DOCUMENTO TÉCNICO

Protección perimetral con vigilancia inteligente

Un estudio de las opciones de sensores, aplicaciones y aspectos esenciales para garantizar una solución de seguridad preparada para el futuro en toda una serie de industrias

Julio 2021

AXIS COMMUNICATIONS

Índice

1 Resumen

Una valla suele ser un componente fundamental del «nivel exterior» de la seguridad de una instalación y puede actuar como barrera, como pantalla o como elemento disuasorio, tanto para las personas como para los animales. Se pueden incorporar otros elementos para mejorar la eficacia de la valla, ya que cualquier barrera física solo puede retrasar o dificultar un acceso no autorizado.

Junto a las vallas se utilizan varios tipos de detectores. Los detectores mediante cable pueden seguir el recorrido de la valla, y los sensores de radar (microondas), las barreras de infrarrojos o los láseres pueden colocarse en lugares estratégicos.

Todos los tipos de detectores pueden generar falsas alarmas, causadas, por ejemplo, por animales, plantas y árboles en movimiento y por las inclemencias meteorológicas. También puede haber otros factores restrictivos, como los choques de frecuencias cuando se utilizan sensores de microondas o las limitaciones físicas del entorno de la instalación.

Las cámaras representan una ventaja evidente para quienes desean vigilar zonas amplias o varios lugares a la vez. Las soluciones de red modernas combinan el procesamiento informático en la cámara y la inteligencia artificial. La escalabilidad inherente, la eficacia y el carácter disuasorio de la tecnología significan que las videocámaras podrían ser un elemento extraordinariamente rentable para un sistema de seguridad.

Aunque las cámaras y el software de detección de movimiento han ampliado el rango y las capacidades de la protección perimetral, estas soluciones pueden estar limitadas por la incapacidad de detectar en condiciones meteorológicas adversas. Las cámaras térmicas, cuando se calibran correctamente y se combinan con la analítica de vídeo, pueden proporcionar una vigilancia y un control eficaces, que no se ven afectados por las condiciones de iluminación y prácticamente no se ven alterados por las condiciones meteorológicas extremas.

La analítica de vídeo ha evolucionado mucho a lo largo del tiempo y ahora es habitual, incluso en las cámaras destinadas al mercado de la seguridad doméstica. La analítica puede reducir los requisitos de almacenamiento grabando solo el vídeo que contiene la actividad de interés. Al procesar gran parte de las secuencias de vídeo grabadas dentro de la propia cámara, la carga sobre la red se reduce considerablemente, puesto que las cámaras solo transmiten el vídeo que es pertinente. Esto tiene ventajas evidentes en un escenario de sala de control.

Como ocurre con cualquier medida de seguridad, la evaluación de una solución de protección perimetral debe ser adecuada y proporcionada. Como siempre, la amenaza ha de ser el aspecto principal a tener en cuenta.

Un enfoque convergente con respecto a la seguridad que incluya aportaciones consideraciones por parte de otros departamentos, como el de informática y el de operaciones, se está convirtiendo rápidamente en la práctica recomendada. Esto incluye la necesidad de implicar a aquellas personas que se encargan de la ingeniería lo antes posible.

Demostrar la ROI de una solución de seguridad diseñada para prevenir un incidente es notoriamente difícil. Esto se debe principalmente a la falta de ingresos potenciales para medir el coste. Es posible demostrar una ROI más tangible; algunos ejemplos son las soluciones que no solo alertan al personal de un comportamiento sospechoso o de un acceso no autorizado, sino que también generan respuestas automatizadas.

2 Introducción

Las soluciones electrónicas de protección perimetral se han reservado tradicionalmente para instalaciones gubernamentales de alta seguridad y espacios comerciales, o para las residencias de personas muy adineradas. Gracias a los avances tecnológicos, a un mercado más competitivo y a la consiguiente reducción de costes, las soluciones relativamente tecnológicas están ahora al alcance de muchas más personas.

¿En qué consiste una solución moderna de protección perimetral? ¿Cómo funciona la tecnología y cómo puede proporcionar tanto tranquilidad como auténtica protección?

En este documento técnico se examinan algunas de las opciones actuales mediante sensores para proteger un perímetro y se ofrece información sobre la tecnología que hay detrás de las soluciones.

3 Soluciones de protección perimetral

3.1 Soluciones físicas

Las soluciones físicas suelen ser un componente fundamental del «nivel exterior» de un enfoque compartimentado de la seguridad de una instalación, que suele consistir en una valla perimetral, a menudo construida con malla metálica o soldada, en paneles soldados o de hormigón. Una valla perimetral tiene muchas finalidades, una de las más importantes es presentar una barrera física que retrase o impida los accesos no autorizados. Una valla también puede evitar la vigilancia al proteger un bien; también sirve como elemento disuasorio e impide la entrada de animales. También se pueden incorporar elementos como sistemas antiescalada, vías de acceso de vehículos, sistemas de disuación de entrada, cimientos y paneles de vallas para mejorar la eficacia de la valla de un perímetro.

Sin embargo, cualquier barrera física invariablemente solo servirá para retrasar un acceso no autorizado. Por lo tanto, el perímetro también debe estar equipado con tecnología de detección automática de intrusos, que es capaz de proporcionar alertas verificables en tiempo real, datos de localización, seguimiento de objetivos y la capacidad de generar pruebas y los datos para la investigación posterior al incidente.

3.2 Detección de intrusos en el perímetro físico

A menudo se utilizan varios tipos de «detectores» mediante cables para proteger los perímetros amplios. Estos detectores mediante cables suelen estar enterrados en el suelo o montados en la valla, siguen el recorrido de la valla y no es necesario que estén en línea recta. También proporcionan cobertura en las esquinas y en **zonas muertas**. Algunos proveedores ofrecen vallas provistas de soluciones de detección automática.

Como ocurre con cualquier solución de detección, los detectores por cable pueden generar falsas alarmas, que reciben el nombre de «falsos positivos». Las causas más comunes de los falsos positivos son los animales, las plantas y los árboles en movimiento, así como las condiciones meteorológicas adversas. Las soluciones mediante cable ofrecen todo su potencial cuando se complementan con videovigilancia. El vídeo puede utilizarse no solo para verificar un acceso no autorizado, sino también para confirmar la causa de una alarma. Una solución mediante cable solo podrá proporcionar una alerta del propio acceso no autorizado; no puede proporcionar información sobre el número de intrusos ni ningún otro detalle necesario para preparar una respuesta.

3.3 Otros sensores de detección de intrusos

Otros detectores de intrusos, como los sensores de radar (microondas), las barreras de infrarrojos o los láseres, se pueden colocar en lugares estratégicos del perímetro. Una vez más, estas tecnologías pueden verse limitadas por aspectos como los falsos positivos y la capacidad de detección limitada con respecto a la distancia y altura si no se siguen adecuadamente las normas de instalación.

El uso del radar en el perímetro puede resultar especialmente problemático en un entorno donde se utilicen otros dispositivos electrónicos. Estos podrían funcionar en la misma frecuencia y espectro, y aunque una elección cuidadosa de la frecuencia o una reducción de la potencia podrían reducir las interferencias, también dificultarán el alcance efectivo del dispositivo.

4 Soluciones basadas en vídeo

4.1 La aplicación de las videocámaras

Las tecnologías de CCTV autónomas de antaño se parecen poco a las soluciones de cámaras de red de alta tecnología disponibles hoy en día. Las soluciones de red modernas son capaces de combinar el procesamiento informático en la cámara y la inteligencia artificial. No obstante, este nivel de tecnología existe desde hace poco tiempo y aún está en sus inicios.

Las cámaras representan una ventaja evidente para quienes desean vigilar zonas amplias o varios lugares a la vez. La escalabilidad inherente, la eficacia y el carácter disuasorio de la tecnología significan que las videocámaras podrían ser un elemento extraordinariamente rentable para un sistema de seguridad.

Según la legislación local, la tecnología de las cámaras puede utilizarse para supervisar más allá del perímetro físico, proporcionando un margen de vigilancia adicional y brindando al operador un tiempo extra para poder responder. Las soluciones que aprovechan la analítica de vídeo permiten activar una alarma según una serie de reglas establecidas. Por ejemplo, una alarma suena si una persona se acerca a menos de 50 metros de una valla; se podría activar un nivel más alto de alarma si esa misma persona continuase merodeando o accediese a la zona de 10 metros.

4.2 Soluciones de videovigilancia termográficas

La combinación de cámaras de videovigilancia y software de detección de movimiento ha ampliado el rango y las prestaciones de las soluciones de protección perimetral desde la simple detección hasta el análisis complejo de los accesos no autorizados. Sin embargo, la eficacia del vídeo puede verse muy limitada por su incapacidad para detectar en condiciones meteorológicas adversas.

La mayor disponibilidad de la tecnología de las cámaras térmicas ha hecho que destaque su uso en entornos perimetrales. Las cámaras térmicas (o termográficas), cuando se calibran correctamente y se combinan con la analítica de vídeo, pueden proporcionar una vigilancia y un control eficaces, que no se ven afectados por las condiciones de iluminación y prácticamente no se ven alterados por las condiciones meteorológicas extremas. Los sensores que utilizan la tecnología térmica proporcionan un contraste superior en comparación con una cámara típica de luz visible y, por consiguiente, son beneficiosos para la protección perimetral debido a una capacidad de detección de intrusos muy mejorada.

Los sensores térmicos generan una imagen utilizando la radiación infrarroja que emiten objetos como vehículos o personas. Cuando se combinan con la analítica de vídeo, las cámaras térmicas modernas con suficiente potencia de procesamiento pueden distinguir entre diferentes tipos de objetivos de intrusos y pueden alertar al operador basándose en una lista predefinida de condiciones. Algunas de ellas podrían ser

la dirección y la velocidad de una persona o un vehículo. Las cámaras tradicionales también son capaces de hacerlo, pero ha de ser con luz visible. Estas cámaras se analizan en el siguiente apartado.

4.3 Cámaras de luz visible

Todas las cámaras de vigilancia de luz visible convencionales necesitan una iluminación natural o aumentada para generar imágenes. La iluminación necesaria para hacer posible la videovigilancia es un área de especialización por derecho propio y se han redactado informes independientes acerca de esta importante cuestión. Sin embargo, es necesario reiterar el hecho evidente pero vital de que las cámaras estándar necesitan luz visible. La luz puede ser un reto en cualquier entorno, con efectos obvios a medida que cambia la calidad de la luz. Algo que no siempre se tiene en cuenta o se entiende, sobre todo por parte de quienes tienen que encontrar la solución, son los efectos de las condiciones meteorológicas.

Las cámaras térmicas tienen sus ventajas, pero esto no quiere decir que las cámaras térmicas deban o puedan sustituir directamente a la cámara de luz visible, ni mucho menos. Estas dos tecnologías ofrecen todo su potencial cuando se encuentran integradas en la misma solución. Las cámaras tradicionales no pueden detectar objetos a los mismos rangos que las cámaras térmicas, pero estas últimas no pueden proporcionar el nivel de detalle forense que ofrecen las cámaras de luz visible. Estas dos tecnologías se combinan a menudo: la cámara térmica proporciona la alarma de detección y la cámara de luz visible proporciona pruebas forenses y seguimiento del objetivo.

4.4 Analíticas de contenido de vídeo

La videovigilancia en red ha aportado una escala sin precedentes a las operaciones de seguridad. Una jerarquía de permisos eficaz permite controlar el acceso, la distribución y el almacenamiento de vídeo entre un número teóricamente ilimitado de actores. Un avance tecnológico en particular está proporcionando niveles de escalabilidad aún mayores: la analítica de vídeo

La analítica de vídeo ha evolucionado mucho a lo largo del tiempo, sobre todo gracias al desarrollo de la tecnología de las cámaras IP. Así lo demuestran las cámaras destinadas al mercado de la seguridad doméstica, muchas de las cuales incorporan ya algún nivel de función analítica que les permite, por ejemplo, detectar el movimiento en la escena. La cámara puede incorporar otras funciones adicionales, como la detección de traspaso de línea, objetos en movimiento o incluso el recuento de personas.

La analítica de vídeo puede resolver la necesidad de espacio de almacenamiento al grabar solamente aquellas secuencias que contienen actividad. Por otra parte, al procesar gran parte de las secuencias de vídeo grabadas dentro de la propia cámara, (lo que se conoce como «inteligencia en el extremo») la carga sobre la red se reduce considerablemente, puesto que las cámaras solo transmiten el vídeo que es pertinente. Esta característica presenta beneficios evidentes en un escenario de sala de control, con un operador de seguridad que solo tiene que examinar el vídeo cuando se recibe una alerta; una mejora importante tanto para el operador de seguridad como para la eficiencia operativa de la organización.

Las arquitecturas de sistemas para analítica de vídeo pueden clasificarse en dos grandes categorías: centralizadas y distribuidas. En las arquitecturas centralizadas, las cámaras y los sensores obtienen vídeo y otro tipo de información y lo envían a un servidor central, donde se procede a su análisis. En las arquitecturas distribuidas, los propios dispositivos en el extremo (cámaras de red y codificadores de vídeo) son capaces de procesar el vídeo y extraer la información pertinente. El análisis en el extremo prescinde de los servidores de analíticas dedicados, y como la compresión solo se utiliza cuando se transfieren los datos de vídeo a un servidor central, el análisis se puede realizar ahora en la señal de vídeo sin comprimir. El resultado es una arquitectura mucho más flexible y económica. De hecho, los mismos servidores que normalmente solo podían procesar unos pocos flujos de vídeo debido a la potencia de procesamiento

necesaria, ahora pueden manejar cientos de flujos de vídeo cuando gran parte del procesamiento se lleva a cabo en las cámaras.

4.4.1 Velocidades de procesamiento y GPU

Aunque algunas de las principales empresas tecnológicas han pronosticado que la acertada predicción de Gordon E. Moore (también conocida como «ley de Moore») sobre la mejora exponencial de las velocidades y la capacidad de procesamiento experimentará una ralentización en un futuro próximo, el actual aumento de potencia combinado con la reducción de tamaño ha hecho que los fabricantes y desarrolladores de cámaras puedan cambiar la forma en que se hace uso de la potencia de procesamiento.

Hasta hace poco, cualquier capacidad de procesamiento adicional se utilizaba para mejorar la calidad de la imagen, aportando una mayor resolución y una compresión de vídeo más eficiente. Sin embargo, por el momento, el mercado parece haber alcanzado casi una meseta en su demanda de una resolución de imagen cada vez mayor. Por ello, los fabricantes utilizan ahora la potencia de procesamiento para ofrecer niveles de inteligencia nunca antes vistos en el extremo. En muchos casos, esto significa que las potentes analíticas de vídeo basadas en servidores pueden beneficiarse ahora del procesamiento en la propia cámara.

Gracias a las características de menor tamaño y mayor velocidad de los procesadores modernos, las cámaras pueden albergar unidades de procesamiento gráfico (GPU, por sus siglas en inglés), que proporcionan capacidades de procesamiento en paralelo y abren nuevas oportunidades y posibilidades analíticas. Esta nueva capacidad ha hecho que los desarrolladores de software cambien su foco de atención para ofrecer versiones renovadas de las analíticas basadas en servidor existentes y probadas en variantes basadas en el extremo, contribuyendo a impulsar la demanda de cámaras más inteligentes, capaces de ofrecer un valor que se extiende mucho más allá de la seguridad y la videovigilancia.

4.4.2 Deep learning e inteligencia artificial (IA)

Las GPU han propiciado un gran avance en el rendimiento analítico en el extremo, pero está creciendo la demanda de otros tipos de tecnología aplicable a entornos de vigilancia, con prestaciones como el recuento de personas y la gestión de la ocupación. Los avances en IA y aprendizaje automático han llevado a la integración de unidades de procesamiento de deep learning (DLPU, por sus siglas en inglés) en las cámaras, lo que está suponiendo una revolución en el sector.

Una DLPU está diseñada específicamente para una aplicación más amplia de la analítica de deep learning. La analítica basada en deep learning puede proporcionar una precisión superior para la detección y la clasificación, ya que el algoritmo está eficazmente entrenado sobre el aspecto que presenta un conjunto de objetos prescritos. Esto significa que una solución de detección de intrusos en un perímetro puede configurarse para que solo emita alertas para objetos y escenarios muy específicos; una versión avanzada de «If-this-then-this» (ITTT).

En algunos casos, es posible que solo se vea una parte de un objeto, como el parachoques trasero de un coche, pero el sistema de analíticas del sistema seguirá reconociéndolo e identificándolo. En el momento de redactar este artículo, y a pesar de algunas reivindicaciones que se han realizado, la mayoría de las soluciones probadas del mercado se limitan a identificar y diferenciar entre personas y tipos de vehículos. Sin embargo, algunos ejemplos de modelos de analíticas basados en cámaras capaces de efectuar una discriminación más detallada, como el color de la ropa que lleva una persona, se encuentran en una fase avanzada de pruebas.

Estos avances tecnológicos podrían dar lugar a sistemas de detección muy específicos, capaces de identificar y diferenciar entre empleados, clientes, público en general o posibles amenazas. Desde el punto de vista de la seguridad, la analítica avanzada en un entorno donde la seguridad física esté bien aplicada solo puede dar lugar a un sistema aún más eficiente y preciso para detectar y prevenir la delincuencia. La evolución hacia la siguiente etapa en cuanto a capacidades podría no estar tan lejos.

5 Costos

5.1 Evaluación y medición de un rendimiento de la inversión

Al igual que ocurre con cualquier medida de seguridad, ya sea desde el punto de vista de la vulnerabilidad o de la resiliencia, la evaluación de una solución de protección perimetral debe ser adecuada y proporcionada. Como siempre, la amenaza debe ser el principal aspecto a tener en cuenta; en el caso de prácticamente cualquier gran empresa o instalación gubernamental moderna puede ser desde intrusos accidentales hasta manifestantes o incluso terroristas.

Un enfoque convergente con respecto a la seguridad que incluya aportaciones consideraciones por parte de otros departamentos, como el de informática y el de operaciones, se está convirtiendo rápidamente en la práctica recomendada. Esto incluye la necesidad de implicar a las personas con experiencia en requisitos de ingeniería, y se las debe involucrar lo antes posible. A la hora de tener en cuenta las medidas que se van a aplicar, históricamente, un buen punto de partida para el perímetro habrían sido siempre las medidas más tradicionales, que suelen disuadir y retrasar a un posible intruso. Solo entonces el diseñador de seguridad pasaría a los sistemas técnicos de detección «complementarios». Pero dadas las muchas medidas y sistemas que ahora se integran entre sí, es necesario un enfoque más calculado y holístico.

Demostrar la ROI de una solución de seguridad diseñada para prevenir un incidente es notoriamente difícil. Esto se debe principalmente a la falta de ingresos potenciales para medir el coste. Por lo general, el personal de seguridad trabajará con sus compañeros del departamento financiero para determinar el coste de los diferentes tipos de incidentes de seguridad, ya sean costes directos ocasionados por la pérdida o destrucción de activos o costes menos inmediatos pero igualmente perjudiciales asociados a la pérdida de reputación.

Sin embargo, es posible demostrar una ROI más tangible, sobre todo con ciertas tecnologías capaces de reducir una actividad manual específica o de permitir que el personal de seguridad se reasigne a otras tareas. Algunos ejemplos son las soluciones que no solo alertan al personal de un comportamiento sospechoso o de un acceso no autorizado, sino que también pueden producir una respuesta suave automatizada. Entre ellos podrían estar los sistemas de audio IP que pueden emitir anuncios pregrabados, o la señalización luminosa que informa a un posible intruso de que ha sido detectado y le insta a que abandone el lugar.

Si se incorporan cámaras de vigilancia a la solución, se puede aumentar la eficacia mostrando al intruso alguna prueba de que ha sido identificado, como una pantalla donde se muestra que se ha capturado su matrícula o incluso una imagen del propio intruso. Solo cuando esta medida no produce el resultado deseado es necesario que el equipo de seguridad se despliegue para investigar o emprender una acción más directa. Este planteamiento por fases en respuesta a las alertas podría ser más adecuado si se utiliza más allá del perímetro, pero contribuirá a reducir la necesidad de que el personal de seguridad se involucre en una etapa inicial, liberando de este modo horas de trabajo en favor de una mayor eficiencia.

5.2 Evaluación de costes

La estimación de los costes debe basarse en un cálculo del coste total de propiedad (CTP). El CTP incluye todos los costes asociados a una solución a lo largo de su ciclo de vida: los costes materiales y humanos, los costes de los estudios, los costes de instalación del sistema, los costes de funcionamiento, los costes de mantenimiento, los costes de desmantelamiento y de reciclaje. Para ello puede ser necesario realizar un cambio de enfoque por parte de los departamentos de finanzas y compras, ya que podría ser necesario reasignar el capital entre los presupuestos de gastos de explotación y de capital.

Como con cualquier activo tangible, la organización necesitará conocer la vida útil de la solución de detección perimetral. Los responsables de seguridad e informática pueden ayudar a sus compañeros de finanzas explicando y demostrando cómo la adquisición de la tecnología adecuada como plataforma para

futuras soluciones supondrá un ahorro de dinero. Una característica de los dispositivos avanzados de vigilancia inteligente es que, hasta cierto punto, están intrínsecamente preparados para el futuro. Es decir, los dispositivos con una potencia de procesamiento adecuada son capaces de aprovechar reiteradamente los avances tecnológicos a lo largo del tiempo, sobre todo a través de la analítica de procesamiento basada en la IA y el aprendizaje automático.

6 La propuesta de Axis Communications

El enfoque abierto de Axis con respecto a la integración con soluciones de socios significa que sus sensores en red, combinados con analítica de vídeo contrastada y el uso de la IA, permiten a los aeropuertos implementar soluciones de protección perimetral integradas de alto rendimiento que son ciberseguras y rentables para toda la empresa y durante toda la vida útil del sistema.

Cuando los sensores térmicos no son apropiados, la tecnología de microondas (radar) es una excelente alternativa, capaz de ofrecer muchas de las mismas ventajas que la térmica, con un número potencialmente menor de falsos positivos. La tecnología de radar de Axis se beneficia del mismo aprendizaje automático y deep learning que las cámaras de vigilancia más avanzadas. Las unidades de radar de Axis pueden detectar, clasificar y rastrear con precisión a personas y vehículos con una tasa de falsas alarmas prácticamente nula.

La tecnología de radar funciona las 24 horas del día de forma ininterrumpida y prácticamente no se ve afectada por los desencadenantes comunes, como sombras o haces de luz en movimiento, pequeños animales o insectos, o condiciones meteorológicas adversas. El resultado es un funcionamiento muy rentable, que hace que el personal de seguridad pueda centrarse en las verdaderas amenazas confirmadas. El radar también puede proporcionar la velocidad de un objeto, lo que permite calcular con precisión el punto de contacto o incluso aplicar límites de velocidad.

El rendimiento de una solución suele ser la primera parte de cualquier solicitud de información (RFI, por sus siglas en inglés) o cuestionario de análisis de mercado. Las cámaras Axis incorporan los procesadores ARTPEC desarrollados por Axis, con la mejor capacidad del sector, que permiten integrar en la cámara (en el extremo) algunas de las soluciones más avanzadas de analítica de vídeo para la protección perimetral. Lo más importante es que esto también garantiza que la solución aprovecha la potencia de la tecnología propia y no de los componentes de terceros.

Esta inteligencia «en el extremo» significa que varias cámaras pueden rastrear múltiples eventos que se producen de forma simultánea en diferentes lugares. Esta «arquitectura técnica distribuida» permite ampliar la solución a tantas cámaras como sea necesario, y al mismo tiempo prescinde de las inversiones en tecnología de servidores centralizados.

Con el AXIS Perimeter Defender (APD), aprobado por el Gobierno del Reino Unido, se detectan cuatro tipos diferentes de eventos, para uno o más individuos o vehículos:

- Acceso no autorizado en una zona predefinida
- • Traspaso de zonas en un orden y una dirección predefinidos
- • Traspaso de zonas condicional
- Presencia de merodeadores

APD puede proporcionar algo más que una alarma contra intrusos y el vídeo correspondiente. También proporciona metadatos que pueden utilizarse para mostrar vídeo superpuesto, mostrando los límites y las trayectorias de las personas y los vehículos en movimiento. Para un enfoque más integrado, las cámaras Axis (de luz visible o térmicas) también funcionan con altavoces IP para emitir mensajes automáticos en caso de detección, potencialmente como una solución autónoma. Este tipo de advertencia automática

permitirá una «escalada» de medidas y contramedidas, algo importante a la hora de determinar la intención de un intruso y cualquier respuesta posterior necesaria.

APD puede integrarse directamente en el software que se utiliza habitualmente en las plataformas empresariales (por ejemplo, Genetec, Milestone, Seetec, Prysm, Qognify, etc.).

Axis proporciona herramientas de diseño complementarias para ayudar en la planificación posterior al estudio, y asistencia en todas las etapas de un proyecto, desde la búsqueda de los productos adecuados en función de criterios específicos hasta el cálculo preciso de las necesidades de almacenamiento, la instalación de la tecnología y la gestión de los sistemas. Aprovechar las herramientas de Axis ayudará a los consultores a planificar y estimar, y a un integrador a gestionar los proyectos de una manera más fluida y eficiente. Estas herramientas permiten incluso garantizar más fácilmente la seguridad del sistema instalado, puesto que el software incluido facilita la instalación de actualizaciones y parches de seguridad.

A medida que las amenazas y las contramedidas evolucionan, hay un aspecto esencial que se mantiene constante: la integridad y la seguridad del perímetro. El perímetro es un aspecto fundamental a tener en cuenta para quienes implementan el deber de una organización de proporcionar un entorno seguro para el personal, los visitantes y el público en general. Este documento pretende promover los beneficios para las organizaciones de un enfoque tecnológico integrado para la planificación de la seguridad perimetral. También destaca el hecho de que la inversión en tecnología para la seguridad debe estar respaldada por una ROI demostrable. En cualquier caso, conocer las capacidades tecnológicas relevantes actuales y entender las tendencias futuras es una buena estrategia de seguridad operativa y compras para cualquier profesional de la seguridad, independientemente de su departamento, cargo o sector.

Referencias de productos

Cámaras IP térmicas:

AXIS Q19 y más en www.axis.com/es-es/products/thermal-cameras

Software de análisis:

AXIS Perimeter Defender

www.axis.com/es-es/products/axis-perimeter-defender

Altavoces IP externos:

AXIS C1310-E www.axis.com/es-es/products/axis-c1310-e

Radar de seguridad IP:

D2110-VE www.axis.com/es-es/products/axis-d2110-ve

T10169467/ES/M1.3/2107

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*.