

Guía de soluciones de red

# CUIDADO DE LA SALUD

A medida que aumentan los costes operativos, Allied Telesis está aquí para garantizar que ofrezca las soluciones sanitarias más seguras, fiables y eficientes a sus pacientes.



## Necesidades y objetivos de las redes sanitarias

**49%** de los proveedores sanitarios están en proceso de transformar su modelo de negocio en los próximos 12 meses.

*Fuente: Gartner Research, 2019*

El sector sanitario está experimentando cambios empresariales y cambios tecnológicos más rápidamente que ningún otro sector importante. En todo el mundo, la demanda de servicios sanitarios supera la capacidad de los proveedores de servicios para atender a los pacientes y prestar una atención personal de alta calidad. Hay escasez de profesionales e instalaciones sanitarias, sobre todo en zonas rurales o remotas. Los costes de la asistencia sanitaria aumentan mucho más deprisa que los ingresos personales y la capacidad de pago de los pacientes, lo que obliga a los proveedores de servicios sanitarios a prestarlos a menor coste.

La parte tecnológica del negocio también está experimentando cambios. Una habitación de hospital moderna tiene, por término medio, 15 dispositivos conectados en red que controlan el estado del paciente y le administran medicación u otras formas de atención. Los historiales médicos se han digitalizado, por lo que los profesionales sanitarios necesitan acceso móvil continuo a la red para acceder a estos historiales y a otra información relevante. Además, muchos servicios se ofrecen a distancia a través de la red, como la telemedicina y la atención ambulatoria.

Las tecnologías disruptivas, como la IA, brindarán oportunidades para crear nuevos modelos de negocio y de prestación de asistencia. Sin embargo, esto requerirá una infraestructura más ágil que pueda responder rápidamente a la evolución de nuevos modelos de prestación de asistencia sanitaria que puedan satisfacer las crecientes expectativas de los consumidores. Este es el reto al que se enfrentan los proveedores de asistencia sanitaria.

Otra perturbación es la descentralización de la infraestructura sanitaria para reducir la distancia entre el paciente y el tratamiento. Aunque esto beneficia al consumidor de servicios sanitarios, también añade complejidad a las soluciones informáticas.





Los elementos clave de una red sanitaria ágil y preparada para el futuro son:



#### Acceso fiable de alta velocidad por cable e inalámbrico

Los profesionales sanitarios que utilizan diversos dispositivos móviles necesitan acceder de forma fiable y segura a la información de los pacientes desde cualquier lugar, y con suficiente ancho de banda para imágenes médicas y vídeo en tiempo real. Los sistemas de apoyo al paciente, como la telemedicina y los monitores de salud remotos, necesitan una conexión sin interrupciones. El acceso a Internet de alta velocidad para invitados también debe soportar un tráfico de alta densidad.



#### Seguridad general

Los historiales de los pacientes contienen información extremadamente sensible y de gran valor. Por lo tanto, la red debe estar protegida contra el acceso no autorizado, así como contra la fuga o el robo de datos.

Paralelamente a la ciberseguridad, debe implantarse la seguridad física para proteger los activos y a los pacientes.



#### Fácil gestión de la red

La red debe gestionar fácilmente los dispositivos cableados e inalámbricos dentro y fuera de las instalaciones desde un centro de operaciones remoto.

Encontrar una red que satisfaga todas sus necesidades puede parecer una tarea imposible, pero con una solución de red Allied Telesis adaptada a su organización, es posible y sencillo.

### Prioridades de las redes sanitarias

- Facilitar el acceso a la información y los recursos, pero manteniendo la seguridad de los datos confidenciales
- Proporcionar un acceso seguro a la red a los profesionales sanitarios y al personal
- Proporcionar acceso a Internet a pacientes y familiares
- Proteger los datos confidenciales de los pacientes frente a accesos no autorizados
- Prepararse para las nuevas aplicaciones empresariales
- Soporte y optimización de conexiones WAN multisitio
- Ser fácil de configurar, gestionar y solucionar, minimizando los costes de administración y los tiempos de inactividad
- Gestión centralizada para centros remotos sin recursos informáticos
- Recuperación automática en caso de fallo del equipo o del enlace, así como de bucles accidentales

# Solución Allied Telesis para sanidad

Allied Telesis es un líder de la industria en soluciones de redes **robustas**.

Con nuestro historial demostrado de suministro de soluciones de red avanzadas altamente fiables y ricas en funciones, cada vez son más los proveedores sanitarios que recurren a Allied Telesis para alcanzar sus objetivos.

Allied Telesis lleva muchos años implementando redes sanitarias de vanguardia, por lo que comprendemos la necesidad de suministrar servicios de red avanzados sin aumentar la complejidad operativa. Nuestra cartera de productos y servicios de alto valor proporciona la seguridad, la movilidad y la red de alto rendimiento que necesita, con una gestión sencilla para reducir los costes operativos, tanto ahora como en el futuro.

Veamos cómo Allied Telesis responde a los retos a los que se enfrenta la asistencia sanitaria y proporciona soluciones que permiten obtener mejores resultados para los pacientes y las entidades que los tratan.

## Mirando al futuro

Los productos de Allied Telesis optimizan sus inversiones en tecnología al integrarse totalmente con los sistemas y aplicaciones existentes. A medida que se desarrollan nuevas aplicaciones empresariales, su red puede adaptarse fácilmente, ya que nuestros productos le ayudan a construir una infraestructura más eficiente y progresiva.

A medida que se implementan nuevas e interesantes tecnologías en la prestación de cuidados continuos, los productos de Allied Telesis se mantienen a la vanguardia en el suministro de una infraestructura de red que facilite el acceso de los pacientes a los mejores cuidados.



### Acceso imparable a la red

Proporcione acceso en cualquier momento garantizando que su red esté siempre en funcionamiento, incluso en caso de fallo del enlace o del equipo de red, sin necesidad de intervención humana.



### La red de autodefensa

Nuestra seguridad de borde inteligente protege su red cableada e inalámbrica de las amenazas poniendo automáticamente en cuarentena los dispositivos sospechosos, creando así un entorno seguro para el almacenamiento de datos confidenciales de los pacientes.



### Gestión WAN fiable y sencilla

Seleccione la ruta óptima entre el edificio principal y los emplazamientos remotos para obtener un mejor rendimiento y un menor coste.



### Wi-Fi sin compromisos

Garantice conexiones Wi-Fi fiables y de alto rendimiento dondequiera que se necesiten y proporcione soporte de alta densidad de dispositivos para equipos médicos y acceso de cuidadores.



### Gestión de redes más fácil

Automatice la gestión de su red utilizando una única herramienta inteligente para añadir inteligencia y seguridad con una gestión sencilla y para reducir los riesgos y los costes de asistencia al tiempo que permite la asistencia remota en el sitio.

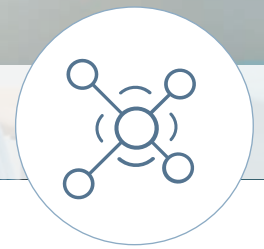


### Seguridad por vídeo digital

Cartera de productos dedicada al transporte seguro y fiable de secuencias de vídeo a través de la red IP.



## ACCESO IMPARABLE A LA RED



La transición del papel a la historia clínica electrónica concentra el flujo de información en la infraestructura informática. Al mismo tiempo, el desarrollo de un sistema sanitario integrado requiere una comunicación ininterrumpida entre distintos hospitales y con clínicas y centros remotos.

A medida que esta transición se implanta plenamente, la alta disponibilidad y accesibilidad de la infraestructura informática se convierte en vital para todo el ecosistema sanitario.

La solución de acceso a la red imparable de Allied Telesis se ha desarrollado para garantizar que cualquier red sea capaz de sobrevivir a múltiples fallos sin dejar de mantener la conectividad en una amplia gama de arquitecturas de red, proporcionando así una solución de alta disponibilidad.

Dentro de un sistema complejo, la alta disponibilidad tiene que considerar múltiples factores, donde la alta disponibilidad informática es sólo uno de los factores.

### Alimentación de equipos de red

En el hospital, la continuidad del suministro eléctrico debe garantizarse mediante una batería de reserva y un generador automático. Los equipos de red pueden confiar en esta única fuente de alimentación, pero también deben estar diseñados para resistir en caso de fallo de la fuente de alimentación interna.

Allied Telesis propone toda una serie de equipos con un sistema de fuente de alimentación redundante para que, si falla una de las dos unidades, el equipo pueda seguir funcionando a pleno rendimiento, incluso en caso de apagón.

### Fuente de alimentación simplificada para dispositivos de red

Muchos dispositivos de los hospitales están conectados directamente a conmutadores de red. El uso de equipos con PoE para alimentar estos dispositivos permite además suministrar energía de reserva al conmutador y devolver energía a los dispositivos conectados.



## VCSTACK

VCStack y la agregación de enlaces proporcionan una solución en la que los recursos de red se reparten entre los miembros del chasis virtual, lo que garantiza la resistencia de los dispositivos y las rutas.

VCStack puede extenderse a largas distancias, con conectividad de fibra. Una VCStack de larga distancia es perfecta para entornos de red distribuidos o soluciones de duplicación de datos.

### Apilamiento virtual

Se pueden conectar varios conmutadores Allied Telesis para formar un único conmutador virtual. En conjunto, la tecnología de apilamiento de chasis virtual con agregación de enlaces proporciona una solución resistente capaz de sobrevivir a un fallo de enlace o de equipo.

### Protección de anillos

Cuando la distancia entre los dispositivos es grande, una topología en anillo para la red es la solución óptima. Allied Telesis proporciona protocolos de protección de anillo para salvar su red de fallos de enlace al tiempo que proporciona una infraestructura resistente.

### Núcleo redundante y recuperación en caso de catástrofe

En el caso de que se requiera un mayor grado de resiliencia, Allied Telesis también puede proporcionar conmutadores de núcleo con una configuración óptimamente redundante para una arquitectura de recuperación ante desastres. Esto se consigue mediante una pila virtual con dispositivos de red ubicados en diferentes salas o incluso edificios.

## EPSRING

Las soluciones Allied Telesis Ethernet Protection Switched Ring (EPSRing) proporcionan núcleos de red distribuidos de alto rendimiento, alta fiabilidad y flexibles y escalables.

El tiempo de recuperación en caso de caída de enlaces o nodos es extremadamente rápido -de hasta 50 ms-, lo que hace que esta solución sea ideal para la prestación de una red sanitaria con servicios de voz, vídeo y datos.





## CIBERSEGURIDAD DE LA RED



Los ciberataques a instituciones médicas van en aumento y son cada vez más frecuentes. El acceso no autorizado a los datos de los pacientes, el ransomware y otros tipos de ataques afectan a las operaciones diarias y suponen un grave riesgo para la privacidad de los pacientes.

Mantener la seguridad de las conexiones internas a los recursos al tiempo que se permite el acceso a Internet al personal y los invitados es obligatorio para el sector sanitario.

Los modelos de seguridad tradicionales que se centran en evitar que los ataques entren en la red no son suficientes, ya que los ataques pueden venir fácilmente desde dentro. Por ejemplo, un portátil, una tableta o un dispositivo IoT infectados y conectados a la red pueden suponer una grave amenaza.

Paralelamente, los atacantes han aumentado la sofisticación de sus métodos y ahora las amenazas se presentan de tantas formas que mantener una red segura pero eficaz se ha convertido en un reto que requiere mucho tiempo y dinero.

Mientras que el enfoque tradicional basado en cortafuegos es eficaz para detectar y bloquear amenazas y virus procedentes de Internet, muestra sus limitaciones si el ataque procede del interior de la red. En este caso, el ataque se propagará hacia el este/oeste de la red (es decir, de un dispositivo conectado a otro), donde sólo podrá ser detectado por el cortafuegos una vez que la amenaza intente cruzar la frontera con Internet. Una vez detectada la amenaza, se puede alertar a un administrador y pedirle que inicie el proceso de corrección.

Por desgracia, este proceso depende de los recursos humanos, con un tiempo de reacción que puede ser de minutos a horas o incluso días, dependiendo de la disponibilidad de recursos y de las habilidades personales.

# 66%

de los pacientes les preocupa la privacidad cuando la información sanitaria se intercambia electrónicamente.

Fuente: <https://dashboard.healthit.gov>

# AMF-SEC

Para habilitar una red de autodefensa que ayude a las organizaciones a evitar pérdidas de tiempo e interrupciones innecesarias de los servicios de red, el controlador AMF-Sec es clave para nuestra innovadora y galardonada solución AMF Security.

## Características principales:

- Compatible con OpenFlow v1.3
- Adecuado tanto para redes cableadas como inalámbricas
- Integración con aplicaciones empresariales para ahorrar tiempo y dinero
- Se integra con productos de seguridad para detectar amenazas
- El motor del Adaptador de Aislamiento Inteligente bloquea automáticamente las amenazas
- Escalable: añade más aplicaciones empresariales para obtener más valor

## La red de autodefensa

La solución Self-Defending Network ofrece un enfoque integrado de la seguridad de la red que automatiza las operaciones manuales de TI y protege de las amenazas procedentes de dispositivos de acceso tanto cableados como inalámbricos.

Sin necesidad de agentes ni software para los puntos finales, la red de autodefensa es capaz de responder automáticamente a las amenazas una vez identificadas.

Los dispositivos de seguridad y cortafuegos identifican las amenazas y, a continuación, el motor inteligente que implementa la tecnología Isolation Adapter integrada en nuestro controlador AMF-Sec responde inmediatamente para aislar la parte afectada de la red y poner en cuarentena el dispositivo sospechoso. Se pueden aplicar medidas correctoras para que el dispositivo pueda volver a conectarse a la red con una interrupción mínima. Las respuestas son configurables, y un registro exhaustivo proporciona una pista de auditoría clara.

Para habilitar una red de autodefensa que ayude a las organizaciones a evitar pérdidas de tiempo e interrupciones innecesarias de los servicios de red, el controlador AMF-Sec es clave para nuestra innovadora y galardonada solución AMF Security.





## GESTIÓN WAN FIABLE Y SENCILLA



El enfoque centrado en el paciente del sector sanitario sigue la dirección de la descentralización de servicios, en la que los centros asistenciales se ubican en emplazamientos locales. Estos centros locales deben estar conectados a la red principal como si estuvieran en el mismo edificio del hospital, con un acceso seguro y fiable.

Para la infraestructura de red, la calidad de la conexión remota no es un asunto trivial y debe desarrollarse cuidadosamente para mantener el mismo nivel de calidad disponible en el hospital principal. Los principales problemas de la conexión a distancia son la disponibilidad, el coste y la seguridad.

Existen principalmente dos opciones para interconectar sitios remotos: una conexión dedicada alquilada con un Acuerdo de Nivel de Servicio (SLA) específico, o un enlace virtual privado a través de una red pública, cableada o inalámbrica.

La primera solución es más cara pero garantiza el ancho de banda y la disponibilidad del enlace. La segunda solución es menos cara pero no garantiza el rendimiento ni la disponibilidad.

Para ofrecer un servicio de alta disponibilidad, la mejor opción es conectar los sitios remotos mediante múltiples enlaces y dividir el tráfico entre ellos en función de la aplicación, el coste del enlace y otros parámetros. El uso de múltiples enlaces permite disponer de una copia de seguridad en caso de fallo y da lugar a una solución de alta disponibilidad.

Para proteger los datos entre el centro remoto y el hospital principal, siempre es necesario un enlace VPN seguro. La gestión de múltiples enlaces suele requerir una gestión compleja, que implica en gran medida al departamento informático para cualquier cambio necesario.

### Gestión autónoma y segura de la WAN

Disponer de varias conexiones con distintos rendimientos y costes requiere una atención continua. Allied Telesis Software Defined WAN (SD-WAN) simplifica el control de las conexiones de sitios remotos con una herramienta de gestión autónoma y centralizada.

SD-WAN Orchestrator forma parte de Vista Manager y gestiona de forma centralizada las conexiones de las sucursales para una entrega de aplicaciones fiable y segura. Con él puede establecer métricas de rendimiento aceptables, optimizar y equilibrar automáticamente la carga de las aplicaciones y supervisar fácilmente el rendimiento de la WAN.

SD-WAN, con Allied Telesis Application-Aware Firewalls, proporciona una solución integrada de seguridad WAN y gestión del tráfico WAN en un único dispositivo.

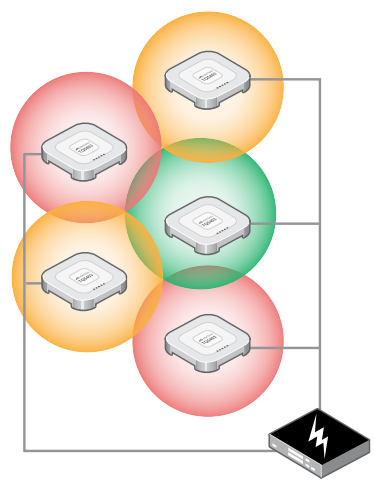
## SD-WAN

Cree redes WAN más seguras y de mayor rendimiento, y mejore la productividad al tiempo que reduce la complejidad y los costes.

La automatización de la WAN reduce la necesidad de recursos cualificados en la sucursal al centralizar la optimización del rendimiento y la supervisión para facilitar la gestión de la WAN.



## CONECTIVIDAD INALÁMBRICA FIABLE



Allied Telesis Autonomous Wave Control (AWC) es una tecnología de red avanzada que utiliza la Inteligencia Artificial (IA) para ofrecer mejoras significativas en la conectividad y el rendimiento de las redes inalámbricas, al tiempo que reduce los costes de despliegue y funcionamiento.

AWC supervisa el entorno Wi-Fi y optimiza la cobertura inalámbrica para ofrecer el mejor rendimiento posible en cualquier condición.

Además de que el personal médico lleve dispositivos móviles de una habitación a otra, un gran número de dispositivos médicos, como monitores de diagnóstico por imagen y wearables, necesitan una red inalámbrica estable para proporcionar información o acceder a ella en tiempo real.

Por motivos de seguridad, los dispositivos con acceso a los datos de los pacientes exigen que el usuario vuelva a autenticarse cuando se interrumpe la conexión de red. Por eso, una solución inalámbrica sin itinerancia ininterrumpida se considera un valor añadido para el mercado sanitario. Los dispositivos médicos también utilizan una conexión inalámbrica como enlace de reserva en caso de que falle la conexión por cable, lo que añade fiabilidad a toda la solución de red.

Aunque seguir la norma técnica inalámbrica mejora el rendimiento general, sigue habiendo limitaciones que requieren profundos conocimientos técnicos para implantar una red inalámbrica estable. En una red inalámbrica, la desconexión del cliente y la lentitud de la comunicación son problemas inalámbricos típicos causados normalmente por uno o varios problemas técnicos. Las interferencias entre canales de radio, las fuentes inalámbricas externas que no están bajo el control de TI y la intensidad de la señal de los puntos de acceso son las principales razones de los problemas inalámbricos.

En un entorno sanitario dinámico, es crucial disponer de una red continua con supervisión y recursos informáticos cualificados que mantengan la instalación bajo control para ofrecer un valioso servicio inalámbrico.

### Wi-Fi sin compromisos

La solución Wi-Fi No Compromise de Allied Telesis garantiza conexiones inalámbricas fiables y de alto rendimiento en todos los lugares donde se necesitan sin aumentar los recursos cualificados.

Al analizar las lagunas de cobertura de la señal y las interferencias de los puntos de acceso Wi-Fi, el Control Autónomo de Onda (AWC) proporciona automáticamente una experiencia inalámbrica de alta calidad. Esto le permite reducir su dependencia de ingenieros de red cualificados y disfrutar de menores costes operativos.

AWC Channel Blanket (AWC-CB) permite controlar puntos de acceso híbridos que proporcionan simultáneamente conectividad Wi-Fi monocanal y multicanal. Channel Blanket es la mejor tecnología de radio para proporcionar una conexión sin fisuras a dispositivos personales y médicos críticos mientras se desplazan por el hospital.

Los pulsómetros, los sensores de glucosa en sangre y las camas inteligentes son sólo algunos de los dispositivos móviles que necesitan una conectividad inalámbrica fiable para ofrecer la mejor atención al paciente. AWC-CB también permite el seguimiento de la ubicación de los dispositivos para encontrar fácilmente los equipos y reducir la pérdida de dispositivos costosos.

## GESTIÓN DE RED SIMPLIFICADA



El aumento de la complejidad de la red eleva significativamente la demanda de recursos especializados y de gestión de la red. La implantación de una solución de automatización simplifica y abarata la gestión de la red.

Vista Manager EX es un enfoque modular de la gestión de redes. Cuenta con un panel de control que muestra los detalles de la red, el estado y los eventos en un mapa topológico, y destaca los problemas críticos para minimizar el tiempo de reacción y ayudar a resolver los problemas de manera oportuna sin necesidad de ingenieros de red altamente cualificados.

Una serie de módulos para controlar la red cableada, los dispositivos inalámbricos, el enlace WAN y las herramientas de automatización facilitan la conexión en red y modularizan la solución.

### Autonomous Management Framework Plus (AMF Plus)

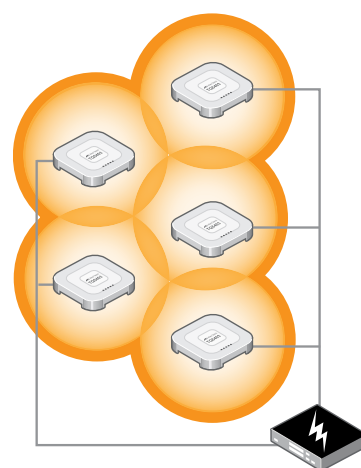
Reduzca los costes operativos de la red con la inteligencia y automatización añadidas de la gestión centralizada.

Los servicios automatizados que incluyen actualizaciones de firmware, copias de seguridad, recuperación y aprovisionamiento sin intervención son sólo algunas de las funciones de AMF Plus para minimizar los recursos necesarios para gestionar una red sanitaria compleja.

### Control Autónomo de Ondas (AWC) - módulo adicional

Analice y optimice el rendimiento de redes inalámbricas complejas. Instale y olvídense de su red inalámbrica con una herramienta autónoma que analiza los patrones de tráfico y configura automáticamente los puntos de acceso para satisfacer la demanda.

## AWC-CB



Allied Telesis AWC Channel Blanket (AWC-CB) es la solución de canal único para el punto de acceso inalámbrico Allied Telesis.

Todos los puntos de acceso que son miembros de la misma manta operan en el mismo canal. El controlador inteligente AWC-CB gestiona las interferencias y el acceso de los clientes.

Junto con el enfoque multicanal tradicional, proporciona una solución de acceso inalámbrico completa para cualquier entorno.

## AMF PLUS

Allied Telesis Autonomous Management Framework Plus (AMF Plus) es una plataforma de gestión de red escalable.

Es compatible con los productos de conmutación, cortafuegos e inalámbricos de Allied Telesis, así como con una amplia gama de dispositivos de terceros, como cámaras de videovigilancia y teléfonos IP, para la automatización de redes.

## WAN definida por software (SD-WAN)

Gestione de forma centralizada y optimice automáticamente el tráfico entre sucursales con SD-WAN. Consulte la sección "Gestión WAN fiable y sencilla" para obtener más detalles.

## Protocolo simple de gestión de redes (SNMP) - módulo adicional

Detecte y gestione automáticamente una amplia gama de dispositivos en un entorno de varios proveedores dentro de Vista Manager EX con el complemento SNMP.

Las diferentes vistas de la red permiten la visibilidad de la forma que prefiera. Amplíe la supervisión de la red con notificaciones y alertas automatizadas para una gestión proactiva.

## VISTA MANAGER™

Vista Manager EX ofrece una supervisión de última generación y crea automáticamente un mapa topológico completo de conmutadores, cortafuegos y puntos de acceso inalámbricos.

Con la creación y asignación simplificadas de VLAN, el análisis de tráfico y las operaciones SD-WAN, la gestión sin esfuerzo de todos los dispositivos de red es ahora una realidad.

## VISTA MANAGER™ MINI

Una versión de Vista Manager integrada en nuestros principales conmutadores y cortafuegos Allied Telesis ofrece una solución de gestión de red fácil y rápida para instalaciones pequeñas y medianas.

Sin necesidad de herramientas externas, Vista Manager Mini proporciona un fácil acceso a la potencia de AMF Plus y AWC para la gestión cableada e inalámbrica.





## SEGURIDAD FÍSICA



Los sistemas de control de acceso a edificios ayudan a proteger el entorno físico del hospital, pero no totalmente. Esto se debe al gran volumen de personal que trabaja en el hospital, y de pacientes y visitantes que entran y salen, lo que dificulta un control total.

Por lo tanto, se necesita un sistema de videovigilancia avanzado para controlar tanto el interior como el exterior del centro médico y verificar lo que ocurre en zonas específicas.

### Seguridad por vídeo digital

En cualquier implementación de videovigilancia, todos los dispositivos de almacenamiento, cámaras de vigilancia y sistemas de gestión de vídeo dependen de la infraestructura de red para transportar el vídeo.

Es necesario tener en cuenta el efecto de la videovigilancia en la red para evitar un impacto negativo en el rendimiento de otros servicios.

El tráfico generado por las cámaras IP, en combinación con el tráfico existente en los enlaces principales de servicios, debe calcularse de antemano para garantizar correctamente una transmisión fluida y fiable.

La parte clave de la instalación se alimenta mediante PoE con un consumo de energía que depende de múltiples factores como el tipo de cámara y los accesorios (calefactor, motores, etc.). En la fase de diseño de la red, es necesario seleccionar los conmutadores de acceso conectados con las cámaras IP para que sean capaces de suministrar energía suficiente para alimentar todas las cámaras conectadas.

### Compatibilidad con ONVIF

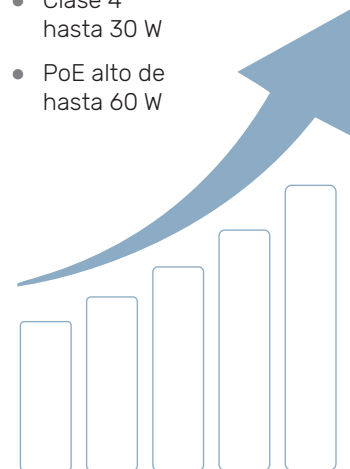
Allied Telesis ha simplificado la instalación y configuración de redes de videovigilancia añadiendo soporte para protocolos ONVIF a nuestra solución de automatización de redes AMF Plus. Esto permite un despliegue, gestión y mantenimiento más sencillos de las cámaras de seguridad remotas.

### Integración de hitos

El complemento de integración de Milestone es un complemento para XProtect VMS de Milestone System que permite el control directo de cámaras IP conectadas a conmutadores Allied Telesis. El plug-in simplifica la gestión remota de cámaras para el personal de seguridad mediante la integración de tareas administrativas comunes en la interfaz gráfica de XProtect, ahorrando tiempo y costosas llamadas.

### clase PoE

- Clase 0 hasta 15 W
- Clase 1 hasta 4 W
- Clase 2 hasta 7 W
- Clase 3 hasta 15 W
- Clase 4 hasta 30 W
- PoE alto de hasta 60 W



## ACERCA DE ALLIED TELESIS

Durante más de 30 años, Allied Telesis ha estado proporcionando conectividad fiable e inteligente para todo, desde organizaciones empresariales hasta complejos proyectos de infraestructuras críticas en todo el mundo.

En un mundo que avanza hacia las ciudades inteligentes y la Internet de las cosas, las redes deben evolucionar rápidamente para hacer frente a los nuevos desafíos. Las tecnologías inteligentes de Allied Telesis, como Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) y Enterprise SDN, garantizan que la evolución de la red pueda seguir el ritmo y ofrecer soluciones eficientes y seguras para personas, organizaciones y "cosas", tanto ahora como en el futuro.

Allied Telesis es reconocida por innovar la forma en que se prestan y gestionan los servicios y las aplicaciones, lo que se traduce en un aumento del valor y una reducción de los costes operativos.

Visítenos en línea en [alliedtelesis.com](http://alliedtelesis.com).

