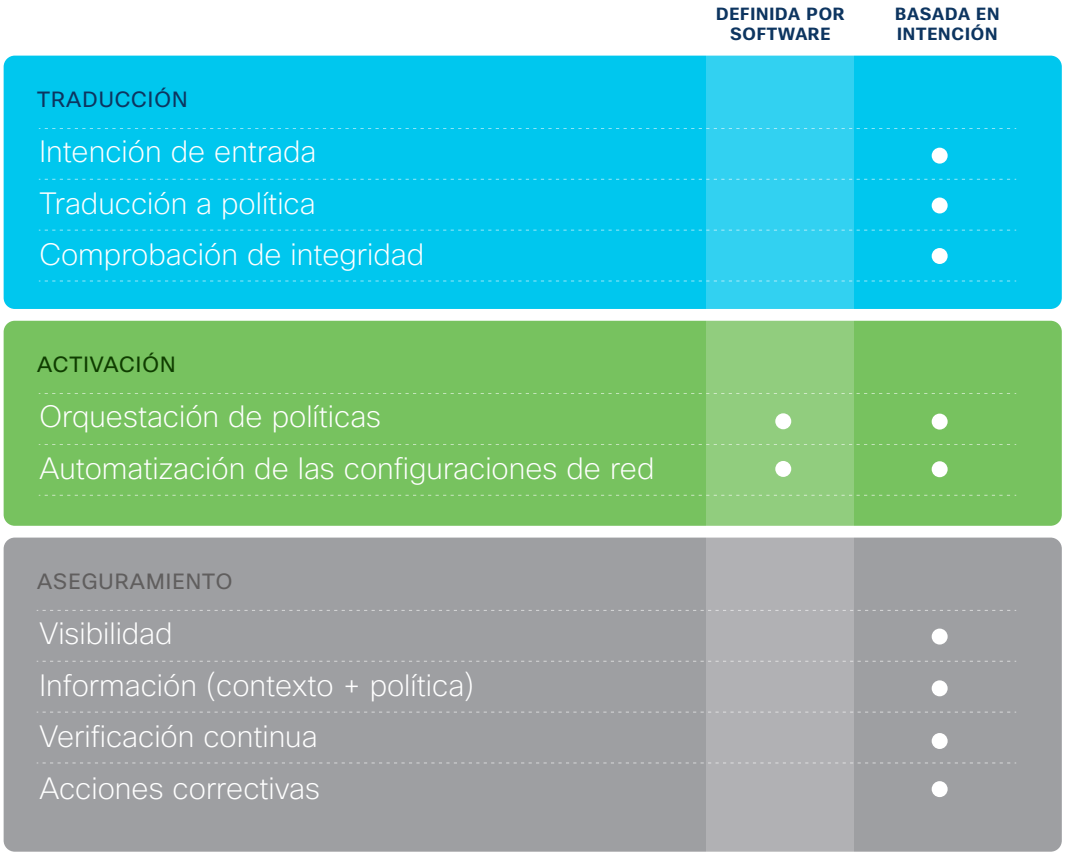
Para lograrlo, las redes deben comprender la intención cambiante del negocio y supervisar las condiciones dinámicas de la red para poder satisfacer continuamente esa intención. Según un borrador del Grupo de Trabajo de Ingeniería de Internet (Internet Engineering Task Force, IETF): “La intención constituye una política declarativa con alcance en toda la red. Un operador humano define 'qué' se espera, y la red calcula una solución que cumpla con los requisitos”.[16]

La red basada en intención es un modelo de red relativamente nuevo que fue introducida por primera vez en el mercado en el año 2017, y desde entonces, ha sido ampliamente adoptado por la industria de redes.

Para ser útil, el sistema también debe verificar continuamente que se está cumpliendo la intención y, en caso contrario, proporcionar orientación

para su rectificación. Gartner afirma que "las configuraciones basadas en políticas pasarán a ser soluciones de redes basadas en intención (IBN) con automatización y supervisión automática, lo que garantizará que la red en verdad cumpla con la intención de las políticas establecidas en el momento de la configuración".[15]

Figura 7: IBN: Desarrollar sobre los fundamentos de la SDN



En nuestra *Encuesta sobre tendencias de redes a nivel global 2019*, observamos que el 26% de los estrategas de redes identificaron a la implementación de redes basadas en la intención en uno o más dominios como una prioridad tecnológica para lograr la red ideal. Y aunque en la actualidad solo el 4.3% de los encuestados clasifican a su red como basada en la intención, el 35% planea pasar a una red basada en intención dentro de los próximos dos años.[14]

John Apostolopoulos explica que un controlador de IBN se amplía a SDN con el fin de entregar un sistema más completo para adaptar continuamente la red y lograr la intención deseada de negocio. Aumenta las capacidades de automatización de la SDN con la capacidad de traducir la intención en políticas, recopilar datos, proporcionar visibilidad e información relevante y, luego, asegurar que la red en verdad esté haciendo lo previsto. La retroalimentación de bucle cerrado proporcionada por la IBN es fundamental para lograr los beneficios deseados.[17]

Una red basada en intención captura la intención del negocio y utiliza analítica, aprendizaje automático, razonamiento automático y automatización para alinear la red de forma continua y dinámica frente a las cambiantes necesidades del negocio, así como también para adaptarse a las cambiantes cargas de la red y otros efectos del entorno. Eso puede significar aplicar y asegurar continuamente los requisitos de rendimiento del servicio y las políticas de operaciones de TI, cumplimiento y usuario en toda la red.

¿Cómo funcionan las redes basadas en intención? La definición de IBN de Cisco incluye tres bloques de creación funcionales: traducción, activación y aseguramiento.[18]

Figura 8: Elementos de una red basada en intención

Los líderes de TI se encuentran bajo presión para entregar servicios de forma más rápida, más eficiente, en colaboración y competencia con los servicios en la nube. Desde una perspectiva tecnológica, la experiencia en IA, cómputo y capacidad de procesamiento que se requiere para la IBN está cada vez más disponible.

Rohit Mehra de IDC comenta lo siguiente: “Las redes basadas en intención constituyen un importante desarrollo para la industria de las redes. Abarca no solo avanzados niveles de visibilidad, automatización y aseguramiento, sino que es la plataforma sobre la que se desarrollará una nueva funcionalidad de administración de redes basadas en aprendizaje automático”.[19]

Virtualización de las funciones de la red

El modelo de virtualización que ha modificado radicalmente los servicios informáticos ha sido adoptado en las redes en forma de virtualización de las funciones de la red (Network Functions Virtualization, NFV). Le permite a NetOps entregar o modificar rápidamente los servicios de red, e implementarlos y administrarlos en forma remota. Además de la agilidad de TI, la NFV ofrece una consolidación física sustancial, al ahorrar espacio y energía y crear menos puntos de posibles fallas.

La programabilidad como la base de la red

Para que los sistemas y controladores de IBN sean escalables y alcancen todo su potencial, deben desarrollarse sobre una infraestructura de red física o virtual programable. Las interfaces y los dispositivos programables, junto con los circuitos integrados de aplicaciones específicas (Application-Specific Integrated Circuits, ASID) programables, forman la base subyacente para las redes inteligentes.

Para adoptar sistemas automatizados y más eficientes, los equipos de TI continúan alejándose de los enfoques tradicionales de administración manual basados en la interfaz de línea de comandos (Command Line Interface, CLI). En su lugar, están adoptando interfaces impulsadas por modelos de datos (Data Model–Driven Interfaces, DMI). Estas interfaces basadas en modelos estándar proporcionan coherencia, apertura, estructura y eficiencia.

En la delantera del camino hacia un modelo operativo sustentable que ofrezca coherencia y facilidad de uso, los modelos estándar del Grupo de Trabajo de Ingeniería de Internet (Internet Engineering Task Force, IETF) como YANG (Yet Another Next Generation) proporcionan un conjunto completo de interfaces northbound de programación.

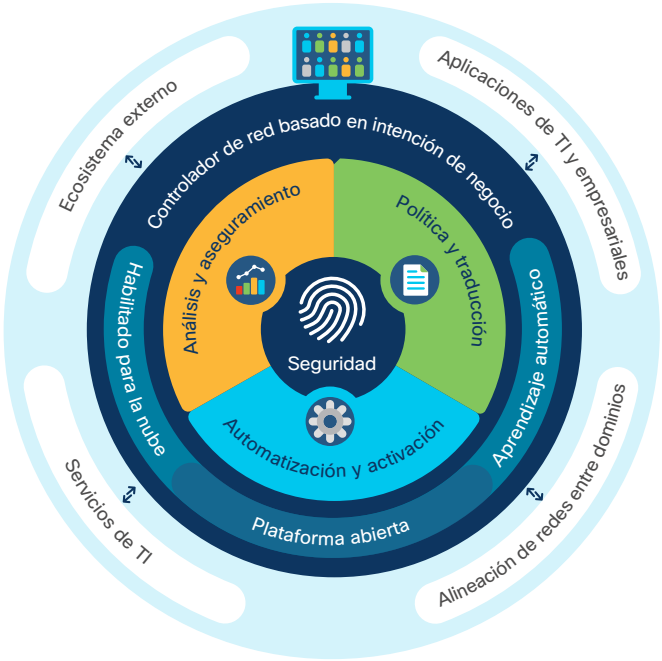
Controladores de IBN de plataforma abierta: procesos de TI y la integración con el negocio

Las interfaces de programación de aplicaciones (API) en el controlador le permiten integrar e intercambiar información con servicios de red y TI adyacentes, otros dominios de TI, aplicaciones de líneas de negocio e infraestructura heterogénea.

Esto convierte a la red en una plataforma abierta que puede aceptar especificaciones de políticas de aplicaciones y dispositivos, aprovechar la automatización centralizada de políticas entre dominios y comprobar que el sistema satisfaga las necesidades del negocio. Esto mejora la prestación de los servicios de TI al optimizar los flujos de trabajo en todos los dominios de red, los sistemas de TI y los procesos de las líneas de negocios que solían administrarse de forma independiente.

En nuestra *Encuesta sobre tendencias de redes a nivel global 2019*, el 34% de los líderes de TI identificó el lograr una mejor coordinación e integración de la red con otros equipos de TI como un área importante para mejorar.[14]

Figura 9: Controlador de plataforma abierta para la integración con aplicaciones empresariales, servicios de TI y dominios de red



Con la extensibilidad de red de las API y del kit de desarrollo de software (SDK), TI puede alinearse mejor a las necesidades de las aplicaciones empresariales y de TI, optimizar las operaciones y garantizar la protección de la inversión.

Alineación de garantía y políticas entre dominios: del cliente a la carga de trabajo

Los equipos de redes deben trabajar en conjunto para lograr una alineación integral de la red con la intención de negocio. Eso significa crear un enlace sin problemas desde dondequiera que el cliente o "cosa" se esté conectando a la red, hasta dondequiera que se hospede el servicio o la aplicación.

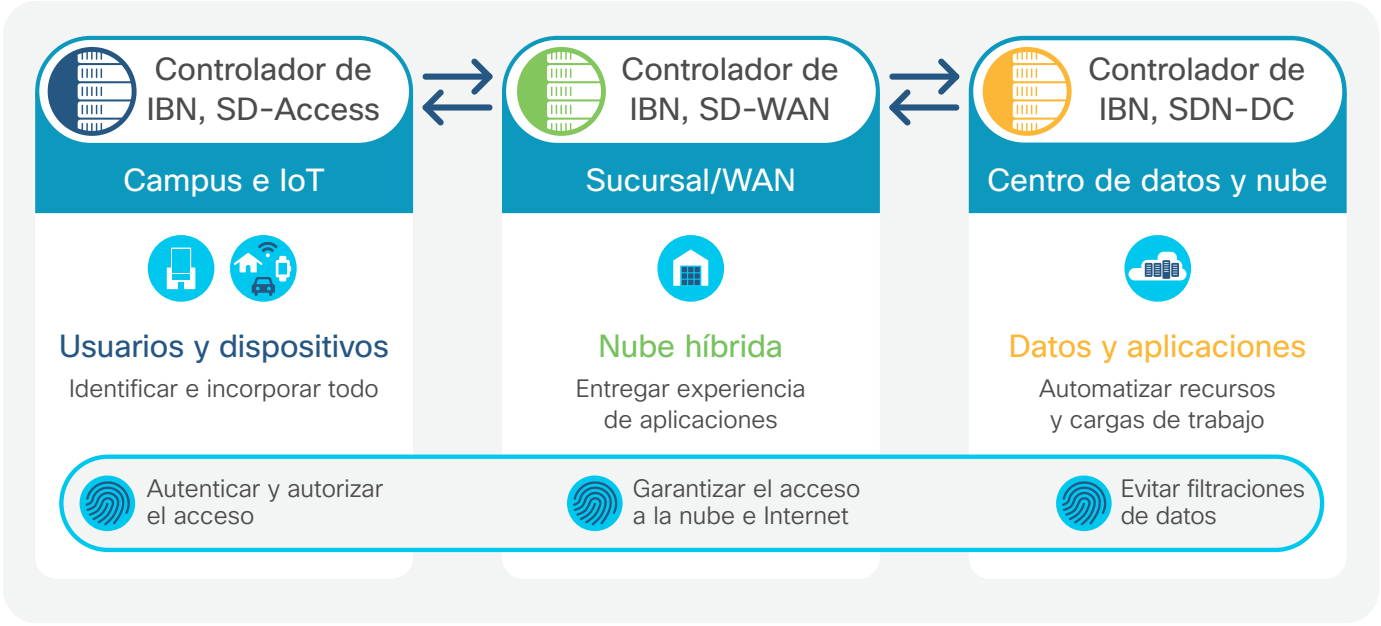
Análisis actual: Para que una empresa tenga éxito con las redes basadas en la intención, debe adoptar completamente la automatización en el centro de datos, el campus, la red de área amplia y la sucursal.[20]

Sin embargo, en muchos casos, eso no se logra con facilidad. En nuestra *Encuesta sobre tendencias de redes a nivel global 2019*, el 27% de los líderes de la TI identificó al "aislamiento de diseño y enfoque operativo en los dominios de acceso, WAN, centro de datos, nube y seguridad" como un obstáculo para la adopción de tecnologías de red avanzadas.[14]

Por una buena razón, en general la red se divide en dominios organizados en torno al objetivo principal del dominio. Sin embargo, para lograr una verdadera e integral visibilidad, control y validación de la intención empresarial, las capacidades de aseguramiento y política deben estar organizadas entre los dominios.

Los líderes de TI están adoptando medidas para lograrlo: un 26% de los líderes de TI identifican la "aplicación y aseguramiento de políticas de redes multidominio en integración" como una prioridad para el aumento de inversión.[14]

Figura 10: Política y aseguramiento: Alineación entre todos los dominios de IBN



Aseguramiento habilitado por IA

Resumen de la sección

Aportes clave

- El uso de la inteligencia artificial (IA) se está convirtiendo en un elemento fundamental para las operaciones, la prestación de los servicios y el aseguramiento de la red, donde la AIOps (la combinación entre operaciones y capacidades de IA) se está convirtiendo en una categoría bien establecida.
- El crecimiento explosivo del volumen de tráfico, los dispositivos móviles y de IoT conectados, las aplicaciones y los microservicios interconectados, junto con las amenazas de seguridad en constante aumento, se ha vuelto abrumador para los equipos de redes.
- Las grandes cantidades de datos, la telemetría y los eventos generados por las redes que admiten un número cada vez mayor de dispositivos y servicios están superando la capacidad de los operadores humanos por sí solos para tomar medidas.
- Fundamental para un modelo de red basada en intención (IBN), la IA utiliza la gran cantidad de datos originados en la red para explorar la complejidad del entorno y proponer dinámicamente ajustes en la red.
- El aprendizaje automático y el razonamiento automático se complementan entre sí para entregar procesamiento de eventos complejos, conocimientos correlacionados y corrección guiada.

Principales hallazgos

- Más del 50% de los estrategas de redes identifican a la IA como una inversión de red prioritaria.
- Solo el 17% de los estrategas de redes cree que la falta de madurez de las tecnologías de IA supone un obstáculo para la modernización de la red.
- Actualmente solo el 22% de los equipos de redes utilizan cualquier tipo de IA para el aseguramiento de red, posiblemente porque la disponibilidad de herramientas genuinamente habilitadas para IA sigue siendo bastante nueva.
- El 72% de los estrategas de redes proyecta utilizar información predictiva habilitada por IA o remediación prescriptiva durante los próximos dos años.

Orientación esencial

- Aproveche el aprendizaje de IA basado en la nube: en algunos casos, se necesitarán cambios en las políticas de datos corporativos para aprovechar las ventajas de las herramientas de IA habilitadas para la nube.

Resumen de la sección (continuación)

- Entrelazamiento entre IA y personas: Defina progresivamente hasta qué punto la IA puede llegar en la toma de decisiones o en la adopción de medidas antes de que un operador humano deba involucrarse para supervisar, aprobar o hacer un cambio.
- Conocimientos sobre IA: El conocimiento experto en redes será un conjunto de habilidades de primer orden necesario para verificar que la IA esté logrando los objetivos de TI y de negocio según lo previsto.

Principal predicción

"Para el año 2025, las herramientas de aseguramiento de red habilitadas por IA automatizarán completamente varias tareas específicas y bien definidas. Sin embargo, la mayoría de las tareas operativas que exigen una toma de decisiones más flexible y contextual seguirán necesitando de la experiencia y la intervención de los operadores humanos".

– JP Vasseur, Cisco fellow, Cisco

Aseguramiento habilitado por IA

La IA está impulsando poderosas transformaciones en diversas industrias y ahora se está convirtiendo en fundamental para las operaciones de TI, donde la AIOps se está convirtiendo en una categoría bien establecida.

¿Qué significan AI, ML y MR?

En pocas palabras, la IA es un campo de estudio que dota de inteligencia similar a la humana a las computadoras para realizar una tarea. Dos de las categorías más importantes de la IA son el aprendizaje automático (Machine Learning, ML) y el razonamiento automático (Machine Reasoning, MR). El aprendizaje automático se puede describir como la capacidad de "aprender estadísticamente" a partir de los datos y sin programación explícita. El razonamiento automático utiliza el conocimiento adquirido para navegar a través de una serie de posibles opciones hacia un resultado óptimo.

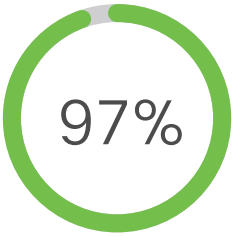
Como tal, el ML le permite a un sistema examinar los datos y deducir el conocimiento. Va más allá de tan solo aprender o extraer conocimiento: pasa a utilizar y mejorar el conocimiento con el tiempo y con la experiencia. En esencia, el objetivo del ML es identificar y aprovechar los patrones ocultos en los datos de "capacitación".

El MR es adecuado para resolver problemas que requieren una amplia experiencia en un dominio. Los seres humanos necesitan capturar explícitamente todos los conocimientos a priori para que un razonador automático pueda operar sobre nuevos datos. El MR es un excelente complemento del ML porque puede basarse en las conclusiones presentadas por el ML y analizar posibles causas y potenciales opciones de mejoras.

La complejidad de las redes impulsa la adopción de la IA

Varios factores están impulsando la adopción de redes habilitadas para IA. A raíz del aumento sin precedentes en la complejidad y la escala de las redes, la IA se vuelve cada vez más necesaria para ayudar a los equipos de TI a ofrecer niveles de red y de servicio coherentes.

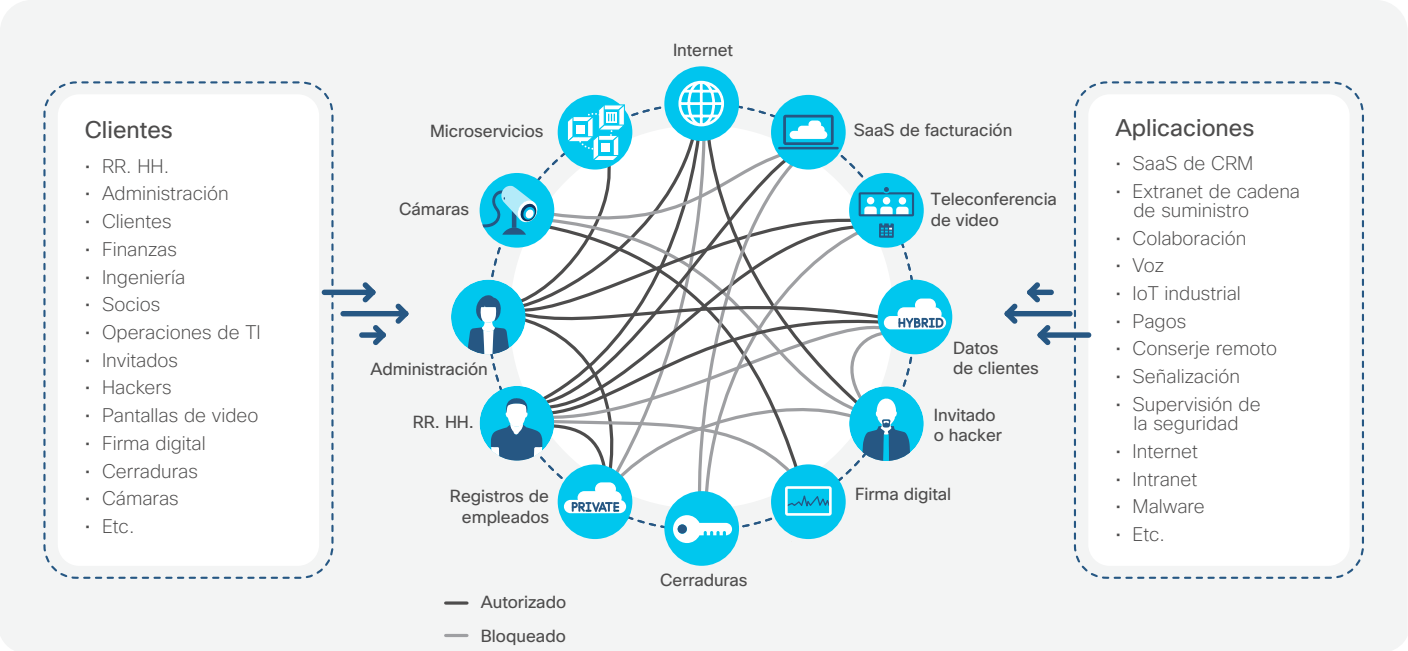
Las redes están brindando respaldo para el crecimiento explosivo del volumen de tráfico, los dispositivos móviles y de IoT conectados, además de las aplicaciones y los microservicios interconectados. Las redes actuales también están generando enormes cantidades de datos que superan la capacidad de administración de los operadores humanos por sí solos, y mucho menos, comprenderlos de manera oportuna.



El costo de las interrupciones de la red

El 97% de los líderes globales de TI encuestados dijeron que habían tenido problemas de rendimiento relacionados con aplicaciones empresariales críticas en los seis meses anteriores. ¿El costo promedio por interrupción de la red? Es de US$402,542 en los Estados Unidos y US$212,254 en el Reino Unido.[21]

Figura 11: La complejidad de las redes de las organizaciones hiperconectadas



La IA ofrece el potencial de que los equipos de redes utilicen mejor estos datos para garantizar así que sus redes funcionen de forma eficaz y en alineación continua con las necesidades del negocio. Por ejemplo, puede ayudar a crear mejores líneas de base, predecir problemas con precisión y ayudar con la solución de problemas de sistemas complejos.

Los estrategas de redes ya reconocen este hecho. Más del 50% identifica a la IA como una inversión prioritaria y necesaria para ofrecer su red ideal,[14] mientras que solo el 17% cree que la falta de madurez de las tecnologías de IA supone un obstáculo para la modernización de la red.[14]

Al utilizar la gran cantidad de datos originados en la red, la IA aprende la complejidad del entorno de comunicaciones y de redes, y puede proponer dinámicamente ajustes en la red. Esta capacidad hace que la IA sea fundamental para un modelo de IBN.

La IA y las tecnologías de redes avanzadas (como la IBN) están claramente modificando la manera en que se hacen las cosas, especialmente para las operaciones de red. Las pruebas de nuevas aplicaciones se pueden realizar en minutos en lugar de semanas. La solución de los problemas de red se vuelve mucho más fácil cuando un motor de garantía identifica las causas de fondo y recomienda correcciones. De hecho, cuando está equipado con potentes paneles que ofrecen información práctica, puede que un futuro operador de red solo necesite buscar en un puñado de lugares, en lugar de hacerlo a través de montones de posibles causas.

Figura 12: Redes basadas en la intención impulsadas por la IA

¿Cómo se aplican ML y MR en un contexto de red?

Como se indicó anteriormente, un elemento importante de las operaciones de redes y de las redes basadas en intención es el aseguramiento de red, que es la verificación continua de que el estado y el comportamiento de la red son coherentes con la intención deseada. El aprendizaje automático y el razonamiento automático ofrecen capacidades únicas que los operadores pueden utilizar para asegurar el rendimiento de red necesario, en especial, en torno a las siguientes tres principales áreas de aseguramiento (ver la Figura 13 a continuación):

Procesamiento de eventos complejos: Al aplicar el ML a la telemetría de red, es posible establecer líneas de base dinámicas de lo que constituyen condiciones de funcionamiento normales para una intención determinada.

Información correlacionada: El ML puede proporcionar información más detallada y visibilidad sobre el funcionamiento de la red e incluso ayudar a predecir cuándo es probable que se produzca una condición anómala en el futuro. El MR mejora la potencia de ML mediante la aplicación de conocimientos expertos precargados y capturados a partir de los flujos de trabajo de la corrección de problemas similares.

Remediación: La remediación permite una alineación constante con la intención mediante la identificación de las acciones correctivas más adecuadas al utilizar las bases de conocimiento proporcionadas; por ejemplo, con el MR.[22]

Estado actual y futuro de la IA para el aseguramiento de la red

Los datos de nuestra *Encuesta sobre tendencias de redes a nivel global 2019* clarifican en qué punto se encuentran las organizaciones en su camino a la adopción del aseguramiento de red habilitado por IA.

Mediante nuestro modelo estándar de preparación de cinco etapas para medir el estado

Figura 13: Casos de uso de ML y MR para el aseguramiento de la red

	Aprendizaje automático	Razonamiento automático
Enfoque de la tecnología	Modelo matemático a partir de grandes conjuntos de datos	Captura de conocimiento humano, lógica simbólica
Aplicabilidad	Análisis predictivo, detección de anomalías, clasificación, regresión	Mecanización de flujos de trabajo decidibles
Función de aseguramiento de la red	• Línea de base dinámica e identificación de problemas • Información y visibilidad • Análisis predictivo	• Solución automática de problemas • Corrección automática

de preparación, solo el 22% de los estrategas de red encuestados informaron que actualmente utilizaban cualquier capacidad de IA para el aseguramiento de red. Esto se puede atribuir al hecho de que las soluciones de aseguramiento de red genuinamente basadas en IA son todavía relativamente nuevas. Sin embargo, el 72% de los encuestados sí planea lograr corrección prescriptiva o información predictiva habilitada para IA durante los próximos dos años.[14]

Figura 14: Preparación para el aseguramiento habilitado para IA

Pregunta: ¿Qué oración describe mejor el enfoque actual de su organización para el análisis y la visibilidad del rendimiento?
Fuente: *Encuesta sobre tendencias de redes a nivel global 2019;* n = 1556 estrategas de redes

Consideraciones para seguir adelante con la IA

Según el colega JP Vasseur de Cisco, al evaluar el uso de la IA en la infraestructura de la red, deben tenerse en cuenta los siguientes elementos:

1. **Crear prácticas recomendadas operativas:** Saber lo que la IA **no puede** y **no debe** hacer es tan importante como entender lo que **puede hacer**. Al determinar qué áreas de la empresa podrían beneficiarse más de la IA, asegúrese de identificar también las áreas que presentan el mayor nivel de riesgo y exposición.

2. **Definición de una función objetiva clara:** No existe ningún algoritmo con la capacidad de extraer hechos interesantes de un conjunto de datos sin que el equipo de ML especifique claramente los objetivos. Ser capaz de indicar claramente el objetivo y las métricas de rendimiento antes de comenzar el viaje hacia el ML es de suma importancia.

3. **Entrelazamiento entre IA y las personas:** Definir progresivamente hasta qué punto la IA puede llegar en la toma de decisiones o en la adopción de medidas antes de que un operador humano deba involucrarse para supervisar, aprobar o hacer un cambio es fundamental para el negocio y para la capacidad del equipo de redes a la hora de mantener el control.

4. **Conocimientos sobre IA:** Una dependencia cada vez mayor de la IA tiene el potencial de crear brechas de conocimiento, por lo que el conocimiento de expertos en redes será un conjunto de habilidades de primer orden necesario para verificar que la IA esté logrando los objetivos de TI y empresariales según lo previsto, además de ayudar a los operadores a tomar la decisión correcta a partir de las opciones recomendadas por el sistema de IA.

5. **Dependencia de los datos:** Mejore la recopilación de datos. La IA depende de los cálculos matemáticos para crear información práctica y esos cálculos son igual de buenos que la calidad de los datos que se utilizan. Los expertos en redes deberán trabajar entre diferentes funciones y dominios para garantizar que se pueda confiar en la calidad de los datos para las iniciativas de IA.

6. **¿Dónde se aplica la IA?:** El lugar de aplicación de la IA depende del rendimiento, la seguridad, la capacidad de los datos y la privacidad de la aplicación y los datos. Aunque hay algunas instancias de capacitación de modelos en un entorno local, actualmente la aplicación más común es el aprendizaje automático basado en la nube. La nube proporciona la capacidad informática y de almacenamiento para aprender y ejecutar el ML a partir de grandes cantidades de datos agregados y anonimizados provenientes de varias fuentes. En algunos casos, esto puede plantear preocupaciones de privacidad en términos de quién tiene acceso a esos datos e incluso en qué lugar se almacenan los datos. Además, tenga en cuenta las implicaciones de latencia que podrían afectar a la información en tiempo real para grandes conjuntos de datos; lo que podría ocurrir, por ejemplo, con sensores de video que producen grandes cantidades de datos.

7. **Cambiar el paradigma corporativo:** Es ideal alinear las políticas de datos de su empresa para así poder aprovechar la IA basada en la nube. Al conectar millones de sistemas a un único motor de análisis de IA, se puede alcanzar un tamaño de muestra de datos con la capacidad de proporcionar resultados exponencialmente mejores que con la misma tecnología alimentada con datos de una sola experiencia de red. Los equipos de TI pueden ser clave a la hora de sembrar hoy las semillas que mañana conducirán a las políticas amigables con la nube que admitirán la implementación de IA.

Redes para datos y aplicaciones en entornos multinube

Resumen de la sección

Aportes clave

- Todas las empresas necesitarán servicios basados en la nube, pero siempre será necesario mantener algunos datos y cargas de trabajo en el entorno local.
- En muchos casos, las aplicaciones monolíticas se están disolviendo en microservicios interconectados que se entregan a través de una variedad de cargas de trabajo virtuales y físicas incluidos en los contenedores, en el entorno local, en la nube y en el borde de red de la empresa.
- El centro de datos distribuido no funciona como uno tradicional, de modo que las organizaciones de TI deben adaptarse para satisfacer las crecientes demandas de conectividad de aplicaciones y redes de esta nueva arquitectura.
- La SD-WAN, el acceso directo a la nube, las instalaciones de alojamiento de datos y los intercambios en la nube, junto con los servicios de banda ancha y 5G más asequibles y de mayor capacidad, están surgiendo como los nuevos elementos importantes dentro de la arquitectura que garantizan que los servicios en la nube puedan cumplir con los requisitos empresariales de manera efectiva y asequible.

Principales hallazgos

- La SDN/NFV ya está transportando el 23% del tráfico dentro de los centros de datos empresariales, una cantidad que se espera que crezca al 44% para el año 2021.
- El 29% de los líderes de TI y los estrategas de redes creen que, dentro de dos años, contarán con capacidades de redes basadas en la intención en sus entornos locales, híbridos y de multinube.
- El aumento de la dependencia en la nube está impulsando el aumento del tráfico de WAN, y se espera que el tráfico de WAN de IP empresarial a nivel global se duplique para el año 2022 y alcance los 5.3 exabytes al mes.
- Más del 58% de las organizaciones de todo el mundo ya han implementado alguna forma de SD-WAN y más del 94% de los encuestados cree que contará con una SD-WAN basada en intención de funcionalidad básica o más avanzada implementada dentro de los próximos dos años.

Orientación esencial

- Identifique las aplicaciones y servicios basados en la nube más críticos y priorice todos los planes de SD-WAN para acceder y proteger esas aplicaciones en primer lugar.
- Amplíe la automatización consistente y basada en políticas en nube híbrida y en multinube, teniendo cuidado de considerar toda plataforma, hipervisor o marco de contenedores en toda ubicación y carga de trabajo (nativa en la nube, bare metal, hipervisor, contenedor y sin servidor).

Resumen de la sección (continuación)

- Esquematice los servicios de aplicaciones, cargas de trabajo y componentes de servicios a la red "extendida" para comprender mejor de qué aplicaciones, servicios y microservicios consta la red.
- Los equipos de centros de datos, nubes y redes deben colaborar para desarrollar la coherencia del servicio en todos los dominios de los proveedores de nubes públicas/SaaS, campus, sucursales, centros de datos y borde de red/IoT.
- Las aplicaciones y los servicios necesitarán de integración y entrega continuas entre las cargas de trabajo de entornos locales y en la nube. Y las empresas que implementan los procesos operativos para interconectar y dar soporte a este modelo cosecharán la velocidad y flexibilidad prometidas por la nube.

Principal predicción

"Para el año 2025, espero ver el 20% de las cargas de trabajo distribuidas en el borde de las redes, fuera de los entornos de centros de datos multinube y empresariales. Eso significa que una quinta parte del tráfico, que en general habría estado confinado dentro de un centro de datos, ahora tendrá que asegurarse y protegerse a través de la red empresarial y multinube".

– Vijoy Pandey, Vicepresidente y CTO del grupo de Plataforma y Soluciones de Nube, Cisco

Redes para datos y aplicaciones en entornos multinube

La necesidad de rapidez e innovación está empujando a las organizaciones de TI a modernizar las aplicaciones existentes y a desarrollar rápidamente nuevas aplicaciones que permitan el acceso a la información desde cualquier dispositivo y en cualquier momento. Los desarrolladores de aplicaciones y los usuarios empresariales de hoy en día aprecian la agilidad, la escalabilidad y el autoservicio de la nube.

Sin embargo, mientras que el 85% de las organizaciones de TI están evaluando o ya están utilizando la nube pública, el paso a la nube no nos cuenta toda la historia.[23] De hecho, la frase "el paso a la nube" no ha demostrado ser completamente precisa. Vijoy Pandey, Vicepresidente y CTO del grupo de Plataforma y Soluciones de Nube de Cisco, dice lo siguiente: "En los últimos años, a medida que se intentaba migrar las valiosas cargas de trabajo a la nube pública, se hizo evidente que no era una situación binaria y que había algunas cargas de trabajo, y lo más crítico, algunos datos, que tenían que permanecer en un entorno local".[24]

De entre las organizaciones que actualmente utilizan la nube pública, el 85 % aplica una estrategia de multinube, porcentaje que aumentará al 94 % en los próximos 12 meses.[25]

Pandey también señala que la decisión de mantener los datos en entornos locales se deriva de una serie de preocupaciones, incluidas las regulaciones y la protección de datos: "Otra preocupación es que si necesita obtener mucha información de sus datos, necesita realizar muchos análisis de datos. Para todas esas cargas de trabajo, necesita redes locales y de procesamiento local. Aunque todas las empresas necesitarán contar con servicios basados en la nube, la necesidad de disponer de instalaciones locales nunca desaparecerá. Es por eso que creo que apostar por entornos de multinube e híbridos es el camino por seguir".

El impacto en la red de cambiar los modelos de aplicaciones

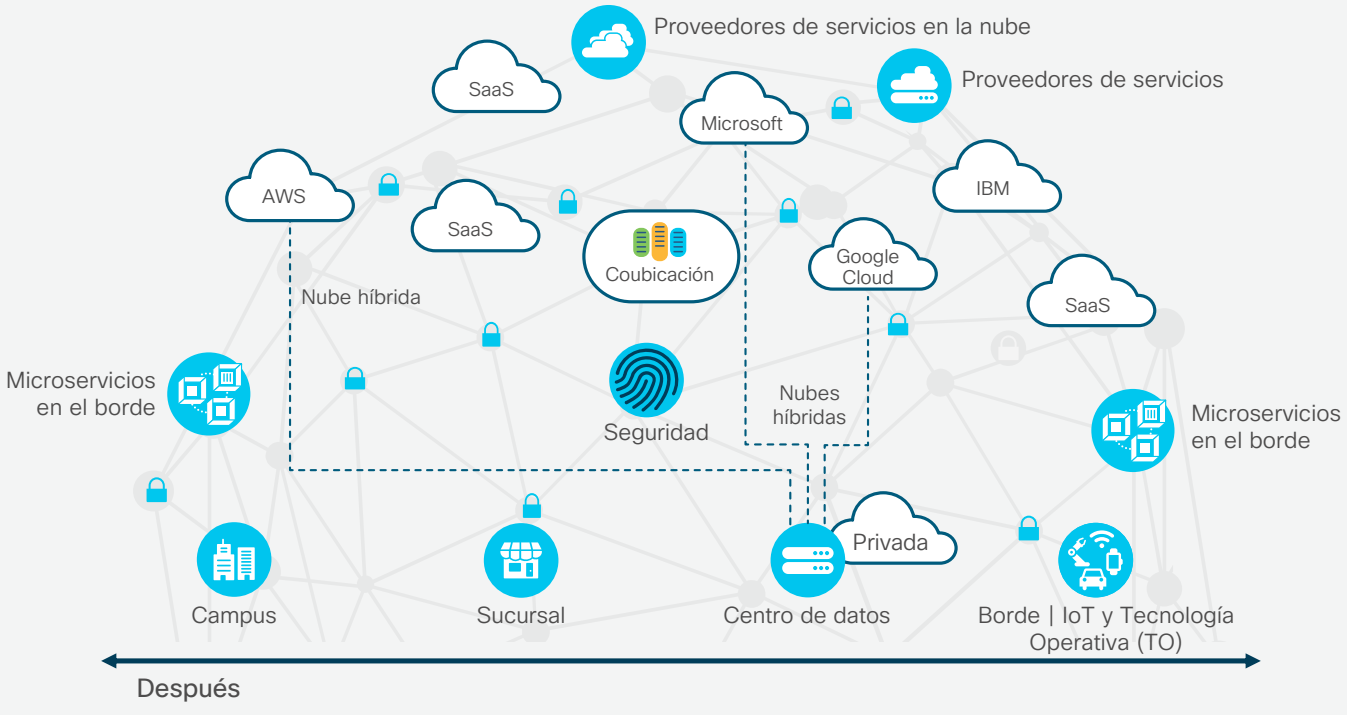
Tradicionalmente, el rendimiento de la red se centraba en dos elementos principales:

- La comunicación entre el cliente y la aplicación el servicio monolítico, generalmente alojado en un centro de datos centralizado.
- La comunicación dentro del centro de datos entre los servidores y el almacenamiento en red.

Figura 15: Antes: Comunicaciones en la carga de trabajo y del cliente al servicio

Pero este enfoque ya no es suficiente, ya que los equipos de aplicaciones siguen adoptando modelos de aplicaciones más ágiles, menos monolíticos y compuestos por múltiples cargas de trabajo o componentes de servicio que no siempre están alojados en las instalaciones, sino más bien distribuidos, más allá de los entornos locales y centros de datos.

Figura 16: Después: Comunicaciones en la carga de trabajo y del cliente al servicio



Mientras que algunos equipos de TI pueden creer que migrar a la nube significa que la red se convierte en algo menos de que ocuparse, nada puede estar más lejos de la realidad. Los equipos de centros de datos y de la nube ya no pueden trabajar por separado de los equipos de redes, un hecho que los líderes de TI ya han reconocido. Ahora identifican a las inversiones en redes para respaldar entornos multinube (públicas, infraestructura como servicio [IaaS] o SaaS) como una de sus prioridades más altas.[14]

Figura 17: Los equipos de TI priorizan la inversión en redes para entornos multinube

Pregunta: Si tuviera la capacidad para reducir el tiempo dedicado a mantener las actividades de statu quo, ¿en cuál de los siguientes servicios de valor agregado pondría más atención?

Fuente: *Encuesta sobre tendencias de redes a nivel global 2019*; n = 505 líderes de TI

Según comenta Tom Edsall, CTO de Cisco para centros de datos y asesor emérito: "A medida que las aplicaciones, las cargas de trabajo, los servicios y los datos se vuelven más distribuidos por todo el continuo de la nube-borde de red, hay una responsabilidad adicional sobre los líderes de TI en su conjunto para garantizar que los servicios sean entregados de forma segura y confiable y con el rendimiento deseado, independientemente de su ubicación física. Los profesionales de centros de datos ahora deben colaborar más estrechamente que nunca con los equipos responsables de las redes de sucursales/borde, WAN y campus".

Al tener en cuenta estos permanentes cambios, ¿dónde deben centrar sus esfuerzos los líderes de TI y de redes hoy en día?

La expansión hacia entornos híbridos y multinube significa administrar variables en permanente cambio (aplicaciones, datos, usuarios y dispositivos) que abarcan todos los dominios de la empresa. Como resultado, los equipos de redes y de Infraestructura y Operaciones (Infrastructure and Operations, I&O) deben trabajar juntos para abordar todas las cuestiones, desde las implicaciones en las redes de los proveedores de nubes públicas y SaaS hasta el impacto en sus entornos locales.

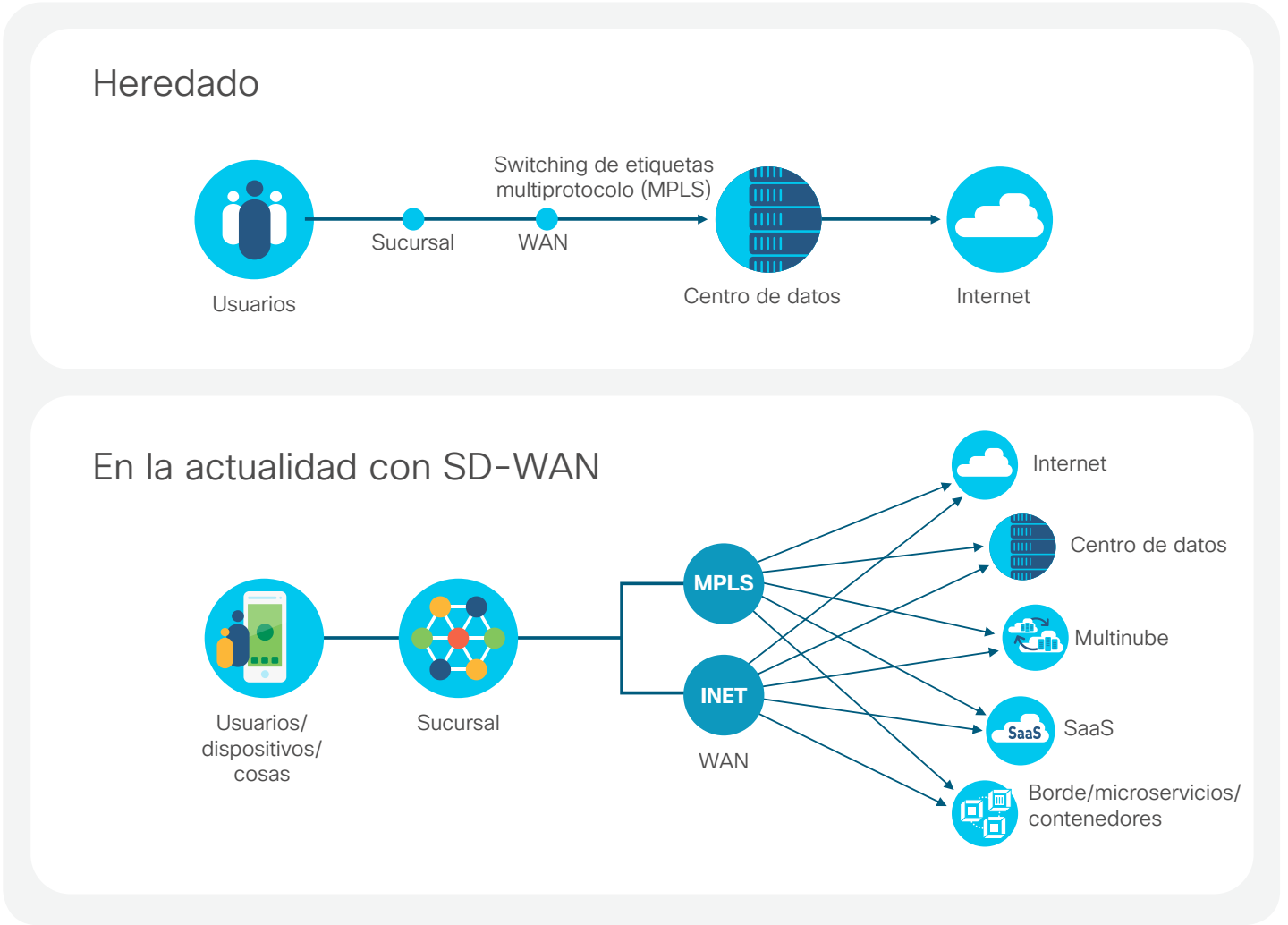
Para ayudar a entender el desafío, analizaremos los requisitos de la red a través de dos lentes:

- Optimización de la conectividad de usuario a multinube
- Networking para un centro de datos en cualquier lugar

Optimización de la conectividad de usuario a multinube

El predominio emergente de los servicios en la nube significa que la conectividad remota a esos servicios se vuelve más crítica que nunca. También significa que las arquitecturas de red de área amplia tradicionales que se centraban en conectar sitios remotos a centros de datos centralizados ya no son óptimas.

Figura 18: El cambiante panorama de la WAN



Ahora que SaaS, IaaS y servicios de borde distribuido pueden ser alojados en cualquier lugar donde haya una conexión de red, una arquitectura de WAN radial heredada puede refrenar a las organizaciones.

↑2X El aumento de la dependencia en la nube también está impulsando el aumento del tráfico de WAN, y se espera que el tráfico de WAN de IP empresarial a nivel global se duplique para el año 2022 y alcance los 5.3 exabytes al mes.[12]

La SD-WAN, el acceso directo a la nube, las instalaciones de alojamiento de datos y los intercambios en la nube, junto con la disponibilidad y asequibilidad de los servicios de banda ancha de gran ancho de banda, están surgiendo como los nuevos elementos importantes dentro de la arquitectura que garantizan que los servicios en la nube puedan cumplir con los requisitos de negocio de manera rentable.

Los equipos de TI necesitan el mismo control en entornos multinube que en sus propias redes para que puedan seguir ofreciendo el servicio que la empresa espera.

SD-WAN

La SD-WAN es un enfoque definido por el software para administrar la WAN que le permite a un controlador centralizado optimizar la experiencia de las aplicaciones multinube y simplificar en gran medida las operaciones de la WAN.

La reciente adopción rápida de la SD-WAN indica que proporciona muchas respuestas a las crecientes demandas de la nube. Y de hecho, la nube es el mayor impulsor de esta adopción de SD-WAN. Casi el 75% de quienes respondieron en la encuesta sobre SD-WAN de IDC comentaron que los servicios de SaaS/nube son importantes (o muy importantes) para las opciones actuales de tecnología WAN.[26]

Esto no es una sorpresa, ya que las opciones y los servicios tradicionales utilizados para conectarse a una nube privada virtual, proporcionados por los proveedores de servicios en la nube, dejan a los equipos de redes empresariales con un control limitado en un escenario multinube.

Según nuestra *Encuesta sobre tendencias de redes a nivel global 2019*, más del 58% de las organizaciones de todo el mundo ya han implementado alguna forma de SD-WAN, y más del 94% de los encuestados cree que contará con una SD-WAN de funcionalidad básica o más avanzada implementada dentro de los próximos dos años.[14]

Además, a medida que los servicios 5G se vuelven más ampliamente disponibles, la SD-WAN los integrará sin problemas en un marco independiente del transporte para obtener la máxima flexibilidad y rendimiento, respaldos continuos mejorados y costos reducidos.

Figura 19: WAN lista para entornos multinube

Pregunta: ¿Qué oración describe mejor el enfoque actual de su organización para el diseño, la implementación y la administración de su arquitectura WAN?

Fuente: *Encuesta sobre tendencias de redes a nivel global 2019;* n = 1556 estrategas de redes

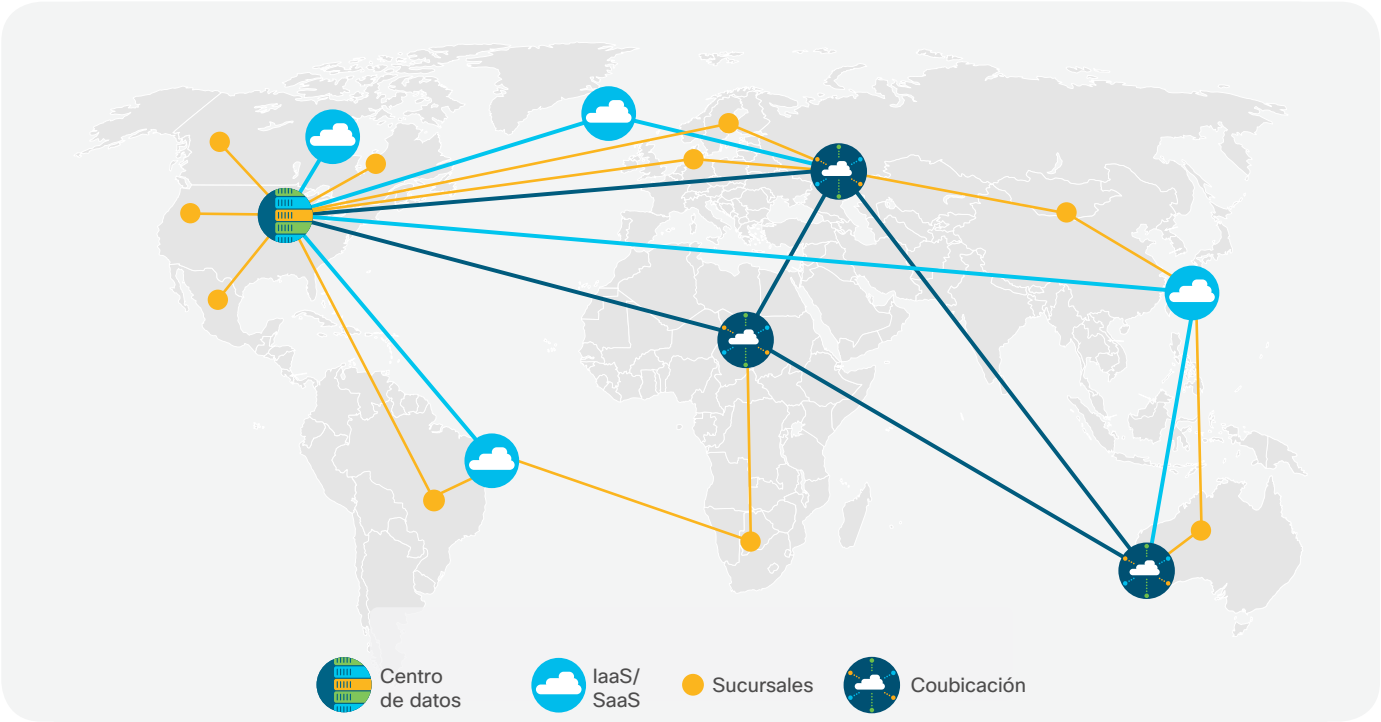
Acceso directo a la nube

El enfoque tradicional de hacer backhaul con el tráfico de las sucursales a través de costosos circuitos WAN al centro de datos o una gateway de Internet centralizada mediante una arquitectura radial puede obstaculizar la transición a los servicios en la nube. También agrega gastos e introduce latencia que degrada la experiencia del usuario.

Hasta ahora, los arquitectos de redes se habían quedado atascados con este enfoque debido al costo y la complejidad de la alternativa, que requiere implementar y administrar capacidades de seguridad distribuidas como firewalls, filtrado de URL y protección DNS en cada Router de sucursal.

Ahora, sin embargo, las capacidades de "acceso directo a la nube" o "acceso directo a Internet" pueden conectar de forma segura a los usuarios directamente de la sucursal a los servicios en la nube. Esto simplifica la administración de políticas en todos los sitios remotos y automatiza el aprovisionamiento de nuevos servicios de red en cuestión de minutos, al tiempo que aplica la seguridad multicapa, incluido el cifrado, la autenticación, la segmentación, el firewall y el cumplimiento de DNS.

Figura 20: SD-WAN segura con acceso directo a la nube y concentradores de coubicación



Alojamiento de datos e intercambio en la nube

Si bien las instalaciones de alojamiento de datos (coubicación) con independencia de portadora no son nuevas, desempeñan un papel muy ampliado en la era de la multinube y son un componente crítico de la nueva arquitectura WAN optimizada para la nube. En esencia, las instalaciones de coubicación como las proporcionadas por Equinix y otros servicios de interconexión se convierten en una extensión de la WAN empresarial y proporcionan visibilidad, acceso de alto rendimiento y seguridad centralizada a múltiples proveedores SaaS e IaaS. (mirar Figura 20 anterior)

Networking para un centro de datos en cualquier lugar

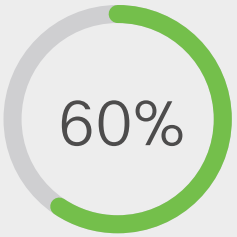
Los centros de datos actuales ya no son ubicaciones individuales. El "centro de datos distribuido" emergente es el resultado de aplicaciones y datos que residen tanto dentro como fuera de las instalaciones, en entornos híbridos, multinube y de borde de red. Pero un centro de datos distribuido no funciona como uno tradicional. Las organizaciones de TI deben adaptar y modificar su tecnología y operaciones para satisfacer las crecientes demandas de conectividad de aplicaciones y redes de este nuevo tipo de arquitectura.

El centro de datos en cualquier lugar requiere que los equipos de TI garanticen la coherencia de las operaciones y la tecnología en las instalaciones, en todo el borde empresarial y en los entornos híbridos y de multinube.

Automatización

La creciente escala, complejidad y portabilidad de las cargas de trabajo dentro de los centros de datos está obligando a los administradores de redes a reemplazar los procesos manuales y aplicar herramientas de automatización para administrar las políticas de red y la conectividad.

La adopción de redes definidas por el software, la automatización y la NFV para servicios de Nivel 4 a 7 coloca las redes de centros de datos en una posición viable para admitir un ágil entorno de nube local. Esto permite la orquestación centrada en las cargas de trabajo de la red junto con los servicios de procesamiento y almacenamiento. De hecho, podría considerar como atrasada a una red de centros de datos que aún no ha adoptado un modelo de DevOps basado en controladores e impulsado por API.



Casi el 60% de los líderes de TI y los estrategas de redes afirman que ya han implementado algún tipo de SDN en sus centros de datos.[14]

Casi el 60% de los líderes de TI y los estrategas de redes afirman que ya han implementado algún tipo de SDN en sus centros de datos.[14] La SDN/NFV ya está transportando el 23% del tráfico dentro de los centros de datos empresariales, una cantidad que se espera que crezca al 44% para el año 2021.[23] Esos centros de datos sin SDN tendrán dificultades para admitir modelos de aplicaciones ágiles y flexibles.

Redes basadas en intención para el centro de datos

Desarrolladas a partir de los fundamentos de SDN, las redes basadas en intención les permiten a los equipos de centros de datos obtener una arquitectura holística de validación de bucle cerrado que analiza el comportamiento del centro de datos en tiempo real con respecto a políticas definidas, y permite un método eficiente y confiable para introducir cambios en la red. Esto les permite a los equipos de TI mantenerse al día con los cambios dinámicos de las cargas de trabajo y alinearse continuamente con las necesidades de las aplicaciones del negocio.

En un escenario de centro de datos, también es muy importante validar las políticas antes de activarlas. Con la IBN, esto se puede lograr mediante la verificación continua, automatizada y en toda la red, incluidas las políticas de cumplimiento.

Extensión de la IBN a los entornos multinube

Para garantizar la seguridad y los niveles de servicio deseados para las organizaciones de hoy en día, los equipos de centros de datos deben ampliar el control y la visibilidad más allá de los entornos locales. Los equipos de TI pueden ampliar la aplicación y la automatización con base en políticas de IBN a entornos multinube para que las políticas se puedan implementar en las cargas de trabajo de forma coherente, independientemente de la ubicación.

En dos años, el 29% de los consultados a través de nuestra *Encuesta sobre tendencias de redes a nivel global 2019* planean contar con capacidades de redes basadas en la intención que mantengan la alineación con la intención del negocio al garantizar acciones de red automatizadas en todos los entornos multinube.[14]

Tom Edsall, CTO de Cisco para centros de datos, explica que "IBN es el esfuerzo más audaz y global de la industria de redes para crear un modelo de red para todo el sistema que aborde todas las últimas tendencias tecnológicas y las necesidades en rápida evolución de las organizaciones ágiles".

> "La red basada en intención es el esfuerzo más audaz y global de la industria de redes para crear un modelo de red para todo el sistema que aborde las últimas tendencias tecnológicas y las necesidades en rápida evolución de las organizaciones ágiles".
>
> **– Tom Edsall, CTO de Cisco para centros de datos y asesor emérito**

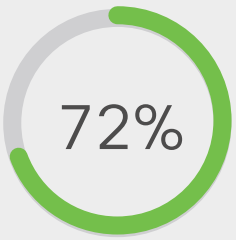
La clave para una correcta implementación local, multinube o híbrida es mantener la simplicidad. Para lograrlo, los arquitectos de red deben considerar lo siguiente:

- Que no haya superposición de redes en la nube
- Que no haya dependencia de agente, lo que permite una amplia aplicabilidad para cualquier carga de trabajo
- Adaptabilidad a la escala de la nube

Infraestructura de red subyacente

En el centro de datos, la infraestructura de red subyacente debe proporcionar programabilidad abierta y telemetría para admitir la automatización y la analítica, elementos fundamentales para los sistemas IBN. La infraestructura de red del centro de datos también debe seguir el ritmo de los aumentos masivos en el tráfico. El tráfico IP de los centros de datos a nivel global se multiplicará por tres durante los próximos cinco años. En general, el tráfico IP de los centros de datos crecerá al 25% (tasa de crecimiento anual compuesto) hasta el año 2021.[23]

3X El tráfico IP de los centros de datos a nivel global se multiplicará por tres durante los próximos cinco años.[23]



Para el año 2021, el tráfico dentro del centro de datos representará el 72% de todo el tráfico del centro de datos.[23]

Las infraestructuras de red necesitan la flexibilidad y la capacidad para admitir el tráfico de cliente de alto rendimiento a aplicación (norte-sur) y, cada vez más, el tráfico de servidor a servidor o de máquina virtual a máquina virtual (este-oeste). Hoy en día, en general esto se hace con una arquitectura "spine and leaf" plana admitida por uno o más protocolos de superposición de capa de control.

Según el *Índice global de nube de Cisco*, para el año 2021, el tráfico dentro del centro de datos representará el 72% de todo el tráfico del centro de datos y superará con creces el tráfico del centro de datos al usuario (15%) y del centro de datos al centro de datos (14%).[23]

Se requerirán aumentos continuos en el rendimiento de Ethernet switching para admitir las crecientes necesidades de tráfico informático, así como el tráfico de almacenamiento basado en archivos e incluso algunos basados en bloques.

La conmutación de 400 Gbps que se está convirtiendo en predominante, las especificaciones de IEEE para 800 Gbps e incluso 1.6 Tbps en preparación, las atractivas ventajas operativas y de capital de Ethernet hacen inevitable que esta se convierta en una alternativa al tradicional switching de canal de fibra para algunas cargas de trabajo.

Consideraciones para diseñar la red para un entorno multinube

En este entorno de aplicaciones ampliado y más distribuido, los arquitectos de redes y nubes, los ejecutivos de centros de datos y los equipos de infraestructura y operaciones necesitan desarrollar una estrategia de red que optimice la experiencia de las aplicaciones. Estas son algunas cuestiones iniciales por tener en cuenta al hacerlo:

1. **Observe la estrategia de aplicaciones de la organización:** comienza con la aplicación. Los estrategas de TI y de redes deben comprender a la perfección la huella de datos y cargas de trabajo en expansión de la organización.
2. **Colaborar para incorporar coherencia en multinube:** las organizaciones necesitan que su entorno multinube (incluido el entorno local) trabaje como uno solo. Entre toda la complejidad, los equipos de redes y centros de datos deben colaborar para desarrollar la coherencia en todos los dominios de los proveedores nubes públicas/SaaS, campus, sucursales, centros de datos y borde/IoT con el fin de lograr la optimización de costos, rendimiento, visibilidad, seguridad y experiencias de usuario.
3. **Amplíe la coherencia de la automatización basada en políticas en nube híbrida y en multinube:** los equipos deben considerar la implementación de la automatización basada en políticas en toda plataforma, hipervisor o marco de contenedor, y en toda ubicación y carga de trabajo (nativo en la nube, desprovista de software, hipervisor, contenedor y sin servidor).
4. **Asigne los servicios de aplicaciones, cargas de trabajo y componentes de servicios a la red ampliada:** los profesionales y los estrategas de redes deben comprender a la perfección de qué aplicaciones, servicios y microservicios consta la red.
5. **Priorice el rendimiento de las aplicaciones en su estrategia de SD-WAN:** identifique sus aplicaciones y servicios basados en la nube más críticos y priorice su plan de SD-WAN para admitir dichas aplicaciones en primer lugar.
6. **Conecte la política de acceso y la política de aplicaciones en todos los silos de redes:** para ofrecer segmentación segura y basada en políticas en todas partes, considere cómo los sistemas de IBN pueden asignar los grupos y las políticas entre los diferentes dominios de red, como WAN y centro de datos.
7. **Desarrolle conjuntos de habilidades de NetDevOps:** a medida que las cargas de trabajo y los servicios requieran servicios de red bajo demanda, no solo dentro de un centro de datos, sino entre ubicaciones remotas, deberán clarificar sus necesidades en la red. Esto requerirá de conjuntos de habilidades de NetDevOps que comprendan cómo conectar los requisitos de las aplicaciones y las políticas de red.
8. **Aumente la SDN con los avances de la IA:** utilice las capacidades de la IA para acelerar la solución de problemas, mejorar la administración de cambios y garantizar el cumplimiento.

Acceso de red e inalámbrico

Resumen de la sección

Aportes clave

- Las capacidades emergentes, como OpenRoaming, proporcionarán roaming global, permanente y sin inconvenientes entre diferentes redes Wi-Fi 6 y redes 5G públicas.
- Los equipos de redes necesitan análisis mejorados y capacidades habilitadas para IA para la planificación inalámbrica, la supervisión del estado, la solución y la corrección de problemas.
- Los equipos de TI necesitan administrar, gestionar y propagar automáticamente una política de acceso coherente a través de diferentes redes de acceso para proteger mejor las aplicaciones, los datos, los usuarios y los dispositivos.
- Las redes inalámbricas deberán identificar y admitir dinámicamente las demandas de las nuevas aplicaciones multimedia inmersivas y los dispositivos de IoT.

Principales hallazgos

- A nivel global, los dispositivos inalámbricos representarán el 43% de todos los dispositivos conectados en red para el año 2022.
- Los dispositivos de máquina a máquina (Machine-to-Machine, M2M) de IoT representarán el 51% de todos los dispositivos en red para el año 2022, la mayoría de ellos conectados en forma inalámbrica.
- El 35% de los estrategas de redes consideran a la solución de problemas de redes como la actividad que consume más recursos y más tiempo de las operaciones de red en la actualidad.
- El 34% de las organizaciones todavía utiliza un enfoque manual para administrar el acceso a través de redes cableadas e inalámbricas.
- El 40% de las organizaciones proporcionan automatización y segmentación de políticas para reducir la superficie de amenazas; y otro 15% aprovecha las soluciones de acceso habilitadas para IA.
- Dentro de dos años, el 27% de las organizaciones planean tener en ejecución un modelo de acceso de red basado en intención.

Orientación esencial

- Tenga en cuenta cómo Wi-Fi 6 y 5G afectarán a los requisitos empresariales futuros de su organización y defina una estrategia inalámbrica acorde.
- Cree una hoja de ruta para automatizar la incorporación y segmentación seguras de todos los dispositivos móviles y de IoT.
- Explore el uso de la clasificación automatizada de dispositivos para permitir la incorporación segura y a gran escala de todos los tipos de dispositivos de IoT.
- Evalúe cómo los servicios basados en la ubicación y el análisis de red pueden ofrecer beneficios empresariales a su organización.

Resumen de la sección (continuación)

- Explore cómo se pueden administrar las tecnologías inalámbricas especializadas necesarias para casos de uso únicos o exigentes (como Bluetooth, Zigbee y Thread) a través de una capa de administración común.

Principales predicciones

"Para el año 2025, las federaciones inalámbricas como OpenRoaming serán predominantes, lo que les permitirá a las organizaciones de TI y a los proveedores de servicios utilizar sistemas de acceso de confianza cero, compartir de forma segura las credenciales de identidad y permitirles a los usuarios finales activar el roaming de forma segura en cualquier red de acceso inalámbrico, tanto privada como pública. La experiencia de usuario será fluida y controlada por políticas, además de ofrecer la mejor experiencia para los usuarios dondequiera que se conecten".

– Matt MacPherson, CTO de Tecnologías Inalámbricas, Cisco

"Hasta el año 2025, las redes Wi-Fi 6 basadas en el estándar IEEE 802.11ax, junto con las extensiones de Wi-Fi 6 planificadas, se convertirán en la forma predominante de Wi-Fi en todas partes. Recién para el año 2024 aproximadamente, la siguiente generación de Wi-Fi basada en el estándar IEEE 802.11be en desarrollo (que probablemente sea comercializado como Wi-Fi 7) comenzará a salir al mercado".

– Andrew Myles, Director Técnico de Cisco, Director (y expresidente) de Wi-Fi Alliance

Acceso de red e inalámbrico

A nivel global, el tráfico IP empresarial alcanzará los 63.3 exabytes mensuales en el año 2022, el triple que en el 2017.[3] El acceso por cable, nacido de los comienzos relativamente humildes de las redes de área local con cable de uso compartido, como Ethernet (10 Mbps), Token Ring (16 Mbps) y FDDI (100 Mbps), se ha beneficiado de las continuas innovaciones en chipsets y óptica hasta convertirse en los entornos de red de área metropolitana y red central Ethernet de 400 Gbps de conmutación para LAN que los clientes pueden implementar hoy en día.

Las innovaciones en curso prometen nuevas y avanzadas capacidades de Ethernet Terabit, como las redes sensibles al tiempo (Time-Sensitive Networking, TSN) para aplicaciones de IoT deterministas en un futuro no muy lejano. Sin embargo, en el mundo móvil actual, el acceso inalámbrico es donde se presta la mayor atención. El acceso a la red inalámbrica a través de la LAN inalámbrica (Wi-Fi) o las redes móviles públicas sigue cambiando nuestras vidas de maneras que pocos podrían haber imaginado.

"Encontramos que la innovación empresarial digital requiere e impulsa la innovación inalámbrica, a la vez que esta abre nuevas posibilidades para otras innovaciones empresariales. Es el ciclo virtuoso".

– Guillermo Díaz, Vicepresidente Senior de Transformación del Cliente, Cisco

"Actualmente, la 'experiencia' es la moneda del negocio y los avances en conectividad inalámbrica serán los facilitadores de las muchas experiencias de la próxima generación. Al combinar lo mejor de Wi-Fi 6 y 5G, los equipos de redes tienen el potencial de hacer realidad estas experiencias".

– Matt MacPherson, CTO de Tecnologías Inalámbricas, Cisco

A nivel global, los dispositivos inalámbricos representarán el 43% de todos los dispositivos conectados en red para el año 2022; y los teléfonos inteligentes, el 24% (6700 millones) de todos los dispositivos en red. Al mismo tiempo, la cantidad de dispositivos de M2M de IoT aumentará a 14,600 millones y representarán el 51% de todos los dispositivos en red para el año 2022, la gran mayoría de los cuales estarán conectados de forma inalámbrica.[12]

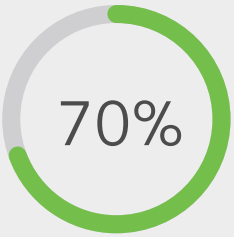
Ofrecer una agradable experiencia de usuario móvil

Las personas de todo el mundo se han acostumbrado a las aplicaciones móviles como Uber, Waze y Webex® que marcan una diferencia significativa en sus trabajos y sus vidas. Quieren que su experiencia móvil sea inmediata, esté siempre disponible, libre de ataduras y omnipresente, además de que sea una experiencia satisfactoria que proporcione acceso ininterrumpido a videos 4K fluidos, navegación superrápida y comunicaciones nítidas de voz sobre IP.

Igualmente importante, las redes inalámbricas deben admitir las nuevas innovaciones empresariales. A medida que las empresas adoptan cada vez más aplicaciones de medios inmersivos, como videos de alta definición, realidad aumentada y realidad virtual, los líderes quieren saber que la red cuenta con el rendimiento, la capacidad, la cobertura y la seguridad para admitir nuevas iniciativas digitales para que puedan moverse rápidamente cuando surjan nuevas oportunidades.

"Imagínese que un comprador pueda recibir una experiencia personalizada y relevante impulsada por los servicios de ubicación y de AR", explica Matt MacPherson, CTO de Cisco de Tecnologías Inalámbricas. "O que un almacén pueda equiparse con millones de sensores para permitir que robots y vehículos eléctricos autónomos cumplan pedidos y envíen productos".

Las nuevas redes Wi-Fi 6 y redes móviles públicas 5G prometen un rendimiento mucho mejor para admitir estos requisitos. Wi-Fi 6 ofrece mayores velocidades de datos, menor latencia, mayor densidad de dispositivos y un rendimiento general mucho mejor. Del mismo modo, para el año 2022, las redes móviles públicas 5G, previstas para su despliegue comercial en el 2020 en un conjunto determinados de países, ofrecerán velocidades más de cuatro veces más rápidas que las que ofrecen las redes 4G.[12]



Wi-Fi es ampliamente utilizada como un mecanismo de descarga móvil y será aún más necesaria en la era 5G. Se ha pronosticado que con 5G se descargará más del 70% del tráfico, en vez del 59% que se descarga con las redes 4G.[27]

Los usuarios móviles también desean una experiencia transparente al acceder a las aplicaciones de Internet públicas, en la nube y empresariales. Esto incluye la incorporación y el roaming a través de las redes.

Al complementar las redes 5G con Wi-Fi 6, los usuarios obtendrán una experiencia transparente y permanente en áreas privadas y públicas, tanto en interiores como en exteriores. Esto incluye soporte para nuevas aplicaciones hambrientas de datos que podrían fácilmente ampliar los límites de los planes de datos móviles de muchos usuarios.

Para ayudar a dar vida a esa visión, OpenRoaming se basa en la tecnología Passpoint de Wi-Fi Alliance.[28]Aunque todavía está en una etapa temprana, OpenRoaming Foundation, un consorcio entre Cisco y varios líderes de tecnología inalámbrica, está haciendo que el ambicioso objetivo de roaming seguro y fluido a través de redes inalámbricas privadas y públicas sea una posibilidad real.

Les brinda a los usuarios un roaming global fácil y seguro entre diferentes redes Wi-Fi 6 y redes 5G públicas a través de una federación basada en la nube de redes de acceso y proveedores de identidad, incluidos los operadores móviles. OpenRoaming demostró su éxito en un reciente Mobile World Congress.[28]

Al usar dispositivos de modo dual, como teléfonos inteligentes y tabletas, los usuarios podrán alternar sin problemas entre redes Wi-Fi privadas, domésticas o empresariales, puntos de acceso Wi-Fi públicos y la red 5G pública.

"Con OpenRoaming, los usuarios móviles nunca tendrán que adivinar qué red Wi-Fi deben usar, sufrir debido a un portal cautivo emergente o utilizar un nombre de usuario y contraseña inseguros. Estarán conectados dondequiera que vayan y podrán descargar, transmitir, chatear por video, jugar e incluso trabajar de la manera en que lo deseen".

– Matt MacPherson, CTO de Tecnologías Inalámbricas, Cisco

Preparación de TI para el éxito inalámbrico

Las operaciones de red tendrán que adelantarse a estos requisitos empresariales emergentes para ofrecer las experiencias de usuarios móviles deseadas, ya que los enfoques tradicionales para implementar y mantener redes inalámbricas no serán sostenibles.

En particular, la solución de problemas de redes inalámbricas ha sido tradicionalmente una actividad reactiva, compleja y que consume muchos recursos para la mayoría de los equipos de red. No es de extrañar que los líderes de redes reconozcan que la solución de problemas de redes es la actividad que consume más tiempo de las operaciones de red en la actualidad.[14]

Y para complicar más las cosas, está el hecho de que, además de las redes Wi-Fi 6 y 5G emergentes, los dispositivos de IoT pueden comunicarse a través de múltiples protocolos inalámbricos de nicho, incluidos BLE, Zigbee y Thread. El desafío de la TI será garantizar que los esfuerzos de administración de la red no se dividan entre estas redes diferentes.

Muchos casos de uso de IoT convergerán en las redes Wi-Fi 6 y 5G convencionales, pero los equipos de TI deben considerar cómo pueden administrar las tecnologías inalámbricas más especializadas necesarias para casos de uso únicos o exigentes a través de una capa de administración común.

Para salir adelante, los equipos de NetOps necesitan un enfoque más proactivo para la planificación inalámbrica, la supervisión, la solución de problemas y la corrección. Esto requiere una visibilidad mucho mejor del rendimiento y el estado de la red inalámbrica mediante analítica y supervisión habilitada por IA.

Estado actual y futuro de la preparación para el acceso a la red

La TI no puede depender de las operaciones de red de acceso manual tradicionales para admitir a los usuarios móviles. En su lugar, las organizaciones necesitan un enfoque basado en el software que abarque todos los dominios de la red.

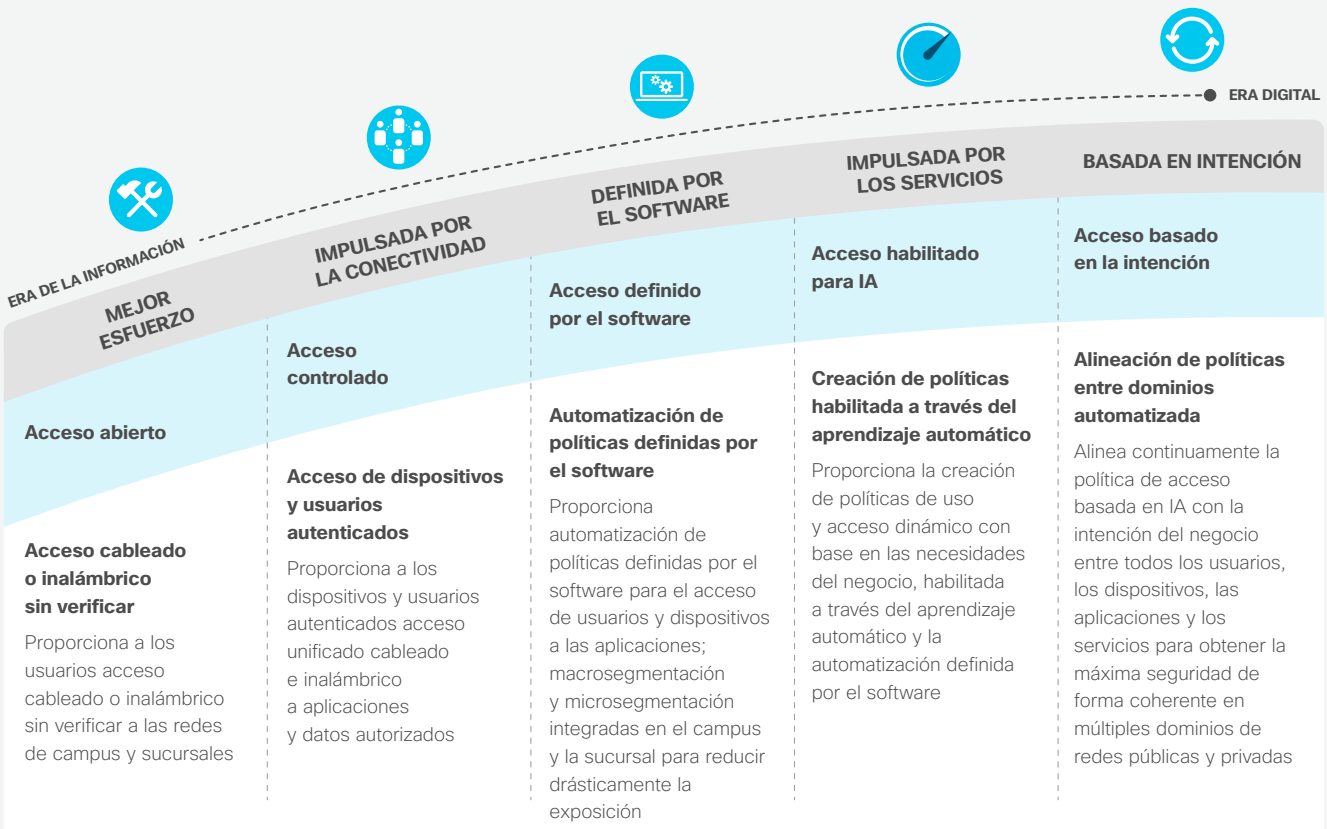
El sistema de administración de redes debe tener la capacidad de administrar, gestionar y propagar la política de acceso coherente automáticamente a través de las diferentes redes de acceso, incluso a medida que los usuarios y las cargas de trabajo continúan avanzando. Debe desbloquear los datos y la información que permitan a la TI dar soporte al negocio en tiempo real y emplear la IA para predecir mejor los problemas y automatizar las tareas de rutina. Y, a la luz del creciente predominio de las aplicaciones de IoT, la red debe reconocer y clasificar automáticamente los dispositivos de IoT y aplicar las políticas relevantes.

En conjunto, estas capacidades les permitirán a los empleados, clientes y líderes empresariales aprovechar al máximo lo que ofrecen las redes Wi-Fi 6 y 5G. Al mismo tiempo, le permitirán a la TI no solo sobrevivir al diluvio inalámbrico,

sino también garantizar la seguridad y la mejor experiencia del usuario en un mundo móvil.

En nuestra *Encuesta sobre tendencias de redes a nivel global 2019*, les preguntamos a los estrategas de redes dónde se encontraban dentro de la adopción de una arquitectura de acceso seguro en relación con el modelo de preparación de cinco etapas. El 72% de los encuestados contestó que planeaba implementar el acceso habilitado para IA o basado en intención en un plazo de dos años, en comparación con el 18% que lo hace hoy en día. Hacerlo les permitirá crear y cambiar las políticas dinámicamente y, a la larga, alinear de forma coherente las políticas de acceso con la intención empresarial de extremo a extremo, entre los usuarios y los servicios, dondequiera que se conecten o se encuentren.[14]

Figura 21: Preparación para el acceso seguro



Dónde se encuentran las organizaciones actualmente

82% 18%

Dónde planean estar dentro de dos años

28% 72%

Pregunta: ¿Qué oración describe mejor el enfoque actual de su organización para la seguridad de la red?

Fuente: *Encuesta sobre tendencias de redes a nivel global 2019;* n = 1556 estrategas de redes

Consideraciones para habilitar el acceso y la conexión inalámbrica para la era digital

1. **Las herramientas de aseguramiento inalámbricas serán una necesidad:** En la mayoría de las industrias, la conectividad de acceso se está volviendo predominantemente inalámbrica para para clientes como para las cosas. Los estrategas de redes necesitan disponer de herramientas y sistemas de aseguramiento inalámbrico de avanzada en ejecución para poder ofrecer experiencias inalámbricas coherentes en todas las redes de acceso de TI y de IoT.

2. **La segmentación inalámbrica y cableada basada en políticas evitará muchos problemas:** La automatización basada en políticas en las redes de acceso, centrales y de sucursales permite crear y administrar segmentos y microsegmentos dinámicamente en función de los grupos de usuarios y aplicaciones para que las redes formen una barrera dinámica de confianza cero ante ataques y amenazas.

3. **Use la clasificación de dispositivos controlados por IA antes de implementar la IoT de forma demasiado amplia:** No tiene sentido económico proteger sensores, monitores y otros dispositivos de IoT de bajo costo mediante soluciones de seguridad costosas. Sin embargo, mediante la clasificación automatizada de dispositivos y la automatización basada en políticas, los segmentos y microsegmentos de IoT se pueden crear y administrar dinámicamente en función de los grupos de aplicaciones y dispositivos de IoT.

4. **Prepárese para Wi-Fi 6, 5G y OpenRoaming:** Los líderes de red deben asegurarse de que sus hojas de ruta inalámbrica tengan en cuenta cómo Wi-Fi 6 y 5G se complementarán entre sí y trabajarán con dispositivos, operadores Wi-Fi y proveedores de servicios para ofrecer capacidades de OpenRoaming.

5. **Considere los servicios basados en la ubicación:** Muchos ejecutivos de negocios de los sectores de comercio minorista, atención médica y educación ya están aprovechando los beneficios de los servicios basados en la ubicación en interiores para mejorar la experiencia del cliente. Según nuestra encuesta, el 51% de los consultados ya está utilizando la conectividad inalámbrica con detección de ubicación para permitir una experiencia del cliente más personalizada a través de aplicaciones móviles. Otro 40% está evaluando la oportunidad.[14]

6. **Prepárese para los microservicios que se ejecutan en dispositivos de borde de red:** Con Kubernetes y otras capacidades de administración y orquestación para cargas de trabajo basadas en contenedores, cada vez es más atractivo para los equipos de aplicaciones comenzar a hospedar componentes de servicios de aplicaciones o redes en dispositivos de red con capacidad para cargas de trabajo en el borde. Tenga en cuenta cómo esto afectará a los requisitos de políticas de red, rendimiento, seguridad y segmentación de la red.

El rol cambiante de la seguridad de la red

Resumen de la sección

Aportes clave

- A medida que las aplicaciones, los datos y las identidades migran a la nube y al borde de la red, la seguridad basada en el perímetro por sí sola no puede proteger eficazmente contra las amenazas actuales.
- La combinación de muchos tipos diferentes de dispositivos y usuarios móviles que se conectan desde cualquier lugar a aplicaciones en red en todas partes da lugar a nuevos desafíos, como la pérdida de visibilidad y control.
- La integración de la seguridad con las capacidades de las redes basadas en la intención da como resultado una potente combinación que optimiza la aplicación de las políticas, la protección y la corrección eficaces en toda la red.

Principales hallazgos

- Los estrategas de redes identificaron a la seguridad como un área de inversión prioritaria, solo superada por la IA.
- El 43% de los equipos de redes identificaron a las capacidades de seguridad de red integradas y mejoradas como una prioridad.
- En 2019, el 48% de los Directores Generales de Seguridad de la Información (Chief Information Security Officer, CISO) identificó al "tiempo de remediación" como un indicador clave de rendimiento (Key Performance Indicator, KPI), frente al 30% en 2018.
- Casi el 75% de los líderes de red estaban seguros de que contarían con definición y aplicación de políticas automatizadas o adaptables habilitadas para IA en dos años.

Orientación esencial

- Desarrolle capacidades de seguridad de red en cinco áreas clave: visibilidad y detección de amenazas, acceso de confianza cero, protección continua, infraestructura de red confiable y flujos de trabajo de SecOps y NetOps integrados.
- Asegúrese de que se incluye una estrategia de seguridad de confianza cero con todos los planes de automatización y aseguramiento de red para administrar eficazmente las amenazas de seguridad, independientemente de qué parte de la red distribuida se vea afectada.
- Al actualizar la infraestructura y los procesos, los equipos de redes deben tener en cuenta los requisitos de confianza para ayudar a garantizar que la propia red sea resistente a las manipulaciones.
- Los equipos de SecOps y NetOps deben analizar cómo compartir los datos y deben integrar las herramientas para optimizar los flujos de trabajo de prevención, detección y respuesta ante amenazas.

Resumen de la sección (continuación)

Principales predicciones

"Para el año 2025, algunas organizaciones de TI de vanguardia habrán implementado un conjunto limitado de flujos de trabajo de seguridad habilitados para la red totalmente automatizados que ayudará a acelerar la corrección de problemas y a reducir la carga de trabajo del equipo de SecOps. La mayor madurez de las plataformas de IBN, las tecnologías de AI/ML y la integración entre las herramientas de seguridad y de red permitirán la automatización de algunos casos de uso bien definidos que no conllevan riesgos para la red o la postura de seguridad de la organización".

– Wendy Nather, jefa del equipo de CISO de Asesoría, Cisco

"En el año 2025, la computación cuántica todavía estará en etapas tempranas. Sin embargo, ya habrá esfuerzos para abordar el nuevo peligro de que la computación cuántica se utilice para vencer los métodos de cifrado actuales".

– David McGrew, Cisco fellow, Cisco

El rol cambiante de la seguridad de la red

La adopción de modelos móviles, de multinube y de IoT está creando nuevos desafíos y oportunidades para la seguridad de la red. El perímetro de la red empresarial tradicional es ahora solo un elemento de un modelo más distribuido donde la identidad de todos los usuarios, las cosas y las aplicaciones debe ser cuestionada, independientemente de si están en el campus o la sucursal, en una VPN, en la red pública o en la nube.

Los equipos de TI necesitan aprovechar los poderes combinados de la red y la seguridad para ser eficaces en el abordaje de los desafíos de ciberseguridad. Los estrategas de redes reconocen fácilmente la importancia de invertir en la seguridad de la red. Cuando se les preguntó de qué manera los equipos de red pueden satisfacer mejor las necesidades empresariales, los consultados en nuestra *Encuesta sobre tendencias de redes a nivel global 2019* identificaron la seguridad como el área número dos en la que invertir después de la IA; un 43% identificó a las capacidades de seguridad de red integradas y mejoradas como una prioridad.[14]

La convergencia de la seguridad con un modelo de red basado en la intención les permite a las organizaciones aplicar y hacer cumplir las políticas de roles empresariales y responder más rápidamente ante las amenazas en todos los servicios de red.

En esta nueva realidad, los equipos de NetOps y las redes que controlan tienen un papel vital en seguridad que desempeñar en cinco áreas clave:

Visibilidad: Los CISO están preocupados por mantener la visibilidad en este nuevo modelo de datos y aplicaciones distribuidas.

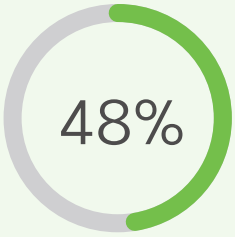
Acceso de confianza cero: La red es un elemento integral para implementar un modelo de confianza coherente donde todos los usuarios, los dispositivos y las aplicaciones son igualmente sospechosos, independientemente de dónde accedan a la red.

Según Forrester Research, un modelo de red de confianza cero debe hacer tres cosas:[29]

1. Segmentar las redes para aplicar controles granulares, así como también para evitar el movimiento lateral.
2. Proporcionar análisis de red granular y visibilidad para la detección y respuesta ante amenazas.
3. Ofrecer capacidad de administración de la seguridad de la red consolidada y sentar las bases para la automatización.

Protección continua: La red debe actuar como una agencia de detección distribuida y como una agencia de aplicación que pueda tomar medidas de forma automática y rápida para detener a los dispositivos infectados.

Infraestructura de red confiable: Con la creciente amenaza de actores malintencionados que buscan información privilegiada o intentan interrumpir las operaciones de red, las organizaciones deben proteger el sistema de red y los dispositivos de red individuales contra los ataques.



En 2019, el 48% de los CISO identificó al "tiempo de corrección" como un indicador clave de rendimiento, frente al 30% en 2018.[30]

Flujos de trabajo de SecOps y NetOps sin interrupciones: Los CISO ven a sus equipos de SecOps y NetOps trabajando juntos, y el 95% dice que son muy o extremadamente cooperativos.[30] Sin embargo, ambos equipos todavía tienden a usar datos, flujos de trabajo y herramientas independientes para recopilar y analizar los datos. Los equipos de SecOps y NetOps deben reconsiderar cómo pueden optimizar los flujos de trabajo, compartir los datos e integrar las herramientas para lograr el objetivo común de prevención, detección y respuesta automatizadas ante las amenazas.

Según Gartner Research, "Para SecOps, el acceso al tráfico de red admite el análisis retrospectivo de los flujos de tráfico, la identificación de los intentos de exfiltración, el análisis de red y los flujos de trabajo de microsegmentación".[31]

Desafíos con la seguridad de la red

Mayor escala y complejidad

La TI debe proteger a la organización y a sus datos frente a los entornos móviles y en la nube más grandes, más complejos y de rápido cambio, además de las amenazas de seguridad que se están tornando más difíciles de enfrentar.

Cargas de trabajo: A medida que las aplicaciones, los datos y las identidades migran a la nube o a Internet, el modelo de TI continúa ampliándose más allá del perímetro de la organización tradicional. Este aumento de los microservicios y de la informática en nubes híbridas y multinubes alojados en el borde requiere un cambio en la forma en que protegemos las cargas de trabajo. La seguridad basada en el perímetro por sí sola no puede proteger eficazmente contra las amenazas actuales.

Clientes: Además, la combinación de muchos tipos diferentes de dispositivos (dispositivos de usuario y dispositivos de IoT interconectados), así como también diferentes tipos de usuarios (empleados, contratistas, terceros) que se conectan desde cualquier lugar a aplicaciones en red en todas partes introduce incluso más complejidad.[30]

Infraestructura: Por último, a medida que evoluciona la sofisticación de las amenazas, los atacantes buscan cada vez más subvertir la infraestructura subyacente de conmutación y enrutamiento con el fin de espiar, robar o manipular datos y lanzar ataques contra otras secciones de la red.[32]

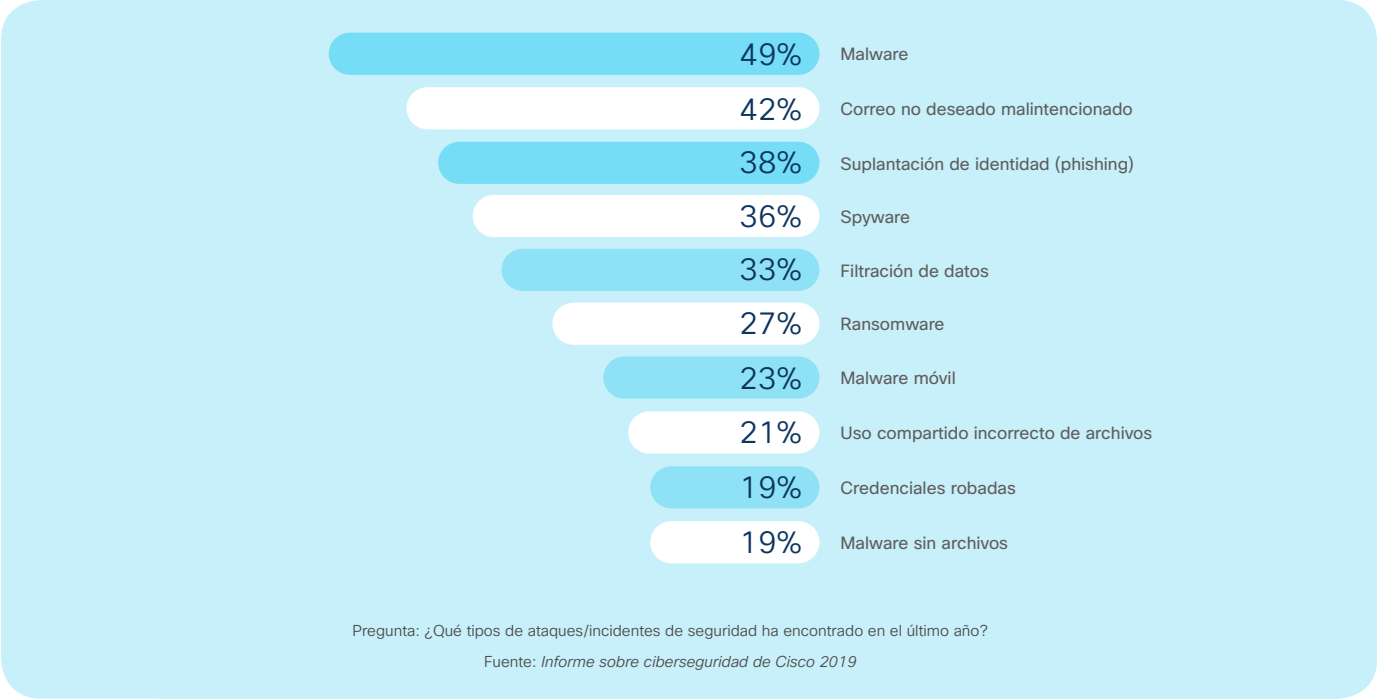
> "Al igual que cualquier otra organización grande, tenemos que lidiar con la complejidad a escala. Inspeccionamos 47 TB de tráfico de Internet, analizamos 28 mil millones de flujos y registramos 1,200 millones de eventos de seguridad a diario".
>
> – Marisa Chancellor, Directora de Seguridad de la Infraestructura, Cisco

El panorama de amenazas: la innovación continua de los atacantes

A medida que el beneficio potencial de los ataques de ciberseguridad se vuelve más atractivo, la naturaleza de los ataques se vuelve más sofisticada. Algunas de las tendencias de amenazas más preocupantes incluyen las siguientes:

- Ransomware de propagación automática basado en la red
- Ataques de malware cifrados, ocultos dentro del tráfico cifrado, que conforman un increíble 70% de todos los ataques maliciosos en 2017[4]
- Botnets de IoT implementadas en dispositivos de IoT sin parches y sin supervisión

Figura 22: Las amenazas cibernéticas de hoy en día



Pregunta: ¿Qué tipos de ataques/incidentes de seguridad ha encontrado en el último año?

Fuente: *Informe sobre ciberseguridad de Cisco 2019*

Para obtener la información más reciente sobre el panorama de las amenazas en evolución, consulte el Informe sobre amenazas de la serie de ciberseguridad de Cisco actual.[33]

Cumplimiento

Los equipos de seguridad también se enfrentan a la adhesión a las regulaciones nuevas y emergentes. Esto significa garantizar y demostrar la existencia y vigencia de políticas de seguridad.

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea entró en vigor en 2018, con la exigencia de un enfoque proactivo de la privacidad de los datos. Además, los sectores de atención médica, servicios financieros, comercio minorista, gobierno federal y otros sectores están exigiendo estándares de cumplimiento adicionales, con el riesgo de fuertes multas por incumplimiento.

Proliferación de dispositivos de IoT: aumento de la superficie de ataque

Los dispositivos de IoT conectados siguen proliferando sin una seguridad adecuada, en gran parte porque a menudo son desconocidos o no son detectados por la TI. Cada dispositivo conectado amplía la superficie de ataque de una organización. Para los dispositivos de IoT, los ataques a nivel de la red pueden incluir ataques distribuidos de denegación de servicio (DDoS), suplantación de identidad por radiofrecuencia (RFID) y amenazas de software malintencionados y dirigidas por contraseña.

Brechas en la visibilidad

La proliferación de nuevos microservicios y aplicaciones en la nube puede introducir brechas en la visibilidad y el control de la TI sobre la superficie de ataque. Ahora los usuarios pueden instalar y habilitar aplicaciones que pueden ser inseguras o exigir permisos de acceso excesivos.

"Muchos dispositivos de IoT cuentan con poca seguridad intrínseca, rara vez usan credenciales o certificados digitales y pueden verse fácilmente afectados. Por lo tanto, la automatización del reconocimiento de dispositivos, la clasificación y la activación de políticas de acceso a la red se convierten en primordiales para impedir o detener las filtraciones de seguridad".

– Tim Szigeti, Ingeniero Principal, IoT de Cisco

La cantidad y la gama de dispositivos móviles (corporativos y personales) seguirán creciendo; y la tendencia de 'traiga su propio dispositivo' genera que haya más teléfonos inteligentes personales, laptops, tabletas, etc., que acceden a las aplicaciones críticas, además de menos visibilidad y control.

Abordaje de los desafíos de seguridad con una red inteligente

Un equipo de NetOps con una red inteligente proporciona un poderoso aliado a SecOps en la continua lucha para mantener la seguridad de la organización y sus datos. Al adoptar un modelo de red basada en intención donde las capacidades de seguridad son fundamentales, la TI puede dar de alta a la red para determinar de forma automática y eficaz qué elemento es nuevo, cuál es importante y cuál es inusual, independientemente de dónde se encuentre en la red distribuida.

En última instancia, la combinación de redes basadas en intención y la seguridad proporciona visibilidad y control continuos sobre quién y qué está conectado a la red. También contribuye a un modelo completo de acceso de confianza cero y desarrolla la prevención, detección y respuesta rápida ante amenazas desde dentro de la red, no desde fuera, para obtener protección permanente en todas partes. (ver Figura 23 a continuación)

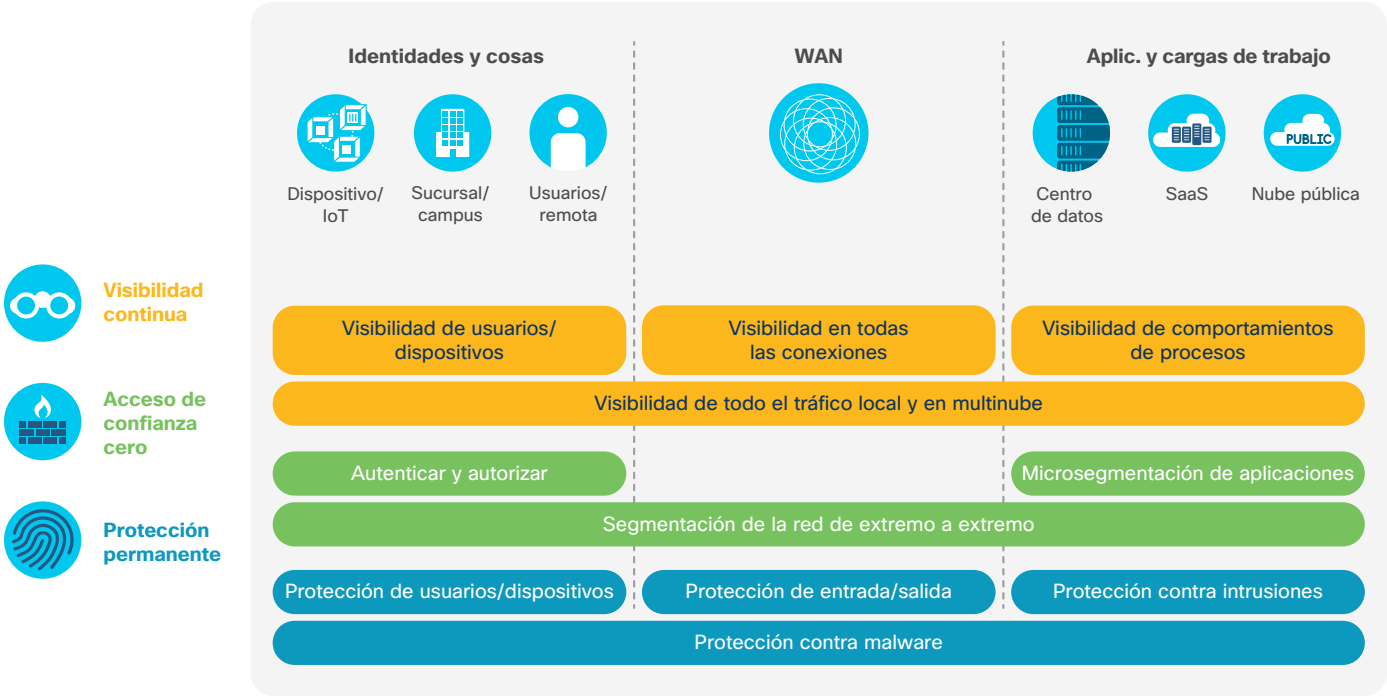
Visibilidad de la red y detección de amenazas

Nunca fue más cierto que no se puede proteger lo que no se puede ver. La visibilidad es fundamental para que los equipos de TI protejan la información y los activos de la red. Esto incluye la visibilidad de los usuarios, los dispositivos, las aplicaciones, etc., dondequiera que estén, con el fin de monitorear actividades anómalas y establecer políticas.

"Estamos lidiando con un movimiento a gran escala a SaaS y estamos perdiendo la visibilidad y el control tradicionales que supimos tener en el pasado".

– Marisa Chancellor, Directora de Seguridad de la Infraestructura, Cisco

Figura 23: Modelo integrado de seguridad de red



Una vista completa de todas las redes de IoT, multinube, centros de datos, WAN y acceso permite el mapeo de cada flujo que atraviesa la red para que los equipos puedan determinar una línea de base dinámica del comportamiento normal de la red. Al disponer de red inteligente que proporciona visibilidad completa, el equipo de red cuenta con un recurso invaluable para ayudar al equipo de seguridad a detectar y corregir las amenazas de forma más rápida y precisa, incluso en el tráfico cifrado.

Acceso de confianza cero

A partir de una base de visibilidad avanzada, el modelo de seguridad de confianza cero integral les permite a los equipos de NetOps administrar el acceso, independientemente del tipo y la ubicación de los dispositivos y las cargas de trabajo en cuestión. Si se aplica adecuadamente, puede proteger las cargas de trabajo y los datos dentro de la nube privada o pública y la fuerza de trabajo, incluso cuando los usuarios no están conectados a la red. Las capacidades clave de un modelo de confianza cero incluyen las siguientes:

Proteger el acceso a la red: En un modelo de acceso de confianza cero, la TI aplica controles precisos sobre quién, qué, cuándo, dónde y cómo se permiten los puntos de conexión de usuarios y de IoT en la red cableada e inalámbrica. También pueden aplicar un enfoque de confianza cero mediante controles de políticas basados en grupos y segmentación de cliente a aplicación y de extremo a extremo para restringir el acceso a los recursos de la red.

Contener de forma proactiva las infracciones de las aplicaciones: el personal de TI puede mitigar el movimiento lateral no autorizado entre cargas de trabajo dentro o fuera del centro de datos, lo que puede ayudar a reducir la superficie de ataque en caso de que un atacante ya esté dentro.

Mitigar el riesgo de acceso no autorizado a aplicaciones: Cuando cualquier tipo de usuario (empleado, contratista, tercero, etc.) inicia sesión en cualquier aplicación dentro o fuera de las instalaciones, debe verificar su

identidad mediante la autenticación de dos factores (2FA) y verificar la seguridad de su dispositivo, para así mitigar el riesgo de acceso no autorizado a las aplicaciones y los datos debido a contraseñas robadas o débiles.

Protección permanente en cualquier lugar

Para proporcionar protección a todos los usuarios y sistemas empresariales, la red debe progresar al ritmo de los tiempos, ampliando la protección más allá de sus perímetros tradicionales. Las arquitecturas basadas en la intención, como SD-WAN, proporcionan una plataforma controlada de forma centralizada para implementar y administrar una pila de seguridad de borde completo que amplía la protección a cada entrada o salida de la red. Para obtener una protección completa, esta pila debe incluir segmentación de red, firewall, gateway web segura, protección contra malware y seguridad de la capa DNS.

Para cualquier archivo malicioso que consiga ingresar, la detección de malware puede instruir rápidamente a la red para que mueva automáticamente los dispositivos infectados a un segmento de red restringido o en cuarentena. Y al actualizar continuamente la inteligencia contra amenazas para bloquear los archivos maliciosos y ampliar dicha inteligencia a los puntos de conexión y hasta la nube, el sistema puede bloquear este tipo de amenazas, si se producen de nuevo.

Creación de una infraestructura de red confiable

A medida que las organizaciones se digitalizan y las amenazas aumentan, hay una mayor necesidad de verificar la seguridad y la integridad de la infraestructura de red y los dispositivos de red individuales.

La creación de una infraestructura de red "confiable" requiere que la seguridad se implemente de forma integral en todo el ciclo de vida del producto. Esto ayuda a proteger contra la alteración y la manipulación durante la fabricación, la distribución, la implementación y la operación continua, lo que es especialmente importante ya que los revendedores externos, los integradores de sistemas o los proveedores de servicios administrados a menudo participan en estos procesos.

Al actualizar el equipo, los equipos de red deben buscar una serie de capacidades importantes, como el arranque seguro anclado por hardware, los identificadores de dispositivos únicos seguros y la capacidad de eliminar claves y activar el restablecimiento de fábrica.

En resumen, las redes aumentan su capacidad para hacer frente a las amenazas actuales y futuras. Depende de NetOps y SecOps tomar medidas para incorporar estas capacidades de seguridad avanzadas en sus diseños y operaciones de red para que puedan trabajar en conjunto para lograr visibilidad, protección y confianza permanentes.

Estado actual y futuro de la seguridad de la red

Entonces, ¿dónde se encuentran las organizaciones hoy en día en la construcción de su modelo de seguridad de red general para lograr una protección continua?

En nuestra *Encuesta sobre tendencias de redes a nivel global 2019*, les preguntamos a los líderes de redes cómo evaluarían su enfoque actual de la seguridad de la red con respecto a nuestro modelo de preparación de cinco etapas. Si bien actualmente las organizaciones están distribuidas de manera bastante uniforme entre todas las etapas, casi tres cuartas partes estaban seguras de que tendrían algún tipo de definición y aplicación automatizada de políticas de seguridad habilitadas para IA dentro de ese período.[14]

Figura 24: Preparación para la seguridad de la red basada en intención

Pregunta: ¿Qué oración describe mejor el enfoque actual de su organización para la seguridad de la red?
Fuente: *Encuesta sobre tendencias de redes a nivel global 2019;* n = 1556 estrategas de redes

Reporte sobre tendencias globales en redes 2020

Tendencias en las operaciones de red

Transición de reactiva a optimizada para la empresa

Resumen de la sección

Aportes clave

- Los modelos tradicionales de operaciones de red no son sostenibles para admitir los servicios empresariales requeridos frente a las demandas digitales cada vez mayores.
- Los equipos de TI están modernizando las operaciones de TI y adoptando enfoques de DevOps para aprovechar los sistemas basados en controladores y las herramientas habilitadas para IA que automatizan o eliminan muchas de las tareas de red tradicionalmente repetitivas.
- Las nuevas plataformas avanzadas de redes abiertas permiten una mejor integración en otros procesos operativos y sistemas de TI y seguridad, además de ofrecer nuevas oportunidades para los desarrolladores de aplicaciones empresariales.
- En esta próxima época de operaciones de red, los líderes y los equipos estarán mejor posicionados para alejarse de los modelos operativos reactivos y ofrecer continuamente los servicios precisos que el negocio necesita.

Principales hallazgos

- El 73% de los equipos dedican más de la mitad del tiempo a mantener el statu quo de la red.
- Si pudieran liberar recursos de las tareas de mantenimiento diarias que los mantienen ocupados, los líderes de TI priorizarían los recursos de sus equipos de red para que se enfoquen en la multinube, aceleren las implementaciones de aplicaciones y protejan mejor la red, las aplicaciones y los datos.
- Más de un tercio de los líderes de TI priorizaron la importancia de lograr una mejor coordinación e integración de la red con otros equipos de TI y líneas de negocio.

Resumen de la sección (continuación)

Orientación esencial

- Al adoptar modelos de aseguramiento y automatización basados en controladores, los equipos de redes deberían centrar sus esfuerzos en tres áreas críticas del proceso: administración del ciclo de vida, administración de las políticas y administración de la garantía.
- Para mejorar la calidad, el costo, la agilidad y la seguridad del servicio, los administradores de redes deben dejar de administrar dispositivos individuales, centrar su atención en el controlador de red y administrar el sistema de red de extremo a extremo a través del controlador.
- Los equipos de redes deben adoptar un enfoque de plataforma abierta y dirigido por DevOps para integrar la red en los procesos de TI y optimizar los flujos de trabajo de extremo a extremo, para poder obtener eficiencias y responder mejor a las necesidades empresariales.
- Los equipos de operaciones de red deben equiparse con las capacidades de AIOps emergentes para ofrecer mejores resultados empresariales y de red.

Principales predicciones

Unión del negocio y la TI: "Los equipos ajustarán el tiempo dedicado a mantener las redes hacia un enfoque externo en cómo la red puede satisfacer mejor las necesidades de la organización y dar soporte a la innovación empresarial. Los nuevos roles de operaciones serán asignados a la traducción de la intención empresarial y los requisitos de las aplicaciones en políticas de redes".

NetOps extiende la supervisión a la nube: "A medida que los servicios empresariales multinube se conviertan en la norma, los equipos de NetOps ampliarán la visibilidad y la supervisión predictiva a la WAN, las redes públicas y hasta el punto de presencia en la nube. Para obtener más información, los sistemas empresariales de redes basadas en intención comenzarán a integrar los datos de los sistemas de los proveedores de servicios y los proveedores de servicios en la nube para garantizar la uniformidad de la calidad de la experiencia de los servicios en la nube".

– Rich Plane, CTO Experiencia del Cliente, Cisco

Transición de reactiva a optimizada para la empresa

Según la investigación de Cisco, los equipos de liderazgo de TI están encabezando la transformación digital de sus organizaciones. Para lograrlo, están impulsando una transformación separada pero igualmente importante: la de modernizar la infraestructura y las operaciones de TI para satisfacer las demandas digitales emergentes.[34]

Por primera vez, los equipos de redes, al adoptar un enfoque de plataforma abierta y dirigido por DevOps, cuentan con las herramientas y las tecnologías para integrar la red en los procesos de TI y optimizar los flujos de trabajo de extremo a extremo para obtener eficiencias y responder mejor a las necesidades empresariales.

Este enfoque también proporciona la oportunidad de construir puentes operativos entre dominios de red, así como también de integrarse directamente con las aplicaciones para dar un mejor soporte a las cambiantes necesidades de las líneas de negocio.

Al adoptar nuevas formas de pensar sobre las operaciones de red y nuevas formas de trabajar, los líderes y los equipos de TI estarán mejor posicionados para ofrecer los servicios exactos que las líneas de negocio necesitan, ya sean mejores servicios existentes o nuevos servicios que permitan negocios.

63%

Según nuestra *Encuesta sobre tendencias de redes a nivel global 2019*, el 63% de los líderes de TI planean establecer redes avanzadas que puedan satisfacer dinámicamente las necesidades empresariales en un plazo de tres años.[14]

Estado actual y futuro de las operaciones de la red

Preparación operativa para dar soporte a la transformación digital

En nuestra *Encuesta sobre tendencias de redes a nivel global 2019*, les preguntamos a los líderes de TI y a los estrategas de redes cómo clasificarían su preparación operativa actual de la red con respecto a la administración de la garantía en cinco etapas de madurez que van desde Reactiva hasta Optimizada para la empresa.

Aunque solo el 23% considera que actualmente se encuentran en la etapa Predictiva u Optimizada para la empresa, el 71% planea estar en ese punto en dos años, lo que subraya la urgencia que las organizaciones sienten por prepararse ante el aumento de las demandas sobre la red empresarial.[14]

La manera en que los avances en la red están cambiando las operaciones de red

El reciente aumento de las tecnologías de red avanzadas cambiará prácticamente todos los aspectos de las operaciones de red, por lo que se pueden esperar cambios importantes en las siguientes áreas.

Integración de las operaciones de red en el proceso de la TI

Los viejos tiempos en que las redes eran operadas en silos tecnológicos por parte de ingenieros con experiencia principalmente en un área están desapareciendo rápidamente. En nuestra investigación, casi un tercio de los líderes de TI enfatizó la importancia de lograr

Figura 25: Preparación para las operaciones de red: administración de la garantía

Pregunta: ¿Qué oración describe mejor el enfoque actual de su organización para la preparación operativa de la red?
Fuente: *Encuesta sobre tendencias de redes a nivel global 2019;* n = 1556 estrategas de redes

una mejor coordinación e integración de la red con otros equipos de TI, mientras que el 26% comentó sobre la importancia de mejorar su capacidad de interactuar con las líneas de negocio.[14] Un 27% adicional identificó que un diseño de silos y un enfoque operativo en dominios de red separados los estaba frenando.[14]

Gracias a las interfaces abiertas que proporcionan los controladores de redes basadas en la intención, los equipos de NetOps renunciarán a su silo operativo aislado para convertirse en una parte totalmente

integrada de los flujos de trabajo de TI. El 34% de los líderes de TI identificó a este cambio como el que más ayudaría al equipo de redes a satisfacer mejor las necesidades de la organización.[14]

Sin embargo, para poder lograr los niveles deseados de agilidad de TI y alineación de la intención continua, los equipos de NetOps se encargarán de mejorar la integración entre los dominios de red (acceso, WAN, centro de datos, nube, etc.), así como también con otros dominios de TI, como la administración de servicios de TI (IT Service Management, ITSM) y los sistemas SecOps.

En esta figura, se muestra cómo NetOps podrá utilizar un enfoque de DevOps de red y plataforma abierta para integrar los procesos y las tecnologías de red con otros sistemas internos e incluso externos.

Alineación completa entre TI y la intención de negocio

En esencia, la red existe para proporcionar los servicios necesarios para dar soporte a los empleados, clientes y socios; en otras palabras, para dirigir el negocio. Pero la realidad es que los enfoques tradicionales de operaciones manuales a menudo no satisfacen las dinámicas necesidades empresariales. Esto está a punto de cambiar.

Con las redes basadas en la intención, las operaciones de red serán mucho más automatizadas y dinámicas, y estarán directamente informadas por la intención de TI y el negocio. Dicha intención incluiría las necesidades de rendimiento de las aplicaciones, las políticas de seguridad y su cumplimiento, además de los procesos de TI.

Figura 26: Oportunidades de integración con el enfoque de DevOps de red de plataforma abierta

Con el tiempo, la traducción de la intención de TI y el negocio en políticas de red se convertirá en una parte integral del rol de las operaciones de red.

Automatización para reducir la complejidad de las operaciones de red

No cabe duda de que la automatización de las tareas de operaciones está cambiando el rostro de las operaciones de red. Una cuarta parte de los líderes de TI y estrategas de redes identificó a la automatización como la tecnología que tendría el mayor impacto en el diseño y estrategia de la red durante los próximos cinco años.[14]

Sin embargo, esto significará dejar atrás los enfoques manuales tradicionales para la configuración y el mantenimiento de la red. Algunos equipos encontrarán esto como inquietante, y el 20% de los líderes de TI identificará la renuencia entre los equipos de NetOps para adoptar la automatización y las tecnologías de IA como el obstáculo principal para la modernización.[14]

Gestión de problemas e incidentes preventiva versus reactiva

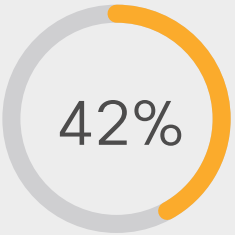
Como se analizó anteriormente, muchas organizaciones se encuentran en una etapa reactiva de preparación operativa. El desafío aquí es que el 25% de los encuestados indicaron que una mentalidad operativa reactiva les estaba impidiendo alcanzar sus objetivos de redes.[35] Esto también está a punto de cambiar. Mediante el uso de la IA y la integración con otros sistemas de TI, los equipos de NetOps podrán lograr un estado de mantenimiento predictivo que solucione los problemas mucho antes de que se conviertan en incidentes y afecten los servicios.

Inteligencia humana y artificial trabajando en conjunto

Los ingenieros de red necesitan toda la ayuda que puedan obtener para lidiar con la complejidad de la red.

Es por eso que los equipos de NetOps se están armando con nuevas capacidades de operaciones controladas por IA (AIOps), como el aprendizaje automático y el razonamiento automático, que pueden ofrecer una línea de base de rendimiento más precisa, detección de anomalías, análisis automatizado de la causa raíz, orientación para la corrección de problemas e información predictiva.

En lugar de tamizar a través de miles de eventos, los equipos de NetOps contarán cada vez más con estas tecnologías para presentar con precisión solo los más importantes, junto con las principales opciones de corrección. El equipo de AIOps también puede trabajar para ajustar este resultado, enriquecer el contenido e integrar el conocimiento con los principales sistemas de administración empresarial y de servicios.



El movimiento hacia la AIOps está cobrando impulso, ya que el 42% de los líderes de TI creen que la IA tendrá un mayor impacto en sus operaciones automatizadas en el futuro.[35]

Incorporación de la conectividad de la tecnología operativa a las operaciones de red

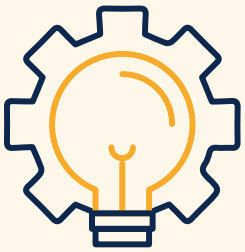
El hecho de que los dispositivos de IoT se consideren activos empresariales y de que los datos operativos que producen sean vitales para las operaciones empresariales subraya claramente la necesidad de contar con nuevos enfoques para la administración de la infraestructura.

- En los casos de uso de IoT, como la supervisión en tiempo real, los problemas operativos podrían tener consecuencias graves, incluso potencialmente mortales.
- En las redes grandes, los dispositivos de IoT podrían ser millones, por lo que la automatización es la única manera de administrarlos de manera eficaz.
- En algunos casos, no hay garantía de que haya una conexión constante entre la sede central y los dispositivos de IoT remotos (lo que está impulsando la inversión en analítica del borde de red y fog).

Presentación de un marco de operaciones de red de última generación

Para ayudar en la preparación para un futuro de las operaciones de redes impulsadas por redes basadas en intención, los expertos en tecnología de Experiencia del Cliente de Cisco han creado un marco que ofrece orientación estratégica, prácticas recomendadas, diseños validados, procesos probados y ajustes recomendados.

En el centro de este modelo, se encuentran tres áreas críticas del proceso: administración del ciclo de vida, administración de las políticas y administración del aseguramiento.
La simplificación operativa que ofrece IBN permite planificar y construir una transformación operativa en torno a estos procesos principales.

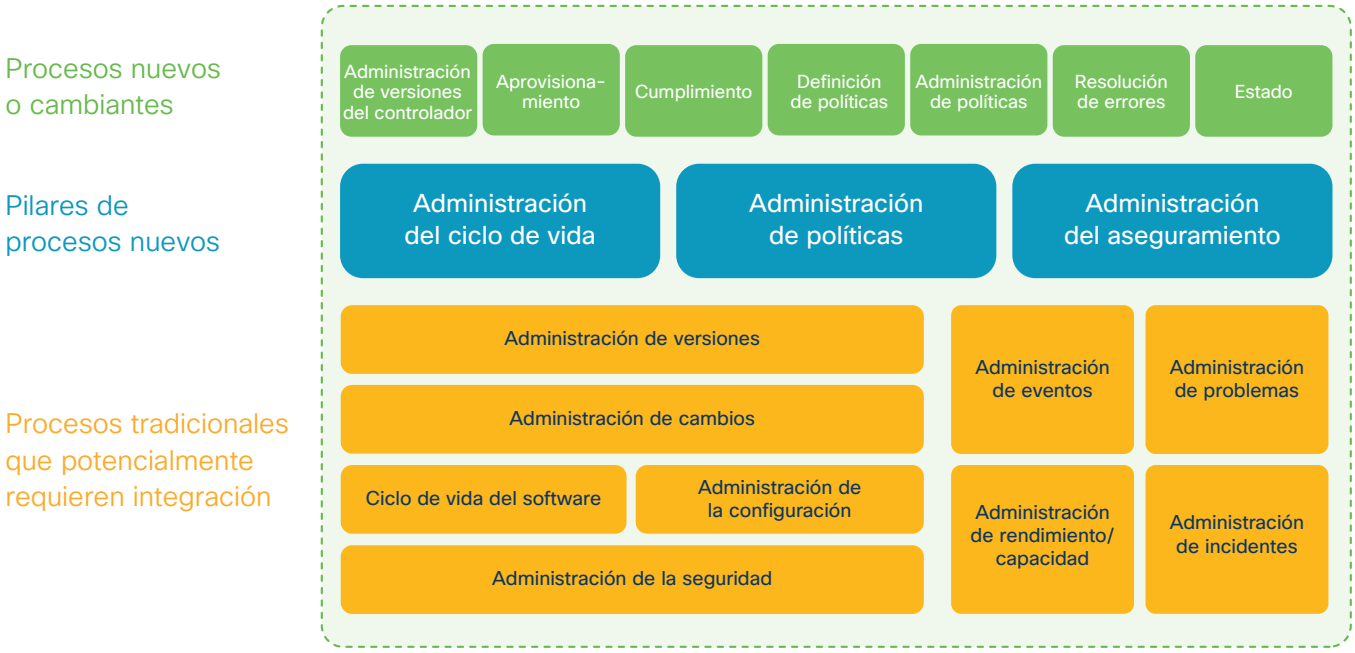


Una nueva mentalidad: administración del controlador de red

Según Jake Hartinger, Arquitecto de Soluciones de Experiencia del Cliente de Cisco, uno de los cambios más profundos en las operaciones de red será el cambio de enfoque del dispositivo al controlador. Hasta ahora, los administradores de red normalmente han aprovisionado y recopilado información de la red al iniciar sesión en los dispositivos.

Con los modelos de garantía y automatización basada en controladores, los administradores se centrarán en la administración del controlador, las integraciones y los procesos en relación con el controlador. Cuanto más una organización sea capaz de aceptar este cambio único, más rápido podrá mejorar la calidad del servicio, el costo, la agilidad y la seguridad.[36]

Figura 27: Modelos de operaciones emergentes para la nueva red



Administración del ciclo de vida

El cambio a los sistemas de aprovisionamiento y automatización dirigidos por controladores requiere una adhesión mucho más estricta a los estándares de seguridad, software y hardware. Un usuario que haga un cambio en la interfaz de línea de comandos (CLI) puede encontrar que el controlador anula el comando en actualizaciones futuras porque no está definido como política.

Para evitar este escenario, la organización deberá contar con prácticas de administración del ciclo de vida bien definidas en torno a la administración de versiones y la administración de cambios, especialmente con las automatizaciones que se centran en la red o el servicio como un sistema.

En pocas palabras, la administración del controlador de red implica la administración de nuevo hardware de controlador, software, puntos de integración y API, además de la configuración de la interfaz de usuario que administra las capacidades de garantía y políticas. Dado que las capacidades del controlador cambiarán continuamente en el futuro previsible, la definición de un proceso de administración del ciclo de vida único para el controlador de red y las integraciones será de gran importancia.

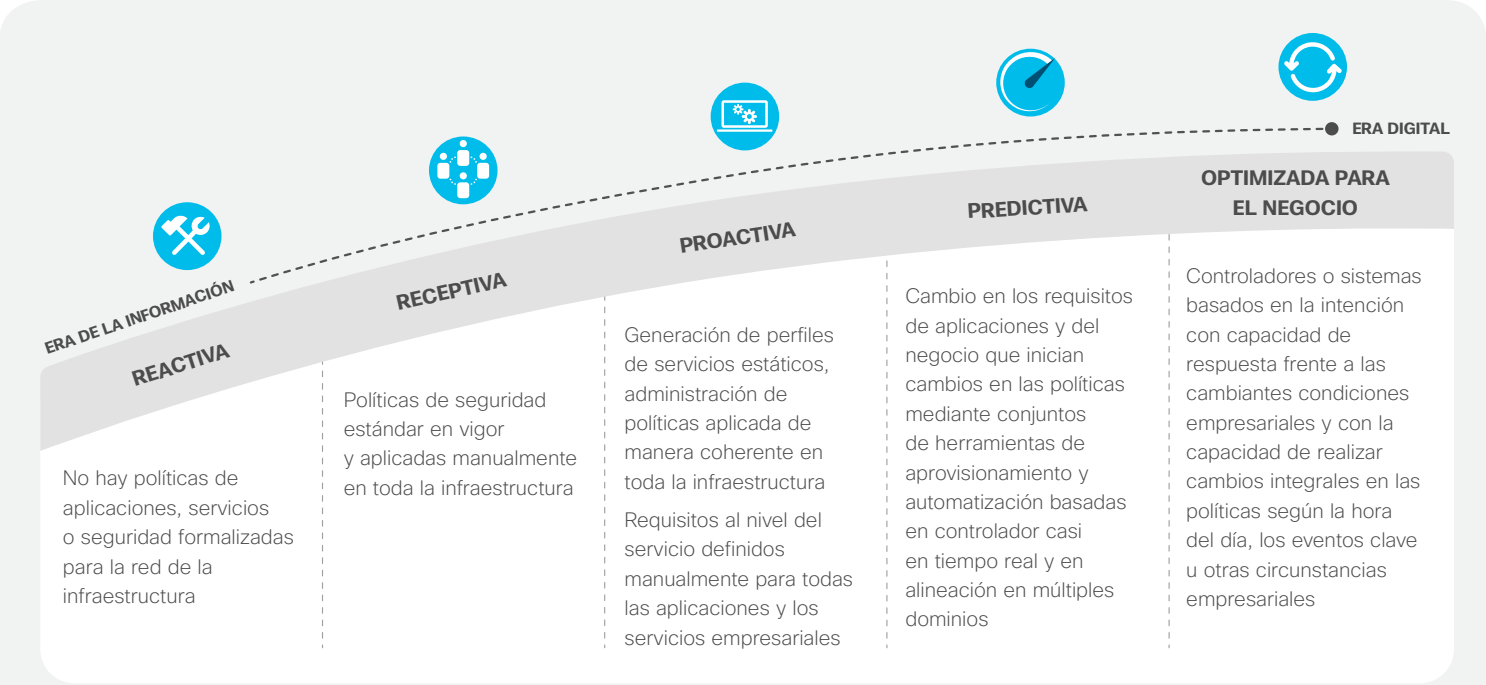
Figura 28: Preparación para las operaciones de red: administración del ciclo de vida

Administración de políticas

La administración de la política de red también es esencial porque, para lograr el éxito y la sustentabilidad, los controladores de red dependerán de pautas y estándares de red más estrictos para el hardware, el software, las configuraciones e incluso las integraciones del dispositivo de red. Primero debe definirse la política y, luego, actualizarse. También debe configurarse dentro de los controladores de red para garantizar que los estándares definidos se aprovisionen de manera permanente. Además, la política debe verificarse mediante métodos de verificación del cumplimiento.

Debido a que los cambios de políticas pueden tener una huella de activación muy amplia, lo que puede afectar a las configuraciones de miles de dispositivos, deben ser de naturaleza prescriptiva, para que se puedan probar y verificar como válidas y aprobadas. A la larga, a medida que se generalizan los modelos de verificación de políticas que simulan cualquier cambio antes de su activación, habrá espacio para una mayor flexibilidad en las opciones de configuración.

Figura 29: Preparación para las operaciones de red: administración de políticas



Administración del aseguramiento

Las redes pequeñas tienden a administrarse fácilmente mediante la intervención humana directa, pero las redes más grandes se vuelven casi imposibles de administrar sin herramientas, datos de red y procesos bien definidos.
Hoy en día, solo uno de cada cinco equipos de operaciones cuenta con la capacidad de usar analítica avanzada para identificar y solucionar potencialmente los problemas que afectan al servicio antes de que ocurran.[14]

Mediante un modelo de red basada en intención y habilitada por IA, la administración del aseguramiento mejora e integra estos recursos con analítica, integraciones de API, capacidades de correlación, informes e inventario avanzados, además de enriquecimiento. En particular, la analítica y el enriquecimiento proporcionan detalles adicionales sobre los errores de la red que facilitan una rápida resolución o un mejor estado. Y con la expectativa de que el sistema habilitado para IA seguirá mejorando en función de los aprendizajes a partir de un gran número de implementaciones adicionales, los equipos de operaciones seguirán beneficiándose.

En las redes más grandes, el resultado es mejor calidad del servicio, rápida resolución de los problemas y eficiencia operativa.
Un equipo de AIOps podría enfocarse en el filtrado, el enriquecimiento y las API con sistemas de administración empresarial o de servicios para automatizar completamente los flujos de trabajo de aseguramiento.

Además de estas tres áreas de procesos principales, recomendamos examinar las posibles interacciones con los tradicionales procesos de ITSM, dominios de TI y sistemas para identificar otras potenciales oportunidades de integración.

Predicciones sobre el futuro de las operaciones de red para 2025

Según Rich Plane, CTO de Experiencia del Cliente de Cisco, dentro de cinco años, los equipos de operaciones de red van a ser mucho más eficaces en hacer lo que sus organizaciones necesiten que hagan. Estas son sus predicciones sobre cómo sucederá.

1. **Aseguramiento de extremo a extremo:** Los equipos de operaciones de red podrán realizar la detección predictiva de los problemas y el análisis de la causa raíz entre cualquier cliente o dispositivo y cualquier servicio empresarial, alojado en cualquier lugar, y determinar rápidamente si la red es la causa de alguna degradación del rendimiento del servicio y dónde se encuentra dicho problema.

2. **Unión entre el negocio y TI**: Las operaciones de red podrán ajustar su enfoque y pasar a participar casi exclusivamente de la supervisión y solución de problemas de la red a tener también un enfoque externo, hacia el negocio y cómo la red puede satisfacer mejor las necesidades de este. Los nuevos roles de operaciones serán asignados al análisis y la traducción de la intención empresarial y los requisitos de las aplicaciones en políticas de redes.

3. **NetOps y SecOps** operan desde una única fuente de verdad: Los equipos de NetOps y SecOps desarrollarán flujos de trabajo integrados, optimizados y habilitados mediante el intercambio de datos y las entregas e interacciones automatizadas entre plataformas y herramientas.

4. **NetOps extiende la supervisión a la nube:** A medida que los servicios empresariales multinube se conviertan en la norma, los equipos de NetOps ampliarán la visibilidad y la supervisión predictiva a la WAN, las redes públicas y hasta el punto de presencia en la nube. Para obtener más información, los sistemas empresariales de IBN comenzarán a integrar los datos de los sistemas de los proveedores de servicios y los proveedores de servicios en la nube para garantizar la uniformidad de la calidad de la experiencia de los servicios en la nube.

5. **Administración de cambios basada en modelos:** Los procesos más avanzados de NetOps, como los análisis de hipótesis de los cambios que se realicen en la red, se extenderán más allá del centro de datos y se generalizarán.

6. **Flujos de trabajo autodirigidos y de autocorrección:** Algunos flujos de trabajo de menor impacto se automatizarán por completo, lo que permitirá que la red tome medidas de administración correctivas o del ciclo de vida sin la intervención de un operador humano. El resultado de este enfoque basado en datos y validado por la intención será la obtención de niveles mucho más altos de continuidad del servicio debido a la oportunidad de minimización de los errores.

Reporte sobre tendencias globales en redes 2020

Tendencias en los profesionales de redes

Nuevos conjuntos de habilidades para la red moderna

Resumen de la sección

Aportes clave

- Las nuevas tecnologías están eliminando muchas de las tareas manuales en muchas industrias, y TI no es una excepción.
- La buena noticia para TI y las redes es que la demanda laboral sigue siendo fuerte para aquellos que adquieran nuevos conjuntos de habilidades requeridas, como la programabilidad de redes.
- A medida que las operaciones de red se vuelvan más automatizadas, los administradores de redes asumirán roles que se alinean con las nuevas prácticas operativas relacionadas con la administración del ciclo de vida, las políticas y el aseguramiento de red.
- Los estrategas de redes asumirán roles de alto valor orientados a mejorar la alineación del negocio, la integración de los procesos de la TI, la mejora de la seguridad y el mejor uso de los datos.

Principales hallazgos

- En promedio, actualmente las tareas de mantenimiento de redes consumen el 55% del tiempo y de los recursos de un equipo de redes.
- El 27% de los líderes de TI identificó a la falta de las habilidades necesarias como el obstáculo principal en la transición hacia una red avanzada.
- El 22% de los líderes de TI prefiere dotar de nuevas capacidades mediante la inversión en capacitación, educación continua y certificaciones.
- Los estrategas de redes identifican a la IA, la integración de TI/TO (Tecnología de la Información/Tecnología Operativa), la automatización y DevOps de redes como las áreas principales en lo que respecto a mejorar las habilidades.

Orientación esencial

Estrategas: Consideren la posibilidad de adquirir experiencia técnica, empresarial y de software que les permitan desarrollarse en una o más de las siguientes áreas:

- El traductor empresarial se centrará en alinear el rendimiento de la TI con la intención empresarial dinámica.
- El guardián de la red se centrará en unir las arquitecturas de red y de seguridad.
- El arquitecto de datos de red se centrará en aprovechar la IA y la analítica de la red.
- El arquitecto de integración de red se centrará en la integración entre los dominios de red y de TI.

Resumen de la sección (continuación)

Profesionales: Adquieran proactivamente la combinación adecuada de habilidades técnicas y de software que les permitan desarrollarse en una o más de las siguientes áreas emergentes:

- El comandante de red se centrará en la administración del ciclo de vida de la red.
- El orquestador de la red se centrará en la traducción y automatización de políticas.
- El detective de red se centrará en el aseguramiento del servicio y la seguridad de la red.

Líderes: Consideren estas recomendaciones para construir el equipo de la red del futuro:

- Desarrollar una cultura de aprendizaje continuo.
- Encontrar el equilibrio entre la dotación de nueva capacidades y la contratación de nuevo personal.
- Invertir más en capacitación y desarrollo.
- Rotar al personal para aumentar la agudeza en el negocio.
- Fomentar un ambiente laboral inclusivo.

Principal predicción

"Para el año 2025, el 75% de los equipos de redes dedicará menos de un tercio de su tiempo a mantener el statu quo de la red, y dos tercios de su tiempo, a la innovación y la creación de valor para el negocio".

– Joe Clarke, Ingeniero Distinguido, Cisco

Nuevos conjuntos de habilidades para la red moderna

Durante los próximos dos años, las tecnologías de redes avanzadas modificarán casi todos los roles de la red. Dado que TI asume un papel más central en la transformación del negocio, los profesionales de TI deben adaptarse.

El 60% de los líderes empresariales cree que la TI está liderando la estrategia de transformación empresarial de la organización. Sin embargo, el 93% de los ejecutivos dice que la brecha de habilidades les impide transformarse lo suficientemente rápido.[34]

Ya sea que una línea de negocio esté implementando una nueva aplicación de IoT, un nuevo servicio en la nube o una nueva política de cumplimiento, los profesionales de TI deben comprender qué se requiere de la red y cuál será su rol para poder ofrecer los servicios de red necesarios de forma oportuna y segura.

En esta sección del informe, examinaremos cómo tres roles clave de TI (estratega de red, profesional de red y líder de TI) están cambiando. Además, identificaremos los nuevos conjuntos de habilidades que estos roles necesitarán para supervisar un entorno de red empresarial en rápida evolución.

Líder de TI

- Supervisión general de TI y redes
- Supervisa la estrategia de redes y el presupuesto

Títulos: CIO, Vicepresidente de Infraestructura de TI, Director de TI

Estratega de redes

- Responsable de definir la estrategia, la hoja de ruta, la arquitectura y las preferencias tecnológicas de las redes

Títulos: Estratega de Redes, Arquitecto de Redes/TI, Administrador de Redes

Profesional de redes

- Responsable de implementar, configurar, mantener y solucionar los problemas de la red

Títulos: Ingeniero de Red, Administrador de Red, Ingeniero de Soporte de Red

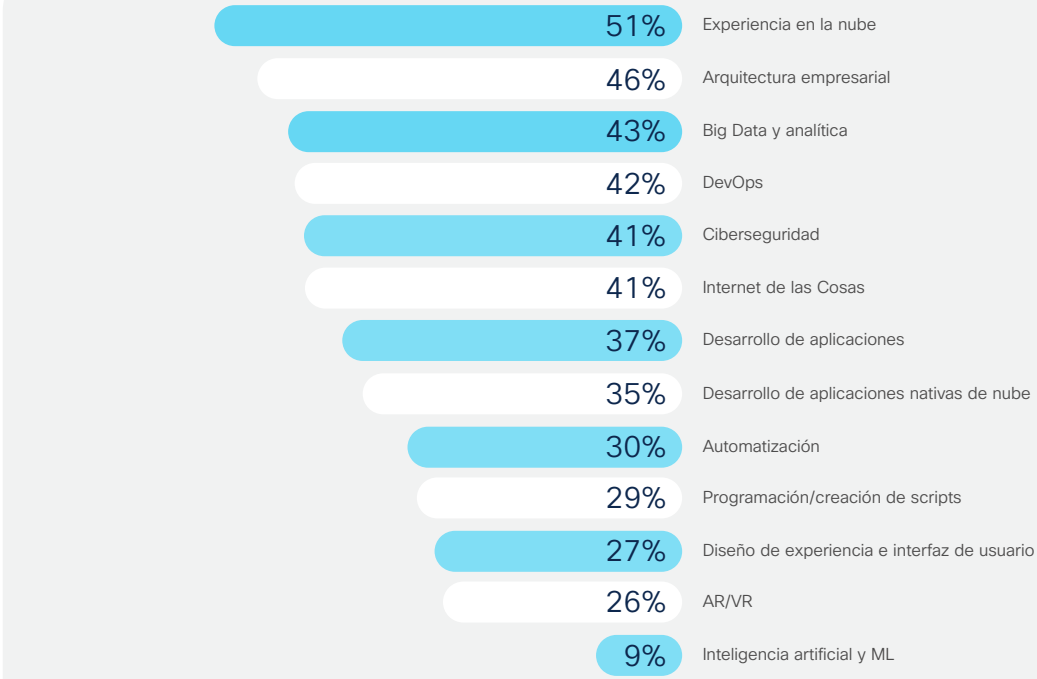
Preparación para el cambio de los conjuntos de habilidades de red

No debería sorprender que, a medida que la red empresarial evoluciona, también lo hacen las habilidades necesarias para construirla y administrarla. En dos encuestas recientes, los líderes de TI y los estrategas de redes revelan las brechas de habilidades que están detectando en los lugares habituales y no tan habituales.

Las mayores brechas de habilidades en tecnología de la información

Los datos de nuestra encuesta de talentos de TI revelan que, en el área de la TI en general, las tecnologías avanzadas, como la experiencia en la nube, la arquitectura empresarial, el Big Data y el análisis, DevOps y la ciberseguridad, encabezan la lista de las habilidades técnicas y la experiencia necesarias.[34] Por cierto, la necesidad de experiencia en las primeras cuatro brechas de habilidades temáticas (nube, arquitectura empresarial, análisis de datos y DevOps) ofrece pruebas sólidas de los roles cambiantes de la TI.

Figura 30: Principales brechas de habilidades de TI



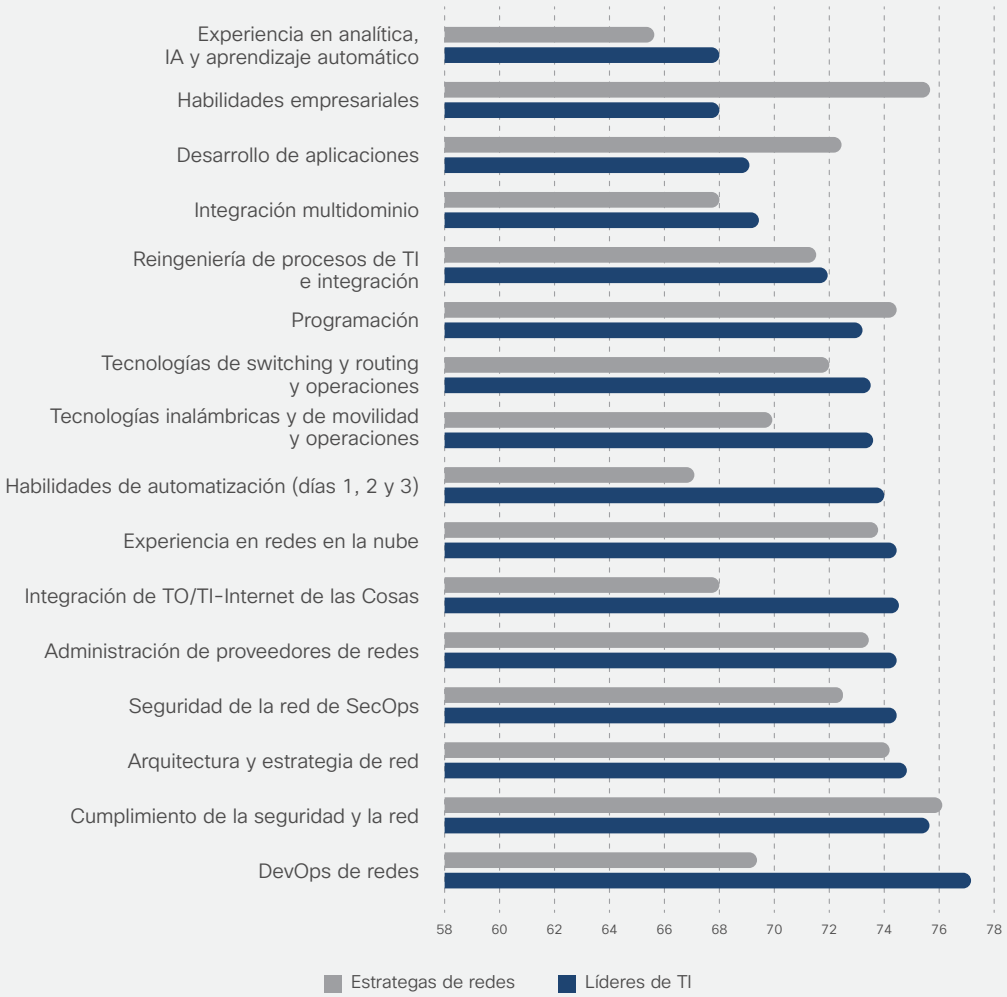
Pregunta: ¿Cuáles son las habilidades tecnológicas o experiencia más importantes que su departamento de TI necesita para apoyar la transformación del negocio?
Fuente: *Estrategias de profesionales de TI de última generación*, Cisco, octubre de 2018; n = 600 ejecutivos de negocios y de TI

Las mayores brechas de habilidades de redes

En nuestra *Encuesta sobre tendencias de redes a nivel global 2019*, les pedimos a los líderes de TI y a los estrategas de redes que calificaran la preparación de sus equipos para crear y mantener una red que satisfaga las demandas futuras de su organización.

En general, los líderes y los estrategas expresan un buen nivel de confianza en las capacidades de sus equipos de redes. Los líderes de TI identificaron el análisis y la IA, junto con las habilidades empresariales y las habilidades de desarrollo de aplicaciones, como los puntos a los que había que prestar más atención. Mientras que los estrategas de redes también reconocieron el análisis y la IA como una brecha, identificaron la integración de TI/TO, la automatización y DevOps de redes como otras áreas importantes para mejorar.[14]

Figura 31: Confianza en la preparación de los equipos de redes en cuanto a los diferentes conjuntos de habilidades



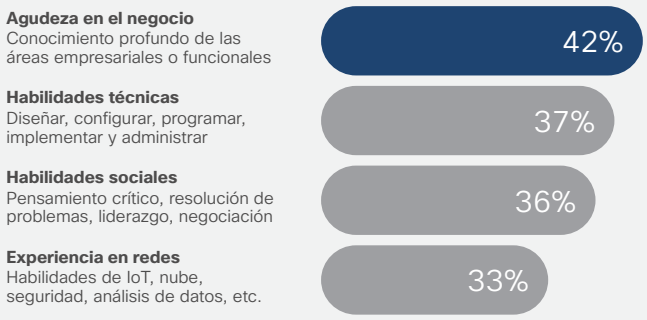
Pregunta: Al pensar en los conjuntos de habilidades y las capacidades actuales de su equipo de redes, ¿cómo calificaría el nivel de preparación del equipo para construir y mantener una red que satisfaga las demandas futuras de su organización en cada una de las siguientes áreas?

Fuente: *Encuesta sobre tendencias de redes a nivel global 2019;* n = 2061 (505 líderes de TI; 1556 estrategas de redes)

Creciente necesidad de habilidades sociales y laborales

Nuestra propia encuesta de talentos de TI revela que la falta de agudeza en el negocio es la brecha de habilidades número uno en el área de TI de hoy en día.[34] Cubrir esta brecha será fundamental a medida que las organizaciones migren a redes basadas en la intención. Al hablar el idioma del negocio, la TI puede traducir eficazmente los objetivos del negocio, o la intención, en políticas de TI de alto nivel, que a su vez pueden determinar las configuraciones de los dispositivos y la infraestructura.

Figura 32: La agudeza en el negocio es identificada como la principal brecha de habilidades



Pregunta: ¿Cuáles son las mayores brechas en experiencia y habilidades de TI que necesita para dar soporte a las iniciativas de transformación empresarial?
Fuente: *Estrategias de profesionales de TI de última generación*, Cisco, octubre de 2018; n = 600 ejecutivos de negocios y de TI

Cómo lo hace Cisco: desarrollo de la agudeza en el negocio

En Cisco, hemos creado el programa "Customer Zero" (Cliente cero), un programa que coloca a profesionales de TI en el desarrollo de productos, donde pueden desarrollar destreza en el negocio y habilidades sociales, como el pensamiento crítico y la resolución de problemas profundos. Esto alienta a los empleados a adaptarse y transformarse de maneras que nos ayuden a mantenernos competitivos.

Los roles cruzados más importantes del futuro

En un futuro próximo, algunos roles de TI se transformarán en posiciones cruzadas y abarcarán más de un área. Los administradores de red, por ejemplo, que agregan capacidades de programación o análisis de datos a su conjunto de habilidades, pueden desempeñar un rol emergente de una manera que amplíe eficazmente su contribución y aumente el valor de su trabajo.

Estos roles cruzados requerirán combinaciones únicas y muy solicitadas de áreas técnicas discretas y habilidades basadas en el lenguaje. Por ejemplo, los profesionales podrían programar la red a través de API y lenguajes de programación. O bien, los equipos de NetOps y SecOps podrían colaborar para crear flujos de trabajo operativos optimizados entre los dos equipos.

"Necesitamos ingenieros de redes y de infraestructura con el impulso para diseñar, construir y operar infraestructuras de misión crítica. Necesitamos desarrolladores de software con el impulso para escribir aplicaciones innovadoras que se ejecuten en la infraestructura y que automaticen los flujos de trabajo y las tareas. Las organizaciones más eficaces contarán con equipos de expertos en dominios tanto en software como en infraestructura que podrán trabajar juntos de manera eficaz".[37]

– Susie Wee, Vicepresidente Senior y CTO, Cisco DevNet

Nuevos roles para los estrategas de redes

Sin lugar a dudas, el trabajo más apremiante para los estrategas de redes será construir una hoja de ruta eficaz y de bajo riesgo hacia una arquitectura de red más ágil y alineada con el negocio.

Los estrategas también necesitarán optimizar la TI mediante la creación de catálogos de red de autoservicio, la integración de la red en los procesos de TI, la integración de los flujos de trabajo de NetOps y SecOps y la convergencia de la TI y la tecnología operativa (TO).
Las organizaciones necesitarán ayuda para diseñar las innovaciones empresariales habilitadas para la red, como la personalización basada en la ubicación, la optimización de la utilización del lugar de trabajo o las aplicaciones de expertos remotos.

El estratega del futuro: entrega de valor más allá de la red

El distinguido ingeniero de Cisco Joe Clarke cree que el rol de estratega de la red abarcará cada vez más las funciones que actualmente se encuentran fuera del radar de la mayoría de los estrategas.
Es probable que los estrategas de redes evolucionen hacia una o más de las siguientes áreas:

El **traductor empresarial** se centrará en alinear el rendimiento de la TI con la intención empresarial:

El traductor trabajará para convertir mejor las necesidades de la empresa en requisitos de nivel de servicio que se puedan aplicar y supervisar en toda la red. El traductor también trabajará para utilizar mejor la red y los datos de la red en pos de la innovación y el valor del negocio.

Habilidades empresariales: Determinar los requisitos empresariales y traducirlos en requisitos de red.

Habilidades de DevOps: Comprender cómo las API de plataforma de red y las tecnologías de procesamiento de lenguaje natural (Natural Language Processing, NLP) pueden conectar la intención empresarial y la TI.

El **arquitecto de integración de red** se centrará en la integración entre los dominios de red y de TI.

Los integradores trabajarán para integrar la red en el proceso de TI y con sistemas externos. El integrador también será responsable de la integración entre los dominios de red para garantizar que la intención sea entregada en todos los dominios relevantes.

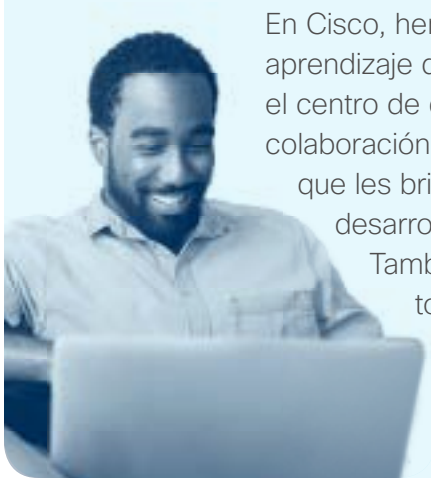
Reingeniería e integración de los procesos de TI: Comprender los procesos y flujos de trabajo de TI para modificar e integrar las operaciones de red en pos de mejorar la eficiencia.

Operaciones de servicio de ITSM: Comprender los procesos de la biblioteca de infraestructura de tecnología de la información (Information Technology Infrastructure Library, ITIL) para vincular eficazmente los sistemas de garantía de la red con las capacidades de ITSM.

DevOps skills: Desarrollar una comprensión de las API ofrecidas por una plataforma de red abierta y cómo pueden habilitar los flujos de trabajo integrados con otros sistemas de TI.

El **guardián de la red** se centrará en unir las arquitecturas de red y de seguridad:

Cómo lo hace Cisco: vías de aprendizaje continuo de TI



En Cisco, hemos desarrollado varias vías de aprendizaje de TI en torno a la empresa, la seguridad, el centro de datos, el proveedor de servicios, la colaboración, DevNet y otros temas avanzados, lo que les brinda a los ingenieros la oportunidad de desarrollar habilidades de vanguardia. También ofrecemos educación continua para todos los niveles asociados, especialistas, profesionales y expertos, así como capacitación y certificaciones gratuitas o con descuento para los empleados.

Los guardianes integrarán la inteligencia distribuida de la red en la arquitectura de seguridad y los procesos de SecOps. El guardián de la red tendrá un papel crítico en la convergencia de redes y seguridad.

Habilidades de seguridad: Definir las arquitecturas de seguridad de la red, implementar las tecnologías de seguridad de la red y comprender el papel de la red en contribuir con la seguridad general.

Habilidades de DevOps:Comprender cómo las API de la plataforma de red pueden habilitar la integración con los sistemas de SecOps.

El **arquitecto de datos de red** se centrará en aprovechar la IA y el análisis de la red:

El arquitecto de datos de red trabajará para aprovechar mejor la gran cantidad de datos que atraviesan la red y las herramientas emergentes habilitadas para IA para mejorar los servicios de TI e informar al negocio.

Habilidades de análisis y de IA: Recolectar datos para tomar mejores decisiones más rápido. Comprender las tecnologías de IA

y cómo se pueden aplicar para la garantía de la red e integrarse con otros sistemas de TI para la garantía general del servicio.

Habilidades para la información empresarial: Comprender el negocio y cómo se pueden utilizar los datos accesibles de la red para informar las decisiones y crear nuevas oportunidades.

Nuevos roles para los profesionales de redes

A medida que la transformación digital se vuelve central en la estrategia de una organización, los profesionales de redes deberán centrarse menos en las tareas de administración repetitivas y más en los servicios de valor agregado que respaldan los objetivos empresariales. Esto se volverá más fácil de hacer a medida que el aumento de los niveles de automatización de las redes avanzadas comience a eliminar las tareas que consumen mucho tiempo de los ingenieros de TI.

Los ingenieros de redes del futuro: entrega de valor más allá de la conectividad

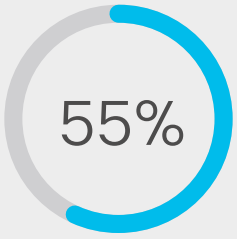
A medida que las redes basadas en la intención se vuelvan más frecuentes, los roles de los profesionales de redes evolucionarán hasta admitir uno o más de los pilares de las operaciones de redes: ciclo de vida, proceso o garantía. En este escenario, los profesionales de redes necesitarán desarrollar habilidades para llevar a cabo una o más de estos potenciales roles:

> "El ingeniero de red exitoso de hoy en día es aquel que sabe cómo integrar las tecnologías nuevas y las tradicionales y que cierra la brecha entre las redes y el desarrollo de software. Esto requiere una mentalidad de DevOps y una mejor comprensión de cómo la tecnología está vinculada a los objetivos del negocio".
>
> — Joe Clarke, Ingeniero Distinguido, Cisco

El **comandante de red** se centrará en la administración del ciclo de vida de la red:

El comandante se hará cargo de los procesos y las prácticas que aseguren el estado general y el funcionamiento continuo del controlador de red y de la red subyacente.

Habilidades necesarias: Operar, mantener y ajustar un controlador que ofrezca automatización y orquestación en entornos de redes basadas en la intención. Garantizar la sustentabilidad de las integraciones de la plataforma con otros sistemas. Comprender el ciclo de vida de estos controladores y garantizar el estado continuo,



Actualmente, las tareas de administración repetitivas pueden ocupar el 55% del tiempo y de los recursos de los profesionales de redes.[14]

la seguridad, el cumplimiento y la estabilidad de los controladores y la red subyacente.

El **orquestador de la red** se centrará en la traducción y automatización de políticas:

Los orquestadores deben comprender cómo las necesidades empresariales se traducen en políticas de red y, luego, administrar la automatización de dichas directivas. Los orquestadores también serán responsables de la alineación de las políticas con otros dominios de red y de TI.

Habilidades necesarias: Dominar la manera de emplear las herramientas de automatización de la infraestructura, los protocolos de automatización y los modelos de datos. Adquirir pericia con Linux, Python y herramientas de desarrollo de programación de red. Comprender los formatos de datos comunes. Familiarizarse con las metodologías ágiles de desarrollo de software y sentirse a gusto utilizando API y kits de herramientas para interactuar con los controladores y los dispositivos de red.

El **detective de red** se centrará en la garantía del servicio y la red:

Los detectives serán expertos en el uso y el ajuste de las herramientas de garantía de la red que utilicen análisis avanzados e IA para garantizar que la red cumpla con la intención empresarial prometida. Los detectives deberán integrarse con los procesos de administración de servicios de TI y también trabajarán estrechamente con el equipo de SecOps para garantizar que se marquen las anomalías de red y se cierren las posibles brechas de seguridad.

Habilidades necesarias: Identificar y priorizar las tendencias a partir de la información basada en IA para que la organización pueda tomar medidas de forma proactiva. Ajustar y proporcionar comentarios a los sistemas de análisis con el objetivo de mejorar continuamente la detección y corrección de anomalías. Integrar los procesos de detección y resolución de problemas de red en los procesos de TI y seguridad.

Líderes de TI: tomar medidas para cubrir las carencias de habilidades en redes

El desarrollo de habilidades técnicas es actualmente fundamental para lograr una transformación digital exitosa en el futuro. En nuestra *Encuesta sobre tendencias de redes a nivel global 2019*, invitamos a los líderes de la TI a compartir lo que actualmente están haciendo para desarrollar sus habilidades. La reconversión laboral, la expansión y el reequilibrio de las habilidades son los principales enfoques.

Figura 33: Enfoques preferidos para abordar las carencias de habilidades en redes

Pregunta: ¿Cuál es el enfoque principal que el liderazgo de TI de su organización debería priorizar para abordar las brechas actuales en las habilidades necesarias para planificar, implementar y mantener sus futuras necesidades de redes?

Fuente: *Encuesta sobre tendencias de redes a nivel global 2019;* n = 505 líderes de TI

Si bien a los líderes les preocupa la reconversión laboral, sigue siendo el enfoque preferido, tanto para las habilidades empresariales de TI como para las habilidades técnicas de TI.

Figura 34: Las principales preocupaciones sobre la reconversión laboral

Pregunta: Al considerar algún plan para reconvertir laboralmente al equipo de redes en su organización para construir y habilitar de mejor manera una red más avanzada, ¿qué le preocupa más?

Fuente: *Encuesta sobre tendencias de redes a nivel global 2019;* n = 505 líderes de TI

Recomendaciones para los líderes de TI: cómo construir el equipo de la red del futuro

Según Guillermo Díaz, Vicepresidente Senior de Transformación de Clientes de Cisco, estas cinco estrategias pueden ayudar a los líderes a construir un equipo de redes equipado para impulsar un negocio transformado digitalmente.

1. **Desarrollar una cultura de aprendizaje continuo:** Es absolutamente esencial que los líderes de TI cultiven una cultura de aprendizaje continuo. Hacerlo ayudará a los estrategas y a los profesionales de redes a dominar regularmente las habilidades que necesitan para adaptarse a las nuevas tecnologías y procesos operativos. Esto se puede hacer a través de una combinación de oportunidades de desarrollo internas y externas que les brinden a sus equipos educación, experiencia y exposición variadas.

2. **Encontrar el equilibrio entre la reconversión laboral y la contratación de nuevo personal:** Nuestra investigación muestra que los líderes están recurriendo cada vez más a la mejora de las cualificaciones para llenar las carencias de habilidades. Sin embargo, cuando se trata de nuevas tecnologías, parece ser lo contrario. Muchas organizaciones están buscando nuevos talentos para llenar los puestos de tecnología emergentes, en especial en torno a la IA y el ML. Encontrar el equilibrio adecuado entre desarrollo y la contratación dependerá de los objetivos empresariales y operativos y de dónde se encuentre en la transformación de la red.

3. **Invertir más en capacitación y desarrollo:** En una encuesta reciente a líderes de TI, descubrimos que las organizaciones que tienen más éxito en su transformación digital gastan casi un 10% más en capacitación y desarrollo para su personal de TI.[34] Cuando TI puede igualar el ritmo del cambio de la tecnología, puede tomar decisiones más rápidas, más inteligentes y mejores basadas en los datos y en apoyo de los objetivos del negocio.

> "La reconversión laboral es menos costosa que recurrir al mercado externo para contratar a un nuevo especialista, ciertamente en términos de salario y comisión por la contratación, pero también en términos del costo de la incorporación, la transferencia de los conocimientos tácitos de la organización y de la familiaridad con los procesos. El personal existente puede carecer de determinadas habilidades y capacidades nuevas, pero es probable que tengan mucho de lo que sí necesita para darle una ventaja".[38]
>
> — Colin Seward, CIO de Cisco para Europa, Medio Oriente, África y Rusia

Satisfacer las nuevas necesidades: conjunto de certificaciones ampliado de Cisco

Para ayudar a abordar estos nuevos requisitos de capacitación, las certificaciones y los planes de estudio en red, como los proporcionados por Cisco, se están actualizando rápidamente.[37]

4 **Rotar al personal para aumentar la agudeza en el negocio:** Hacer que el personal de la empresa y de TI intercambie sus puestos mediante rotaciones de corto plazo amplía la comprensión, desarrolla un contexto más amplio y permite interacciones más productivas más adelante. Más específicamente, la capacidad de facilitar las rotaciones en las áreas de redes, aplicaciones y empresariales proporciona una combinación de habilidades en tecnología, capacidad de programación y agudeza en el negocio.

5 **Fomentar un ambiente laboral inclusivo:** Las recomendaciones anteriores se centran en el personal idóneo. Crear un lugar de trabajo altamente inclusivo significa aprovechar al máximo el personal idóneo que la organización tiene a disposición. Se observa que las empresas que priorizan la diversidad y la inclusión en la forma en que reclutan, gestionan, desarrollan y recompensan a los empleados superan a los rivales que no lo hacen. Comienza con el liderazgo ejecutivo y el compromiso con los estándares de comportamiento, los programas, las políticas y la capacitación que crean las condiciones para un entorno inclusivo en la organización. La organización de TI de última generación tiene que "predicar con el ejemplo" de una cultura diversa e inclusiva en su funcionamiento diario.

Cómo lo hace Cisco: cómo atraer nuevos empleados idóneos

Encontrar personal idóneo no sucede por accidente. Es por eso que utilizamos programas como nuestros "IT University" (Universidad de TI), "Cisco Networking Academy" (Academia de Redes de Cisco) y Cisco International Internship Program (Programa de Pasantías Internacionales de Cisco) para identificar y contratar nuevos talentos, así como también Cisco Veterans Program (Programa de Veteranos de Cisco), que nos ayuda a capacitar y emplear a empleados con antigüedad interesados en carreras de tecnología.

Sobre este informe

El *Informe sobre tendencias de redes a nivel global 2020* les ofrece a los líderes de TI, los estrategas y los profesionales información sobre las tendencias de redes actuales y futuras en toda la empresa, y ofrece orientación esencial sobre tecnología, operaciones y personal idóneo en redes. El informe se basa en una investigación original de Cisco e incluye nuevos datos de la *Encuesta sobre tendencias de redes a nivel global 2019* de 2061 estrategas y líderes de TI de 13 países. Además, los líderes, colegas e ingenieros distinguidos de Cisco proporcionan análisis y recomendaciones de expertos para las organizaciones que se encuentran en la transición a tecnologías de redes avanzadas.

Este informe está dedicado a Cliff Apsey, cuya pasión por ofrecer las mejores experiencias digitales a los clientes nos inspiró para hacer de este informe una mejor experiencia para usted. Apreciamos el tiempo que pasamos con Cliff y siempre lo extrañaremos.

Fuentes

1. *IDC FutureScape: Predicciones de 2018 sobre infraestructura empresarial a nivel mundial*, IDC, 2017.
2. *Encuesta sobre centros de datos anual del Uptime Institute,* 2019.
3. *Pronóstico de VNI Completo de Cisco 2018, Cisco, 2018.*
4. *Informe de ciberseguridad anual de Cisco 2018, Cisco, 2018.*
5. "J.C.R. Licklider," Salón de la Fama de Internet, 2013.
6. "Historia de la educación en línea", The Quad, 2019.
7. *Pronóstico de datos y dispositivos de IoT de IDC Global Datasphere a nivel mundial, 2019-2023*, IDC, mayo de 2019.
8. Dennis Smith, Dale Kutnick, Lisa Pierce, Invierta en redes para lograr el éxito en el negocio digital, Gartner, mayo de 2019
9. "Breve historia de la globalización", Foro Económico Mundial, enero de 2019.
10. *Digital Vortex 2019: Cambio continuo y conectado, IMD, 2019.*
11. *Reinventado el futuro* (encuesta sobre casos de uso de automatización), Capgemini Research Institute, 2018.
12. "Herramienta de Información Destacada del Pronóstico de VNI", Cisco, 2017.
13. *Cisco Visual Networking Index: Pronóstico y tendencias, 2017–2022 (notas técnicas), Cisco, febrero de 2019.*
14. *Encuesta sobre tendencias de redes a nivel global 2019, , Cisco, 2019.*
15. Jonathan Forest, Neil Rickard, Hoja de ruta estratégica para redes de 2019, Gartner, 10 de abril de 2019
16. *Diferencias entre modelos de intención, política y servicio*, IETF, 3 mayo de 2018.
17. "¿Por qué la red basada en intención es una buena noticia para la red definida por software?" Cisco, 1 de junio de 2018.
18. *Redes basadas en la intención: la unión entre el negocio y la TI, Cisco, enero de 2018.*
19. *Redes basadas en la intención: Evolución de la red del campus empresarial,* IDC, junio de 2018.
20. "Las empresas no pueden tener problemas de compromiso de automatización y ser exitosas", IT Connection, 21 de julio de 2017.
21. "El auge de la AIOps: cómo los datos, el aprendizaje automático y la IA transformarán la supervisión del rendimiento", AppDynamics, 17 de diciembre de 2018.
22. "Aseguramiento de la red con razonamiento automático y aprendizaje automático", Cisco, 25 de julio de 2019.
23. *Índice global de nube de Cisco: Pronóstico y metodología, 2016-2021 (notas técnicas), Cisco, 19 de noviembre de 2018.*
24. "Predicciones 2019: Infraestructura", Cisco, 11 de febrero de 2019.
25. *La multinube es la nueva norma*, IDC, marzo de 2018.
26. *SD-WAN: La seguridad, la experiencia en las aplicaciones y la simplicidad operativa impulsan el crecimiento del mercado, IDC, abril de 2019.*
27. "Conectando lo desconectado: 5G y Wi-Fi 6 jugarán un papel fundamental en saldar la brecha digital", Cisco, 19 de marzo de 2019.

28. "OpenRoaming: Roaming automático y sin interrupciones a través de Wi-Fi 6 y 5G", Cisco, 29 de abril de 2019.
29. *El ecosistema extendido de confianza cero: Redes*, Forrester, 2 de enero de 2019.
30. *Anticipándose a lo desconocido: Estudio de referencia del Director de Seguridad de la Información, Cisco, marzo de 2019.*
31. Sanjit Ganguli, Lawrence Orans, Alineación de los objetivos de las herramientas de NetOps y SecOps con los casos de uso compartidos, Gartner, 24 de julio de 2018
32. *Actores cibernéticos patrocinados por el Estado ruso que apuntan a dispositivos de infraestructura de red, CISA, 16 de abril de 2018.*
33. "Serie del Informe sobre ciberseguridad de Cisco", Cisco, 2019.
34. *Estrategias de profesionales de TI de última generación, Cisco, octubre de 2018.*
35. *Transformación de las operaciones de TI, Cisco Connected Futures, 2018.*
36. *Operaciones de red de última generación, Cisco, septiembre de 2019.*
37. "Incorporación de las prácticas de software y las habilidades de software a las redes mediante las certificaciones de Cisco y DevNet", Cisco, 10 de junio de 2019.
38. *La evolución del equipo de TI, Cisco, 2019.*