NEWSLETTER

grupobeit.com

BLOG DEL CEO

La tecnología más valiosa es la que nunca se detiene

En la mayoría de las organizaciones, la infraestructura tecnológica solo ocupa un lugar en la agenda cuando ocurre una interrupción. Mientras las redes funcionan, los sistemas responden y las operaciones continúan sin contratiempos, la infraestructura permanece invisible...

EDICIÓN 64

Infraestructura invisible que sostiene la operación

Hay algo curioso en la infraestructura tecnológica: mientras todo funciona, casi nadie piensa en ella...

PARTNERS BEIT

ISACA MEXICO CITY

30 de Septiembre de 2026

Evento que busca fomentar el intercambio de conocimientos, discutir las últimas tendencias tecnológicas y actualizar a los profesionales...



EVENTOS BEIT

3ER FORO NACIONAL DE *CIBERSEGURIDAD*

5–9 de octubre de 2026
Universidad Anáhuac México
Campus Norte

TECNOEDIFICIOS

TECNOLOGÍA INTEGRAL PARA EDIFICIOS INTELIGENTES: ENERGÍA, CIBERSEGURIDAD Y CONECTIVIDAD

Ponencia: Elías Cedillo
14 Octubre, 2026
15:00 - 15:50
World Trade Center,
CDMX, México

Edición 64



La tecnología más valiosa es la que nunca se detiene

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

En la mayoría de las organizaciones, la infraestructura tecnológica solo ocupa un lugar en la agenda cuando ocurre una interrupción. Mientras las redes funcionan, los sistemas responden y las operaciones continúan sin contratiempos, la infraestructura permanece invisible. Sin embargo, esta percepción puede llevar a que uno de los activos más estratégicos del negocio sea gestionado de forma reactiva y no como un habilitador del crecimiento.

Para los equipos directivos, la conversación ya no debería centrarse únicamente en la disponibilidad de la tecnología, sino en su capacidad para acompañar la estrategia empresarial. La verdadera modernización no consiste exclusivamente en renovar equipos o adoptar las últimas tendencias tecnológicas. Implica comprender las dependencias críticas de la operación, identificar riesgos, simplificar arquitecturas y garantizar que la organización tenga la flexibilidad necesaria para responder a nuevos desafíos y oportunidades.

Con frecuencia, las limitaciones de infraestructura no se manifiestan como fallas evidentes. Aparecen en forma de lentitud operativa, retrasos en proyectos, dificultades para escalar operaciones o costos crecientes asociados a entornos complejos. Cuando esto ocurre, la tecnología deja de ser un habilitador y comienza a convertirse en una restricción para la innovación y la competitividad.

Además, infraestructura y ciberseguridad ya no pueden analizarse por separado. El crecimiento de usuarios, dispositivos, aplicaciones y servicios digitales exige entornos conectados, visibles y gobernables. Una arquitectura sólida no solo soporta la continuidad operativa, sino que permite adoptar iniciativas como inteligencia artificial, automatización, IoT y servicios en la nube con mayor velocidad y menor riesgo.

La pregunta clave para la alta dirección no es si la infraestructura está actualizada, sino si está preparada para respaldar la dirección que el negocio desea tomar. Evaluar resiliencia, capacidad de adaptación, redundancia y visibilidad tecnológica se ha convertido en una decisión estratégica tan relevante como cualquier inversión orientada al crecimiento.

En esta edición 64 de nuestro Newsletter te invito a explorar por qué la infraestructura debe dejar de verse como un componente técnico y comenzar a entenderse como una inversión en capacidad futura, resiliencia operativa y ventaja competitiva sostenible.

INFRAESTRUCTURA



Edición 64

NEWSLETTER BeIT

Infraestructura invisible que sostiene la operación

Hay algo curioso en la infraestructura tecnológica: mientras todo funciona, casi nadie piensa en ella.

Los usuarios abren una aplicación, consultan información, realizan una videollamada, acceden a un sistema corporativo o trabajan desde otra ubicación y, en la mayoría de los casos, la infraestructura simplemente está ahí. No se ve. No se comenta. No suele aparecer en una reunión de resultados.

Hasta que algo falla.

Entonces un enlace que se cae, un switch que deja de responder, una mala configuración, una saturación de red o un acceso no autorizado pueden convertirse rápidamente en un problema para toda la operación. Lo que parecía un asunto técnico termina afectando productividad, atención al cliente, procesos internos e incluso la continuidad de servicios críticos.

Por eso, hablar hoy de infraestructura de TI ya no significa hablar únicamente de servidores, racks o cableado. La infraestructura empresarial es un ecosistema en el que conviven hardware, software, almacenamiento, conectividad, sistemas de red, servicios en la nube y mecanismos de seguridad. Esa combinación es la que permite que las aplicaciones y los datos estén disponibles y que las personas, sistemas y dispositivos puedan comunicarse entre sí.

Y precisamente ahí es donde la red adquiere un papel que muchas veces se subestima. Una red empresarial no consiste simplemente en “tener Internet”. Detrás de una conexión aparentemente sencilla existe una arquitectura formada por switches, routers, puntos de acceso, direcciones IP, cableado, enlaces, políticas de acceso y diferentes mecanismos que determinan cómo viaja la información de un punto a otro. En una organización, esa infraestructura permite que usuarios, aplicaciones y dispositivos intercambien información y, por lo tanto, sostiene una parte importante de los procesos diarios.

Esto cambia la manera en que deberíamos pensar una red.

La pregunta no debería ser únicamente cuántos megas tenemos o qué modelo de switch está instalado. Una infraestructura realmente útil debe responder a preguntas mucho más incómodas: ¿qué pasa si falla un componente?, ¿cuánto tráfico podemos soportar?, ¿qué aplicaciones son críticas?, ¿qué dispositivos tienen acceso a la red?, ¿qué tan rápido podemos localizar una falla?, ¿qué ocurriría si mañana duplicamos el número de usuarios o incorporamos nuevos servicios?

Porque una red puede funcionar perfectamente hoy y, aun así, estar mal preparada para el crecimiento de la organización.

El problema suele aparecer cuando la infraestructura se construye pensando solamente en la necesidad inmediata. Se instala el cableado necesario, se colocan los equipos disponibles, se configura la conectividad y el proyecto se considera terminado. Con el tiempo llegan nuevas aplicaciones, más usuarios, cámaras, dispositivos móviles, sistemas IoT, servicios en la nube, herramientas de colaboración o cargas de trabajo que requieren mayor capacidad. La red comienza a soportar más de lo que originalmente se había previsto y aquello que parecía suficiente empieza a convertirse en una limitación.
Por eso el diseño de infraestructura tiene que mirar hacia adelante.

El cableado, por ejemplo, no debería considerarse simplemente como una serie de cables escondidos detrás de paredes, plafones o racks. Forma parte de la capacidad física de la red y condiciona la posibilidad de crecer, reorganizar espacios y soportar nuevas tecnologías. Lo mismo ocurre con los cuartos de comunicaciones, la distribución física, la alimentación eléctrica, la refrigeración y la organización de los equipos. La infraestructura física y la infraestructura lógica no son dos mundos independientes; trabajan juntas para que la conectividad pueda mantenerse disponible.

Y mientras la infraestructura crece, también lo hace algo que no puede ignorarse: la superficie de exposición.

Cada nuevo dispositivo conectado, cada acceso remoto, cada servicio en la nube y cada integración puede introducir nuevas posibilidades de comunicación y, al mismo tiempo, nuevos puntos que deben protegerse. La seguridad deja entonces de ser una capa que se coloca al final del proyecto. Tiene que formar parte del diseño desde el principio.

Aquí aparece una diferencia importante entre tener seguridad y gestionar la seguridad.

Una organización puede disponer de firewalls, controles de acceso, herramientas de monitoreo y diferentes soluciones de protección, pero eso no garantiza por sí mismo que exista una visión completa de lo que está ocurriendo. La gestión de seguridad requiere conocer el entorno, establecer políticas, supervisar los eventos, mantener los sistemas actualizados, identificar comportamientos anómalos y contar con mecanismos para responder cuando aparece un incidente.

Esto es especialmente importante porque las redes actuales son mucho más dinámicas que las de hace algunos años.

Ya no existe necesariamente un único lugar desde donde todos trabajan ni un único perímetro que pueda protegerse. Hay oficinas, trabajadores remotos, dispositivos móviles, servicios externos, aplicaciones SaaS, infraestructura en la nube y sistemas que necesitan comunicarse con otros entornos. La infraestructura puede estar distribuida físicamente y, aun así, tiene que comportarse como un entorno administrable y coherente.

La nube tampoco elimina la necesidad de infraestructura. La transforma.

Parte de los recursos pueden estar fuera de las instalaciones de la empresa, pero siguen existiendo necesidades de conectividad, disponibilidad, administración, control de acceso, almacenamiento, procesamiento y seguridad. Los modelos tradicionales, privados, públicos, híbridos e incluso arquitecturas más modernas conviven dependiendo de las necesidades de cada organización.

Por eso resulta poco útil hablar de “infraestructura moderna” únicamente en términos de tecnología nueva. Una infraestructura moderna no necesariamente es la que tiene más equipos o la que incorpora la última plataforma disponible. Es aquella que puede responder de manera razonable a las necesidades reales de la operación y que tiene capacidad para evolucionar.

Eso implica algo que en ocasiones se deja para después: conocer realmente lo que tenemos.

Parece básico, pero muchas organizaciones no cuentan con una visión completamente actualizada de sus activos, conexiones, configuraciones, dependencias y puntos críticos. Y cuando no se conoce la infraestructura, tampoco resulta sencillo protegerla, mantenerla o planificar su evolución.

La seguridad de red, en ese sentido, tampoco debería reducirse a bloquear amenazas. Implica proteger la disponibilidad, integridad y acceso a los recursos, utilizando controles como firewalls, segmentación, autenticación, monitoreo y actualización constante, entre otras medidas.

Al final, infraestructura y seguridad forman parte de la misma conversación.

Una infraestructura rápida, pero sin controles adecuados puede ampliar innecesariamente el riesgo. Una infraestructura muy protegida pero mal dimensionada puede convertirse en un obstáculo para la operación. Una red con buenos equipos, pero sin documentación ni monitoreo, puede ser difícil de mantener. Y una arquitectura diseñada únicamente para las necesidades actuales puede quedarse corta mucho antes de lo esperado.

La madurez está en integrar todas esas piezas.

Por eso, antes de preguntarnos qué tecnología deberíamos comprar, quizá conviene empezar con preguntas más sencillas: ¿sabemos qué tenemos?, ¿sabemos qué depende de ello?, ¿conocemos nuestros puntos críticos?, ¿podemos detectar una anomalía?, ¿tenemos capacidad para crecer?, ¿podemos recuperarnos de una falla?, ¿sabemos quién puede acceder a cada segmento?, ¿nuestra infraestructura está preparada para incorporar nuevas cargas de trabajo?

Las respuestas pueden revelar algo importante.

En muchas organizaciones, el siguiente gran paso tecnológico no comienza comprando tecnología.

Comienza entendiendo la infraestructura existente.

Porque detrás de cada aplicación, cada dato, cada usuario conectado y cada proceso digital existe una infraestructura que hace posible que todo funcione. Puede estar en un centro de datos, en una oficina, en la nube o distribuida entre diferentes entornos. Puede ser visible o estar completamente fuera de la vista del usuario.

Pero está ahí.

Y cuando la infraestructura está correctamente diseñada, documentada, administrada y protegida, ocurre algo que paradójicamente casi nadie nota: el negocio puede concentrarse en operar sin tener que pensar constantemente en la tecnología que lo sostiene.
Ese debería ser uno de los objetivos de una buena infraestructura.
No llamar la atención.
Sino estar preparada cuando realmente importa.

Fuentes consultadas

- **Red Hat**

"¿Qué es la infraestructura de TI?"
Red Hat — Infraestructura de TI

- **IBM**

"Infraestructura de red"
IBM Think — Infraestructura de red

- **Universitat Carlemany**

"Infraestructura de red"
Universitat Carlemany — Infraestructura de red

- **Fortinet**

"Network Security Management"
Fortinet — Network Security Management

- **Fortinet**

"What is Network Security?"
Fortinet — Network Security

3er Foro Nacional de Ciberseguridad

#AMCS2026

Colaboración multisectorial para un entorno digital seguro, resiliente y con derechos

5 – 9 de octubre de 2026

Universidad Anáhuac México
Campus Norte

REGISTRATE AHORA

5, 6 y 7 de octubre de 2026 (Virtual)
8 y 9 de octubre de 2026 (Presencial)

Grupo BeIT

TECNO EDIFICIOS

TecnoEdificios es el evento internacional que ofrece herramientas para una mejor operación y administración de todo tipo de edificaciones así como espacios de aproximación a las tecnologías que hacen posible mejorar la calidad de vida de los usuarios y la eficiencia de los edificios.

En un entorno donde los edificios modernos exigen infraestructura cada vez más inteligente y resiliente, esta ponencia presenta una visión integral de las tecnologías que hacen posible su operación segura y eficiente. Abordaremos soluciones de energía, incluyendo sistemas UPS, regulación de voltajes y enfriamiento, pilares para garantizar la continuidad operativa de cualquier edificación.



PONENCIA

Elías Cedillo
CEO y Fundador GrupoBeIT

TECNOLOGÍA INTEGRAL PARA EDIFICIOS INTELIGENTES: ENERGÍA, CIBERSEGURIDAD Y CONECTIVIDAD

14 Octubre, 2026 | 15:00 - 15:50 |
World Trade Center, CDMX, México

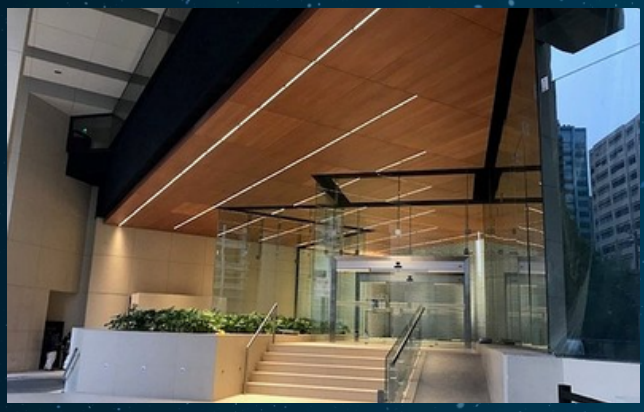
Exploraremos también el papel del SOC (Security Operations Center) en el monitoreo continuo de ciberseguridad y del NOC (Network Operations Center) enfocado en la vigilancia de infraestructura desde la perspectiva de Tecnología Operativa (OT), dos capas esenciales para proteger los activos digitales y físicos de un edificio inteligente.

Finalmente, presentaremos Field Services 2.0, con énfasis en cableado estructurado y sistemas de CCTV con elementos de IA para la prevención de riesgos, como base de la "domótica" que hoy demandan los edificios actuales.

Grupo BeIT | BURÖMC SEGURIDAD INFORMÁTICA | ELIT INFRASTRUCTURE SERVICES | CATO NETWORKS

ISACA Mexico City Chapter +50 Aniversario

Como parte de nuestra alianza con nuestros partners **CATO Networks y Abnormal** aparticiparemos en el evento **ISACA MEXICO CITY CHAPTER**, que busca fomentar el intercambio de conocimientos, discutir las últimas tendencias tecnológicas y actualizar a los profesionales.



CONFERENCISTAS CONFIRMADOS:

- Erik Prusch, CEO de ISACA
- El Senador y Presidente de la Comisión de IA en el Senado quien está coordinando los trabajos para proponer una ley nacional de IA
- PhD Jack Freund referente internacional en la cuantificación de ciber riesgos y coautor del libro "Measuring and Managing Information Risk: A FAIR Approach"
- Heidy Rocha y Mario Cortés de la Agencia de Transformación Digital
- Gabriela Hernández, miembro del Board de ISACA Internacional
- Juan Manuel Portal, ex Auditor Superior de la Federación
- Diana Maldonado, Auditora de Controles de TI, OCD Tech
- Alejandro De Los Santos, Director de Ciberseguridad BANXICO

PANEL ACADÉMICO:

- Dra. Mariko Nakano Miyatake, Profesora e investigadora titular en la Sección de Estudios de Posgrado e Investigación (SEPI) de la ESIME Culhuacán del Instituto Politécnico Nacional (IPN)
- Dra. Rocío Aldeco Pérez, Profesor Asociado y Jefe del Departamento de Ingeniería en Computación de la Universidad Nacional Autónoma de México (UNAM)
- Dra. María Marván, académica investigadora y exconsejera electoral