DOCUMENTO TÉCNICO

Seguridad con la solución corporal de Axis

Octubre 2026

Resumen

Aunque se trata de una solución de plataforma abierta, el sistema de cámaras corporales Axis ofrece un excelente nivel de seguridad.

Para garantizar la seguridad en caso de pérdida de la cámara, la plataforma únicamente utiliza los componentes de software imprescindibles. En cambio, el controlador del sistema asume más funciones, ya que normalmente no está tan expuesto a amenazas físicas. Además, el almacenamiento interno de la máquina utiliza cifrado AES-256, para impedir el acceso no autorizado a los datos. Gracias a la comunicación basada en IPv6 y en certificados, la cámara solo descargará datos en el controlador del sistema o sistema específico del que forme parte.

Cuando se descargan datos de la cámara en el controlador del sistema se utiliza una conexión a la red con cifrado HTTPS. Los datos solo se almacenan temporalmente en la unidad de almacenamiento con cifrado AES-256 del controlador del sistema, ya que se transfieren inmediatamente al destino del contenido a través de otra conexión cifrada HTTPS.

La seguridad y la integridad del controlador del sistema se refuerzan todavía más con un TPM (módulo de plataforma de confianza) conforme con FIPS 140-2. Otras características, que el sistema corporal comparte con muchos dispositivos Axis, son el SO firmado, el arranque seguro y el vídeo firmado.

Cuando las imágenes se transmiten en secuencia en directo a través de AXIS Body Worn Live, las organizaciones pueden elegir entre una implementación alojada por Axis (en la nube) o una de alojamiento propio (in situ). En ambos casos, los datos se cifran tanto en reposo como en tránsito y se cifran íntegramente de extremo a extremo directamente en el visor. Además, el administrador controla estrictamente quién puede ver la secuencia en directo, llegando incluso a especificar el ordenador, el cliente y las credenciales de usuario concretos.

Índice

1 Acrónimos y terminología 4
2 Introducción 4
3 Seguridad en caso de pérdida de la cámara 4
4 Seguridad en la transferencia de datos 4
5 Otras tecnologías de seguridad 5
6 Seguridad con AXIS Body Worn Live 5
6.1 Implementación alojada por Axis 6
6.2 Implementación autohospedada 6

1 Acrónimos y terminología

BWC. Cámara corporal

VMS. Sistema de gestión de vídeo

EMS. Sistema de gestión de evidencias

Destino del contenido. Ubicación en la que se almacenan las grabaciones y los datos de dispositivos como cámaras corporales. Algunos ejemplos de destinos de contenido pueden ser sistemas de gestión de vídeo, sistemas de gestión de pruebas y servidores de contenidos.

2 Introducción

El sistema corporal de Axis es de plataforma abierta, lo que facilita su integración con sistemas externos de gestión de vídeo y gestión de pruebas. Sin embargo, ofrece un excelente nivel de seguridad, ya que este aspecto ha sido siempre prioritario en todas las fases del despliegue del sistema.

Este documento técnico explica cómo funciona el intercambio de datos entre los componentes del sistema corporal Axis. Concretamente, presentamos las medidas adoptadas para proteger el sistema y sus datos, desde la grabación de una cámara corporal hasta el destino del contenido. También mostramos cómo se cifran las secuencias en directo con AXIS Body Worn Live en sus dos modelos de implementación.

3 Seguridad en caso de pérdida de la cámara

Durante su uso cotidiano, la cámara corporal está expuesta a las amenazas de posibles robos o actos vandálicos. Su diseño integra diferentes características para minimizar los efectos de estas amenazas y preservar la seguridad de los datos y el sistema incluso si desaparece una cámara.

La cámara corporal, por ejemplo, funciona con una plataforma de software reducida a la mínima expresión, en comparación con otras cámaras Axis, ya que prescinde de los componentes de software innecesarios. La cámara y el controlador del sistema no son compatibles con VAPIX ni con protocolos como FTP, SSH o SNMP. Además, la cámara tampoco puede funcionar como servidor. La integración con otros sistemas, como VMS y EMS, se gestiona a través del controlador del sistema, normalmente menos expuesto a amenazas físicas que las cámaras en sí.

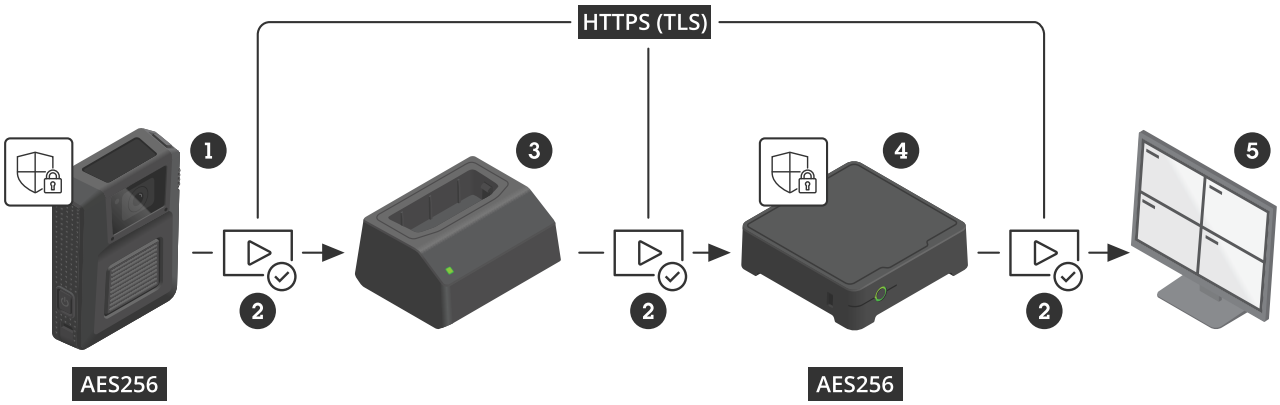
El almacenamiento interno de la cámara corporal utiliza cifrado AES-256 para impedir el acceso no autorizado a los datos en caso de pérdida de la cámara.

La cámara solo descargará datos en el controlador del sistema o sistema específico del que forme parte. Para garantizar que es así, la cámara corporal y el controlador del sistema se comunican mediante IPv6 y utilizan certificados. Cada vez que la cámara se conecta a su base, los certificados se renuevan automáticamente para que se correspondan con los más recientes del controlador del sistema.

Si una cámara permanece desconectada y alejada del sistema durante ocho semanas, entrará en modo seguro y bloqueará la conexión por motivos de seguridad. Para volver a acceder al sistema, es preciso realizar una verificación manual con la frase de contraseña maestra. De este modo se evita que una cámara perdida o alejada del sistema durante mucho tiempo pueda añadirse de nuevo accidentalmente, con los riesgos de seguridad que podría implicar.

4 Seguridad en la transferencia de datos

En la mayoría de los casos, la cámara corporal, con vídeos y metadatos almacenados, se deja de nuevo en su base después de un turno. Todos los datos se descargan al controlador del sistema a través de la base, utilizando una conexión de red cifrada con HTTPS (HTTP con TLS). Los datos se almacenan en el controlador del sistema solo durante un breve periodo de tiempo, en su dispositivo de almacenamiento SSD, que está cifrado mediante AES-256. A continuación, el controlador del sistema transfiere los datos mediante HTTPS al destino del contenido.



Transferencia y almacenamiento seguros de los datos entre la cámara corporal (1) y el destino del contenido (5).

1 *Cámara corporal con Axis Edge Vault*
2 *Vídeo firmado (función de ciberseguridad)*
3 *Base de conexión*
4 *Controlador del sistema con Axis Edge Vault*
5 *Destino del contenido*

También es posible usar una clave de cifrado del destino del contenido para cifrar los datos de la cámara corporal y el controlador del sistema, si el destino del contenido proporciona una clave de cifrado pública. En este caso se aplicará un nivel adicional de cifrado a los datos cuando se envíen al destino del contenido.

5 Otras tecnologías de seguridad

La seguridad y la integridad del controlador del sistema se refuerzan todavía más con un TPM (módulo de plataforma de confianza) conforme con FIPS 140-2.

Tanto las cámaras corporales como el controlador del sistema incorporan Axis Edge Vault, una plataforma de ciberseguridad basada en el hardware que protege todos los datos de los dispositivos y abre la puerta a varias funciones de seguridad. Por ejemplo, el sistema de archivos está cifrado y la clave está protegida con Axis Edge Vault. El *arranque seguro* garantiza que los dispositivos solo pueden arrancar con el software autorizado. El *OS firmado* les obliga a rechazar cualquier actualización si la integridad del software no está garantizada. El *vídeo firmado* aporta un nivel extra de protección, ya que añade una suma de verificación criptográfica a la transmisión de vídeo. De este modo es posible trazar el origen del vídeo hasta la cámara Axis concreta de la que se ha obtenido y verificar así que las imágenes no se han manipulado.

Puede obtener más información sobre el vídeo firmado y Axis Edge Vault en *developer.axis.com/video-streaming-and-recording/signed-video/* y *axis.com/solutions/edge-vault*

El usuario de la cámara solo puede ver el vídeo grabado sobre el terreno a través de la aplicación AXIS Body Worn Assistant. Si la aplicación está activada, la cámara corporal transmite el vídeo directamente a la aplicación, pero no se almacena ningún material para accesos posteriores en la caché ni en la memoria del dispositivo en el que se utiliza la aplicación. En la transmisión de vídeo se aplica también una superposición para disuadir el uso de dispositivos de grabación secundarios para capturar el vídeo. Y si ocurriera, es posible vincular el vídeo a la identidad del usuario de la cámara corporal gracias a la superposición. El conector compatible con USB-C de la cámara corporal no puede utilizarse en ningún caso para visualizar, eliminar o descargar el vídeo.

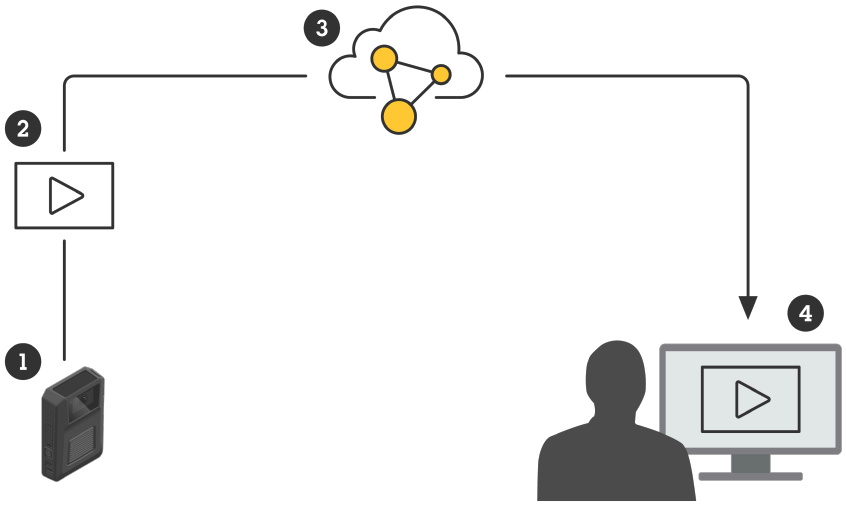
6 Seguridad con AXIS Body Worn Live

AXIS Body Worn Live es una aplicación que permite acceder a datos en tiempo real de cámaras corporales Axis. AXIS Body Worn Live pone a disposición de los usuarios una secuencia en directo de vídeo, audio y otros datos, como coordenadas de posición, y ofrece un resumen situacional único de un incidente en curso. Para adaptarse a los distintos requisitos de las organizaciones en materia de infraestructura y soberanía de los datos, está disponible en dos modelos de implementación: alojado por Axis y autoalojado.

Independientemente del modelo de implementación, el administrador del sistema de la cámara corporal tiene pleno control sobre quién puede ver la secuencia en directo. Los datos se cifran de forma que solo las personas explícitamente autorizadas por el administrador pueden desencriptar y visualizar el vídeo. El administrador también puede revocar el acceso en función de los roles para garantizar la integridad de los datos. En el caso de las implementaciones alojadas por Axis, la persona que desea verlo debe tener acceso al navegador web autorizado, al VMS y a las credenciales de usuario correctas. En el caso de las implementaciones autoalojadas, es preciso tener acceso a la red local y disponer de las credenciales de usuario correctas. Nadie más, ni siquiera Axis, puede acceder a la secuencia en directo, y Axis no tiene acceso a las claves de cifrado de extremo a extremo creadas por los usuarios.

6.1 Implementación alojada por Axis

Cuando se utiliza como servicio en la nube, todos los datos y archivos alojados en AXIS Body Worn Live se cifran mediante AES-256 mientras está en reposo. Todos los canales de comunicación están protegidos mediante HTTPS con TLS y empleando certificados firmados por organismos de confianza. Además del cifrado de la transmisión, AXIS Body Worn Live añade una capa de cifrado auténtico de extremo a extremo mediante el conjunto de cifrado XChaCha20-Poly1305.



Transmisión en directo segura con cifrado de extremo a extremo en una implementación alojada por Axis

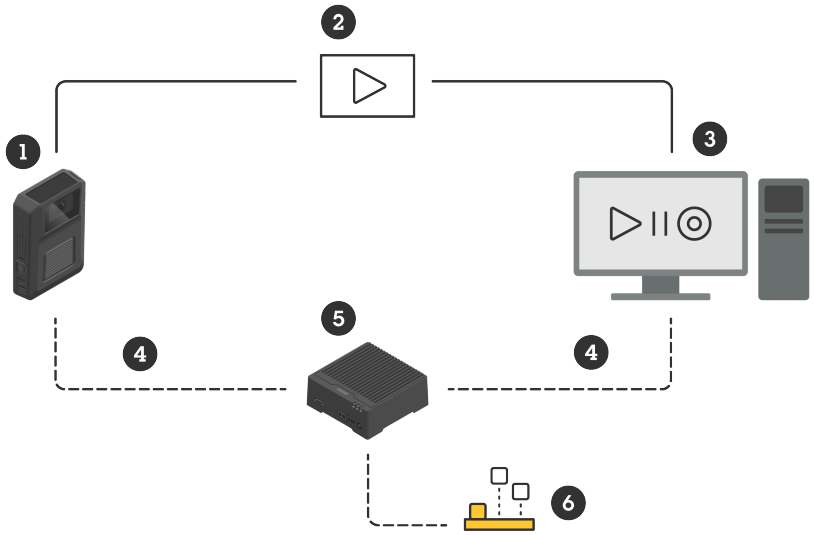
1. *La cámara corporal graba vídeo en directo y recopila otros datos. Los datos ya están cifrados en la cámara.*
2. *Secuencia en directo (cifrado de extremo a extremo).*
3. *Nube alojada por Axis. Los datos y archivos se cifran mediante AES-256.*
4. *Cliente web. Los datos se desencriptan en el navegador web del usuario.*

6.2 Implementación autohospedada

Las organizaciones con políticas estrictas, que exigen que la infraestructura permanezca íntegramente dentro de sus propios entornos de red controlados, pueden instalar la aplicación de servidor AXIS Body Worn Live, Self Hosted de forma local en un dispositivo. Este dispositivo servidor puede ser el Body Worn Activation Kit AXIS W401 o el Connectivity Hub AXIS D3110 Mk II. En ningún momento se almacenan vídeos ni datos confidenciales en el dispositivo servidor local; este se utiliza exclusivamente para mantener la conexión. El canal de comunicación para la transmisión de archivos multimedia entre las cámaras y las integraciones está protegido mediante DTLS 1.0 o una versión posterior. El canal de comunicación para la transmisión de señales y eventos entre el servidor y las integraciones está protegido mediante HTTPS con certificados proporcionados por el cliente y TLS 1.2 o una versión posterior.

Cuando hay un flujo de datos mediante la versión autohospedada, el servidor local realiza la configuración de la señalización WebRTC con autentificación basada en certificados entre el servidor y la BWC. Una vez establecida,

se crea una conexión cifrada de igual a igual directamente entre la cámara corporal (BWC) y el cliente WebRTC del visor (como un VMS). Dado que el flujo de vídeo se envía directamente a través de esta conexión cifrada sin almacenamiento intermedio, se evita cualquier interceptación no autorizada. El sistema está diseñado para operar en redes cerradas y segmentadas sin necesidad de acceso a Internet, lo que minimiza la superficie de ataque frente a amenazas externas.



Transmisión en directo segura en un entorno autohospedado

1 *La cámara corporal graba vídeo en directo y recopila otros datos. Los datos ya están cifrados en la cámara.*
2 *Transmisión punto a punto (encriptada).*
3 *Cliente WebRTC del usuario.*
4 *Señalización WebRTC.*
5 *AXIS Body Worn Live, dispositivo con servidor autoalojado.*
6 *AXIS Body Worn Live, app de servidor autoalojado. Esto se utiliza para la configuración de la señalización de WebRTC.*

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro mejorando la seguridad, la operatividad de las empresas y la inteligencia empresarial. Como líder del sector y empresa especializada en tecnología de redes, Axis ofrece videovigilancia, control de acceso, intercomunicadores y soluciones de audio. Su valor se multiplica gracias a las aplicaciones inteligentes de analítica y una formación de primer nivel.

Axis cuenta aproximadamente con 5.000 empleados especializados en más de 50 países y proporciona soluciones a sus clientes en colaboración con sus socios de tecnología e integración de sistemas. Axis fue fundada en 1984 y su sede central se encuentra en Lund (Suecia).aboutaxis_text2

© 2020 — 2026 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC y VAPIX son marcas comerciales registradas de Axis AB en diferentes jurisdicciones. Todas las demás marcas comerciales son propiedad de sus respectivos titulares.Nos reservamos el derecho de introducir modificaciones sin previo aviso.