

Más Allá del Wi-Fi: Los Riesgos Inalámbricos Ocultos en los Edificios Modernos

Paul F. Weintraub
RCDD, RTPM, ESS, TECH, CAE
Managing Director
Excigent



Orlando Calderon
Sales Engineer Caribbean, Latin America, and Canada
Nextivity





Más allá del Wi-Fi:

Los riesgos inalámbricos ocultos en los edificios modernos

Agenda



Presentadores

Orlando Calderon

Ingeniero de ventas – CALA,
Nextivity



- Más de 30 años de experiencia en telecomunicaciones e ingeniería RF
- Diseño y optimización de redes inalámbricas y soluciones en interiores
- Ventas técnicas y desarrollo de negocios
- Apoya a CALA y Canadá



Paul Weintraub

RCDD, RTPM, ESS, TECH
Director general, Excigent



- Más de 30 años de experiencia en TIC, banda ancha y seguridad
- Enfocado en alinear la estrategia tecnológica con la planificación y ejecución de infraestructura
- Más de 20 años de experiencia en mercados globales
- Experto en infraestructura digital y edificios inteligentes

Resultados de aprendizaje

1. Explicar por qué el Wi-Fi por si solo no es suficiente para atender todas las necesidades de conectividad inalámbrica en interiores, movilidad, seguridad pública, IoT y comunicaciones operativas.
2. Identificar los riesgos de cobertura, confiabilidad, seguridad y operación creados por un desempeño celular e inalámbrico deficiente en interiores.
3. Aplicar un marco práctico para evaluar soluciones inalámbricas en interiores, incluyendo cobertura, capacidad, seguridad pública, ciberseguridad, coordinación con operadores, modelo de despliegue y soporte durante el ciclo de vida.

Pregunta de apertura



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

- El Wi-Fi puede respaldar el acceso a la red local, pero no todas las necesidades inalámbricas
- El servicio celular en interiores puede seguir siendo débil o inconsistente
- Los sistemas de seguridad pública, IoT y operación pueden requerir planificación separada
- Los edificios modernos necesitan una estrategia inalámbrica más amplia

La brecha de preparación inalámbrica

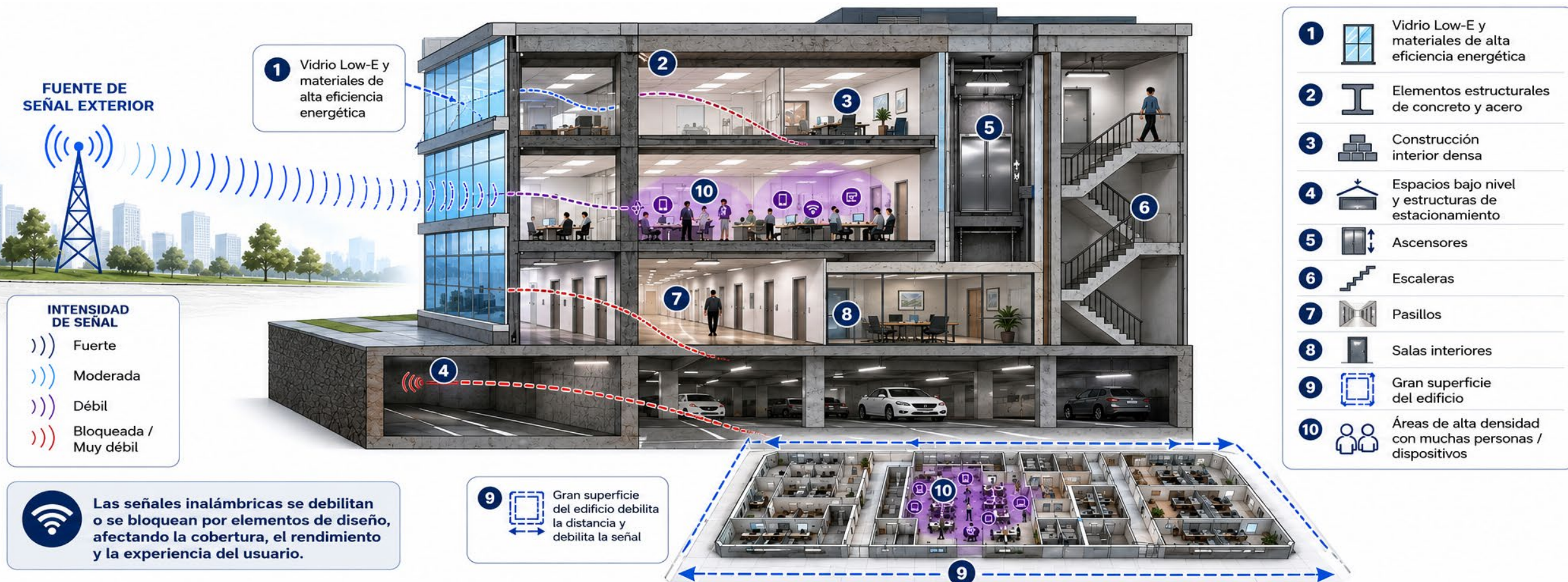
La preparación inalámbrica no es lo mismo que tener Wi-Fi

- Un edificio puede tener Wi-Fi sólido y una cobertura celular deficiente
- Un edificio puede soportar a los usuarios, pero no a los servicios de emergencia
- Un edificio puede soportar a las personas, pero no a los sistemas operativos
- Las distintas capas inalámbricas resuelven problemas diferentes



¿Por qué los edificios modernos debilitan las señales?

El diseño del edificio puede bloquear involuntariamente el rendimiento inalámbrico



Áreas con problemáticas comunes

Dónde suelen aparecer primero los problemas de conectividad inalámbrica



El Wi-Fi tiene un papel importante

El Wi-Fi sigue siendo esencial

- Acceso a la LAN empresarial
- Conectividad para invitados
- Dispositivos de usuario gestionados
- Aplicaciones locales
- Herramientas de colaboración
- Ciertos sistemas de IoT y del edificio



¿Por qué el Wi-Fi por sí solo?

Diferentes casos de uso requieren diferentes capas inalámbricas

- Celular público para movilidad, voz, mensajes de texto y acceso de visitantes
- Comunicaciones de seguridad pública para socorristas
- Redes inalámbricas privadas para control operativo y casos de uso dedicados
- Wi-Fi para acceso empresarial y a la red local
- Redes IoT para sensores, automatización y monitoreo



El problema del comportamiento del usuario

Cuando falla la conectividad, los usuarios improvisan



La conectividad deficiente cambia el comportamiento del usuario y aumenta los riesgos de seguridad, operación y soporte.

Riesgos de seguridad

Las brechas inalámbricas pueden aumentar la exposición a riesgos de seguridad



Riesgos de seguridad

Incertidumbre del usuario: ¿A qué red Wi-Fi es seguro conectarse?



Punto de acceso legítimo

- Conexión segura (WPA2/WPA3)
- Red oficial
- Proveedor confiable

Punto de acceso falso

- Seguridad abierta o débil
- Nombre de red falso
- Riesgo de robo de datos

Si tienes dudas, no te conectes. Verifica la red antes de confiar en ella.

HACKERS

Ataque de phishing a la red Wi-Fi de hoteles apunta a inicios de sesión de Microsoft

Hackers secuestran puertas de enlace Wi-Fi de hoteles para redirigir a viajeros de negocios a páginas convincentes de Microsoft 365

Por Kurt Knutsson, CyberGuy Report • Fox News

Publicado el 2 de agosto de 2026, 7:41 a. m. EDT

Hackers están manipulando equipos Wi-Fi en hoteles y centros de conferencias, convirtiendo una conexión cotidiana a internet en un camino hacia páginas falsas de inicio de sesión de Microsoft 365. El ataque de phishing por Wi-Fi en hoteles representa un riesgo particular para los viajeros de negocios. Podría conectarse antes de una reunión, abrir su laptop y ver lo que parece ser una pantalla normal de inicio de sesión de Microsoft.

La seguridad pública es diferente

Las comunicaciones de emergencia no son cobertura por conveniencia

- Los requisitos de seguridad pública pueden estar determinados por códigos
- Los requisitos de la AHJ varían según la jurisdicción
- Las áreas críticas pueden incluir escaleras, sótanos, pasillos y estacionamientos
- Las pruebas y la documentación forman parte del ciclo de vida
- La seguridad pública no debe asumirse a partir de la cobertura Wi-Fi o celular comercial

Comunicaciones operativas

La conectividad inalámbrica respalda más que teléfonos y *laptops*

- Personal de seguridad
- Operaciones de instalaciones
- Equipos de mantenimiento
- Sistemas de edificios inteligentes
- Sensores y monitoreo
- Herramientas de almacén y logística
- Automatización de edificios e IoT



Call Buttons



Temperature Sensor



Position Tracking



Air Quality Sensor



Audible Alarm Detection



Occupancy Detector



Acoustic Event Detection



Noise Level Sensor



Leak Detector



Smart Labels

El ecosistema inalámbrico en interiores

Una estrategia completa puede incluir múltiples capas

- Wi-Fi
- Celular público
- Comunicaciones de seguridad pública
- LTE privado / 5G privado
- IoT y sistemas del edificio
- Monitoreo y soporte durante el ciclo de vida

Estrategia inalámbrica completa



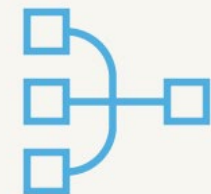
Wi-Fi



Public Cellular Coverage



Private Cellular Coverage



Low Power Sensor Networks

Cobertura, capacidad, confiabilidad y resiliencia

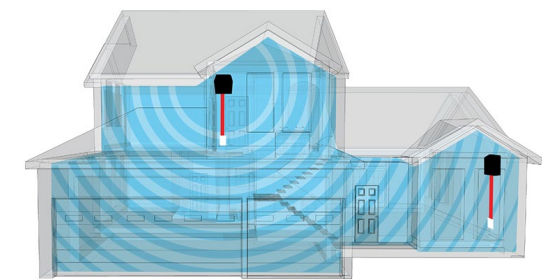
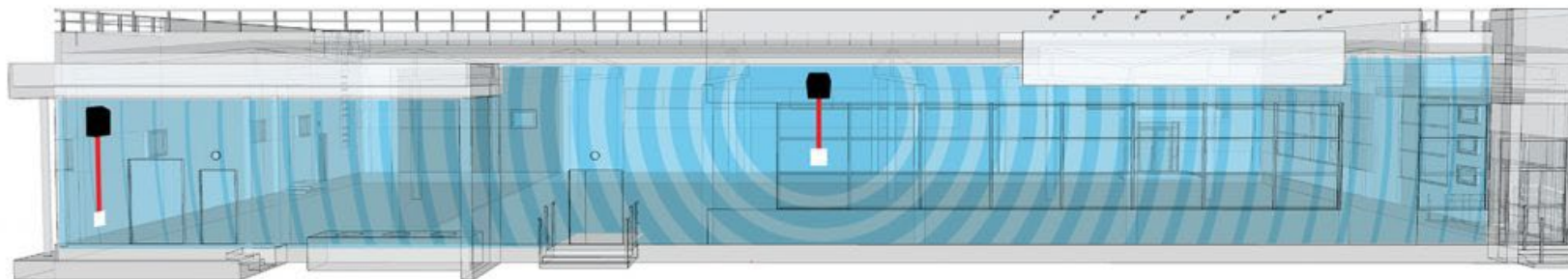
Cuatro preguntas que todo equipo de edificio debe hacerse

- **Cobertura:** ¿Pueden los usuarios conectarse donde lo necesitan?
- **Capacidad:** ¿Puede el sistema soportar el número esperado de usuarios y dispositivos?
- **Confiabilidad:** ¿El desempeño se mantiene consistente con el tiempo?
- **Resiliencia:** ¿Pueden continuar las comunicaciones críticas durante interrupciones?

Celular público dentro de los edificios

¿Por qué importa la cobertura celular en interiores?

- Continuidad de voz, mensajes de texto y datos móviles
- Experiencia de visitantes, inquilinos, empleados y clientes
- Aplicaciones móviles y flujos de autenticación
- Expectativas de múltiples operadores
- Pueden existir brechas en interiores aun cuando la cobertura exterior sea fuerte

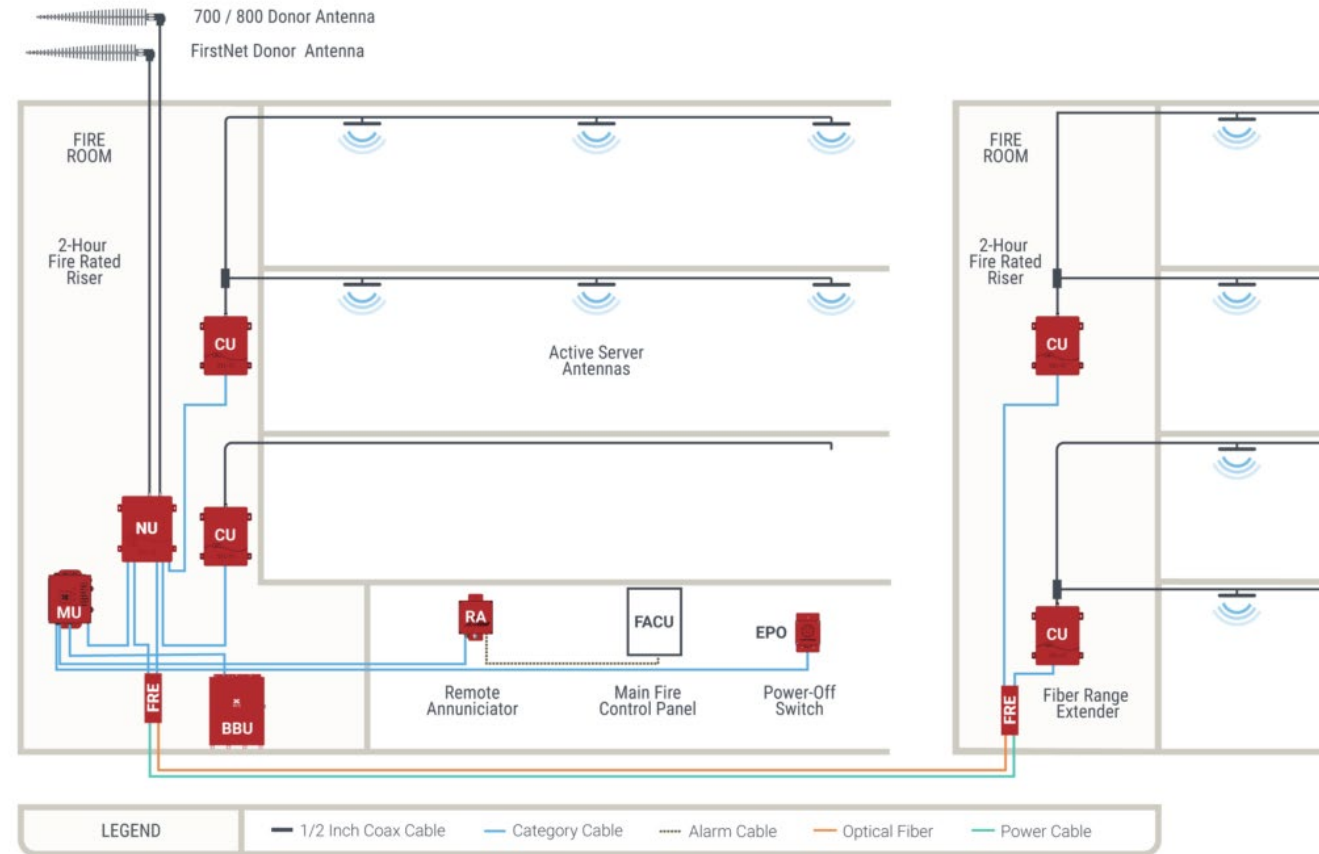


Ejemplos de diseños

Seguridad pública / ERCES-BDA

Las comunicaciones para respondedores de emergencia requieren una evaluación separada

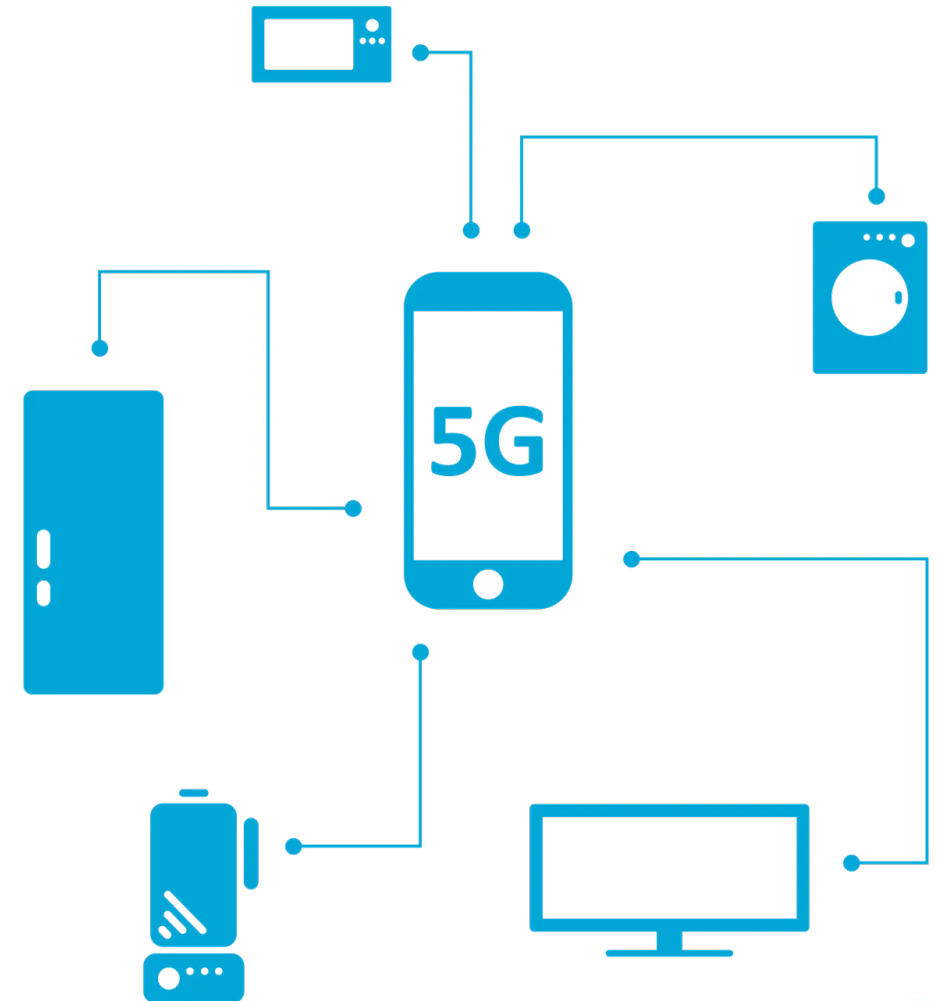
- Pueden aplicar requisitos de código y de la AHJ
- Las expectativas de cobertura pueden incluir áreas difíciles del edificio
- Puede requerirse prueba y recertificación
- La documentación y el mantenimiento son responsabilidades continuas
- La cobertura de seguridad pública debe planificarse desde el inicio, no tratarse como una idea posterior



Redes inalámbricas privadas / 5G privado

¿Dónde pueden encajar las redes inalámbricas privadas?

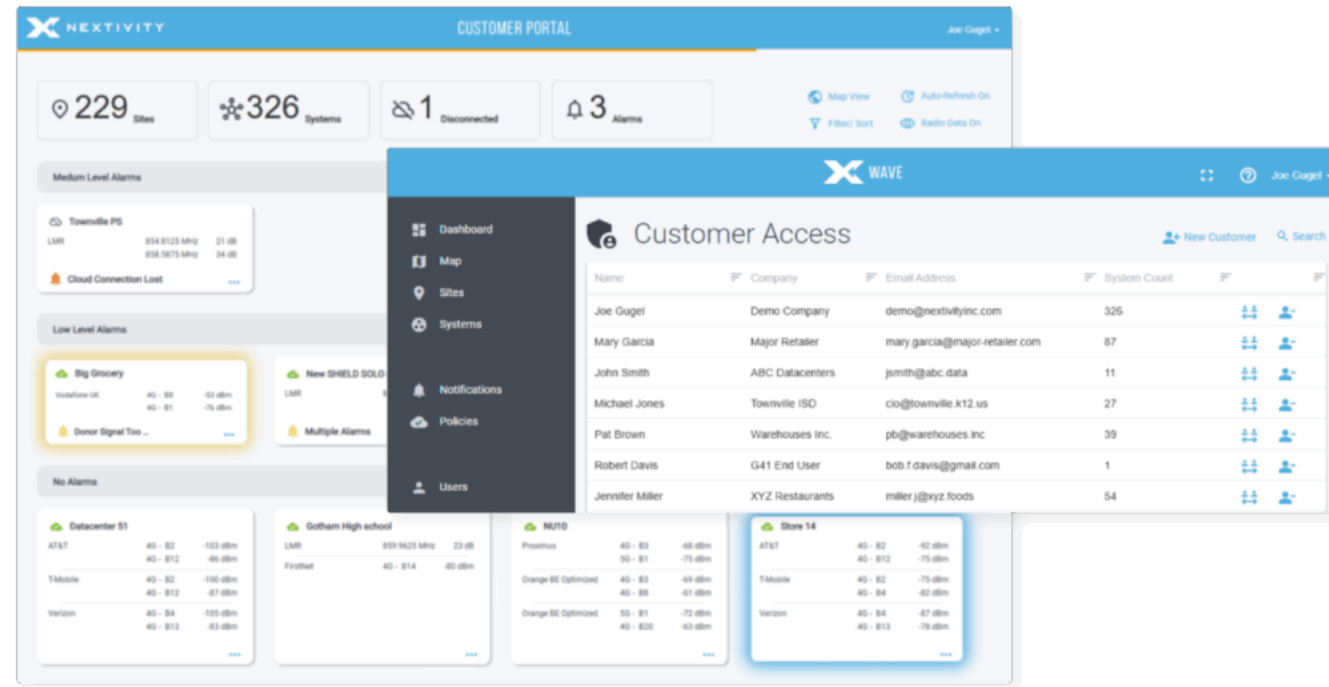
- Operaciones industriales
- Almacenes y logística
- Edificios inteligentes y campus
- Redes operativas seguras
- IoT y automatización
- Conectividad dedicada para aplicaciones específicas



Monitoreo y soporte durante el ciclo de vida

La instalación no es el final del ciclo de vida inalámbrico

- Cambian las distribuciones de los inquilinos
- Cambia la densidad de usuarios
- Cambian los sistemas del edificio
- La cobertura y el desempeño pueden desviarse con el tiempo
- El monitoreo ayuda a identificar problemas antes de que los usuarios los escalen
- La responsabilidad debe definirse desde el inicio



Marco práctico de evaluación

Comience con los requisitos antes de seleccionar una solución

- ¿Qué casos de uso deben ser soportados?
- ¿Quién depende del sistema inalámbrico?
- ¿Dónde están las áreas críticas de cobertura?
- ¿Qué capacidad y confiabilidad se requieren?
- ¿Qué riesgos de seguridad deben controlarse?
- ¿Qué requisitos de seguridad pública aplican?
- ¿Quién es responsable del soporte durante el ciclo de vida?

Lista de verificación para evaluar el edificio

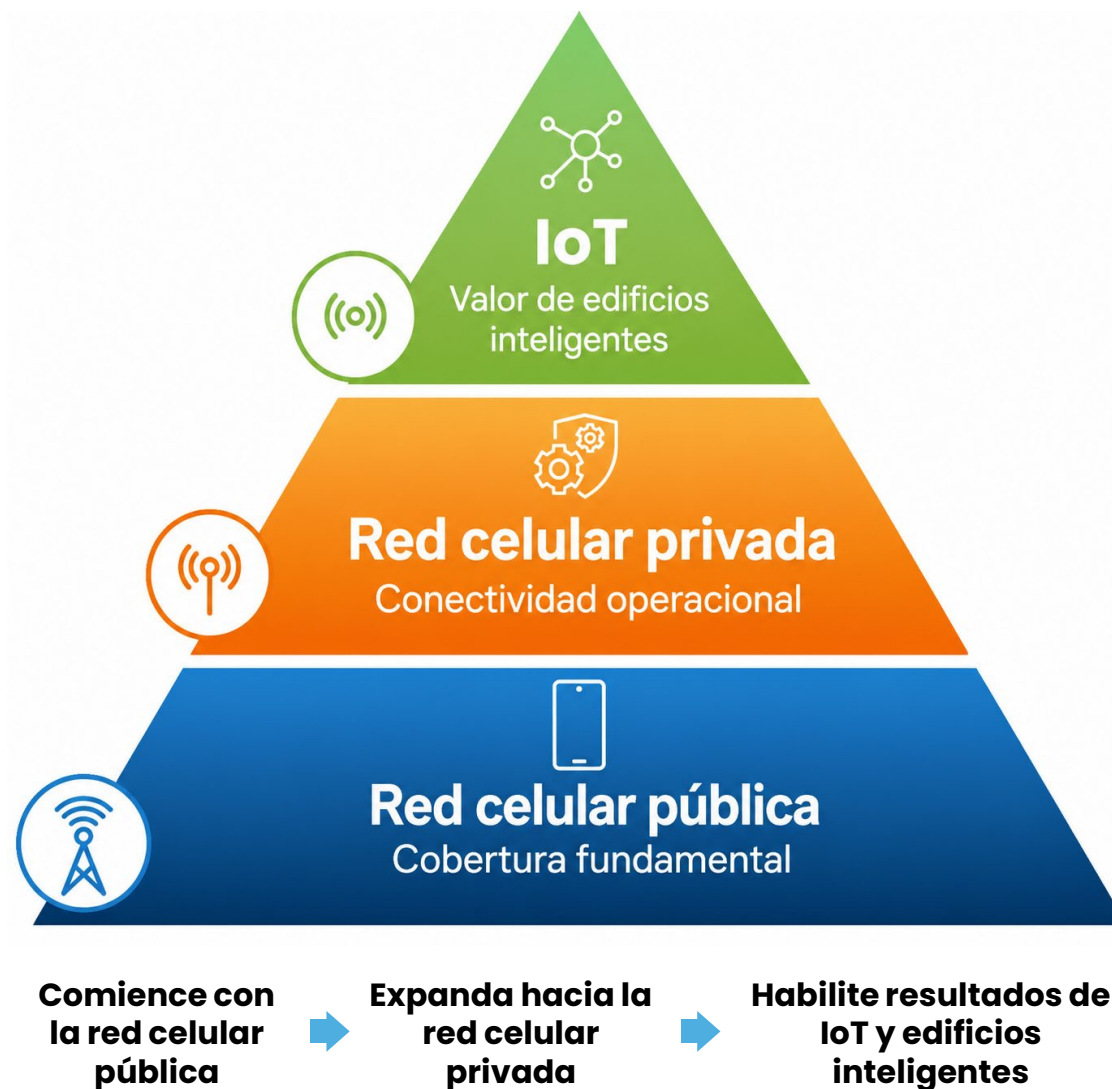
Comprender el entorno antes de diseñar la solución

- Tamaño y distribución del edificio
- Materiales de construcción
- Niveles existentes de señal interior y exterior
- Zonas muertas conocidas
- Densidad de usuarios y tipos de dispositivos
- Expectativas de los operadores
- Requisitos de seguridad pública
- Necesidades operativas e IoT
- Expansión futura o cambios de inquilinos

Modelos de despliegue

No existe un único enfoque que sirva para todos los edificios

- Optimización de Wi-Fi
- Extensión de señal celular
- Sistemas de antenas distribuidas
- Celdas pequeñas
- Redes inalámbricas privadas
- Sistemas de seguridad pública
- Enfoques híbridos



Matriz de decisión

Alinear el enfoque con el requisito

Requisito		Pregunta Clave
	Movilidad	¿Los usuarios necesitan continuidad de voz, mensajes de texto y datos móviles?
	Seguridad pública	¿Se requieren comunicaciones para los servicios de emergencia?
	Seguridad	¿Los usuarios están recurriendo a soluciones alternativas no seguras?
	Operaciones	¿Los sistemas del edificio o los flujos de trabajo dependen de la conectividad inalámbrica?
	Capacidad	¿El sistema puede soportar la demanda máxima?
	Ciclo de vida	¿Quién monitorea y mantiene el desempeño?

Escenario real: Oficina / Edificio comercial

Problemas comunes



Escenario real: Salud / Instalaciones de misión crítica

Problemas comunes

- La movilidad y las comunicaciones del personal son esenciales
- La cobertura de seguridad pública es importante
- La construcción densa puede crear desafíos de RF
- Múltiples grupos de usuarios dependen de diferentes capas inalámbricas
- La confiabilidad y el soporte durante el ciclo de vida son críticos



Escenario real: Centro de datos

Problemas comunes

- El personal, los visitantes y los contratistas necesitan comunicación confiable dentro de áreas críticas
- La cobertura celular puede respaldar llamadas de emergencia, alertas y seguridad de trabajadores solitarios
- La comunicación inalámbrica de respaldo ayuda durante fallas de red o de sistemas
- Las alertas de UPS, HVAC, supresión de incendios, baterías y sistemas de acceso pueden necesitar redundancia
- Una cobertura interior deficiente puede afectar la seguridad, el tiempo de respuesta, el cumplimiento y la continuidad operativa



Demostración práctica

Enfocarse en el proceso de decisión, no en la marca

- ¿Cómo se identifica el problema de cobertura?
- ¿Cómo el caso de uso impulsa el diseño?
- ¿Cómo las capas inalámbricas difieren según el requisito?
- ¿Cómo el monitoreo respalda la gestión del ciclo de vida?
- ¿Cómo una mejor planificación reduce el riesgo después de la instalación?



Errores comunes que se deben evitar

Evite estas suposiciones

- “Tenemos Wi-Fi, así que la conectividad inalámbrica está cubierta”
- “La señal exterior significa que la señal interior estará bien”
- “La seguridad pública es lo mismo que la cobertura celular comercial”
- “La cobertura equivale a capacidad”
- “La instalación es el final del proyecto”
- “Una sola capa inalámbrica puede servir todos los casos de uso”

Conclusiones clave:

- El Wi-Fi es esencial, pero es solo una capa de la preparación inalámbrica
- La cobertura celular interior, la seguridad pública, las redes inalámbricas privadas y el IoT tienen requisitos diferentes
- Una cobertura inalámbrica deficiente crea riesgos operativos, de seguridad física y de ciberseguridad
- La cobertura, la capacidad, la confiabilidad y el soporte durante el ciclo de vida deben evaluarse en conjunto
- El enfoque correcto comienza con el caso de uso, no con el producto

Preguntas y discusión:

- ¿Dónde falla con mayor frecuencia la conectividad inalámbrica en sus edificios?
- ¿Qué sistemas dependen de la continuidad inalámbrica?
- ¿Se incluyen con suficiente anticipación las necesidades de seguridad pública y operación?
- ¿Quién es responsable del desempeño después de la instalación?
- ¿Qué cambiaría si la conectividad inalámbrica se tratara como infraestructura del edificio?