The bridge to possible

Informe de tendencias globales en redes **2021**

Edición especial sobre la capacidad de resiliencia empresarial: conozca las cinco tendencias que impulsan la agilidad y la resiliencia en tiempos de perturbación.

Contents

Introducción: Resiliencia

Introducción: Desde la continuidad empresarial hasta la resiliencia empresarial

Ni como individuos ni como empresas anticipamos o estuvimos preparados para una disrupción global a largo plazo como el COVID-19. Practicamente de la noche a la mañana, fuerzas laborales enteras comenzaron a trabajar de forma remota mientras que algunas empresas se las ingeniaron para poner sus bienes y servicios en línea y otros hicieron el cambio de cadenas de suministro estratégico a nuevos proveedores y geografías.

Lógicamente, la pandemia ha sido un llamado de atención para cada nación, municipalidad y organización. ¿Qué cambió? Después de todo, no es la primera dificultad que enfrentan las empresas; 7 de 10 organizaciones sufrieron al menos una fuerte crisis en los últimos 5 años y el 95 % está convencido de que no será la última.[1]

Las organizaciones sufrieron al menos una fuerte crisis en los últimos 5 años.

Fuente: “PwC: Encuesta sobre la crisis global 2019”

Las disrupciones provocadas por el ser humano, como ciberataques, obligaciones regulatorias y agitaciones sociales se han convertido en una parte cada vez más común de nuestro escenario. Mundialmente, estamos sufriendo los duros impactos de huracanes, incendios forestales y otras **alteraciones naturales** a un ritmo creciente y de manera regular.

Recorrer correctamente las futuras disrupciones requiere que los líderes de TI adopten una nueva mentalidad. Una con un renovado énfasis en la agilidad necesaria para lograr la **resiliencia empresarial,** en lugar del enfoque más prescriptivo y reactivo que ha sido la base de la planificación tradicional sobre **continuidad del negocio.** A diferencia de los esfuerzos actuales de continuidad del negocio, la resiliencia empresarial ubica a las organizaciones para prepararse incluso para lo inesperado.

[1] PwC, “Encuesta de crisis global de PwC 2019”.

Continuidad del negocio frente a la resiliencia empresarial

Continuidad del negocio: La capacidad de una organización de seguir ofreciendo productos o servicios a niveles preestablecidos aceptables luego de una interrupción. *

Resiliencia empresarial: La capacidad de una organización de absorber y adaptarse en un entorno cambiante para poder cumplir sus objetivos, sobrevivir y prosperar. **

* Organización Internacional de Normalización, “Seguridad y resiliencia: Vocabulario”, ISO 22300-2018

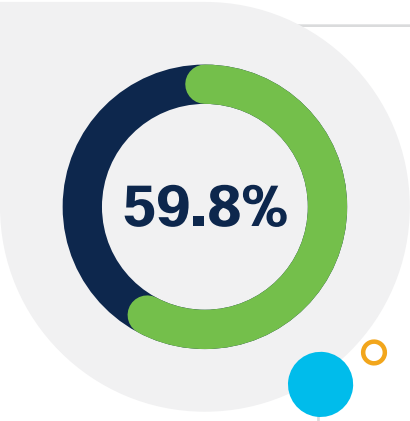
** Organización Internacional de Normalización, “Seguridad y resiliencia: Resiliencia de las organizaciones, principios y atributos”, ISO 22316-2017

Figura 1. De la continuidad del negocio a la resiliencia empresarial

Cinco tendencias de redes

La red: 5 tendencias para permitir la resiliencia empresarial

Los procesos empresariales fundamentales dependen de una compleja red de tecnologías digitales que ofrecen las bases para lograr la resiliencia empresarial.



La mayoría de los profesionales de continuidad del negocio (59,8 %) consideran la resiliencia de TI como el factor más importante en respuesta a la presente pandemia.

Fuente: BCI, “El futuro de la continuidad y la resiliencia empresarial”

Como la única plataforma que une, protege y permite un conjunto cada vez más dinámico y distribuido de usuarios y dispositivos, y aplicaciones y cargas de trabajo cada vez más divididas y dispersas, la red cumple una función central en ayudar a las organizaciones a generar su resiliencia.

En otras palabras, ya no es suficiente la resiliencia de la red que mantiene la conectividad y el tiempo de funcionamiento de la red. Las empresas necesitan que se permita la resiliencia por parte de una plataforma de red avanzada que pueda responder rápidamente a cualquier circunstancia, permitir nuevos modelos operativos y servicios, integrarse con los procesos de TI y proteger a sus empleados, las actividades principales, los clientes y la marca. En realidad, es la misma red avanzada necesaria para respaldar las iniciativas de transformación digital.

Resiliencia de la red frente a las redes de resiliencia empresarial

Resiliencia de la red: La capacidad de ofrecer y mantener un nivel aceptable de servicio frente a los errores y desafíos del funcionamiento normal de una red de comunicaciones determinada, según las instalaciones dispuestas.*

Redes de resiliencia empresarial: Redes diseñadas para permitir que las organizaciones respondan con rapidez, seguridad y eficacia frente a las interrupciones previstas o inesperadas.

* Unión Internacional de Telecomunicaciones, “Requisitos para la resiliencia de redes”.

Generar agilidad y resiliencia para la fuerza laboral, lugar de trabajo y operaciones.

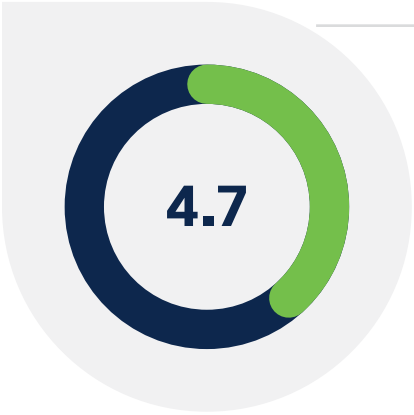
Hemos optado por destacar cinco tendencias que deben evaluar los líderes de redes como parte de sus esfuerzos para respaldar los planes de resiliencia de sus organizaciones Se relacionan a mejorar la resiliencia de cuatro esferas clave: **fuerza de trabajo, lugar de trabajo, carga de trabajo** y **operaciones de TI.**

Figura 2. Base de red para la fuerza laboral, el lugar de trabajo, la carga de trabajo y la resiliencia operativa.

Fuerza laboral: Remota, segura

Tendencia n.º 1: Fuerza laboral: Ampliar la seguridad a una fuerza laboral remota

La mayoría de las organizaciones se están dando cuenta de que los nuevos enfoques más flexibles que funcionarán serán parte de una realidad permanente para los empleados.



En la actualidad, un promedio de 4,7 veces más de empleados están trabajando desde el hogar en comparación con lo que sucedía antes de la pandemia. Muchos equipos de TI lucharon con la escalabilidad para hacer frente a la demanda repentina.

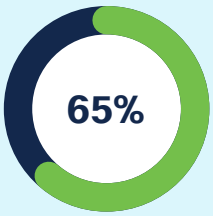
Fuente: Freeform Dynamics, "Una nueva perspectiva sobre el lugar de trabajo moderno", informe patrocinado por Cisco, julio de 2020

Como resultado, TI se enfrenta a un nuevo conjunto de requisitos empresariales:

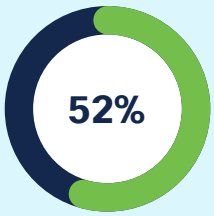
- Permitir que los trabajadores sean productivos y colaboren desde cualquier lugar
- Optimizar el rendimiento de TI, el costo y la seguridad para cada trabajador
- Ampliar la gestión y las operaciones de TI de clase empresarial

Pero cumplir esos requisitos tiene sus propios desafíos. En particular, la seguridad del trabajador remoto, así como el comportamiento del usuario final, siguen siendo las preocupaciones y desafíos actuales para la mayoría de las organizaciones de TI.

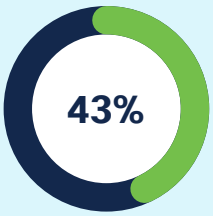
Los 4 desafíos principales para autorizar a los trabajadores remotos:



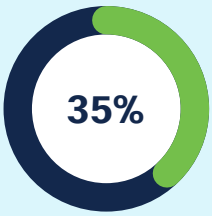
Seguridad (65 %)



Comportamiento del usuario final (52 %)



Rendimiento de la aplicación (43 %)



Operaciones de TI (35 %)[2]

[2] "Encuesta sobre redes de resiliencia empresarial 2020"

Al utilizar dispositivos y conexiones personales para acceder a aplicaciones y datos corporativos, los trabajadores remotos son particularmente vulnerables a ataques de ciberseguridad. Muchos eluden la VPN y se conectan directamente a servicios y aplicaciones en la nube, que sigue siendo el entorno más difícil para defender.[3]

Consideraciones sobre redes: al admitir modelos seguros de trabajo desde el hogar, los equipos de TI deben adoptar algunos o la totalidad de los siguientes enfoques:

- **Escalar las VPN para proteger a los trabajadores remotos:** las VPN empresariales siguen ofreciendo una de las formas más eficaces y rápidas de ampliar el control y la protección para los trabajadores remotos.
- **Utilizar la autenticación multifactor (MFA) para proteger las aplicaciones:** MFA, que verifica la identidad de cada usuario antes de permitirle acceder a la red o a aplicaciones y datos confidenciales, es fundamental para proteger la organización.
- **Implementar un perímetro de servicio de acceso seguro (SASE) para ayudar a garantizar la protección para el acceso multinube:** la seguridad basada en la nube y SASE ayudan a defenderse de las amenazas basadas en Internet, independientemente de la conexión, el dispositivo del usuario o el entorno de nube.

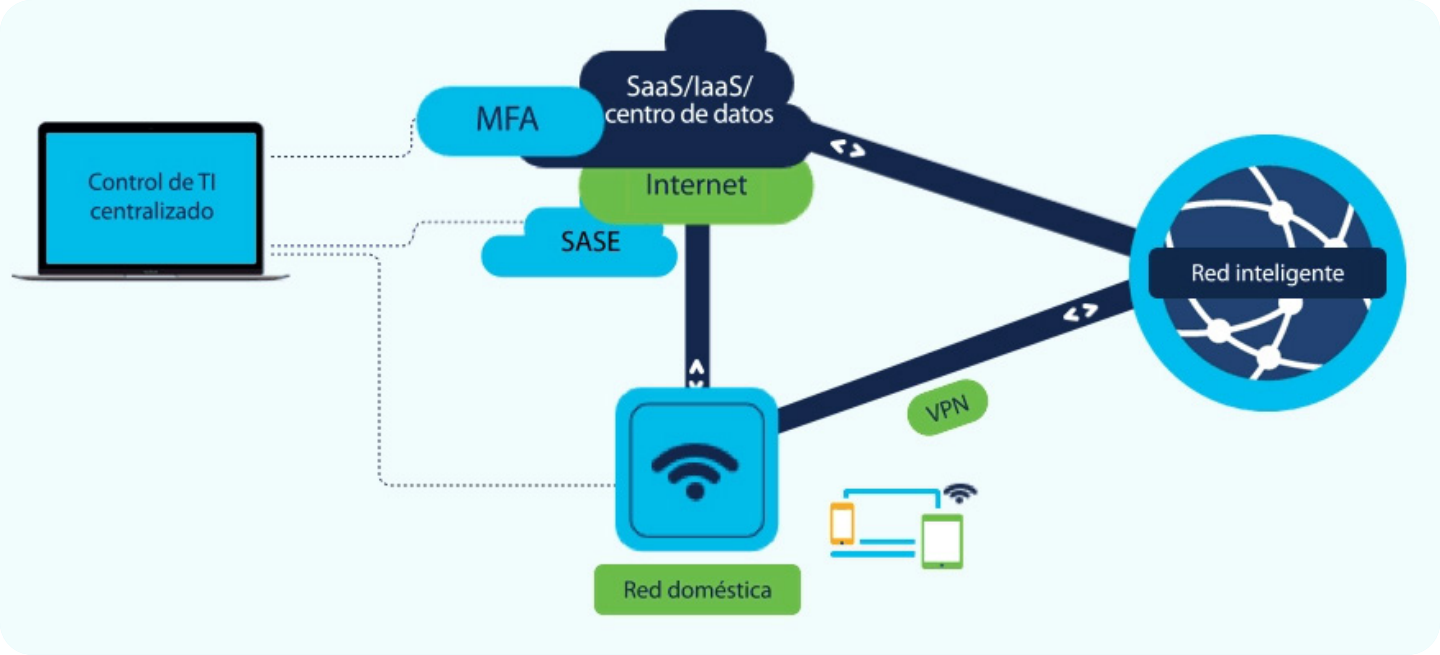


Figure 3. Proteger la fuerza laboral remota con VPN, MFA y SASE

Más información sobre la conexión y proteger su fuerza laboral remota

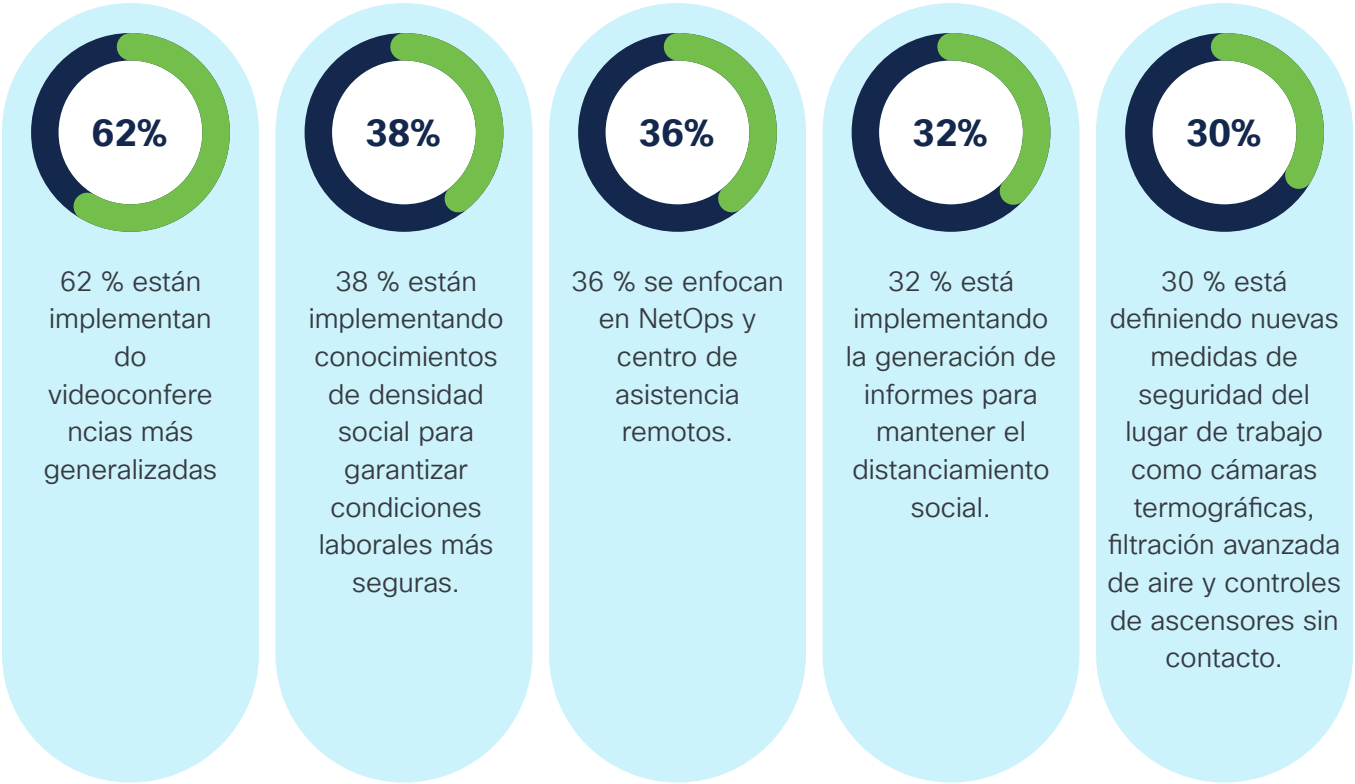
[3] Cisco Umbrella, "Tendencias sobre ciberseguridad 2019".

Lugar de trabajo: Seguro, confiable

Tendencia n.º 2: Lugar de trabajo: Permitir el regreso seguro a los lugares de trabajo en las instalaciones

Mientras que quedan muchos interrogantes, está claro que los lugares y los espacios de trabajo evolucionarán como consecuencia de la actual pandemia. Innumerables compañías se encuentran en el proceso de potenciar los servicios existentes como las videoconferencias y Wi-Fi basado en ubicaciones. Otros están desarrollando nuevos servicios y medidas de seguridad, como el monitoreo de la distancia física, el informe de proximidad, un aumento en la automatización del lugar de trabajo e incluso robots que respaldan la productividad humana y la comunicación.

Cómo se están preparando los equipos de red para un regreso seguro al lugar de trabajo



Fuente: “Encuesta sobre redes de resiliencia empresarial 2020”

Consideraciones de red: una red moderna y ágil es un motor fundamental que facilita la reincorporación segura y sin inconvenientes de los trabajadores a las instalaciones.

- **Prueba de esfuerzo de la red:** en muchos casos, la red ha estado sin funcionar unas cuantas semanas. No den por hecho que todavía pueda ofrecer los servicios por cable e inalámbricos necesarios.
- **Automatizar el acceso seguro basado en identidades:** las organizaciones necesitan la capacidad de administrar, proteger y segmentar de manera uniforme la incorporación de usuarios y dispositivos y el acceso a servicios, ya sea que se conecten desde las instalaciones, desde el hogar o desde redes públicas.
- **Mejorar la seguridad de los empleados y los clientes mediante análisis basados en ubicaciones:** permitir el monitoreo, las alertas y conocimientos del lugar de trabajo para ayudar a proteger la salud y seguridad de los empleados, partners, usuarios temporales y clientes al aprovechar las redes de Wi-Fi.

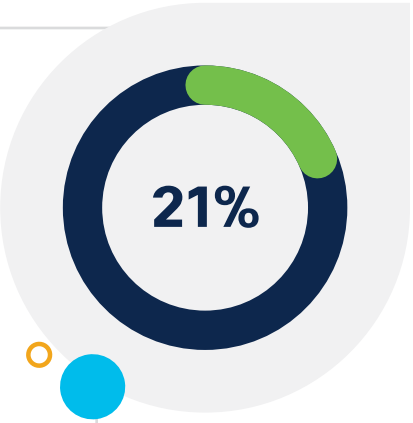
Más información sobre cómo crear un entorno seguro para el lugar de trabajo

Carga de trabajo: Multinube

Tendencia n.º 3: Carga de trabajo: Facilitar la multinube para una mayor resiliencia

Los líderes de TI utilizan servicios en la nube como un medio para mejorar la resiliencia empresarial como consecuencia de la pandemia global. Esto incluye una adopción cada vez mayor del modelo multinube (distribución de aplicaciones, cargas de trabajo y datos en las instalaciones, centros de datos y proveedores de nube pública) para reducir costos, aumentar la flexibilidad y protegerse y propagar el riesgo de fallas catastróficas.

> "21 % de las organizaciones están trasladando las cargas de trabajo adicionales a la nube pública debido a problemas de CapEx relacionados con la pandemia. "
>
> IDC, "Encuesta de impacto del COVID-19, Wave 5", 2020



Consideraciones de la red: para garantizar una experiencia uniforme para los usuarios y los equipos de DevOps, las organizaciones necesitan una estrategia de red proactiva y multinube que alinee la red con las prioridades de la nube, la seguridad y las operaciones de TI.

Las estrategias exitosas de redes multinube se basan en tres pilares fundamentales:

- **Carga de trabajo:** adoptar un modelo operativo en la nube para simplificar las políticas, la seguridad y la administración de cargas de trabajo y servicios en los centros de datos en las instalaciones, múltiples nubes diferentes y otros entornos informáticos.
- **Acceso:** adoptar enfoques de SD-WAN y SASE para ayudar a garantizar un acceso multinube seguro y uniforme (que incluya SaaS) para los usuarios y dispositivos corporativos y redes públicas desde el campus, las sucursales o el hogar o fuera de la oficina.
- **Seguridad:** reducir el riesgo asociado con los usuarios, dispositivos y aplicaciones distribuidas en varias nubes y otros entornos informáticos.

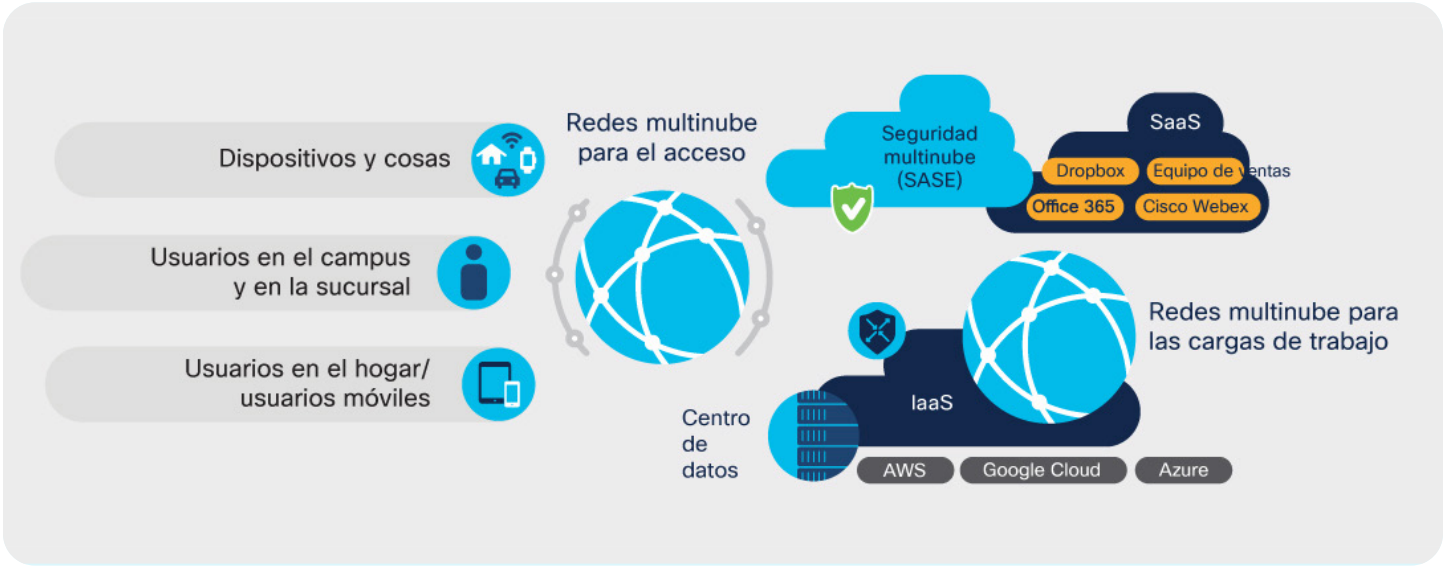


Figure 4. Red multinube: Carga de trabajo, acceso y seguridad

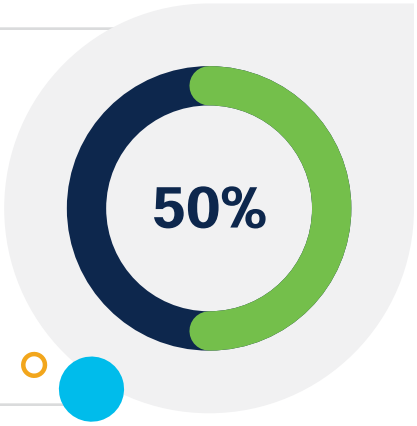
Más información sobre el desarrollo de una estrategia multinube segura y eficaz

Operaciones: Automatizadas

Tendencia n.º 4: Operaciones, automatizar operaciones para una recuperación más rápida

El aumento en la cantidad de trabajadores remotos dispersos no es lo único que pone una presión extraordinaria en los equipos de NetOps actuales. La pandemia también ha impulsado niveles inigualables de grandes fluctuaciones en la cantidad de clientes, los patrones de tráfico de aplicaciones y nuevos casos de uso como el aprendizaje electrónico, videoconferencias, eventos virtuales, atención remota y otros servicios que dependen de la red.

> "50 % prioriza la automatización de la red para abordar las interrupciones actuales. "
>
> Encuesta sobre redes de resiliencia empresarial 2020



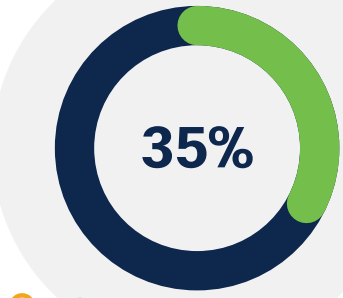
No es de sorprender que en la actualidad, la mitad de los profesionales de redes, reconozcan la automatización de la red como un requisito fundamental para garantizar un servicio y rendimiento continuos durante una interrupción.

Fuente: Informe de tendencias globales en redes de Cisco 2020

Consideraciones de la red: los equipos de NetOps pueden lograr una mejora constante y responder rápidamente a las crecientes interrupciones y amenazas al adoptar un enfoque por etapas:

- **Automatizar las tareas administrativas repetitivas** como el aprovisionamiento de la red, la configuración y la administración de imágenes para reducir la carga administrativa y mejorar el cumplimiento en cada dominio.
- **Automatizar el acceso a la red, la incorporación** y la segmentación para proteger a los grupos de usuarios y cosas distribuidos y mitigar la difusión de ataques a la ciberseguridad.
- **Automatizar la política de red en el centro de datos empresariales** con la segmentación centrada en las aplicaciones que protege a las aplicaciones y los datos y sigue la carga de trabajo.
- **Automatizar la política más allá del centro de datos hacia la nube** con un modelo operativo en la nube que ofrece una política uniforme de aplicaciones en las instalaciones y en entornos de nube híbrida.
- **Automatizar la segmentación integral basada en políticas multidominio** para definir un modelo integral de acceso de confianza cero desde los usuarios y las cosas hasta las cargas de trabajo.

> “35 % planean que sus redes estén basadas en la intención en todos los dominios para 2022, con un aumento de apenas el 4 % respecto de 2019. ”
>
> Informe de tendencias globales en redes de Cisco 2020



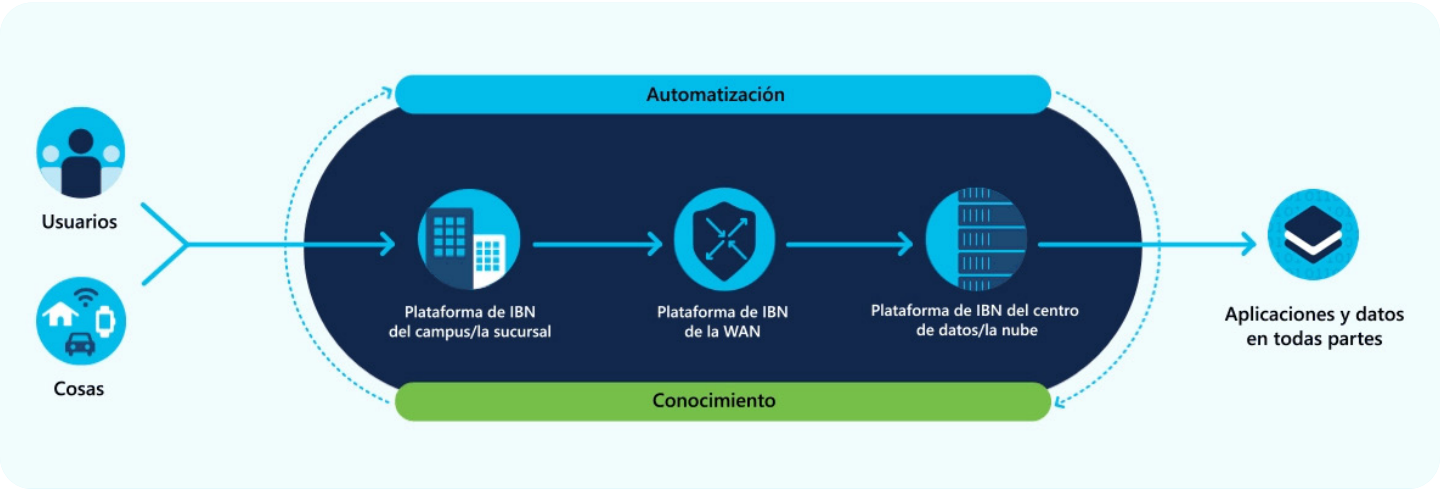


Figure 5. Automatización y conocimiento desde el usuario hasta la carga de trabajo desde cualquier lugar

Descubra cómo automatizar la política en varios dominios de red

Operaciones: Habilitadas para IA

Tendencia n.º 5: Operaciones: Aprovechar análisis de red impulsada por IA para ideas más inteligentes

Administrar la complejidad y la escalabilidad de las redes modernas y el aluvión resultante de eventos y problemas que apremian a varias plataformas de monitoreo diferentes puede ser abrumador e ineficaz, especialmente cuando sucede una interrupción.

> "4400: Cantidad promedio de eventos mensuales relacionados con las redes inalámbricas en una red empresarial. * "
>
> Fuente: Telemetría de Cisco: Cisco DNA Center, 2020

* Basada en más de 600 redes empresariales. Los eventos incluyen fallas/tiempos de incorporación, rendimiento de radio y tiempos de respuesta/fallas de DHCP. Estos números de eventos ya se han reducido con las líneas de base dinámicas habilitadas para IA.

Sin duda, los equipos de NetOps necesitan la ayuda de análisis avanzados para tomar decisiones de corrección inteligentes y oportunas.

Al utilizar los análisis de red habilitados para IA y técnicas de aprendizaje automático, los equipos de NetOps logran tener un conjunto de problemas más controlable sobre el que pueden tomar medidas.

> "A nivel global, Cisco AI Network Analytics, una aplicación dentro de Cisco DNA Center, resuelve 2,6 millones de "eventos" mensuales en 15 080 "problemas" procesables, una reducción del 99,4 %. *"
>
> Fuente: Telemetría de Cisco: Cisco DNA Center, 2020

* Basado en más de 700 redes empresariales, a nivel mundial.

Esta reducción permite que los equipos concentren todos sus esfuerzos en aquello que realmente importa y que puede provocar un impacto empresarial negativo.

Y este problema ya no se limita a la red empresarial. Ahora que la mayoría de las transacciones en redes surgen o terminan fuera de la red empresarial tradicional, los equipos de NetOps también necesitan visibilidad y análisis para las redes públicas a las que están conectadas. Esto es particularmente importante durante períodos de tensión inusual, como la reciente pandemia.

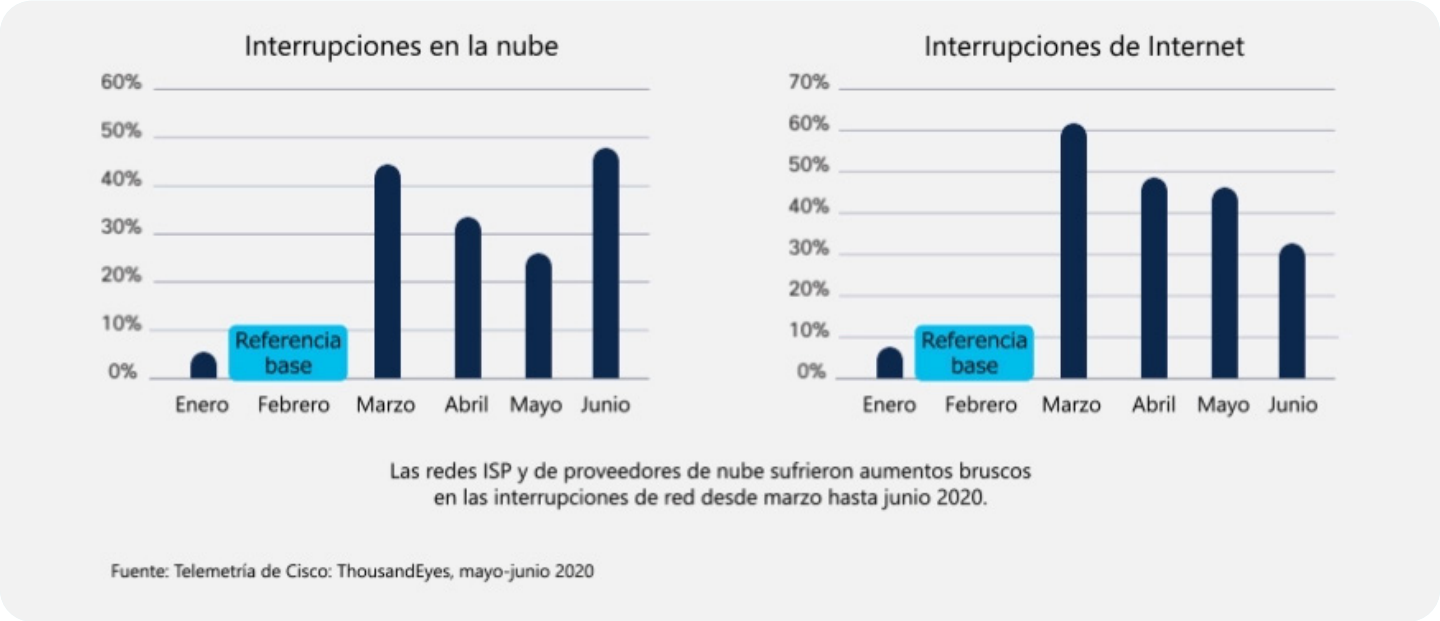
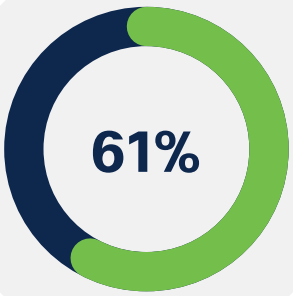


Figure 6. La interrupción del servicio de Internet y de la nube aumenta durante la pandemia

> “Cisco ThousandEyes identificó un 61 % de aumento en la cantidad de interrupciones de red en las redes ISP y un 44 % de aumento en las redes de proveedores de nube entre febrero y marzo de 2020. ”
>
> Cisco ThousandEyes, “Informe de rendimiento de Internet: Edición sobre el impacto del COVID-19”, 2020



Consideraciones de red: para comprender un tsunami de eventos, los equipos de NetOps deben adoptar análisis de red habilitadas para IA y sistemas de aseguramiento para lograr lo siguiente:

- **More accurate detection:** Improve the accuracy of automated issue and anomaly detection within and across network domains.
- **Faster remediation:** Correlate events to detect and clearly describe the most likely root cause of issues and anomalies.
- **Automated policy management:** Identify devices, applications, and trends and offer recommended policy updates.
- **Fewer degradations:** Identify patterns and trends and provide contextual insights that accelerate proactive, corrective, and preventive action.
- **Peer intelligence:** Provide intelligence and analytics that help network administrators compare their network performance to global, industry, or regional benchmarks.

Conozca cómo puede utilizar el conocimiento habilitado para IA para administrar mejor sus redes:

Conocimiento de red para el centro de datos

Resumiendo

Conclusión: mejorar la resiliencia empresarial con una plataforma de red avanzada

Los eventos desestabilizadores seguirán cambiándonos a nosotros y a nuestras redes durante nuestras carreras profesionales. Es momento de repensar cómo su **estrategia de red** permite una **estrategia de resiliencia** y priorizar las nuevas funcionalidades de red mas necesarias para mantenerse un paso adelante de lo que se viene.

La automatización y el conocimiento habilitado para IA ofrecido por las redes basadas en la intención brindan una potente plataforma para ayudarlo a adaptarse a cualquier circunstancia. Ofrecen la agilidad, seguridad, inteligencia y velocidad necesarias para admitir la resiliencia para:

- **Fuerza laboral:** potenciar a los trabajadores con un rendimiento seguro y de clase empresarial y acceder a sus aplicaciones mientras se trabaja desde el hogar, la oficina o cualquier otro lugar
- **Lugar de trabajo:** permitir que los empleados regresen de forma segura a la oficina con el monitoreo, las alertas y el conocimiento habilitados para Wi-Fi
- **Carga de trabajo:** facilitar modelos de resiliencia empresarial y proteger datos y aplicaciones dondequiera que se encuentren las cargas de trabajo en nubes públicas y centros de datos en las instalaciones
- **Operaciones:** automatizar las políticas integrales de red y la segmentación y simplificar las tareas administrativas a la vez que se mejora la visibilidad, se reducen las alertas y se permite una corrección más rápida

En esta nueva normalidad, se trata de tener una red que pueda adaptarse para admitir lo que venga. Al pensar acerca de su estrategia de resiliencia, tenga en cuenta cómo su red puede ser un facilitador clave de dicha estrategia.

Más información sobre la resiliencia empresarial

Aspectos adicionales que pueden interesarle

Resiliencia empresarial

Webinars

Cisco Digital Network Architecture (Cisco DNA)

C96-744645-00 01/21