BICSICALA 360

Una visión completa al mundo de las TIC en Latinoamérica

Nº7 | Julio / Septiembre 2026



LA INFRAESTRUCTURA QUE NUNCA FALLA NO EXISTE

DISEÑAR PARA RESISTIR, DETECTAR Y RECUPERAR

BICSI CALA

SISTEMA DE ENERGÍA CON ADMINISTRACION DE FALLA

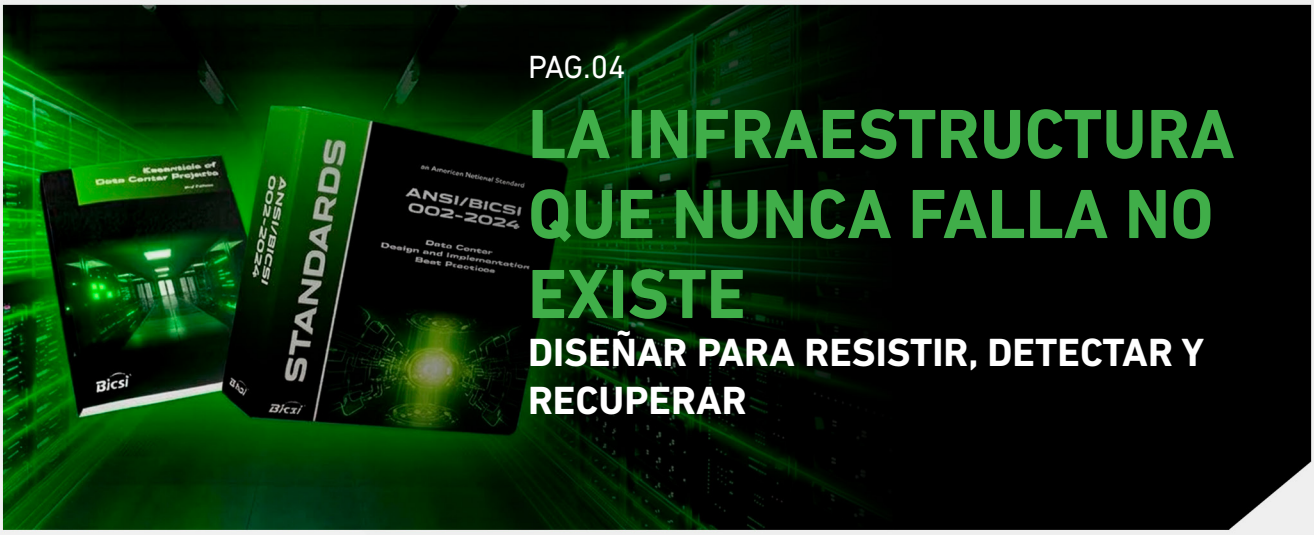
MÁS ALLÁ DEL WI-FI: LA BRECHA DE PREPARACIÓN INALÁMBRICA EN LOS EDIFICIOS MODERNOS

DETECCIÓN POR FIBRA ÓPTICA PARA LA PROTECCIÓN DE INFRAESTRUCTURA DE TERCEROS EN DATA CENTERS

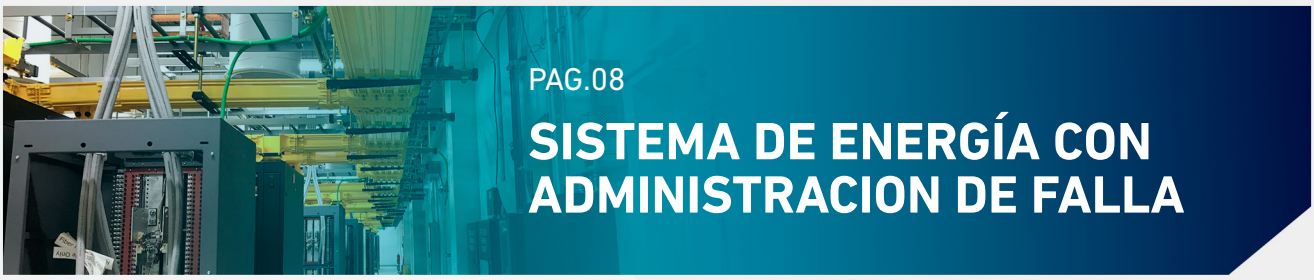
WWW.BICSI-CALA.ORG

CONTENIDO

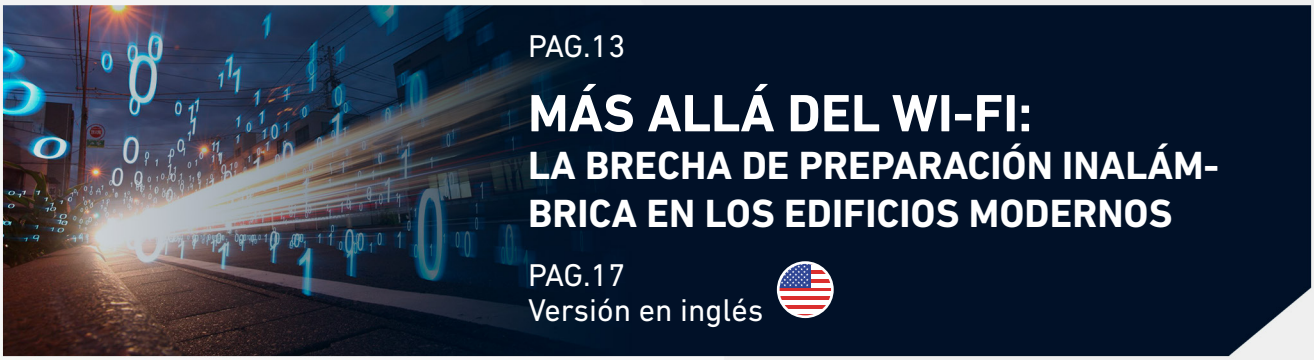
PAG.03
EDITORIAL



PAG.04
LA INFRAESTRUCTURA QUE NUNCA FALLA NO EXISTE
DISEÑAR PARA RESISTIR, DETECTAR Y RECUPERAR

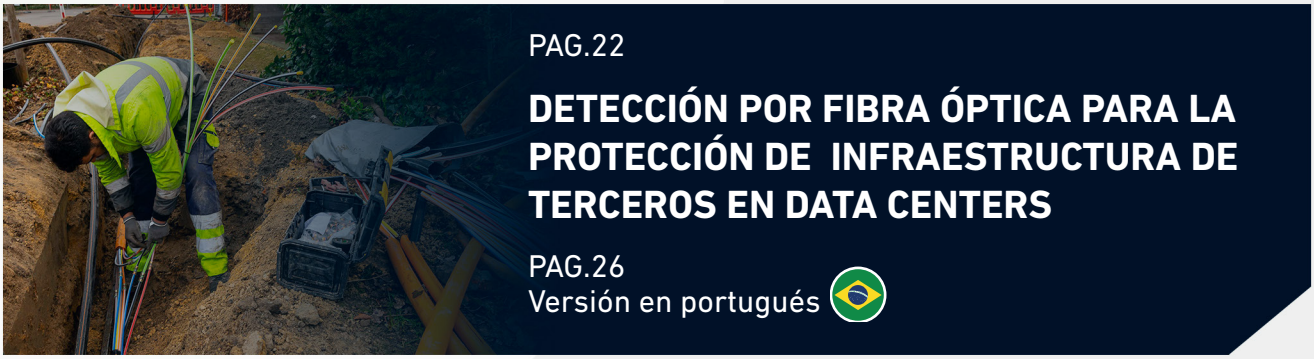


PAG.08
SISTEMA DE ENERGÍA CON ADMINISTRACION DE FALLA



PAG.13
MÁS ALLÁ DEL WI-FI:
LA BRECHA DE PREPARACIÓN INALÁMBRICA EN LOS EDIFICIOS MODERNOS

PAG.17
Versión en inglés



PAG.22
DETECCIÓN POR FIBRA ÓPTICA PARA LA PROTECCIÓN DE INFRAESTRUCTURA DE TERCEROS EN DATA CENTERS

PAG.26
Versión en portugués

BICSICALA360

Para información contáctenos:
Teléfono: +507 3108364
E-mail: info@ctp.la
Web: www.ctp.la

Equipo de Edición:
Beatriz Bezos, RCDD, DCDC, ESS, NTS, OSP, PE, PMP
Miguelangel Ochoa, RCDD

Equipo Creativo:
Leilanit Nava
Francisco Nava

Publica:
CTP
CALA Telecom Partners

RUC: 155745649-2-2023 DV 38
Costa del Este, Ave. Centenario, PH Dream Plaza, Piso 10, Ciudad de Panamá, Panamá, ZIP 07173
Teléfono: +5073108364
E-mail: info@ctp.la

CALA Telecom Partners es especialista en servicios consultoría en Tecnologías de Información y Comunicaciones (TICs) y procesos de outsourcing de marketing (MPO) con presencia en toda Latinoamérica.

© 2026 CALA Telecom Partners

Érase una vez hace aproximadamente 20 años cuando escuchaba de parte de algunas personas relacionadas a la tecnología de la información decir que el cableado estructurado estaba próximo a desaparecer para ser reemplazado por las redes inalámbricas, nada más lejos de la realidad entonces y ahora, ambas tecnologías han evolucionado de la mano para crear redes más robustas y confiables.

Nuevamente escucho del público en general como sacado de las películas de ciencia ficción, que la humanidad está próxima a dejar de existir tal como la conocemos hoy día, para ser desplazada por la IA, y desde mi punto de vista igual que ocurrió con las redes de cableado y las inalámbricas vamos a evolucionar juntos para ser más fuertes y agiles en el desarrollo de tecnologías y trasmisión del conocimiento.

Pensemos ahora en que democratizar el conocimiento es posible apoyados por la IA como una herramienta de capacitación, así como por eventos como el BICSI ICT Summit, El Cable Skills Challenge y las ediciones de la revista BICSI CALA 360, pero hay un reto que sigue siendo el mismo de hace 20 años que desde mi experiencia es y será siempre lograr un hilo conductor que permita mantener aterrizado y humanizado ese conocimiento, de manera que sea fácilmente asimilado por el recurso humano encargado de instalar y poner en marcha las tecnologías presentes y futuras, desde el instalador de cables de red, hasta el diseñador de centros de datos, los cuales están obligados de forma indiscutible a caminar juntos en búsqueda del anhelado entorno tecnológico libre de fallas.

Durante 30 años hemos diseñado con una restricción de 100 metros y mínimo 1 cuarto de telecomunicación por cada piso, pero ¿qué pasa cuando se elimina le restricción de los 100 metros?, cambiamos la arquitectura.

El NEC 2023, Artículo 726, introduce la energía Clase 4, Fault-Managed Power: hasta 450VDC que se interrumpe en microsegundos ante contacto humano, segura al tacto y listada UL 1400-1. Por primera vez podemos alimentar dispositivos a 2 km con una sola batería central, sin canalización metálica ni electricista licenciado.

Esa misma convergencia aplica al perímetro: una sola fibra monomodo G.652D con un interrogador DAS se convierte en kilómetros de sensores acústicos continuos que, junto a otras tecnologías, nos permiten alcanzar instalaciones con entornos más seguros para las personas y para los datos que se administran y resguardan en ellas. En esta edición de la revista BICSI CALA 360 también veremos que el reto no es la tecnología, es el diseño, analizaremos por qué razón la redundancia no es resiliencia, que la documentación también es infraestructura y por qué en un entorno inalámbrico la cobertura no lo es todo.

Bienvenidos



Fidel Vega
RCDD
BICSI CALA Leadership Committee - Panama Chair
+507 67479273 / fvega@sistemasespeciales.net

BICSI CALA 360 es una publicación trimestral de CALA Telecom Partners S.A. y se envía en formato electrónico a los miembros, titulares de credenciales de BICSI y profesionales de la región CALA. Invitamos a sus lectores a enviar propuestas y sugerencias. Nuestros artículos son carácter técnico con enfoque agnóstico y se aceptan gustosamente propuestas para su publicación con la aprobación del Equipo de Edición. CALA Telecom Partners se reservará el derecho de editar y alterar dicho material por razones de espacio u otras consideraciones, así como de publicarlo o utilizarlo de cualquier otro modo.

Los artículos, opiniones e ideas expresadas aquí son responsabilidad exclusiva de los autores contribuyentes y no reflejan necesariamente la opinión de BICSI CALA y de CALA Telecom Partners, sus miembros o su personal.

BICSI CALA y de CALA Telecom Partners no se responsabilizan en modo alguno de las opiniones e ideas expresadas en los artículos. Se insta a los lectores a que actúen con cautela profesional a la hora de llevar a cabo cualquiera de las recomendaciones o sugerencias realizadas por los autores. Ninguna parte de esta publicación puede ser reproducida en ninguna forma ni por ningún medio, electrónico o mecánico, sin el permiso de CALA Telecom Partners. Si desea hacer alguna pauta publicitaria, póngase en contacto con CALA Telecom Partners. S.A., escribiendo a info@ctp.la. La publicación de publicidad no debe considerarse como una aprobación por parte de BICSI CALA ni de CALA Telecom Partners. S.A. quien se reserva el derecho, a su sola y absoluta discreción, de rechazar cualquier anuncio en cualquier momento por cualquier parte.

Copyright © 2025, CALA TELECOM PARTNERS, S.A. Todos los derechos reservados.

LA INFRAESTRUCTURA QUE NUNCA FALLA NO EXISTE

DISEÑAR PARA RESISTIR, DETECTAR Y RECUPERAR



Guillermo Inchausti

VPA de Arquitectura
Banco General Panamá

ginchausti@bgeneral.com

Por qué los estándares, un buen diseño, materiales certificados, documentación actualizada y capacidad de recuperación forman parte de una misma estrategia de resiliencia.

Durante muchos años, quienes trabajamos en tecnología hemos dedicado gran parte de nuestro esfuerzo a evitar que las cosas fallen. Duplicamos servidores, enlaces, fuentes de poder y componentes de red. Construimos clusters, instalamos UPS y generadores, distribuimos cargas entre centros de datos y contratamos servicios de distintos proveedores.

Todo esto sigue siendo necesario. Pero la experiencia operativa nos enseña una realidad: la infraestructura que nunca falla no existe. Los equipos fallan. Los cables se dañan. Las configuraciones cambian. Los proveedores tienen incidentes. Las comunicaciones se interrumpen y las personas cometen errores.

¿CÓMO EVITAMOS QUE NUESTRA INFRAESTRUCTURA FALLE?

TAMBIÉN DEBEMOS PREGUNTAR: **¿QUÉ TAN PREPARADOS ESTAMOS PARA DETECTAR, CONTENER Y RECUPERAR EL SERVICIO CUANDO FALLE?**

LA RESILIENCIA COMIENZA EN EL DISEÑO

Es fácil asociar resiliencia con recuperación ante desastres, pero comienza mucho antes: desde el diseño de la infraestructura.

Estándares como ANSI/BICSI 002 para centros de datos, la familia ANSI/TIA-568 para cableado de telecomunicaciones y la serie ISO/IEC 11801 para cableado genérico ofrecen marcos para construir infraestructuras consistentes, interoperables y capaces de soportar los servicios para los cuales fueron diseñadas.

ISO/IEC 11801, por ejemplo, define requisitos para sistemas de cableado multivendor que pueden soportar servicios de voz, datos y video, incluyendo aplicaciones que suministran energía a través del cableado. Seguir estándares no elimina las fallas. Lo que hace es reducir variaciones innecesarias, establecer criterios técnicos comunes y permitir que diseño, instalación, pruebas, operación y mantenimiento trabajen sobre reglas conocidas. Esto tiene un efecto directo sobre la resiliencia.

Una infraestructura bien diseñada es más sencilla de probar, mantener, modificar y reparar.

LA CALIDAD DE LOS COMPONENTES TAMBIÉN IMPORTA

Un buen diseño puede perder gran parte de su valor cuando se implementa con componentes cuya calidad o desempeño no ha sido comprobado.

Cableado, conectores, patch panels, fibra y otros elementos pasivos pueden permanecer instalados durante muchos años y soportar varias generaciones de equipos activos. Por eso, utilizar productos certificados o verificados contra estándares reconocidos no debería verse únicamente como un requisito del proyecto. Es una forma de reducir riesgo.



Programas independientes de certificación y verificación permiten comprobar que determinados productos cumplen requisitos definidos de seguridad o desempeño. UL, por ejemplo, dispone de programas de verificación de desempeño para cables y sistemas de cableado basados en estándares reconocidos de la industria. La diferencia puede parecer poco importante cuando todo funciona. Durante una falla, deja de serlo.

REDUNDANCIA NO ES RESILIENCIA

También debemos evitar confundir redundancia con resiliencia. Podemos tener dos enlaces de comunicaciones y descubrir que ambos utilizan la misma ruta física. Podemos tener dos centros de datos que dependen del mismo proveedor. Podemos tener equipos redundantes conectados a infraestructura física que comparte un punto único de falla.

> **La redundancia es una característica del diseño. La resiliencia es la capacidad de continuar operando o recuperar el servicio dentro de límites aceptables.**

Por eso, un diseño resiliente debe analizar rutas físicas, energía, telecomunicaciones, cableado, equipos, servicios externos y dependencias compartidas. No basta con dibujar dos líneas en un diagrama lógico. Hay que saber por dónde pasan realmente.

LA DOCUMENTACIÓN TAMBIÉN ES INFRAESTRUCTURA

Hay otro componente que con frecuencia recibe menos atención: la documentación. Un centro de datos puede estar construido con excelentes materiales y bajo buenos estándares, pero durante un incidente alguien tendrá que identificar rápidamente qué puerto, cable, panel, circuito, enlace o equipo está relacionado con el problema.

En ese momento, una documentación incompleta puede transformar una falla sencilla en una interrupción prolongada. Los estándares de administración de infraestructura de telecomunicaciones, como ANSI/TIA-606, establecen prácticas consistentes de identificación y administración. Etiquetado consistente, diagramas actualizados, identificación de rutas, registros de conexiones y documentación de cambios no son tareas administrativas menores. Son herramientas operativas.

> **La documentación reduce el tiempo entre encontrar el problema y poder actuar sobre él.**

CERTIFICAR LA INSTALACIÓN, NO SOLAMENTE COMPRAR BUENOS MATERIALES

Utilizar materiales certificados tampoco garantiza por sí solo una buena infraestructura. La instalación completa debe ser probada. Un cable de excelente calidad puede terminar mal instalado, exceder radios de curvatura, sufrir daños durante la instalación o presentar problemas en sus terminaciones. Por eso, las pruebas y la certificación del cableado instalado son parte esencial del proceso. El objetivo debe ser poder demostrar que la infraestructura instalada cumple el desempeño para el cual fue diseñada.

DISEÑAR PARA RECUPERAR

Finalmente, debemos asumir que incluso una infraestructura correctamente diseñada, instalada, certificada y documentada puede fallar. Aquí comienza la segunda parte de la resiliencia: detectar y recuperar. Monitoreo y observabilidad deben permitir identificar rápidamente una falla y relacionarla con los servicios afectados. Los procedimientos deben indicar qué hacer. La documentación debe permitir encontrar dónde hacerlo. Y las pruebas deben confirmar que las personas responsables realmente pueden hacerlo dentro de los tiempos requeridos.

La recuperación, entonces, no comienza cuando ocurre el incidente. Comienza cuando seleccionamos el estándar, diseñamos la infraestructura, escogemos los materiales, certificamos la instalación, documentamos lo construido y mantenemos esa información actualizada.

Después de muchos años trabajando con tecnología, cada vez estoy más convencido de que la verdadera medida de una infraestructura no es solamente cuánto tiempo funciona sin fallar. También es qué tan rápido podemos entender qué falló y qué tan preparados estamos para recuperar el servicio.

Si este componente falla mañana, ¿sabemos qué servicio afecta, dónde está, cómo está conectado y qué debemos hacer para recuperarlo?

Sobre el Autor:

Guillermo es un ejecutivo de tecnología con amplia experiencia en operaciones, transformación digital, arquitectura empresarial, resiliencia operativa y gestión de riesgos tecnológicos en varias industrias. A lo largo de su carrera ha liderado equipos y proyectos complejos, combinando estrategia, tecnología y continuidad de negocio.



Imagen: De la infraestructura diseñada a la resiliencia del servicio.
Autor: Guillermo Inchausti

SISTEMAS DE ENERGÍA CON ADMINISTRACIÓN DE FALLA (FMPS)



Ing. Pedro Conejo Castillo

Fundador
Tek Nova Conexion

eknovaconexion@gmail.com

Cada vez son más los dispositivos que requieren energía para suplir soluciones a la sociedad, en automatización de servicios e información en tiempo real, convirtiendo un entorno más integrado e inteligente, logrando bajar costos, mejorar la seguridad humana y de los sistemas. Si recordamos hace unos 10 años cuáles eran los dispositivos típicos en nuestro hogar o oficinas, y los compararlos al día de hoy, es increíble la cantidad de incremento, solo mencionando los dispositivos inalámbricos que tenemos hoy día, como iluminación, cámaras de seguridad, redes inalámbricas, sistemas de control de acceso, tabletas para tener en campo lectura de planos, como también ingresar información de procesos, entre otros.

Utilizando el desarrollo en componentes electrónicos y normas como medio para lograr objetivos claves como la seguridad y la eficiencia. quiero referirme al concepto de "Sistemas de energía con Administración de falla", con siglas en inglés (FMPS Fault managed Power systems), este nombre es dado por la clasificación de equipo según el NEC a partir del 2023, y comercialmente el nombre varía, de acuerdo al fabricante, podemos encontrar en el mercado, estos nombres: Electricidad digital, Corriente digital o Corriente de pulso.

> **La seguridad siempre es un factor importante el cual debe tener un alto estándar para proteger la vida humana.**

Precisamente esta tecnología se desarrolla teniendo nuevos beneficios. permitiendo en forma activa igual que se administra un equipo de red o servidor, podemos monitorear constante-mente la línea de energía eléctrica y en caso de falla o corto circuito se interrumpe el suministro eléctrico en la línea en milisegundos, similar a un enlace de datos, cuando es monitoreado y tenemos con base en gráficas de funcionamiento, de esta forma se

cumplen normas y pruebas que garantizan este objetivo. (NEC 2023, art 726).
El voltaje utilizado está en los 450 Vdc, Clase 4 NEC, Estamos de acuerdo en que el voltaje de 450 Vdc es considerado peligroso, sin embargo, los sistemas FMPS se consideran mucho más seguros que los sistemas tradicionales. y son probados UL-1400-1.

En el caso de Costa Rica según el decreto MEIC se tiene aprobado el NEC 2020 versión en español. Como ingeniero colegiado es mi criterio que podemos realizar diseños utilizando estos equipos para Costa Rica, porque el decreto MEIC 36979, en el artículo 90.1, hace referencia a la seguridad humana y a los activos, y los sistemas FMPS mejoran estas dos características. Además, en el artículo 90.D se habla de otros estándares, por lo que se puede también pensar que el NEC 2023 en adelante, es una actualización a la actual, y podemos concluir que estos sistemas son tecnologías recientes y en su momento se va a actualizar la versión del NEC para Costa Rica. Hoy debemos avanzar utilizando lo mejor de esta tecnología y aplicarlo al diseño; en seguridad, eficiencia y bienestar.

Con respecto a la eficiencia los sistemas FMPS, están diseñados para alimentar cargas desde los 2 metros hasta los 2000 metros de distancia con un voltaje de hasta los 450 VDC.

Entre los beneficios que se tienen, está que se utilizan conductores más delgados permitiendo alimentar a cargas con una longitud de hasta de 2000 metros.

Estas cargas pueden variar entre los 600 y 3000 W por canal, dependiendo del fabricante y del diseño de la solución. Esto nos lleva a concluir que es menor el costo de materiales, mano de obra, y tiempo del proyecto. alcanzado el segundo objetivo.

Hasta este momento en forma breve he descrito el funcionamiento, norma de cumplimiento y beneficios. Ahora voy a exponer algunos casos de uso para poder entender más los sistemas FMPS. pero antes vamos a ver cómo se conectan estos sistemas en un diagrama general. Tenemos que conocer que los sistemas FMPS se basan en un equipo llamado transmisor y otra contraparte llamada receptor, los cuales están cableados. El transmisor está en el respaldo central, y los receptores en áreas distantes. las cuales varían según el fabricante.

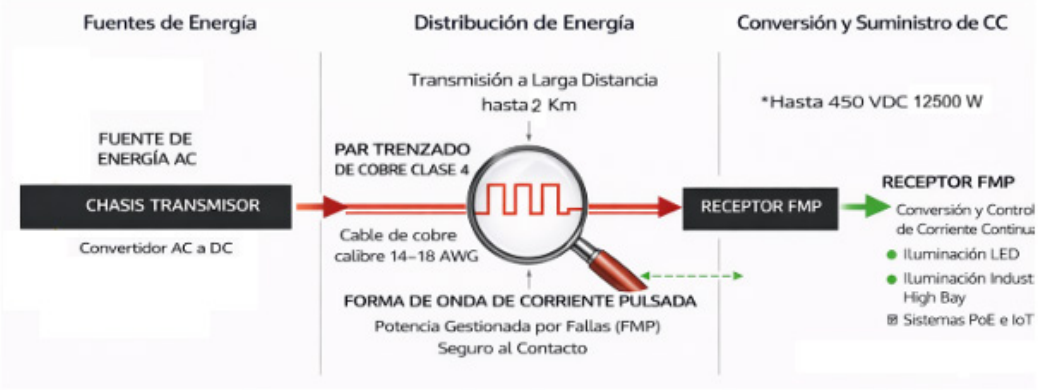


Imagen: Diagrama General de Conexión.
Autor: Pedro M. Conejo Castillo

USOS DE LOS SISTEMAS FMPS:



TELECOMUNICACIONES:
Su uso lo podemos tener desde redes de datos, alimentando equipos como router, switches, ap; en caso de un edificio, podemos tener los transmisores en un único piso con un respaldo central y los receptores en cada piso. También en torres de comunicaciones ISP en sistemas celulares LTE, 5G



CENTROS DE DATOS:
Podemos alimentar desde servidores hasta equipos de comunicaciones.



EDIFICACIONES:
Se pueden usar en iluminación. En hoteles hay grandes beneficios en ahorro energético, ya que se pueden automatizar, elementos como persianas motorizadas: con sensores de presencia podemos apagar luces y controlar el aire acondicionado.



RESIDENCIAS:
En lo personal en los últimos años he comprado luminaria tipo led para disminuir consumo eléctrico, pero en corto tiempo fallan mucho las diminutas fuentes de energía; es mejor tener una sola fuente DC Clase 2 para la iluminación. En edificios inteligentes y centros corporativos de negocios las oportunidades son extraordinarias, para utilizar en comunicaciones, iluminación, y se convierte en un nuevo componente para el concepto de edificios inteligentes.



ESTADIOS:
Se aprovecha para alimentar diversos dispositivos, en forma más segura y económica ya que los conductores tienen un calibre menor para transportar la energía a las largas distancias de este tipo de edificación.



CENTROS EDUCATIVOS:
En centros escolares, campus universitarios, son utilizados en las redes de comunicación, seguridad perimetral en grandes extensiones de área.



ÁREAS INDUSTRIALES:
Es más seguro tener un respaldo de energía central que tener UPS distribuidas, disminuyendo el mantenimiento y aumentando la disponibilidad del proceso. principalmente cuando se tienen zonas clasificadas, por gases, hidrocarburos. como así también en centros hospitalarios.

MEJORAR LA EFICIENCIA EN DISTRIBUCIÓN:
Permite la Transmisión de energía DC de forma segura, cables más pequeños en algunos diseños, mejor integración con energías renovables. Ideal para microredes y energías renovables. Los FMPS combinan muy bien con paneles solares, Bancos de baterías, Sistemas híbridos; Especialmente en arquitecturas tipo microgrid donde se necesita control avanzado.

INFRAESTRUCTURA DIGITALIZADA:
El futuro de la energía es Inteligente, monitoreado, Gestionado remotamente; FMPS encaja perfectamente en edificios inteligentes y sistemas IoT energéticos.

De acuerdo a lo expuesto anteriormente, considero que a futuro los sistemas de energía con administración de falla FMPS serán usados ampliamente para tener mayor seguridad y reducir significativamente el riesgo de incendios eléctricos, choques eléctricos, arcos eléctricos. Es probable que en los próximos 10–20 años se vuelva estándar en edificios comerciales nuevos, sea obligatorio en ciertas aplicaciones críticas, se combine con sistemas DC de baja tensión inteligente y forme parte de redes eléctricas descentralizadas.

FMPS no reemplazará totalmente los sistemas tradicionales de inmediato, pero sí será un complemento clave en infraestructura moderna, especialmente donde la seguridad y continuidad del servicio son críticas.

Si estás trabajando en proyectos eléctricos o de infraestructura energética, es una tecnología que vale la pena considerar estratégicamente.

Como podemos ver, es necesario irnos preparando para introducir a los nuevos diseños esta solución. Será un placer poderle asesorar según sea su caso.



Sobre el Autor:

Pedro es ingeniero en electrónica, fundador y gerente de TEK NOVA CONEXIÓN, con amplia experiencia en obra pública, telecomunicaciones, energía y ciberseguridad NIST 800. Miembro del CIEMI y CFIA, lidera proyectos complejos de medición bajo normas API, integrando estrategia, alcance tecnológico y BIM.

PANDUIT™

MAKE IT HAPPEN

ES2P™ PDU

Diseñado para la nueva era de la infraestructura digital.

Simplifica la administración energética de tus entornos tecnológicos con una plataforma creada para escalar, adaptarse y mantenerse siempre disponible.

La energía detrás de las infraestructuras que evolucionan.

Escala sin complejidad

Encadena hasta **16 PDUs** y simplifica la administración conforme tu infraestructura crece.

Continuidad inteligente

El controlador reemplazable en operación permite el mantenimiento sin interrupciones.

Seguridad diseñada desde el núcleo

Protocolos avanzados y validaciones especializadas para entornos empresariales modernos.

Rendimiento preparado para ambientes exigentes

Confiabilidad térmica diseñada para operar hasta **55°C.**

Flexibilidad arquitectónica

Configuraciones 0U y 1U para integrarse naturalmente a diferentes diseños de rack.



MÁS ALLÁ DEL WI-FI: LA BRECHA DE PREPARACIÓN INALÁMBRICA EN LOS EDIFICIOS MODERNOS

LOS EDIFICIOS MODERNOS PUEDEN TENER UN EXCELENTE WI-FI Y AUN ASÍ NO PROPORCIONAR LA CONECTIVIDAD AL CELULAR, LA MOVILIDAD, LA RESILIENCIA Y LAS COMUNICACIONES OPERATIVAS QUE SUS OCUPANTES Y SISTEMAS NECESITAN.



Paul Weintraub
RCDD, RTPM, ESS, TECH

Director General
Excigent

paul@excigent.com



Orlando Calderon

Ingeniero de ventas para el Caribe, América Latina y Canada
Nextivity

ocalderon@nextivityinc.com

LA BRECHA DE PREPARACIÓN INALÁMBRICA

"El edificio tiene Wi-Fi. Entonces, ¿por qué las personas siguen perdiendo señal?"

Es una pregunta sencilla, pero expone un tema cada vez más importante en el diseño de edificios. La conectividad inalámbrica suele considerarse sinónimo de Wi-Fi. Sin embargo, los usuarios no piensan en términos de capas de red. Solo esperan conexión en sus teléfonos, autenticación fluida en las aplicaciones, recepción oportuna de mensajes y disponibilidad de los servicios móviles mientras se desplazan por el edificio.

Un problema de este tipo suele comenzar con el propio edificio. Los materiales que mejoran la eficiencia energética, el desempeño estructural y la seguridad también pueden dificultar la propagación de la radiación de radiofrecuencia. Ejemplos de esto son el vidrio de baja emisividad, el concreto y el acero. Los interiores densos y espacios de bajo nivel, también pueden debilitar las señales provenientes del exterior. De igual manera los ascensores, las escaleras, los estacionamientos, los cuartos mecánicos y las áreas interiores profundas son zonas problemáticas frecuentes.

Esto crea una brecha en la preparación inalámbrica: el edificio parece estar conectado porque dispone de Wi-Fi, mientras se desatienden tanto un servicio celular confiable como otras necesidades de comunicación.

WI-FI Y CELULAR CUMPLEN FUNCIONES DIFERENTES

La red Wi-Fi es esencial pues soporta el acceso a la LAN empresarial, la conectividad para visitantes, la colaboración, los dispositivos

administrados y muchas aplicaciones locales e IoT. Pero es solamente una capa.
Por su parte, la red celular pública proporciona voz, mensajería y datos móviles sin requerir que el usuario se conecte a la red Wi-Fi del edificio. Esto importa para visitantes, clientes, contratistas y empleados con dispositivos personales, así como para aplicaciones móviles, autenticación multifactor, servicios en la nube y otros procesos que dependen de la conectividad del operador.

Así, la cobertura celular interior también permite la movilidad en oficinas, corredores, ascensores, estacionamientos y otros espacios donde la señal exterior puede no penetrar de forma consistente.

Del mismo modo, los servicios LTE o 5G privados pueden soportar aplicaciones operativas o de campus, mientras que la IoT se enfoca en sensores, automatización y monitoreo. Estas tecnologías son complementarias.

> **Entonces, la pregunta inicial no sería "¿Qué tecnología inalámbrica debemos instalar?", sino "¿Qué necesita soportar el edificio?"**

EL WI-FI PÚBLICO NO ES LO MISMO QUE UNA CONEXIÓN CONFIABLE

La cobertura celular importa por otra razón: los usuarios no deberían asumir que una red Wi-Fi pública es confiable simplemente porque su nombre parece conocido o porque la ofrece un hotel, un aeropuerto, un centro de convenciones, un restaurante u otro lugar público.

Cuando la cobertura celular es deficiente, las personas pueden conectarse a redes Wi-Fi desconocidas, usar puntos de acceso públicos o aceptar cualquier conexión disponible. Esto puede aumentar la exposición a riesgos de ciberseguridad.

Recientemente, una campaña de phishing mediante Wi-Fi en hoteles*, reportada en agosto de 2026, mostró cómo los gateways comprometidos y las configuraciones DNS manipuladas redirigían a los viajeros a páginas fraudulentas de Microsoft 365. Para el usuario, la conexión parecía normal mientras trataba de obtener credenciales o tokens de autenticación.

Por lo tanto, el punto central es más estratégico: la conectividad y la ciberseguridad no pueden abordarse como temas separados.

De hecho, una red celular pública o privada bien diseñada puede proporcionar una ruta de acceso administrada por separado sin depender del Wi-Fi local. La red celular no está exenta de riesgos, pero una buena cobertura interior ofrece una alternativa cuando el Wi-Fi no está disponible, presenta problemas o no es confiable.

Así, en un entorno cambiante, mantener más de una ruta de comunicación viable mejora la resiliencia.

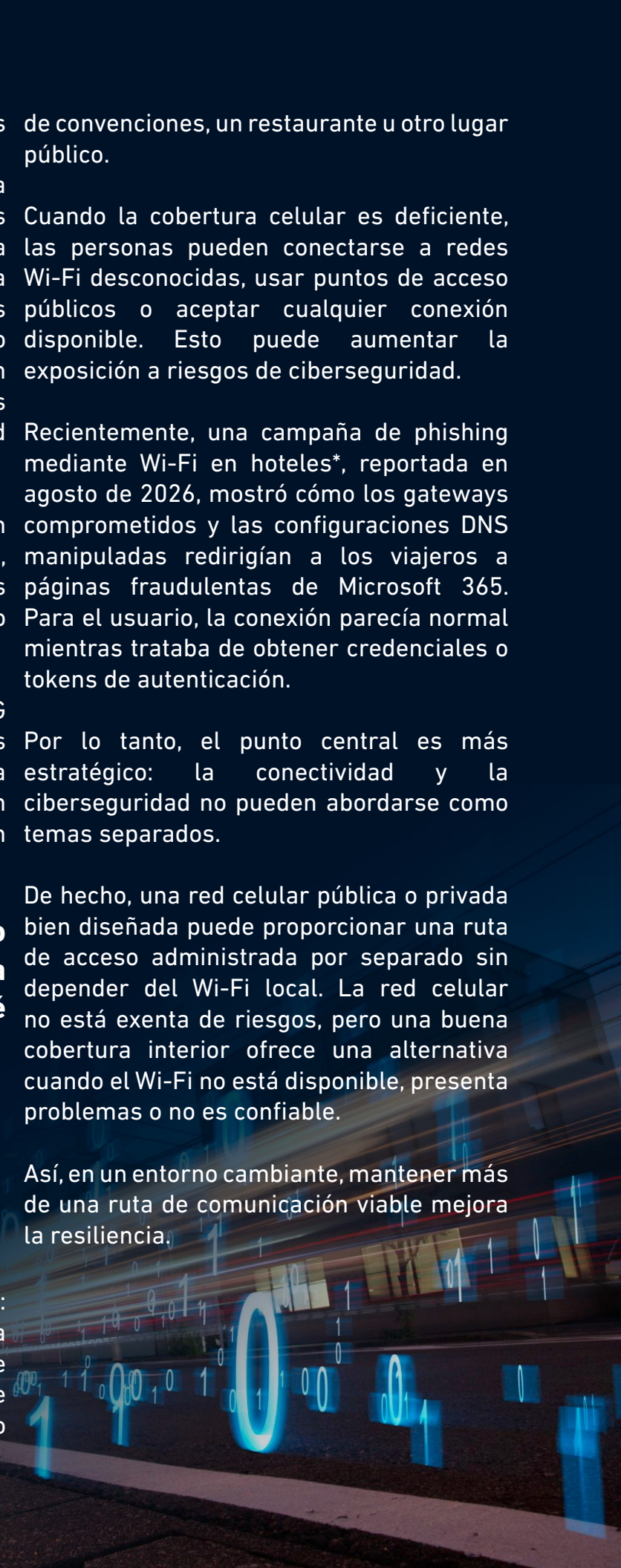




Imagen: El ecosistema inalámbrico en interiores. Una estrategia completa puede combinar múltiples capas inalámbricas alineadas con distintos casos de uso.
Fuente: Paul Weintraub *RCDD, RTPM, ESS, TECH* / Orlando Calderon

LA SEGURIDAD PÚBLICA ES UN REQUISITO INDEPENDIENTE

Por otro lado, las comunicaciones para respondedores de emergencia deben evaluarse por separado de la cobertura celular comercial y del Wi-Fi empresarial. Los requisitos pueden varían según el país y la jurisdicción, y las áreas difíciles pueden requerir atención especial. Una buena cobertura Wi-Fi o de celular comercial no debe considerarse suficiente para las comunicaciones de emergencia.

LA COBERTURA ES SOLAMENTE EL COMIENZO

La intensidad de la señal no determina por sí sola el desempeño inalámbrico. Un marco más útil considera cuatro factores:

1. **COBERTURA:** ¿Pueden los usuarios conectarse donde lo necesitan?
2. **CAPACIDAD:** ¿Puede el sistema soportar la cantidad prevista de usuarios y dispositivos?
3. **CONFIABILIDAD:** ¿El desempeño se mantiene constante a lo largo del tiempo?
4. **RESILIENCIA:** ¿Pueden las comunicaciones importantes continuar durante las interrupciones?

Un teléfono puede mostrar una señal aceptable mientras la red presenta problemas de alta densidad, funciona de manera inconsistente en áreas críticas o carece de una ruta alternativa.

COMENZAR CON LOS REQUISITOS, NO CON EL PRODUCTO

Antes de seleccionar una solución, los propietarios, consultores e integradores deben comprender el entorno. Tams como el tamaño y la distribución del edificio, así como los materiales, los niveles de señal, las zonas muertas y la densidad. También deben formar parte de la evaluación los dispositivos, los operadores, los sistemas operativos, el IoT y los cambios futuros. Igualmente, la cobertura celular pública y, cuando corresponda, las redes privadas deben evaluarse junto con el Wi-Fi.

Solo entonces deben considerarse los modelos de despliegue. Según la instalación, el enfoque puede incluir la optimización del Wi-Fi, la extensión de la cobertura celular, los sistemas de antena distribuidos, las celdas pequeñas, las redes privadas o una arquitectura híbrida.

Cada tipo de instalación puede requerir un enfoque distinto. Sin embargo, mayoritariamente, la cobertura celular interior es la capa que falta, incluso cuando el Wi-Fi es sólido.

Los edificios modernos dependen cada vez más de las comunicaciones inalámbricas como infraestructura esencial. El objetivo ya no es simplemente "tener señal", sino proporcionar la conectividad adecuada donde y cuando se necesita.

La red Wi-Fi conecta a los usuarios con la red del edificio. La cobertura celular interna ayuda a mantenerlos conectados con el mundo exterior. Los edificios modernos necesitan cada vez más de ambas.

Esa es la diferencia entre tener Wi-Fi y estar preparado para un mundo inalámbrico.



Sobre los Autores:

Paul es un líder en TIC con más de 30 años impulsando banda ancha, centros de datos, conectividad y automatización en América, EMEA y APAC. Reconocido conferencista en Fiber Connect, asesora organizaciones globales integrando estrategia tecnológica, infraestructura inteligente, despliegue de cableado híbrido y ejecución comercial.

Orlando es un profesional de telecomunicaciones y radiofrecuencia con más de 30 años liderando diseño inalámbrico, optimización y ventas técnicas en América y Europa. Desde Nextivity, resuelve desafíos complejos de cobertura, capacidad y conectividad en interiores para entornos empresariales, comerciales e infraestructuras de misión crítica.

BEYOND WI-FI: THE WIRELESS READINESS GAP IN MODERN BUILDINGS

MODERN BUILDINGS CAN HAVE EXCELLENT WI-FI AND STILL FAIL TO PROVIDE THE CELLULAR CONNECTIVITY, MOBILITY, RESILIENCE, AND OPERATIONAL COMMUNICATIONS THEIR OCCUPANTS AND SYSTEMS INCREASINGLY DEPEND ON.



Paul Weintraub
RCDD, RTPM, ESS, TECH

General Director
Excigent

paul@excigent.com



Orlando Calderon

Sales Engineer for the Caribbean, Latin America, and Canada
Nextivity

ocalderon@nextivityinc.com

THE WIRELESS READINESS GAP

"The building has Wi-Fi. So why do people still lose signal?"

It is a simple question, but it exposes an increasingly important issue in modern building design. People often treat wireless connectivity as synonymous with Wi-Fi. Yet users do not think in terms of network layers. They expect phones to work, applications to authenticate, messages and calls go through, and mobile services to remain available as they move throughout a building. A facility can therefore have excellent Wi-Fi and still have significant wireless gaps.

The problem often starts with the building itself. Materials that improve energy efficiency, structural performance, and security — such as low-emissivity glass, concrete, and structural steel — can also block radio-frequency propagation. Dense interior construction and below-grade spaces further weaken signals from outside the building, and elevators, stairwells, parking structures, mechanical rooms, and deep interior spaces are frequent trouble spots.

This creates a wireless readiness gap: the building appears connected because Wi-Fi is available, even as reliable cellular service and other communications needs go unaddressed.

WI-FI AND CELLULAR DO DIFFERENT JOBS

Wi-Fi remains essential — it supports enterprise LAN access, guest connectivity, collaboration, managed devices, and many local and IoT applications. But it is only one layer.

Public cellular provides native voice, messaging, and mobile data without requiring users to join the building's network. That matters for visitors, customers,

contractors, and employees using personal devices, as well as for mobile applications, multifactor authentication, cloud services, and other workflows that depend on carrier connectivity.

Reliable in-building cellular also supports mobility as users move through offices, corridors, elevators, parking structures, and interior spaces where outdoor cellular signals may not penetrate consistently.

Private LTE or 5G can support dedicated operational, industrial, campus, or other controlled applications, while IoT networks handle sensors, automation, and monitoring. In many buildings, these technologies complement each other.

> **The design question, then, should not be "Which wireless technology should we install?" It should be "What does the building need to support?"**

PUBLIC WI-FI IS NOT THE SAME AS TRUSTED CONNECTIVITY

Reliable cellular coverage matters for another reason: users should not assume a public Wi-Fi network is trustworthy simply because its name looks familiar or because a hotel, airport, conference venue, restaurant, or other public location offers it.

When cellular service is weak, people may join unfamiliar Wi-Fi networks, use public hotspots, or accept whatever connectivity is available — behavior that can increase cybersecurity exposure.

A hotel Wi-Fi phishing campaign reported in August 2026* showed how compromised Wi-Fi gateway infrastructure and manipulated DNS settings could redirect travelers trying to reach legitimate Microsoft services to fraudulent Microsoft 365 sign-in pages. To the user, the connection could appear normal while attackers targeted credentials or authentication tokens.

The broader lesson is that connectivity and cybersecurity cannot be treated as separate conversations.

A properly designed public or private cellular network can provide a separately managed communications path that does not depend on the building's local Wi-Fi infrastructure. Cellular is not immune to cybersecurity risk, but reliable indoor cellular gives users another connectivity option when Wi-Fi is unavailable, impaired, or untrusted.

In a changing environment where threats, devices, network conditions, and user behavior cannot all be controlled, maintaining more than one viable communications path improves resilience.



Image: The in-building wireless ecosystem. A complete strategy may include multiple layers.
Source: Paul Weintraub *RCDD, RTPM, ESS, TECH* / Orlando Calderon

PUBLIC SAFETY IS A SEPARATE REQUIREMENT

Evaluate emergency responder communications separately from commercial cellular and enterprise Wi-Fi. Requirements may vary by country, jurisdiction, and facility, and difficult areas such as stairwells, parking structures, basements, and other interior spaces may require particular attention. Strong Wi-Fi or commercial cellular coverage should not automatically be assumed to satisfy emergency communications requirements. Public-safety communications are a distinct design consideration.

COVERAGE IS ONLY THE BEGINNING

Signal strength alone does not define wireless performance. A more useful framework considers four factors:

1. **COVERAGE:** Can users connect where they need to?
2. **CAPACITY:** Can the system support the expected number of users and devices?
3. **RELIABILITY:** Does performance remain consistent over time?
4. **RESILIENCE:** Can important communications continue when normal systems or conditions are disrupted?

A smartphone may show acceptable signal strength while the network still struggles under high density, performs inconsistently in critical areas, or lacks an alternate communications path.

START WITH THE REQUIREMENT, NOT THE PRODUCT

Before selecting an in-building wireless solution, owners, consultants, and integrators should first understand the environment. Consider building size and layout, construction materials, indoor and outdoor signal levels, known dead zones, user density, device types, carrier expectations, operational systems, IoT applications, and future changes. Evaluate public cellular coverage—and, where appropriate, private cellular—alongside Wi-Fi.

Only then should you consider deployment models. Depending on the facility, the approach may include Wi-Fi optimization, cellular signal extension, distributed antenna systems, small cells, private wireless, or a hybrid architecture.

A hospital, office tower, warehouse, hotel, and data center may require different approaches. But in many facilities, in-building cellular is the missing layer even when Wi-Fi is strong.

Modern buildings increasingly depend on wireless communications as essential infrastructure. The objective is no longer simply to "get a signal," but to provide the right connectivity for the right application, in the right place, when it is needed.

> **Wi-Fi connects users to the building's network. In-building cellular helps keep them connected to the outside world. Modern buildings increasingly need both.**

That is the difference between having Wi-Fi and being wirelessly ready.



Sobre los Autores:

Paul is an ICT leader with over 30 years driving broadband, data centers, connectivity, and network automation across the Americas, EMEA, and APAC. A seasoned Fiber Connect speaker, he helps global organizations align technology strategy, smart infrastructure planning, hybrid cabling deployment, and strong commercial execution.

Orlando is a telecom and RF professional with over 30 years leading wireless design, optimization, and technical sales across the Americas and Europe. At Nextivity, he solves complex in-building coverage, capacity, and connectivity challenges for enterprise, commercial, and mission-critical environments with proven strategic focus.

VIAVI Solutions

Soluciones de Pruebas de Red Precisas, Confiables y Eficientes para:

- Fibra
- Cable y TV
- 5G/Inalámbricas



Déjenos ayudarle.

Contacte a un experto hoy:

DETECCIÓN POR FIBRA ÓPTICA PARA LA PROTECCIÓN DE INFRAESTRUCTURA DE TERCEROS EN DATA CENTERS



Ricardo Raineri

Business Development Manager Fiber Optics - LATAM
VIAVI Solutions

ricardo.raineri@viavisolutions.com

REPENSAR EL MONITOREO DE PERÍMETRO Y TRAYECTOS

Los campus de data centers dependen de una cadena de activos físicos que un solo operador rara vez controla de extremo a extremo: cercado perimetral, bancos de ductos enterrados, conductos compartidos, vías de acceso y los tramos de fibra de última milla que conectan con los meet-me points de los carriers. Gran parte de esta infraestructura atraviesa terrenos, servidumbres o corredores de servicios públicos propiedad de terceros. El monitoreo tradicional —CCTV, sensores de cerca, rondas de vigilancia— cubre puntos aislados, pero un banco de ductos que se extiende por kilómetros en terreno de terceros es difícil de instrumentar económicamente con sensores discretos.

La Detección Acústica Distribuida (DAS, por sus siglas en inglés) ofrece un enfoque distinto: en lugar de instalar múltiples sensores puntuales, convierte una fibra de telecomunicaciones ya existente en un elemento de detección continuo a lo largo de toda su longitud.

¿CÓMO FUNCIONA DAS?

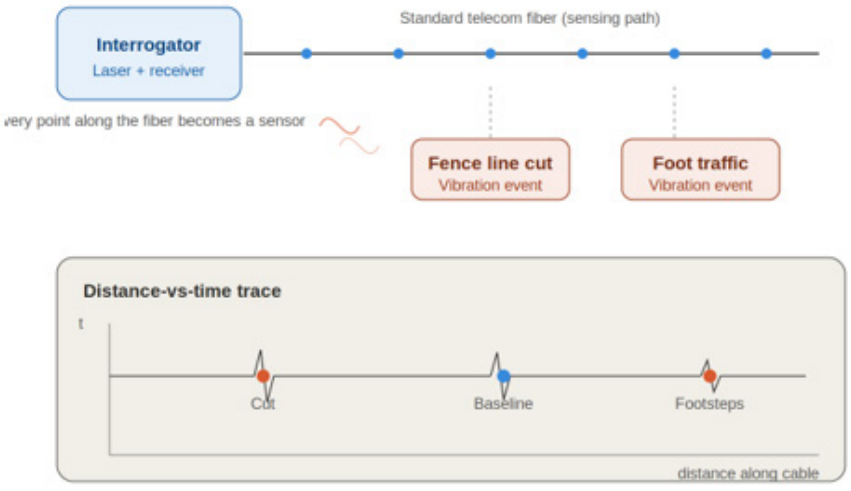


Imagen: Principio de DAS: una interrogadora envía pulsos láser por la fibra de detección; las perturbaciones se localizan en una traza de distancia versus tiempo.
Fuente: Ricardo Reineri

DAS (distributed acoustic sensing) se basa en la retrodispersión de Rayleigh en fibra óptica. Una unidad interrogadora emite pulsos láser cortos en una fibra monomodo estándar y analiza continuamente la luz que se retrodispersa desde imperfecciones microscópicas a lo largo del vidrio. En condiciones estáticas, el patrón de retrodispersión de cualquier sección de fibra es estable. Cuando una perturbación mecánica —una vibración, una tensión o una onda acústica— llega a la fibra, cambia localmente el índice de refracción y la longitud del trayecto óptico, lo cual altera de forma medible la fase e intensidad de la retrodispersión que regresa.

> **Al medir el tiempo de ida y vuelta de cada pulso, el sistema calcula la distancia exacta a lo largo de la fibra donde ocurrió la perturbación, típicamente con una resolución de pocos metros en rangos de decenas de kilómetros.**

El resultado es un registro en vivo de distancia versus tiempo: cada punto a lo largo del cable se convierte en un sensor acústico. No se requiere modificar la fibra, tender cableado adicional ni alimentación eléctrica a lo largo de la ruta; solo acceso a una fibra oscura disponible en el extremo cercano.

POR QUÉ ENCAJA EN EL CASO DE USO TPI

El monitoreo de Infraestructura de Terceros (TPI) es precisamente el escenario donde la detección distribuida tiene una ventaja estructural:

Cobertura continua sin poseer el corredor:
Una sola fibra tendida junto a un banco de ductos, dentro de un conducto existente o sujeta a un cercado, ofrece cobertura de longitud completa, incluso donde el activo físico pertenece a un propietario, municipio o carrier y no puede instrumentarse punto por punto.

Sin dependencia de línea de vista:
A diferencia del CCTV, el desempeño de DAS no depende de iluminación, visibilidad climática o ubicación de cámaras. Detecta el acoplamiento mecánico a la fibra, lo cual funciona igual bajo tierra, dentro de ductos o a lo largo de cercas.

Clasificación de eventos, no solo detección:
Distintas actividades físicas producen firmas acústicas diferenciables: la excavación genera ráfagas irregulares de baja frecuencia y alta energía; un corte o escalada de cerca produce un transitorio agudo; el movimiento vehicular cerca de una ruta enterrada genera un patrón sostenido y cuasi-periódico. El procesamiento de señales —extracción de características más clasificación de patrones, cada vez más asistida por aprendizaje automático— separa estas firmas del ruido de fondo como viento, tráfico o lluvia.

Reutilización de fibra oscura existente: Como DAS opera sobre fibra monomodo estándar G.652, los campus que ya cuentan con hilos de reserva en su planta externa pueden activar la detección sin obra civil nueva, una ventaja material de costo y tiempo frente a desplegar cable sensor dedicado o barreras físicas adicionales.

MODELO DE COBERTURA EN UN CAMPUS DE DATA CENTER

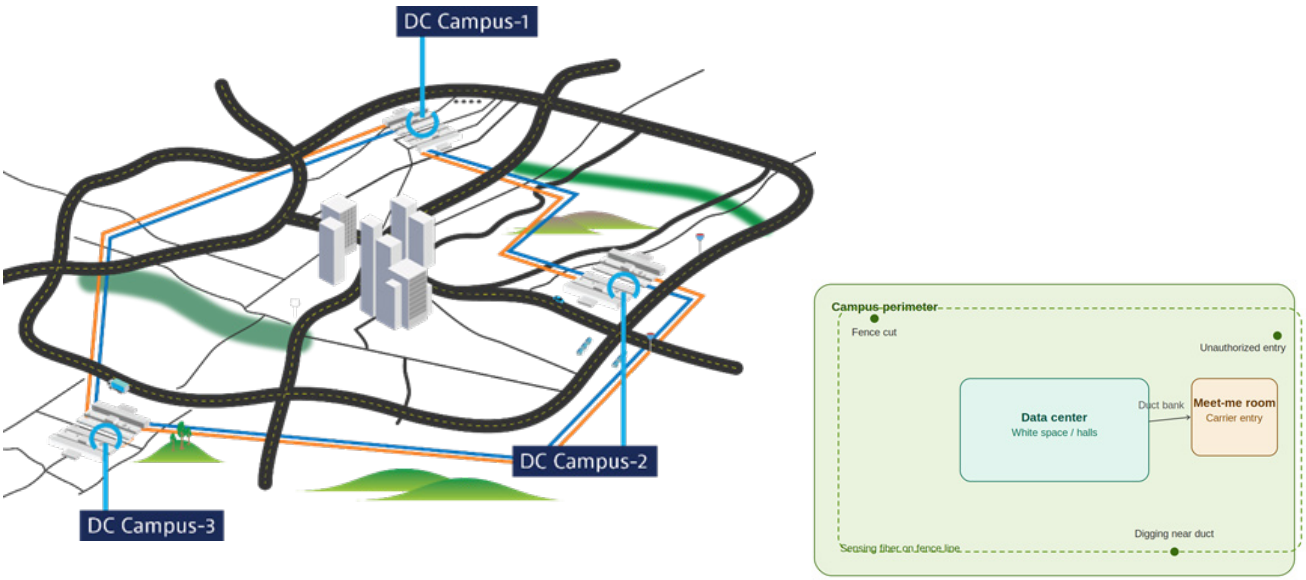


Imagen: Cobertura TPI típica: una fibra de detección continua a lo largo de la cerca perimetral, el banco de ductos y las trayectorias internas.
Fuente: Ricardo Reineri

En la práctica, una sola fibra de detección continua se enruta para cubrir las capas de infraestructura con mayor riesgo de interferencia no detectada:

- La línea de cerca perimetral exterior, para detectar escalamiento, corte o excavación bajo la cerca.
- Los bancos de ductos y conductos que conectan el campus con el meet-me room del carrier o puntos de presencia, donde la excavación no autorizada es una causa principal de interrupciones.
- Las trayectorias internas de cableado entre edificios, donde pueden ocurrir cortes o manipulación de fibra sin ninguna violación visual del perímetro.

Dado que la interrogadora se ubica en un extremo y la fibra recorre todas estas zonas, una sola trayectoria de detección desplegada puede abarcar varios kilómetros de infraestructura monitoreada desde un solo punto de interrogación, con alarmas reportadas como un valor de distancia que se mapea directamente sobre una capa de GIS o de gestión de activos.

CONSIDERACIONES DE INTEGRACIÓN Y OPERACIÓN

Para que DAS sea operativamente útil y no solo una fuente de datos, varios factores importan:

Zonificación de alarmas:
La traza cruda de distancia-tiempo debe mapearse a la geografía real (segmento de cerca, tramo de ducto, entrada de edificio) para que una alerta sea accionable y no solo una coordenada.

Gestión de falsas alarmas:
La lluvia, el contacto de vegetación por viento y el tráfico legítimo de mantenimiento producen acoplamiento mecánico a la fibra. La precisión de clasificación —no la sensibilidad bruta— determina si los equipos de operación confían en el sistema.

Coexistencia con tráfico en vivo:
La detección puede operar sobre una fibra oscura dedicada o, en algunos diseños de sistema, sobre una fibra que también transporta tráfico de datos mediante separación de longitud de onda, algo relevante cuando el conteo de fibra de reserva es limitado.

Ubicación y alcance de la interrogadora:
El rango de detección y la resolución espacial se compensan con la pérdida de fibra y la tasa de repetición de pulsos; la planificación de rutas debe tratar la ubicación de la interrogadora como un parámetro de diseño de red, no como algo secundario.

Integración con las operaciones de seguridad existentes:
Las alarmas con etiqueta de distancia son más útiles cuando se correlacionan con registros de control de acceso, cobertura de CCTV en la ubicación señalada y sistemas de tickets, convirtiendo un evento de capa física en un disparador de flujo de trabajo de seguridad.

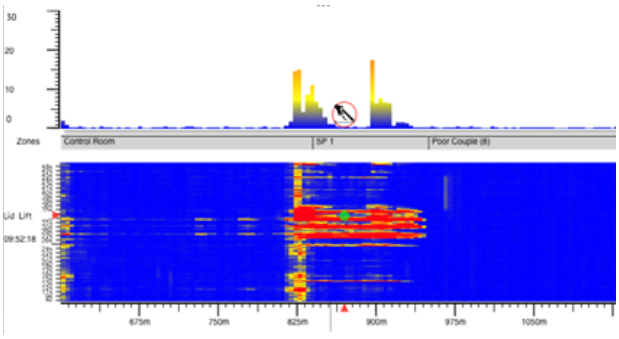


Imagen: Firmas acústicas representativas usadas para clasificar eventos Ejemplo: (Manipulacion de cable).
Fuente: Ricardo Reineri

CONCLUSIÓN

Para operadores de data centers que gestionan infraestructura que se extiende más allá de su propio cercado —ductos compartidos, trayectorias propiedad de carriers, conductos multi-inquilino—, DAS convierte un activo ya instalado (fibra de reserva) en un instrumento de detección continuo de varios kilómetros. La física está bien establecida; el diferenciador en despliegues reales es qué tan bien se clasifica, zonifica e integra la señal acústica en los flujos de trabajo operativos existentes. A medida que el riesgo TPI se vuelve una parte más explícita de la planificación de resiliencia de los data centers, la detección distribuida por fibra es una de las pocas tecnologías capaces de cubrir económicamente infraestructura lineal propiedad de terceros de extremo a extremo.

Sobre el Autor:

Ingeniero Eléctrico con MBA por la FGV-SP y más de 20 años de trayectoria, actualmente se desempeña como BDM Fiber Optics LATAM en Viavi Solutions y es miembro de la comisión de normas técnicas COBEI-ABNT.

SENSORIAMENTO POR FIBRA ÓPTICA PARA PROTEÇÃO DE INFRAESTRUTURA DE TERCEIROS EM DATA CENTERS



Ricardo Raineri

Business Development Manager Fiber Optics - LATAM
VIAVI Solutions

ricardo.raineri@viavisolutions.com

REPENSANDO O MONITORAMENTO DE PERÍMETRO E TRAJETOS

Os campi de data centers dependem de uma cadeia de ativos físicos que um único operador raramente controla de ponta a ponta: cercamento perimetral, bancos de dutos enterrados, condutos compartilhados, vias de acesso e os trechos de fibra de última milha que conectam aos meet-me points das operadoras. Grande parte dessa infraestrutura atravessa terrenos, servidões ou corredores de utilidades de propriedade de terceiros. O monitoramento tradicional — CFTV, sensores de cerca, rondas de vigilância — cobre pontos isolados, mas um banco de dutos que se estende por quilômetros em terreno de terceiros é difícil de instrumentar economicamente com sensores discretos.

O Sensoriamento Acústico Distribuído (DAS, na sigla em inglês) oferece uma abordagem diferente: em vez de instalar múltiplos sensores pontuais, transforma uma fibra de telecomunicações já existente em um elemento de sensoriamento contínuo ao longo de toda a sua extensão.

COMO FUNCIONA O DAS?

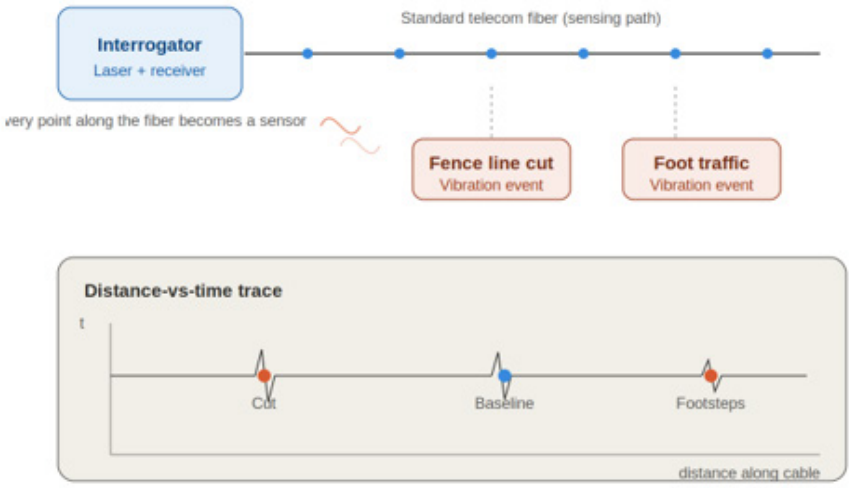


Figura: Princípio do DAS: uma interrogadora envia pulsos laser pela fibra de detecção; as perturbações são localizadas em um traço de distância versus tempo.
Fonte: Ricardo Reineri

O DAS (Distributed Acoustic Sensing)baseia-se no retroespalhamento de Rayleigh em fibra óptica. Uma unidade interrogadora emite pulsos curtos de laser em uma fibra monomodo padrão e analisa continuamente a luz retroespalhada por imperfeições microscópicas ao longo do vidro. Em condições estáticas, o padrão de retroespalhamento de qualquer seção da fibra é estável. Quando uma perturbação mecânica — uma vibração, uma tensão ou uma onda acústica — atinge a fibra, ela altera localmente o índice de refração e o comprimento do trajeto óptico, o que modifica de forma mensurável a fase e a intensidade do retroespalhamento que retorna.

> **Ao cronometrar o tempo de ida e volta de cada pulso, o sistema calcula a distância exata ao longo da fibra onde ocorreu a perturbação, tipicamente com resolução de poucos metros em alcances de dezenas de quilômetros.**

O resultado é um registro em tempo real de distância versus tempo: cada ponto ao longo do cabo se torna um sensor acústico. Não é necessário modificar a fibra, instalar cabeamento adicional ou fornecer alimentação elétrica ao longo da rota — apenas acesso a uma fibra escura disponível na extremidade próxima.

POR QUE ISSO SE APLICA AO CASO DE USO DE TPI

O monitoramento de Infraestrutura de Terceiros (TPI) é exatamente o cenário em que o sensoriamento distribuído tem uma vantagem estrutural:

Cobertura contínua sem possuir o corredor:
Uma única fibra instalada junto a um banco de dutos, dentro de um conduto existente ou fixada a um cercamento oferece cobertura de ponta a ponta, mesmo quando o ativo físico pertence a um proprietário, município ou operadora e não pode ser instrumentado ponto a ponto.

Sem dependência de linha de visada:
Diferentemente do CFTV, o desempenho do DAS não depende de iluminação, visibilidade climática ou posicionamento de câmeras. Ele detecta o acoplamento mecânico à fibra, o que funciona igualmente bem no subsolo, dentro de dutos ou ao longo de cercas.

Classificação de eventos, não apenas detecção:
Atividades físicas diferentes produzem assinaturas acústicas distinguíveis: escavação gera rajadas irregulares de baixa frequência e alta energia; um corte ou escalada de cerca produz um transiente agudo; movimento de veículos próximo a uma rota enterrada gera um padrão sustentado e quase periódico. O processamento de sinais — extração de características somada à classificação de padrões, cada vez mais assistida por aprendizado de máquina — separa essas assinaturas do ruído de fundo, como vento, tráfego ou chuva.

Reaproveitamento de fibra escura existente:
Como o DAS opera sobre fibra monomodo padrão G.652, campi que já possuem fios de reserva em sua planta externa podem ativar o sensoriamento sem novas obras civis — uma vantagem material de custo e tempo em comparação à instalação de cabo sensor dedicado ou barreiras físicas adicionais.

MODELO DE COBERTURA EM UM CAMPUS DE DATA CENTER

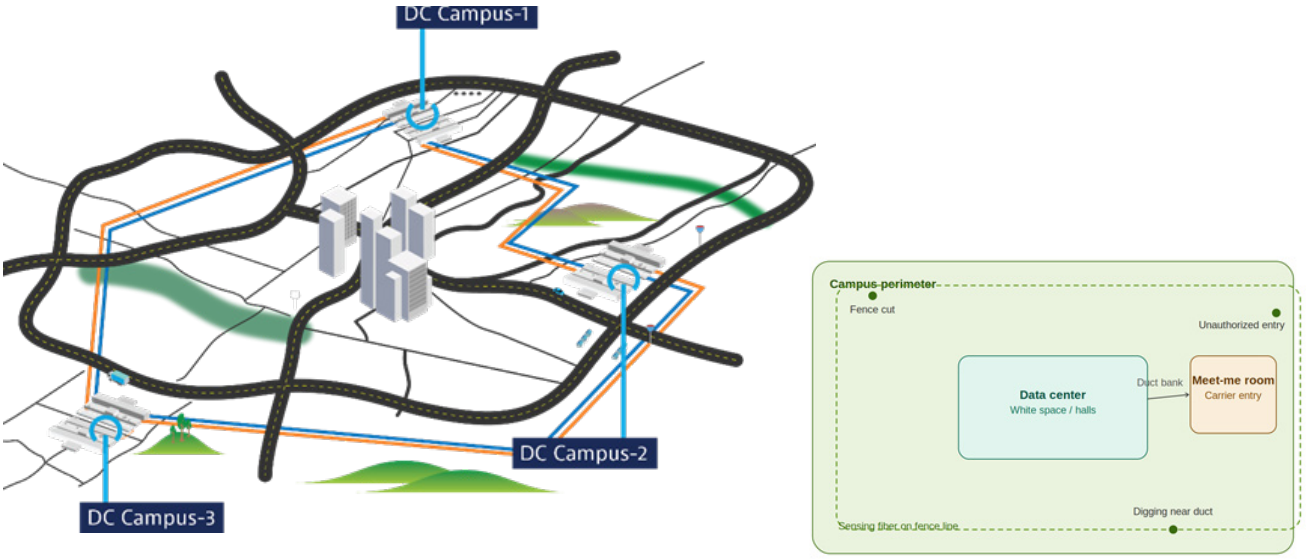


Figura: Cobertura TPI típica: una fibra de detección continua a lo largo de la cerca perimetral, el banco de ductos y las trayectorias internas.
Fuente: Ricardo Reineri

Na prática, uma única fibra de sensoriamento contínuo é roteada para cobrir as camadas de infraestrutura com maior risco de interferência não detectada:

- A linha de cerca perimetral externa, para detectar escalada, corte ou escavação sob a cerca.
- Os bancos de dutos e condutos que conectam o campus à meet-me room da operadora ou a pontos de presença, onde escavações não autorizadas são uma das principais causas de interrupções.
- Os trajetos internos de cabeamento entre edifícios, onde cortes ou adulteração de fibra podem ocorrer sem qualquer violação visual do perímetro.

Como a interrogadora fica em uma extremidade e a fibra percorre todas essas zonas, um único trajeto de sensoriamento implantado pode abranger vários quilômetros de infraestrutura monitorada a partir de um único ponto de interrogação, com alarmes reportados como um valor de distância que se mapeia diretamente sobre uma camada de GIS ou de gestão de ativos.

CONSIDERAÇÕES DE INTEGRAÇÃO E OPERAÇÃO

Para que o DAS seja operacionalmente útil, e não apenas uma fonte de dados, vários fatores importam:

Zoneamento de alarmes: O traço bruto de distância-tempo precisa ser mapeado para a geografia real (segmento de cerca, trecho de duto, entrada de edifício) para que um alerta seja acionável, e não apenas uma coordenada.

Gestão de falsos alarmes: Chuva, contato de vegetação movida pelo vento e tráfego legítimo de manutenção produzem acoplamento mecânico à fibra. A precisão de classificação — não a sensibilidade bruta — determina se as equipes de operação confiam no sistema.

Coexistência com tráfego em operação: O sensoriamento pode operar em uma fibra escura dedicada ou, em alguns projetos de sistema, em uma fibra que também transporta tráfego de dados por meio de separação de comprimento de onda, algo relevante quando o número de fibras de reserva é limitado.

Posicionamento e alcance da interrogadora: O alcance de detecção e a resolução espacial têm relação de compromisso com a perda da fibra e a taxa de repetição de pulsos; o planejamento de rotas deve tratar a localização da interrogadora como um parâmetro de projeto de rede, não como algo secundário.

Integração com as operações de segurança existentes: Alarmes com marcação de distância são mais úteis quando correlacionados com registros de controle de acesso, cobertura de CFTV no local sinalizado e sistemas de tickets, transformando um evento de camada física em um gatilho de fluxo de trabalho de segurança.

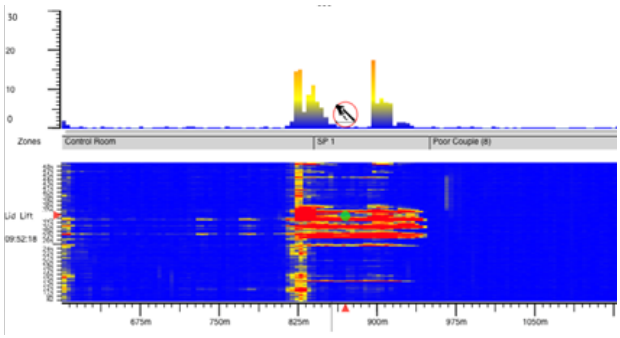


Figura: Assinaturas acústicas representativas usadas para classificar eventos. Exemplo: (Manipulação de cabo).
Fonte: Ricardo Reineri

CONCLUSÃO

Para operadores de data centers que gerenciam infraestrutura que se estende além de seu próprio cercamento — dutos compartilhados, trajetos de propriedade de operadoras, condutos multi-inquilino —, o DAS transforma um ativo já instalado (fibra de reserva) em um instrumento de sensoriamento contínuo de vários quilômetros. A física é bem estabelecida; o diferencial em implantações reais está em quão bem o sinal acústico é classificado, zoneado e integrado aos fluxos de trabalho operacionais existentes. À medida que o risco de TPI se torna uma parte mais explícita do planejamento de resiliência dos data centers, o sensoriamento distribuído por fibra é uma das poucas tecnologias capazes de cobrir, de forma economicamente viável, infraestrutura linear de propriedade de terceiros de ponta a ponta

Sobre o Autor:

Engenheiro Eletricista com MBA pela FGV-SP e mais de 20 anos de trajetória, atualmente atua como BDM Fiber Optics LATAM na Viavi Solutions e é membro da comissão de normas técnicas COBEI-ABNT.


Bicsi
CALA