DOCUMENTO TÉCNICO

Guía rápida de las fichas técnicas de Axis

Homologaciones, certificaciones y protocolos

Mayo 2022

Índice

1 Introducción

Axis Communications cumple las normas aplicables del sector y las normativa de cumplimiento obligado en todos los productos que lanza al mercado. Este documento complementa las fichas técnicas de Axis con definiciones y descripciones breves de las siglas, homologaciones, certificaciones y protocolos que figuran en las mismas.

Este documento ofrece información sobre las secciones de las fichas técnicas resaltadas y ampliadas a continuación.

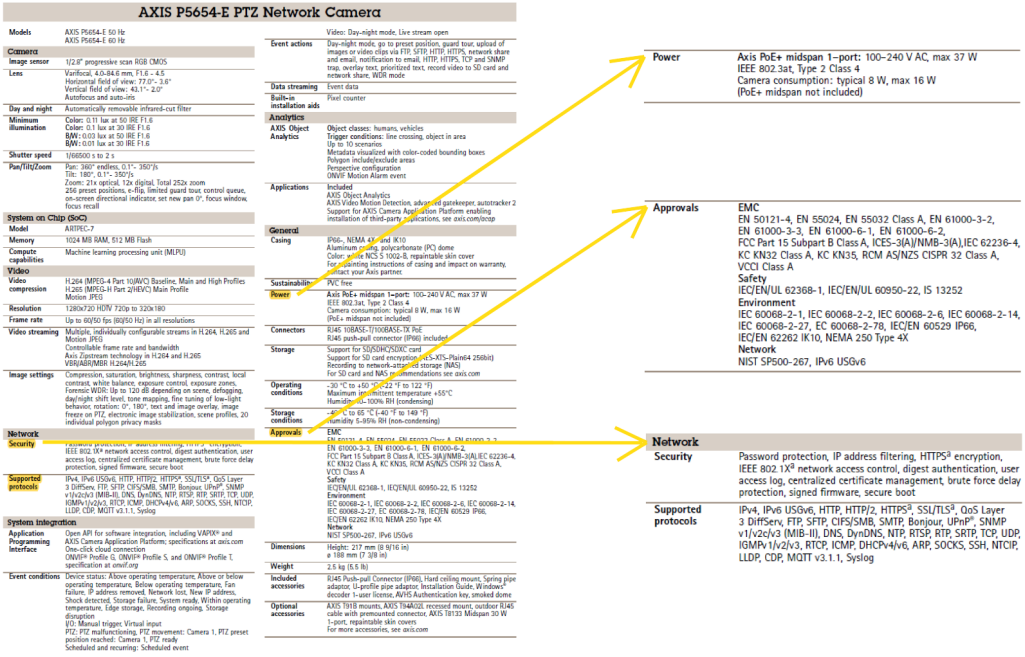

Figure 1. Apartados de la hoja de datos de Axis resaltados en los que se centra este documento.

2 Homologaciones

El apartado de homologaciones de las fichas técnicas de Axis se refiere al cumplimiento de diversas normas. El apartado se divide normalmente en subsecciones dedicadas a CEM, Seguridad, Medio Ambiente, Red y Otros, donde "Otros" puede referirse a la protección contra explosiones o a la seguridad en el control de acceso. También puede haber una subsección para las homologaciones que afecten al midspan, en aquellos casos en los que se venda un midspan con el producto.

2.1 CEM (compatibilidad electromagnética)

Todos los fabricantes de vídeo en red deben declarar la CEM de sus productos de vídeo en red. En determinadas circunstancias, los fabricantes puede certificar directamente la compatibilidad, pero la mayoría recurre a laboratorios de pruebas acreditados, que emiten un informe para avalar el cumplimiento. Las homologaciones de CEM se basan en dos partes: emisiones e inmunidad.

La emisión se refiere a la capacidad del equipo para funcionar satisfactoriamente sin emitir demasiada energía electromagnética que pueda perturbar a otros equipos ubicados en ese entorno.

La inmunidad es un indicador de la capacidad de los productos electrónicos para tolerar la influencia de fenómenos electromagnéticos y la energía eléctrica (radiada o conducida) de otros productos electrónicos. En Europa, la CEM está incluida en la marca CE, que a su vez está recogida en la legislación sobre armonización de la UE.

Las normas que se enumeran a continuación definen los límites y métodos de prueba de emisiones electromagnéticas, así como las pruebas de inmunidad. Como no existe una única prueba que cubra el cumplimiento globalmente, pueden existir diferentes códigos para diferentes regiones o aplicaciones.

2.1.1 Normas aplicables a los equipos de tecnología de la información (ETI)

Estas normas se aplican a equipos multimedia (MME) con una tensión de CA o CC que no supera los 600 V. Aquí equipos multimedia (MME) hace referencia a equipos de tecnología de la información (ETI), equipos de audio, equipos de vídeo, equipos de radiodifusión y equipos de control de iluminación para fines recreativos.

- EN 55032 Clase A: norma sobre emisiones (comercial, industrial, empresarial), armonizada con las normas internacionales
- EN 55032 Clase B: norma sobre emisiones (residencial), armonizada con las normas internacionales
- EN 55035: norma sobre inmunidad, armonizada con las normas internacionales

2.1.2 Normas armonizadas por país o región

- EN 61000-6-1 y EN 61000-6-2: normas de cumplimiento genéricas (Europa)
- FCC Parte 15 Subparte B Clase A y B: FCC dicta reglas y normativas para dispositivos de telecomunicaciones en relación con las emisiones, no sobre inmunidad (Estados Unidos)
- ICES-3(A y B)/NMB-3(A y B) (Canadá)
- VCCI Clase A y B (Japón)
- KS C 9832 Clase A y B, KS C 9835, KS C 9547, KS C 9815 (Corea)
- RCM AS/NZS CISPR 32 Clase A y B (Australia/Nueva Zelanda)

2.1.3 Normas adicionales por aplicación o producto

- EN 50121-4, IEC 62236-4: ofrece criterios de rendimiento para equipos de señalización y telecomunicaciones que podrían interferir con otros equipos en entornos ferroviarios.
- EN 50130-4: se aplica a los componentes de sistemas de alarma, como sistemas de control de acceso, sistemas CCTV, sistemas de detección y alarmas contra incendios, sistemas de alarma silenciosa, sistemas de alarma contra intrusos y sistemas de alarma sociales.

2.2 Seguridad

- Directiva sobre baja tensión (2014/35/UE): proporciona objetivos generales para la seguridad de los equipos. Garantiza que los productos se puedan usar de forma segura sin riesgo de que se produzcan lesiones físicas o daños materiales.

- IEC/EN/UL 62368-1: cumplimiento por parte de cámaras de red, codificadores y fuentes de alimentación de los requisitos dispuestos para reducir los riesgos de incendio, descarga eléctrica o lesión en cualquier persona que pudiera entrar en contacto con el equipo.
- IEC/EN/UL 60950-22: requisitos de seguridad específicos para productos de exterior y carcasas de exterior
- IEC/EN 62471-1: límites de exposición a lámparas y sistemas de lámparas para garantizar la seguridad fotobiológica y evitar riesgos para los ojos y la piel
- EN/UL/CSA 60065: se aplica a los aparatos electrónicos diseñados para recibir corriente de la red eléctrica, de un equipo de abastecimiento, de baterías o de una fuente de alimentación remota, y que tienen por finalidad recibir, generar, grabar o reproducir audio, vídeo o señales asociadas.
- IS 13252: cumplimiento por parte de cámaras de red, codificadores y fuentes de alimentación de los requisitos específicos de India dispuestos para reducir los riesgos de incendio, descarga eléctrica o lesión en cualquier persona que pudiera entrar en contacto con el equipo.

2.3 Entorno

2.3.1 Clasificación IP

La IEC (International Electrotechnical Commission; Comisión Electrotécnica Internacional), en su norma IEC 60529, define las clasificaciones IP (protección contra entrada o protección internacional) con un código de dos dígitos. Dicho código define el nivel de protección de los aparatos eléctricos contra la entrada de objetos sólidos o polvo, el contacto accidental y el agua.

Tabla 2.1 Clasificaciones IP - primer dígito después de IP: objetos sólidos extraños

Nivel	Protección contra	Eficaz contra
0	Sin protección	Sin protección
1	Objetos de más de 50 mm	Superficie extensa del cuerpo, como el dorso de la mano, pero sin protección contra el contacto deliberado con una parte del cuerpo.
2	Objetos de más de 12,5 mm	Los dedos u otros objetos pueden penetrar hasta 80 mm, siempre y cuando estén a salvo de piezas peligrosas. Los objetos con un diámetro de 12,5 mm no pueden penetrar totalmente.
3	Objetos de más de 2,5 mm	Objetos como herramientas y alambres gruesos no pueden penetrar de ninguna forma.
4	Objetos de más de 1 mm	Objetos como alambres y tornillos no pueden penetrar de ninguna forma.
5	Protección contra el polvo	No se evita por completo la penetración del polvo, aunque no se produce en un volumen suficiente como para impedir que el equipo funcione correctamente.
6	Estanco al polvo	Sin penetración de polvo.

Tabla 2.2 Clasificaciones IP - segundo dígito después de IP: líquidos

Nivel	Protección contra	Eficaz contra
0	Sin protección	Sin protección especial
1	Goteo de agua	El goteo de agua (gotas que caen verticalmente) no tiene efectos perjudiciales.
2	Goteo de agua con una inclinación de hasta 15°	El goteo de agua en vertical no tiene efectos perjudiciales si la carcasa se inclina en un ángulo de hasta 15° con respecto a su posición normal.
3	Pulverización de agua	La pulverización de agua a un ángulo de hasta 60° con respecto a la línea vertical no tiene efectos perjudiciales.
4	Salpicadura de agua	El agua proyectada contra la carcasa desde cualquier dirección no tiene efectos perjudiciales.
5	Agua a presión	Los chorros de agua proyectados desde una boquilla contra la carcasa desde cualquier dirección no tienen efectos perjudiciales.
6	Agua a alta presión	Los oleajes intensos o el agua proyectada en chorros potentes no pueden penetrar en la carcasa en un volumen perjudicial.
7	Inmersión breve en agua	No resulta posible la penetración de un volumen perjudicial de agua cuando se sumerge la carcasa en agua en unas determinadas condiciones de presión y tiempo.
8	Inmersión continua en agua	El equipo es apto para una inmersión continua en agua en determinadas condiciones, especificadas por el fabricante. Las condiciones deben ser más difíciles que para IPX7 (véanse las entradas anteriores).
9	Agua de limpieza a alta presión y con chorro de vapor	El agua dirigida hacia la carcasa desde cualquier ángulo a muy alta presión no tiene efectos perjudiciales.

2.3.2 Otras normas IEC relevantes

- IEC 60068-2 es una norma para realizar pruebas ambientales de equipos y productos electrónicos que tiene por finalidad evaluar su capacidad de ofrecer resultados en condiciones ambientales como el frío y el calor seco extremos. Los procedimientos que se indican a continuación con respecto a esta norma suelen estar pensados para objetos que alcanzan una temperatura estable durante el procedimiento de prueba.
  - IEC 60068-2-1: frío
  - IEC 60068-2-2: calor seco
  - IEC 60068-2-6: vibración (continua)
  - IEC 60068-2-14: cambio de temperatura
  - IEC 60068-2-27: impactos
  - IEC 60068-2-30: calor húmedo (cíclico)
  - IEC 60068-2-64: vibración (ancho de banda aleatorio)
  - IEC 60068-2-78: calor húmedo (estable)

- IEC 60825 Clase I: norma concebida para asegurar que el tipo de láser empleado en el módulo de enfoque de láser resulte seguro en todo tipo de condiciones de uso normal.

2.3.3 Clasificación NEMA

NEMA (National Electrical Manufacturers Association) es una asociación estadounidense que crea normas para carcasas de equipos eléctricos. NEMA ha presentado su propia norma, NEMA 250, a nivel mundial. NEMA también ha adoptado y publicado una norma IP de armonización, ANSI/IEC 60529, por medio del American National Standards Institute (ANSI).

NEMA 250 comprende la protección contra la entrada de materias, pero también otros factores como la resistencia a la corrosión, el rendimiento y los detalles de construcción. Por ello, el tipo NEMA es comparable a IP, si bien IP no es comparable a NEMA.

Las normas de UL, UL 50 y UL 50E, se basan en la norma NEMA 250. NEMA permite la autocertificación, mientras que UL exige que los productos superen unas pruebas e inspecciones de terceros para obtener el nivel de cumplimiento.

Tabla 2.3 Clasificaciones NEMA para carcasas en lugares no peligrosos

NEMA	Clasificación IP equivalente	Interiores	Exteriores	Protección contra
Tipo 1	IP10	X		Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión). Sin protección contra líquidos.
Tipo 3	IP54	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo arrastrado por el viento). Entrada de agua (lluvia, aguanieve, nieve). No resultará dañado por la formación de hielo en el exterior de la carcasa.
Tipo 3R	IP14	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión). Entrada de agua (lluvia, aguanieve, nieve). No resultará dañado por la formación de hielo en el exterior de la carcasa.
Tipo 3S	IP54	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo arrastrado por el viento). Entrada de agua (lluvia, aguanieve, nieve). Los mecanismos externos permanecen operativos cuando se cargan de hielo.
Tipo 4	IP56	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo arrastrado por el viento). Entrada de agua (lluvia, aguanieve, nieve, salpicaduras de agua y chorro de agua con manguera). No resultará dañado por la formación de hielo en el exterior de la carcasa.

Tabla 2.3. Clasificaciones NEMA para carcasas en lugares no peligrosos (Continuación)

NEMA 4X	IP56	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo arrastrado por el viento). Entrada de agua (lluvia, aguanieve, nieve, salpicaduras de agua y chorro de agua con manguera). Proporciona un nivel de protección adicional contra la corrosión. No resultará dañado por la formación de hielo en el exterior de la carcasa.
Tipo 6	IP67	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión). Entrada de agua (agua dirigida con una manguera y entrada de agua durante una inmersión temporal puntual a poca profundidad). No resultará dañado por la formación de hielo en el exterior de la carcasa.
Tipo 6P	IP67	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión). Entrada de agua (agua dirigida con una manguera y entrada de agua durante una inmersión prolongada a poca profundidad). Proporciona un nivel de protección adicional contra la corrosión. No resultará dañado por la formación de hielo en el exterior de la carcasa.
Tipo 12	IP52	X		Sin paneles de desmontaje rápido. Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo en circulación, pelusa, fibras y residuos proyectados). Entrada de agua (goteo y salpicaduras ligeras).
Tipo 12K	IP52	X		Con paneles de desmontaje rápido. Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo en circulación, pelusa, fibras y residuos proyectados). Entrada de agua (goteo y salpicaduras ligeras).
Tipo 13	IP54	X		Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo en circulación, pelusa, fibras y residuos proyectados). Entrada de agua (goteo y salpicaduras ligeras). Pulverizaciones, salpicaduras y escapes de aceite y refrigerantes no corrosivos.

NEMA TS 2 es una guía de diseño que se aplica a equipos de señalización del tráfico.

2.3.4 Clasificación IK

Las clasificaciones IK pueden consultarse en IEC/EN 62262, una norma internacional que especifica los grados de protección frente a impactos mecánicos externos. Aprobada inicialmente en 1994 como norma europea (EN 50102), fue adoptada como norma internacional en 2002.

Muchos fabricantes optan por someter a pruebas la parte más débil de un producto para garantizar su robustez a lo largo de toda su vida útil.

Nivel	IK01	IK02	IK03	IK04	IK05	IK06	IK07	IK08	IK09	IK10	IK10+*
Energía del impacto (julios)	0,14	0,2	0,35	0,5	0,7	1	2	5	10	20	50*

Masa (kg)	<0,2	<0,2	0,2	0,2	0,2	0,5	0,5	1,7	5	5	
Altura de caída (mm)	56	80	140	200	280	400	400	300	200	400	

* Impacto de hasta 50 J. El fabricante debe especificar la energía, el peso y la altura de caída del elemento que impacta.

2.4 Otras homologaciones

2.4.1 Protección contra explosiones

- IEC/EN/UL/SANS/CSA 60079-0: requisitos generales para construcción, pruebas y marcado de equipos y componentes antideflagrantes diseñados para emplearse en atmósferas explosivas.
- IEC/EN/UL/SANS/CSA 60079-1: requisitos específicos para la construcción y pruebas de equipos eléctricos con el tipo de carcasas ignífugas de protección "d", diseñados para utilizarse en atmósferas con gases explosivos.

2.4.2 Homologaciones para midspans

En aquellos casos en los que se incluye un midspan con el producto, las homologaciones relacionadas de manera específica con el midspan se indican en este apartado de la ficha técnica. Se pueden obtener explicaciones en los apartados anteriores de este documento.

2.4.3 Seguridad en el control de acceso

- UL 294: define los requisitos relativos a la construcción, el rendimiento y el funcionamiento de sistemas de control de acceso.

3 Certificaciones

Cuando se instala una cámara en un entorno potencialmente explosivo, la carcasa debe cumplir unas normas de seguridad muy concretas. Debe proteger el entorno de posibles fuentes de deflagración presentes en la cámara y en otros equipos.

Los productos europeos deben cumplir la directiva ATEX, y la norma internacional correspondiente es IECEx. En Norteamérica se utilizan principalmente las clases/divisiones del NFPA70 (National Electric Code, NEC) y del CSA C22.1 (Canadian Electric Code, CEC) en lugar del sistema de zona descrito en ATEX e IECEx.

Tabla 3.1 Clasificaciones de protección contra explosiones

Clase / División	Atmósfera	Definición	Zona (IECEx y ATEX)
Clase I / División 1	Gas	Área donde la mezcla explosiva está presente de forma continua o presente durante largos periodos de tiempo.	Zona 0

Tabla 3.1. Clasificaciones de protección contra explosiones (Continuación)

Clase I / División 1	Gas	Área donde podría formarse una mezcla explosiva durante el funcionamiento normal.	Zona 1
Clase I / División 2	Gas	Área en la que es poco probable que se forme una mezcla explosiva durante el funcionamiento normal y, en caso de producirse, solo existirá durante un breve periodo de tiempo.	Zona 2
Clase II / División 1	Polvo	Área donde la mezcla explosiva está presente de forma continua o presente durante largos periodos de tiempo.	Zona 20
Clase II / División 1	Polvo	Área donde podría formarse una mezcla explosiva durante el funcionamiento normal.	Zona 21
Clase II / División 2	Polvo	Área en la que es poco probable que se forme una mezcla explosiva durante el funcionamiento normal y, en caso de producirse, solo existirá durante un breve periodo de tiempo.	Zona 22

4 Alimentación

4.1 Clases de Power over Ethernet (PoE)

Las clases de PoE garantizan una distribución eficiente de la energía al especificar la cantidad de energía que necesitará un dispositivo alimentado (DA).

Tabla 4.1 Clases de PoE

Clasificación	**Tipo**	**Nivel de potencia garantizado en el equipo de fuente de alimentación (EFA)**	**Nivel de alimentación máximo empleado por el dispositivo alimentado (DA)**
0	Tipo 1, 802.3af	15,4 W	0,44 W - 12,95 W
1	Tipo 1, 802.3af	40,0 W	0,44 W - 3,84 W
2	Tipo 1, 802.3af	7,0 W	3,84 W - 6,49 W
3	Tipo 1, 802.3af	15,4 W	6,49 W - 12,95 W
4	Tipo 2, 802.3at*	30 W	12,95 W - 25,5 W
6	Tipo 3, 802.3bt	60 W	51 W
8	Tipo 3, 802.3bt	100 W	71,3 W

*Este tipo también recibe el nombre de PoE+.

5 Red

5.1 Protección y control de seguridad

Hay varias formas de contrarrestar las amenazas dirigidas hacia los activos del sistema. Algunas amenazas suponen un riesgo para los dispositivos, mientras que otras constituyen un riesgo para las redes o los datos en tránsito o en almacenamiento. A continuación, detallamos algunos controles de seguridad que se pueden aplicar a dispositivos y redes:

- Las credenciales (usuario y contraseña) protegen contra el acceso sin autorización al vídeo y evitan el acceso sin autorización a la configuración del dispositivo. Disponer de diferentes niveles de privilegios de cuentas permite controlar quién puede acceder a cada contenido.
- La filtración de dirección IP (cortafuegos) reduce la exposición a la red local de un dispositivo y lo protege frente a clientes que intenten acceder a él sin autorización. Esto reduce los riesgos en caso de que se descubra la contraseña de un dispositivo y también mitiga los riesgos en caso de que se localice una nueva vulnerabilidad crítica.
- IEEE 802.1X: protege la red de clientes sin autorización. 802.1X es un sistema de protección de infraestructura de red que utiliza switches y un servidor RADIUS gestionados. El cliente de 802.1x instalado en el dispositivo ofrece autenticación al dispositivo que se encuentra en la red.
- HTTPS (Hypertext Transfer Protocol Secure; protocolo protegido para transferencia de hipertexto): protege los datos (vídeo) frente a interceptaciones en la red. El uso de certificados firmados en HTTPS proporciona una vía para que un cliente de vídeo detecte si está accediendo a una cámara auténtica o a un ordenador malintencionado que se hace pasar por una cámara.
- Firmware firmado: es implementado por el proveedor del software, que firma la imagen de firmware con una clave privada, que es secreta. Cuando un firmware tiene adjunta esta firma, un dispositivo validará el firmware antes de aceptarlo e instalarlo. Si el dispositivo detecta que la integridad del firmware está en peligro, rechazará la actualización del firmware. El firmware firmado de Axis se basa en el método de cifrado de clave pública RSA aceptado por el sector.
- Arranque seguro: proceso de arranque que consiste en una cadena ininterrumpida de software validado criptográficamente, comenzando por la memoria inmutable (ROM de arranque). Como está basado en firmware firmado, el arranque seguro garantiza que un dispositivo pueda iniciarse solo con un firmware autorizado. El arranque seguro garantiza que el dispositivo Axis está libre de cualquier posible malware tras restablecer la configuración predeterminada de fábrica.
- TPM: un módulo de plataforma de confianza es un componente que proporciona un conjunto de características de cifrado adecuadas para proteger la información frente a accesos no autorizados. La clave privada se almacena en el TPM y nunca sale del TPM. Todas las operaciones criptográficas que requieren el uso de la clave privada se envían al TPM para su procesamiento. Esto garantiza que la parte secreta del certificado esté protegida incluso en caso de hackeo.
- Axis Edge Vault: módulo informático criptográfico seguro (módulo seguro o elemento seguro) en el que el ID de dispositivo de Axis se instala y almacena de forma segura y permanente.

Para acceder a más recursos sobre ciberseguridad, visite *axis.com/cybersecurity*

5.2 Protocolos compatibles

Son muchos los protocolos que intervienen cuando se transfieren datos de forma segura de un dispositivo en red a otro.

5.2.1 Modelos de referencia de protocolos

La mejor manera de entender cómo interactúan los diferentes protocolos es examinar el modelo de comunicación OSI (Open Systems Interconnection; interconexión de sistemas abiertos). También está el modelo de referencia TCP/IP.

5.2.1.1 Modelo de referencia OSI

Modelo que describe la comunicación de datos entre sistemas abiertos. Para prestar un servicio, cada capa utiliza los servicios de la capa inmediatamente inferior. Cada capa debe seguir determinadas reglas, o protocolos, para realizar servicios.

Capa 7: aplicación

Realiza funciones como transferencia web, de archivos y correos electrónicos para las aplicaciones.

Las aplicaciones como tales, como es el caso de los navegadores web o los programas de correo electrónico, existen por encima de esta capa y no están cubiertas por el modelo OSI.

Capa 6: presentación (datos)

Garantiza que los datos enviados por la capa de aplicación de un sistema los pueda leer la capa de aplicación de otro sistema. Convierte formatos de datos dependientes del sistema, como ASCII, en un formato independiente, permitiendo el intercambio de datos sintácticamente correctos entre diferentes sistemas.

Capa 5: sesión (conexión persistente entre hosts pares)

Proporciona un servicio orientado a aplicaciones y se encarga de la comunicación de procesos entre dos sistemas. La comunicación de procesos comienza con el establecimiento de una sesión, que constituye la base para una conexión virtual entre dos sistemas.

Capa 4: transporte (transporte de extremo a extremo [protocolo orientado a la conexión])

Proporciona un servicio fiable de transferencia de datos (a través del control de flujo y control de errores) a la capa 5 y superiores.

Capa 3: red (paquete [direccionamiento/fragmentación])

Realiza la transferencia de datos propiamente dicha, enrutando y reenviando paquetes de datos entre sistemas. Crea y administra tablas de enrutamiento y proporciona opciones para comunicarse más allá de los límites de la red. Los datos de esta capa se asignan a direcciones de destino y de origen, que se utilizan como base para el enrutamiento previsto.

Capa 2: enlace de datos (marcos)

Proporciona transmisión de datos y controla el acceso al medio de transmisión, combinando los datos en unidades denominadas "marcos". La capa 2 se divide en dos subcapas, la superior corresponde al control de enlace lógico (LLC, Logical Link Control) y la inferior corresponde al control de acceso a medios (Media Access Control, MAC). LLC simplifica el intercambio de datos, mientras que MAC controla el acceso al medio de transmisión.

Capa 1: física (bits)

Proporciona servicios que admiten la transmisión de datos como un flujo de bits a través de un medio, por ejemplo, un enlace de transmisión a través de cable o inalámbrico.

5.2.1.2 Modelo de referencia de protocolo de control de transmisión/protocolo de Internet (TCP/IP)

El modelo de referencia TCP/IP es otro modelo que se emplea para entender los protocolos y cómo se produce la comunicación. El modelo de referencia TCP/IP se divide en cuatro capas diferentes que corresponden al modelo de referencia OSI, descrito anteriormente.

Tabla 5.1 Comparación de los modelos de referencia

Modelo OSI	Modelo TCP/IP
Capa 7: aplicación	Capa 4: aplicación
Capa 6: presentación	
Capa 5: sesión	
Capa 4: transporte	Capa 3: transporte
Capa 3: red	Capa 2: Internet
Capa 2: enlace de datos	Capa 1: interfaz de red
Capa 1: física	

5.2.2 Protocolos de capa de aplicación

- **CIFS/SMB** (Common Internet File System/Server Message Block; sistema de archivos comunes de Internet/bloque de mensajes de servidor): se utiliza principalmente para proporcionar un acceso compartido a archivos, impresoras y puertos en serie, así como diversas comunicaciones entre los nodos de una red.
- **DDNS** (Dynamic Domain Name System; sistema dinámico de nombres de dominio): se utiliza para hacer un seguimiento del enlace de un nombre de dominio con el fin de cambiar las direcciones IPv4.
- **DHCPv4/v6** (Dynamic Host Configuration Protocol; protocolo de configuración dinámica de hosts): asignación y gestión automática de direcciones IP.
- **DNS/DNSv6** (Domain Name System; sistema de nombre de dominio): convierte los nombres de dominio en la dirección IP asociada.
- **FTP** (File Transfer Protocol; protocolo de transferencia de archivos): se utiliza principalmente para transmitir archivos desde un servidor a un cliente (descarga) o desde un cliente a un servidor (subida). También se puede utilizar para crear y seleccionar directorios y renombrar o eliminar directorios y archivos.
- **HTTP** (Hypertext Transfer Protocol; protocolo de transferencia de hipertexto): se utiliza principalmente para cargar texto e imágenes desde un sitio web hasta el navegador web. Los sistemas de vídeo en red proporcionan un servicio de servidor HTTP que permite acceder a los sistemas a través de navegadores web para descargar configuraciones o imágenes en directo.
- **HTTP/2**: una revisión profunda del protocolo HTTP definida en RFC 7540 y publicada en febrero de 2015.
- **HTTPS** (HTTP Secure): adaptación del protocolo de transferencia de hipertexto (HTTP) para realizar una comunicación segura en una red de ordenadores; de uso generalizado en Internet. En HTTPS, el protocolo de comunicación está cifrado por medio de Transport Layer Security (TLS, capa de transporte seguro).

- **MQTT** (Message Queuing Telemetry Transport; transporte de telemetría de cola de mensajes): protocolo de mensajería estándar para internet of things (IoT). Se diseñó para simplificar la integración del IoT y se utiliza en una amplia variedad de sectores para conectar dispositivos remotos con una huella de código pequeña y un ancho de banda de red mínimo.
- **NTP** (Network Time Protocol; protocolo de hora de red): se utiliza para sincronizar la hora del cliente o el servidor de un ordenador con la de otro servidor.
- **RTP** (Real-Time Transport Protocol; protocolo de transporte en tiempo real): permite la transferencia de datos en tiempo real entre extremos del sistema.
- **RTCP**> (Real-Time Control Protocol; protocolo de control en tiempo real): ofrece estadísticas fuera de banda e información de control de una sesión de RTP. Se asocia con RTP en la entrega y empaquetado de datos multimedia, pero no transporta ningún dato multimedia por sí solo.
- **RTSP** (Real-Time Streaming Protocol; protocolo de transmisión en tiempo real): control ampliado durante la transmisión de contenidos en tiempo real.
- **SFTP** (Secure File Transfer Protocol; protocolo de transferencia segura de archivos): ofrece acceso a archivos, transferencia de archivos y gestión de archivos a través de cualquier flujo de datos fiable.
- **SIP** (Session Initiation Protocol; protocolo de inicio de sesión); protocolo de comunicación para señalar y controlar sesiones de comunicación multimedia.
- **SIPS** (Session Initiation Protocol Secure; protocolo de inicio de sesión seguro): versión cifrada de SIP.
- **SMTP** (Simple Mail Transfer Protocol; protocolo sencillo de transferencia de correo): el estándar para la transferencia de correo electrónico a través de Internet. Las cámaras de red admiten SMTP para poder enviar alertas por correo electrónico.
- **SNMPv1/v2/v3** (Simple Network Management Protocol; protocolo sencillo de administración de red): se emplea para supervisar y gestionar de forma remota equipos conectados en red, como switches, routers y cámaras de red. La compatibilidad con SNMP permite gestionar las cámaras de red mediante herramientas de código abierto.
- **SOCKS**: permite transferir paquetes de la red entre clientes y servidores a través de un proxy de red seguro.
- **SRTP** (Secure Real-Time Transport Protocol, protocolo de transporte en tiempo real seguro): permite la transferencia cifrada de datos en tiempo real entre terminales del sistema y, por lo tanto, es una variante segura de RTP.
- **SSH** (Secure Shell): permite acceder a dispositivos de red de forma segura para su gestión y depuración en una red no segura.
- **TLSv1.2/v1.3** (Transport Layer Security; seguridad de la capa de transporte): negocia una conexión privada fiable entre el cliente y el servidor.

5.2.3 Protocolos de capa de transporte

- **TCP** (Transmission Control Protocol; protocolo de control de transmisión): entrega de flujos de datos orientada a la conexión, fiable y en orden. Es el protocolo más habitual para el transporte de datos.
- **UDP** (User Datagram Protocol; protocolo de datagramas de usuarios): servicio de transmisión sin conexión, da prioridad a la entrega a tiempo de los datos por encima de la fiabilidad.

- **ICMP** (Internet Control Message Protocol; protocolo de mensajes de control de Internet): envío de mensajes de error e información sobre funcionamiento donde se indica que un servicio solicitado no está disponible o que no se ha podido acceder a un host o router.

5.2.4 Protocolos de capa de red

- **IGMPv1/v2/v3** (Internet Group Management Protocol; protocolo de gestión de grupos de Internet): utilizado por hosts y routers adyacentes en redes IPv4 para crear afiliaciones a grupos de multidifusión; permite utilizar los recursos de una forma más eficiente al trabajar con estos tipos de aplicaciones.
- **IPv4/IPv6** (protocolo de Internet): dirección pública individual necesaria para la comunicación con dispositivos compatibles con Internet. IPv4 es la versión original y utiliza direcciones de 32 bits. IPv6 es la versión más reciente y utiliza direcciones de 128 bits, que se dividen en ocho grupos de cuatro dígitos hexadecimales.
- **USGv6**: perfil técnico para IPv6 definido por el gobierno estadounidense para garantizar la compatibilidad al aprovisionar dispositivos de red compatibles con IPv6.

5.2.5 Protocolos de la capa de enlace de datos

- **ARP** (Address Resolution Protocol; protocolo de resolución de direcciones): se emplea para descubrir la dirección MAC del host de destino.
- **CDP** (Cisco Discovery Protocol; protocolo de descubrimiento de Cisco): protocolo propio de Cisco utilizado como alternativa a LLDP para descubrir información sobre los dispositivos de hardware conectados.
- **IEEE 802.3 (i, u, ab)**: normas para Ethernet que definen la comunicación de datos a 10 Mb/s (10Base-T), 100 Mb/s (100Base-TX) y 1Gb/s (1000Base-T) a través de cables de par trenzado.
- **LLDP** (Link Layer Discovery Protocol; protocolo de descubrimiento de capa de enlace): se utiliza para dar a conocer la identidad y las capacidades de un dispositivo, así como de otros dispositivos conectados dentro de la misma red.

5.2.6 Protocolos de descubrimiento

- **mDNS (Bonjour)**: se puede usar para descubrir productos de vídeo en red con ordenadores Mac o como protocolo de descubrimiento para dispositivos nuevos en cualquier red.
- **UPnP** (Universal Plug and Play): los sistemas operativos de Microsoft pueden detectar de forma automática recursos (un dispositivo Axis) en una red.
- **Zeroconf**: asigna de manera automática un dispositivo de red a una dirección IP sin utilizar entre 169.254.1.0 y 169.254.254.255.

5.2.7 Calidad de servicio

En una red IP es necesario controlar cómo se comparten los recursos de la red para cumplir con los requisitos de cada servicio.

- **QoS** (Quality of Service; calidad del servicio): capacidad para priorizar el tráfico de red de tal modo que se puedan atender los flujos críticos antes que los flujos con menos prioridad. Mayor fiabilidad de una red al controlar la cantidad de ancho de banda que puede usar una aplicación y proporcionar la capacidad de controlar la competencia entre aplicaciones por el ancho de banda disponible.
- **DiffServ** : la red trata de prestar un servicio concreto según la QoS especificada por cada paquete.

5.2.8 Métodos de transmisión de datos

Existen tres métodos diferentes para transmitir datos en una red informática.

- **Unidifusión**: es el más habitual, el remitente y el destinatario se comunican según un patrón de punto a punto. Los paquetes de datos se envían a un solo destinatario y ningún otro cliente recibirá esa información.
- **Multidifusión**: comunicación entre un solo remitente y varios destinatarios de una red. Reduce el tráfico de red al entregar un solo flujo de información a muchos destinatarios.
- **Difusión**: el remitente envía la misma información a todos los demás servidores de la red; todos los hosts de la red reciben el mensaje y lo procesarán de una u otra forma.

T10169734/ES/M2.2/2205

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro a través de soluciones en red que mejoran la seguridad y suponen una nueva manera de hacer negocios. Como líder de la industria del vídeo en red, Axis pone a su disposición productos y servicios de videovigilancia y analítica, control de accesos y sistemas de audio e intercomunicación. Axis cuenta con más de 3800 empleados especializados en más de 50 países, y proporciona soluciones a sus clientes en colaboración con empresas asociadas de todo el mundo. Fundada en 1984, su sede central se encuentra en Lund, Suecia.

Para más información sobre Axis, visite nuestro sitio web *axis.com*.