



AVIGILON™

Seguridad y protección en instituciones financieras

Una guía sobre tendencias del sector, medidas de seguridad
y consideraciones tecnológicas



MOTOROLA SOLUTIONS



Las medidas estrictas de seguridad son vitales en el sector financiero para ayudar a proteger a las personas, la propiedad y los activos. También permiten que las instituciones financieras, como los bancos, mantengan el cumplimiento de las regulaciones del sector en materia de seguridad y privacidad de los datos.

Debido a la naturaleza del negocio, los bancos y otras organizaciones financieras gestionan datos valiosos de la empresa y de sus clientes. Esto los convierte en un objetivo atractivo para delincuentes, como hackers, que buscan obtener estos datos mediante robos internos o externos.

Sin embargo, no solo los activos necesitan protección. Ayudar a aliviar a empleados y clientes es clave. Datos del FBI revelan que [más del 60 %](#) de los robos a bancos involucran el uso o la amenaza de un arma y que [casi el 45 %](#) de los robos en Estados Unidos implican comportamientos agresivos.

Las [medidas eficaces de seguridad y protección](#) pueden ayudar a prevenir que estos incidentes ocurran. En algunos casos, la sola presencia de este tipo de medidas de seguridad, como las cámaras, es suficiente para disuadir a algunos delincuentes. Esto permite que las instituciones financieras mantengan la continuidad operativa y reduzcan cualquier impacto en la calidad del servicio, las pérdidas financieras y el daño reputacional.

Principales riesgos de seguridad a los que se enfrenta la industria bancaria en la actualidad

Al igual que muchas otras industrias, el sector bancario se enfrenta a diversos riesgos y desafíos en materia de seguridad. Sin embargo, debido a la naturaleza del negocio, el daño potencial derivado de un incidente de seguridad es mayor y puede tener consecuencias de amplio alcance.

Acceso no autorizado

Los eventos de acceso no autorizado incluyen cualquier intento de ingresar a un área segura sin permiso o sin credenciales válidas. Este tipo de incidentes suele estar vinculado a delitos en los que empleados acceden a áreas restringidas para cometer fraudes o visitantes que ingresan a áreas exclusivas del personal para causar daños.

Por este motivo, las medidas de control de acceso son un componente central de la seguridad en bancos e instituciones financieras. Los propietarios y operadores de instituciones financieras deben contar con medidas que ayuden a prevenir accesos no autorizados, que van desde personal de seguridad en el lugar hasta tecnologías de control de acceso.

Robos

Los bancos y las instituciones financieras son los objetivos principales para los robos. La gran cantidad de dinero y activos corporativos valiosos almacenados en estas instituciones resulta atractiva tanto para delincuentes organizados como oportunistas, especialmente cuando las sucursales cuentan con medidas de seguridad mínimas o desactualizadas.





[Datos del FBI](#) revelan que durante 2023 se registraron más de 1.350 robos a bancos en todo Estados Unidos. Además, [la información más reciente disponible](#) (2019) indica que los bancos presentan la mayor pérdida promedio en dólares por robo entre todos los tipos de negocios del país (USD 4.213), superando el promedio nacional en más de USD 2.400.

Fraude

El fraude bancario abarca cualquier intento de obtener beneficios financieros mediante el engaño. El fraude en el sector financiero es un problema en crecimiento. El fraude cometido por empleados aumentó un [73%](#) entre 2016 y 2024. Además, el [52%](#) de los colaboradores internos reportó un incremento en el fraude empresarial y el [62%](#) informó un aumento del fraude al consumidor.

Los expertos consideran que la creciente sofisticación y disponibilidad de herramientas de IA están contribuyendo al aumento del fraude financiero. En 2024 se perdieron [USD 16.600 millones](#) debido al fraude, lo que representa un incremento interanual del 33 %, con un [informe reciente de Deloitte](#) que sugiere que la IA generativa podría provocar pérdidas de USD 40.000 millones para 2027.

Robo de cajeros automáticos (ATM)

La seguridad bancaria y financiera también debe extenderse a los activos externos, como los cajeros automáticos. Los delincuentes instalan dispositivos como cámaras o sistemas de skimming en los ATM para robar PINs, utilizan técnicas de ingeniería social para engañar a las personas y obtener información de las tarjetas, e incluso fuerzan o sustraen los cajeros automáticos.

Varios tipos de robos en cajeros automáticos han aumentado en los últimos años: el skimming creció un [109%](#) en 2023 y el robo físico de ATM aumentó un [600%](#) entre 2022 y 2024. Este tipo de delitos es difícil de combatir, ya que combina prácticas de seguridad física y ciberseguridad.

Ataques de ciberseguridad

Los ataques de ciberseguridad tienen como objetivo los sistemas digitales de los bancos para robar datos valiosos o transferir fondos de manera ilícita. Los ciberdelincuentes utilizan diversas tácticas para infiltrarse en estos sistemas, como la ingeniería social para manipular al personal y el uso de malware para modificar datos sensibles.

Los ciberataques aumentaron a nivel global [casi un 50 %](#) en el primer trimestre de 2025, y los ataques dirigidos a instituciones financieras crecieron un [13%](#) hacia finales de 2024. En un [informe publicado recientemente](#), el 64% de las principales instituciones financieras afirmó que los ciberdelincuentes intentaron robar datos no públicos durante 2024.

Explotación de sistemas de seguridad

La rápida innovación del sector tecnológico implica que el software y el hardware de seguridad deben actualizarse con frecuencia para seguir siendo seguros. La capacidad de la IA y de los algoritmos de aprendizaje automático para analizar grandes volúmenes de datos con rapidez facilita que los atacantes identifiquen nuevas vulnerabilidades.

[Los datos indican](#) que se expone una nueva vulnerabilidad de ciberseguridad cada 17 minutos, y que el [75%](#) de estas se explotan dentro de los 19 días posteriores. El uso de sistemas obsoletos en la banca no es poco frecuente; por ejemplo, hasta el [85 %](#) de los cajeros automáticos operan con software o hardware desactualizados.



Medidas clave de seguridad para bancos e instituciones financieras

Son necesarias medidas de seguridad amplias e interconectadas para ayudar a proteger a las instituciones financieras frente a ataques físicos y cibernéticos. A continuación, se presentan algunas de las medidas clave a considerar.

Seguridad física

Infraestructura

Una infraestructura externa e interna reforzada puede ayudar a resistir ataques a la seguridad física. Las paredes de los bancos y las salas internas deben reforzarse con concreto y acero, y las dos o más salidas del establecimiento ([según lo exige la ley](#)) deben estar vigiladas y protegidas por sistemas de seguridad.

[Las regulaciones rigen](#) el diseño y la operación de la infraestructura utilizada para almacenar activos de valor. Los bancos deben contar con al menos una bóveda o caja fuerte con cerraduras resistentes a manipulaciones y un sistema de alarma conectado a las fuerzas de seguridad, además de un sistema de iluminación que permita iluminar el área durante la noche.

Control de acceso

[Los sistemas de control de acceso](#) ayudan a limitar intrusiones al proteger áreas sensibles mediante credenciales rastreables. Se pueden emitir credenciales únicas a las personas autorizadas en forma de dispositivos físicos o datos almacenados en un dispositivo inteligente, con permisos gestionados dentro de una plataforma digital.

Los responsables del negocio y los equipos de seguridad pueden crear, modificar y revocar credenciales según sea necesario desde un sistema de gestión con acceso remoto. También se pueden mantener registros de los eventos de acceso para facilitar investigaciones y garantizar el cumplimiento de regulaciones como la [Bank Secrecy Act](#).

Seguridad por video

Los [sistemas de seguridad por video](#) proporcionan una cobertura integral de las áreas sensibles en todo momento. Zonas clave como accesos, puestos de atención, salas de servidores y bóvedas pueden ser monitoreadas mediante cámaras de seguridad inteligentes con controles remotos, carcasas resistentes a manipulaciones y configuraciones para baja iluminación.

La [analítica de video con IA](#) permite que las cámaras detecten de forma autónoma y alerten a los operadores sobre riesgos potenciales, como movimientos sospechosos, desplazamiento de activos y armas ocultas. Se pueden enviar alertas remotas al personal de seguridad y el material puede marcarse para su revisión en un [sistema central de gestión de video \(VMS\)](#).

Sensores y alarmas

[Los sensores de Internet de las Cosas \(IoT\)](#) instalados en las instituciones financieras ayudan a alertar a los operadores sobre amenazas específicas. Algunos ejemplos incluyen sensores de movimiento para detectar intrusiones, sensores de sonido para identificar voces elevadas o disparos, y sensores ambientales para detectar incendios o desastres naturales.

Los sensores pueden vincularse a alarmas audibles y silenciosas para abordar distintos tipos de amenazas. Por ejemplo, los sensores de sonido pueden funcionar como botones de pánico cuando se pronuncian palabras clave, los sensores de presión pueden activar un bloqueo cuando se mueven activos y los sensores de movimiento pueden activar alarmas en el lugar.



Ciberseguridad

Autenticación Multifactor (MFA)

La MFA protege el acceso a sistemas digitales sensibles mediante dos o más credenciales únicas. Para acceder a datos privados, los usuarios deben ingresar formas adicionales de verificación, como información biométrica o un código PIN enviado a un dispositivo externo seguro, además de una contraseña robusta.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) [indica que una contraseña segura es:](#)

- **Larga:** 16 o más caracteres.
- **Aleatoria:** combinación de letras mayúsculas y minúsculas, números y símbolos.
- **Única:** utilizada solo para una cuenta.

Las recomendaciones de la CISA sugieren que la MFA puede reducir la efectividad de los intentos de hackeo en un [99%](#). Al seleccionar credenciales adicionales, se prefieren los identificadores biométricos como huellas dactilares, escaneos de iris o reconocimiento facial, ya que este tipo de información es mucho más difícil de falsificar que una contraseña.

Software de cifrado

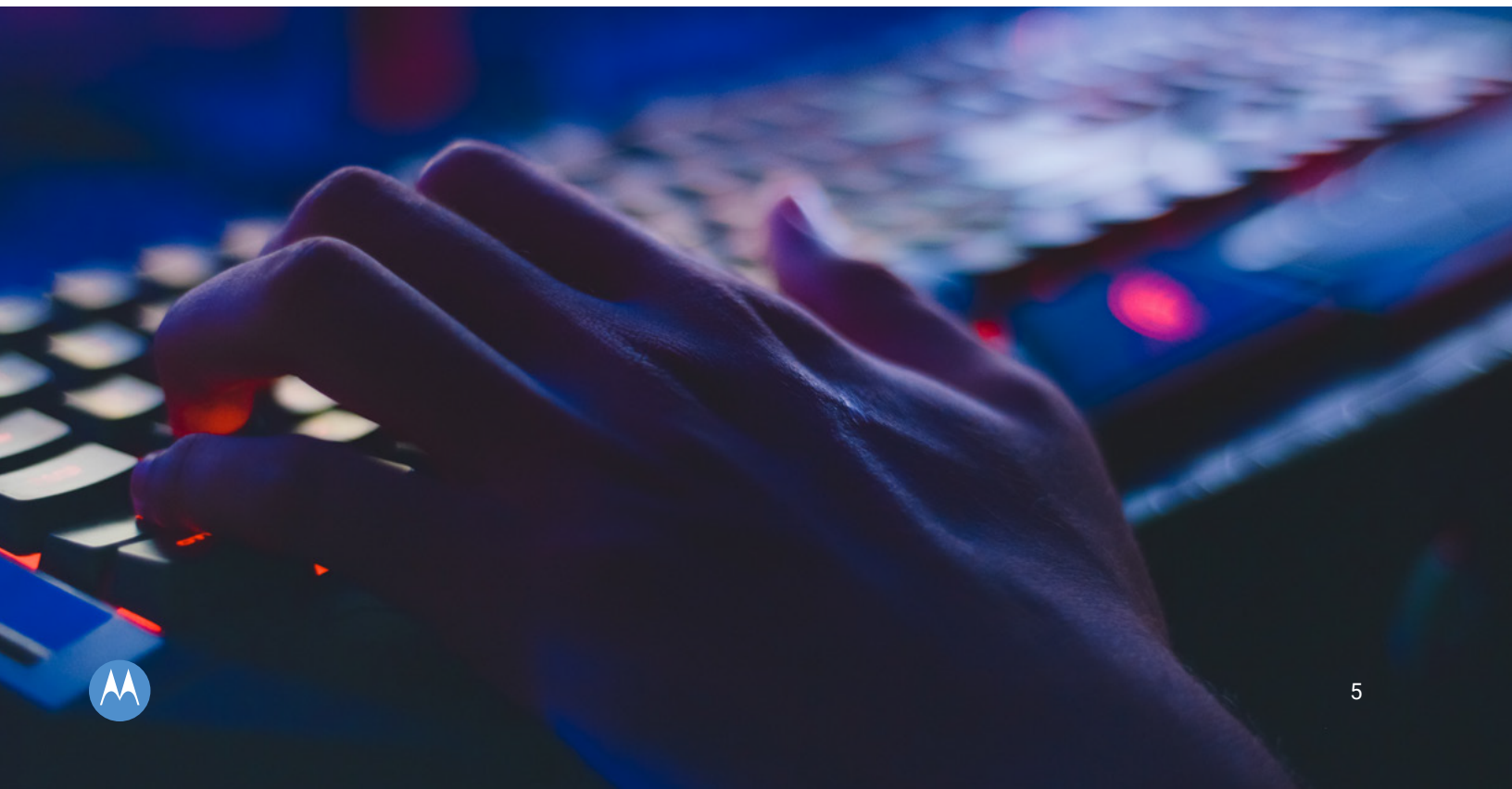
El software de cifrado protege los datos sensibles tanto en reposo como en tránsito. Cuando un mensaje que contiene datos sensibles, como información de clientes o de pagos, es cifrado, se vuelve ilegible para los hackers, ya que solo el remitente y el destinatario tienen acceso a la clave que descifra los datos.

Detección de intrusiones

Los Sistemas de Detección de Intrusiones en Red (NIDS) ayudan a identificar vulnerabilidades y actividades sospechosas en los sistemas digitales. Los NIDS inspeccionan el tráfico entrante y saliente de los sistemas informáticos en busca de señales de actividad anómala y alertan al personal de seguridad sobre acciones asociadas a ciberataques.

Prevención de Pérdida de Datos (DLP)

Las soluciones DLP minimizan el impacto de los ciberataques al rastrear el movimiento de datos sensibles y activar sistemas más amplios para ayudar a prevenir la pérdida de datos. Las herramientas DLP se activan en respuesta a actividades sospechosas, como el envío de datos sensibles por correo electrónico o la copia de archivos en una unidad USB.





Capacitación y educación

Capacitación en concientización

Todos los empleados deben ser capacitados para utilizar y operar de forma segura, en línea con las medidas de seguridad.

Una capacitación efectiva en concientización sobre seguridad debe cubrir:

- **Tecnologías:** por ejemplo, cómo utilizar sistemas de control de acceso, cómo reportar el uso indebido de credenciales, cómo activar alarmas, cómo contactar al personal de seguridad y cómo permanecer dentro del campo de visión de las cámaras.
- **Comportamientos:** por ejemplo, cómo detectar intentos de tailgating, cómo identificar armas ocultas, cómo reconocer operaciones de reconocimiento y cómo desescalar situaciones volátiles.
- **Respuestas:** por ejemplo, cómo responder de manera segura y evacuar ante amenazas comunes, como eventos de agresor activo, robos, amenazas de bomba, incendios y desastres naturales.

Capacitación en ciberseguridad

El error humano es un factor clave en la mayoría de los ciberataques. En 2024, el [95%](#) de las filtraciones de datos involucraron algún tipo de error provocado por los usuarios, lo que refuerza la importancia de la capacitación en ciberseguridad.

Las instituciones financieras deben garantizar que todos los empleados reciban entrenamientos periódicos sobre el uso seguro y la protección de los sistemas digitales.

Los aspectos críticos que deben abordarse incluyen la concientización sobre phishing e ingeniería social, la gestión de credenciales, las mejores prácticas para el intercambio de archivos y planes seguros de eliminación de datos.

Capacitación en cumplimiento normativo

Los bancos y las instituciones financieras están regulados por normativas de amplio alcance que establecen cómo deben manejarse los datos sensibles y los activos de alto valor. La capacitación en seguridad del personal debe cubrir las mejores prácticas para garantizar el cumplimiento de estas normas y las consecuencias del incumplimiento de las políticas.

Ejemplos de regulaciones que deben abordarse incluyen:

- **Bank Secrecy Act (BSA):** detalla los estándares de registro y reporte para bancos nacionales, asociaciones federales de ahorro y agencias federales y de bancos extranjeros.
- **Payment Card Industry Data Security Standard (PCI DSS):** establece estrictos estándares de seguridad diseñados para proteger los datos de tarjetas de pago contra accesos no autorizados.
- **Gramm-Leach-Bliley Act (GLBA):** define estándares para la protección de información personal no pública y la implementación de disposiciones de ciberseguridad, como la MFA, en los bancos.



Tendencias emergentes y tecnologías en seguridad bancaria

La transformación digital y los avances en inteligencia artificial y aprendizaje automático continúan influyendo en nuevas tendencias y tecnologías en la seguridad del sector financiero, entre ellas:

Regulaciones antifraude

La [Government Accountability Office \(GAO\)](#) señala que los llamados a implementar medidas de cumplimiento más estrictas en la industria financiera para abordar los ciberataques impulsados por IA y las estafas con medios sintéticos podrían influir en futuros ajustes regulatorios.

Seguridad en la nube

La creciente sofisticación de las amenazas contra las instituciones financieras está llevando a muchos bancos a explorar [estrategias de seguridad](#) basadas en la nube. En 2022, al menos el **82%** de los grandes bancos contaba con una estrategia clara de nube, frente al 47% en 2018.

Control de acceso biométrico

Las regulaciones más estrictas que rigen el manejo de datos sensibles están impulsando a muchas instituciones financieras a explorar controles de acceso inteligentes. En 2023, el **64%** de las instituciones financieras a nivel global ya utilizaban autenticación biométrica.

Analítica de video con IA

Las cámaras equipadas con analítica de video basada en IA están ganando popularidad en la industria financiera, ya que permiten al personal de seguridad identificar y responder ante amenazas e informar sobre el funcionamiento de diversas tecnologías.

Seguimiento de activos mediante RFID

Las etiquetas RFID adheridas a activos de alto valor proporcionan visibilidad en tiempo real de las operaciones, lo que ayuda a los bancos a mantener el cumplimiento de las regulaciones de registro. Se proyecta que el mercado de sistemas de seguimiento de activos mediante RFID alcance los **41.700 millones de dólares** para 2031.



Consideraciones al implementar medidas de seguridad bancaria

Asegurar de manera eficaz a las instituciones financieras requiere una combinación específica de personal capacitado, estrategias basadas en datos y tecnologías avanzadas.

Las implementaciones deben diseñarse para responder a las necesidades particulares de cada organización, tanto en términos de configuración como de gestión diaria.

Evaluaciones de riesgo

Los líderes y los equipos de seguridad deben analizar las instalaciones, realizar un inventario de los activos de valor e identificar posibles amenazas y vulnerabilidades. Una [evaluación de riesgos exhaustiva](#) ayuda a los equipos a priorizar medidas y tecnologías rentables y adecuadas para su organización.

Este proceso debe incluir un recorrido por las instalaciones para inspeccionar las medidas existentes, pruebas de penetración y la revisión de informes históricos de incidentes. Todos los riesgos y vulnerabilidades identificados deben evaluarse y priorizarse según su gravedad y la probabilidad de que ocurran de manera inminente.

Presupuesto

Las evaluaciones de riesgos deben proporcionar a los líderes una comprensión clara de las necesidades actuales de seguridad; con esta información, los fondos disponibles pueden asignarse a mejoras prioritarias. Es importante tomarse el tiempo para evaluar los pros y los contras de actualizar los sistemas existentes o invertir en nuevas soluciones.





Requisitos de instalación

La planificación del presupuesto para las medidas de seguridad financiera también debe contemplar los costos y requisitos de instalación. Los equipos deben revisar la infraestructura de seguridad para confirmar si las tecnologías y los sistemas propuestos requerirán nuevas soluciones de energía, comunicaciones o almacenamiento de datos.

Se pueden contratar instaladores e integradores profesionales de sistemas de seguridad para instalar y configurar tecnologías como cámaras, sensores y sistemas de control de acceso. Estos profesionales pueden asesorar a los líderes sobre la ubicación y la configuración más efectivas de los dispositivos, con el fin de garantizar una cobertura óptima.

Mantenimiento

Las medidas de seguridad bancaria físicas, digitales y organizacionales requerirán cierto nivel de mantenimiento para funcionar de manera eficaz. Por ejemplo, las cámaras deben limpiarse, el software de seguridad requiere actualizaciones y la infraestructura debe inspeccionarse de forma periódica.

El mantenimiento menor suele poder realizarse de manera interna. Sin embargo, los productos de seguridad clave, como cámaras, alarmas y sistemas de control de acceso, deben ser inspeccionados regularmente por profesionales. Algunos proveedores actualizan automáticamente el software a través de la nube para ayudar a mitigar nuevas amenazas cibernéticas.

Escalabilidad

Los planes futuros deben tenerse en cuenta en las decisiones de seguridad. Los líderes deben considerar si la incorporación de nuevos productos o la expansión a otras ubicaciones requerirá integración, por ejemplo, entre nuevas sucursales bancarias, y si resultaría beneficioso gestionar múltiples sistemas de seguridad desde una única plataforma.



Soluciones Avigilon para bancos e instituciones financieras



Seguridad por video con IA

El portafolio integral de [cámaras de seguridad con IA](#) de Avigilon, parte del ecosistema de seguridad y protección de Motorola Solutions, ofrece video de alta resolución respaldado por funciones y capacidades avanzadas que refuerzan la seguridad en bancos y otras instituciones financieras.

Desde cámaras domo y bullet hasta soluciones de giro, inclinación y zoom (PTZ) y reconocimiento de matrículas, Avigilon ofrece opciones on-premise y basadas en la nube que permiten a los equipos de seguridad observar actividades en tiempo real, detectar con precisión y responder rápidamente ante posibles amenazas. Combinada con potentes analíticas de [video basadas en IA](#), la organización puede fortalecer la seguridad y las operaciones diarias mediante el uso de analíticas avanzadas para identificar individuos prohibidos, detectar actividades sospechosas y supervisar niveles de personal y flujo de personas, con el fin de gestionar las operaciones de manera eficiente.

Avigilon también ofrece [sistemas de gestión de video \(VMS\) on-premise y en la nube](#). El VMS permite una seguridad proactiva al facilitar que los operadores reciban alertas de amenazas en tiempo real, identifiquen eventos y busquen rápidamente grabaciones para detectar riesgos y evitar que los incidentes ocurran o escalen. Además, el VMS puede integrarse con otros sistemas de seguridad, como el control de acceso y tecnologías de sensores, lo que ayuda a crear una solución unificada.

Ver soluciones



Control de acceso

Avigilon ofrece [soluciones de control de acceso escalables](#), tanto on-premise como en la nube, para instituciones financieras, diseñadas para gestionar puntos de entrada y ayudar a proteger áreas restringidas frente a personal no autorizado.

La solución de control de acceso permite a los bancos gestionar eventos de acceso, identificar y responder rápidamente a posibles amenazas en tiempo real, así como iniciar bloqueos de seguridad en las instalaciones. Los operadores también pueden consultar registros detallados de acceso durante la investigación de incidentes y otorgar o revocar credenciales de acceso, lo que refuerza aún más la seguridad en todas las instalaciones.

Cuando se integra con la seguridad por video de Avigilon, los equipos de seguridad bancaria obtienen una mayor conciencia situacional y procesos más eficientes. Por ejemplo, los operadores pueden mejorar los procedimientos de verificación al confirmar visualmente a una persona que solicita acceso, analizando el video en vivo captado por una cámara Avigilon cercana al punto de entrada. Esto no solo eleva los estándares de verificación, sino que también incrementa la seguridad al ayudar a mantener fuera a personas no autorizadas.

Ver soluciones





Protección del sitio

[Avigilon Alta Protect](#) es un sistema moderno de protección de instalaciones con IA que combina analíticas de video y audio, datos de sensores y un potente motor de reglas (Rules engine) para detectar, disuadir y responder rápidamente ante actividades sospechosas.

A diferencia de los sistemas de alarma tradicionales, Alta Protect aprovecha las analíticas de IA basadas en cámaras de Avigilon e integra control de acceso y datos adicionales de sensores para mejorar las alertas y reducir los falsos positivos. Esto permite a los equipos y operadores de seguridad bancaria mejorar los tiempos de respuesta ante incidentes, ayudar a proteger las instalaciones y reforzar la seguridad del personal y de los clientes.

[Ver soluciones](#)



Tecnología de sensores

El [Sensor inteligente Halo](#), dispositivo todo en uno, está diseñado para monitorear condiciones ambientales, detectar intrusiones, analizar la ocupación y optimizar el uso de energía en bancos y otras instituciones financieras.

Ideal para su uso en áreas sensibles a la privacidad donde no se permiten cámaras, como los baños, los sensores avanzados de la solución pueden detectar con precisión el uso de dispositivos de vapeo, ruidos fuertes, cambios en la calidad del aire y más. Esto ayuda a los equipos de seguridad a responder ante eventos de protección y seguridad, incluidos clientes vapeando en baños, comportamientos agresivos hacia el personal y otras amenazas a la seguridad.

El sensor inteligente Halo también permite a los bancos mejorar la calidad del aire y reducir los niveles de ruido para crear un ambiente cómodo y profesional tanto para el personal bancario como para los visitantes.

Cuando se integra con los sistemas de seguridad de Avigilon, ofrece alertas en tiempo real sobre eventos críticos, lo que permite una respuesta más rápida a los incidentes y un mayor nivel de seguridad.

[Ver soluciones](#)





Casos de estudio

Descubra cómo las instituciones financieras han utilizado las soluciones de seguridad física de Avigilon para reforzar la protección, mejorar la seguridad y optimizar las operaciones.

Ayudando a mantener segura a Brooklyn Cooperative Federal Credit Union

La protección de los activos y la seguridad del personal son prioridades clave para Brooklyn Cooperative, junto con la capacidad de cumplir con los estándares críticos de seguros. Para lograrlo, la organización implementó el sistema de seguridad por video Avigilon Unity con el fin de proteger sus activos y, al mismo tiempo, mantener un entorno acogedor para sus miembros.

Brooklyn Cooperative ahora puede cumplir e incluso superar los requisitos establecidos por su aseguradora, lo que permite reducir las primas. Gracias a la cobertura detallada del vestíbulo de los cajeros automáticos, la cooperativa de crédito también puede resolver reclamos por fraude con tarjetas de débito, disminuyendo los costos por responsabilidad. Además, el equipo de seguridad de Brooklyn Cooperative supervisa las áreas de almacenamiento y las oficinas para ayudar a proteger la información confidencial contra pérdidas o robos, y puede buscar y localizar grabaciones en una fracción de tiempo en comparación con el sistema anterior.

“

Avigilon es mil veces más fácil de usar que nuestro sistema anterior. Identificamos al responsable en menos de 10 minutos y recuperamos con éxito los fondos perdidos.

– Samira Rajan, CEO de Brooklyn Cooperative Federal Credit Union

[Leer caso de estudio](#)

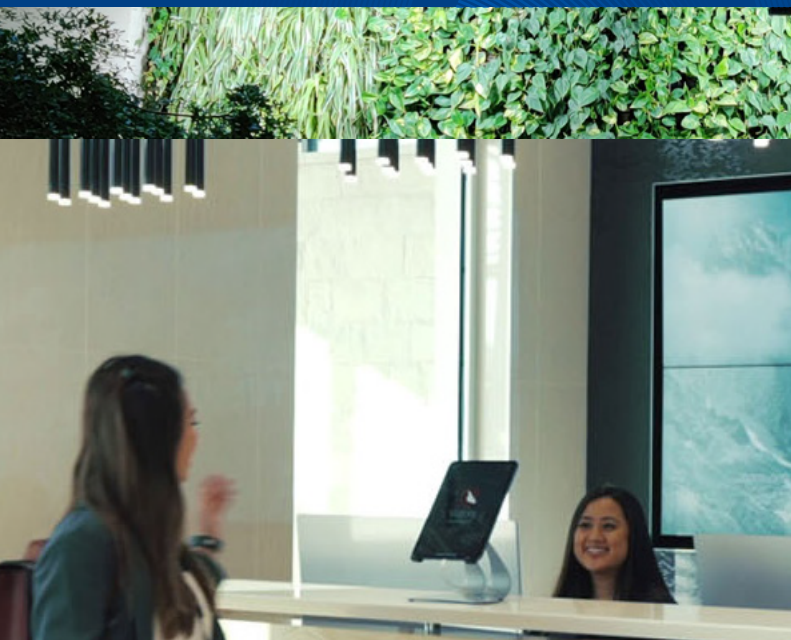




“

Las tecnologías de búsqueda de video de Avigilon son eficientes y efectivas y, al integrar la seguridad por video con el control de acceso, pueden reducir horas de trabajo a solo minutos.

– Ghaleb Karout, Subgerente Ejecutivo del Departamento de Infraestructura de TI de CSC



“

Avigilon Alta es realmente fácil de usar, especialmente porque está integrada en nuestros smartphones. Es sencillo ingresar en cualquier momento y a cualquier hora.

– Emi Matsumoto, Tecnología de la Información, K1

Soluciones de seguridad en las que CSC puede confiar

Con más de 350 empleados distribuidos en dos ubicaciones y estrictos requisitos de seguridad y privacidad, CSC necesitaba implementar una solución que ofreciera capacidades tanto de seguridad por video como de control de acceso para cumplir con las regulaciones del sector. Como resultado, CSC implementó la solución Avigilon Unity para ayudar a proteger a las personas, las instalaciones y los activos de manera más eficiente.

CSC ha utilizado con frecuencia los beneficios que brinda la integración de la seguridad por video y la tecnología de control de acceso dentro de la plataforma Avigilon Unity, especialmente las funciones de Identity Search y Appearance Search. El equipo de seguridad eligió Avigilon porque sus soluciones responden a las necesidades actuales de seguridad y valora que se incorporen de forma continua nuevas funciones y tecnologías que aportan mayor valor al sistema.

[Leer caso de estudio](#)

Soluciones elegantes para una firma de inversión orientada al futuro

Con múltiples tipos de espacios que requieren distintos niveles de acceso y seguridad, la gestión del control de acceso de K1 Investments debía ser segura, personalizable y estar disponible de forma remota las 24 horas del día, los 7 días de la semana, para permitir el ingreso incluso cuando no hubiera personal físicamente en la oficina. Por sobre todo, buscaban crear un espacio de alta tecnología, orientado al futuro, que fuera tan funcional como atractivo.

El diseño sofisticado y la tecnología de vanguardia de Avigilon Alta fueron la combinación perfecta para la visión de K1 de su sede de alta tecnología. La solución permitió al personal utilizar acceso sin contacto para ingresar a las instalaciones las 24/7 y posibilitó que los operadores gestionaran usuarios y niveles de acceso desde la nube. Además, la tecnología de Alta ayuda a K1 a cumplir con los requisitos de cumplimiento normativo y a proteger la información altamente sensible de sus clientes.

[Leer caso de estudio](#)



Checklist completo de seguridad para bancos e instituciones financieras

Los riesgos que enfrentan los bancos y las instituciones financieras suelen ser complejos y sofisticados. Por lo tanto, es fundamental implementar medidas de seguridad integrales. Para orientar soluciones bien integradas y efectivas, a continuación se presenta un checklist completo de seguridad para bancos e instituciones financieras.

Evaluaciones de riesgo

- Se han identificado los activos físicos (efectivo, tecnología, etc.) y digitales (datos, sistemas, etc.).
- Se han recopilado y analizado informes internos de incidentes y registros de delitos locales.
- Los sistemas y las medidas de seguridad existentes se han revisado con profesionales especializados.
- Se han identificado y priorizado los riesgos y las vulnerabilidades.
- Las mejoras y los controles han sido propuestos y acordados por las partes interesadas.

Cámaras de seguridad

- Cámaras resistentes a las condiciones climáticas cubren entradas, salidas y perímetros exteriores.
- Cámaras adecuadas monitorean áreas internas de alto riesgo (cajas, bóvedas, etc.).
- Las cámaras de CCTV están instaladas en posiciones elevadas e inaccesibles al público.
- Las cámaras funcionan correctamente y brindan una cobertura integral de las áreas objetivo.
- Las cámaras utilizan analíticas de video con IA para detectar amenazas comunes.
- Las cámaras están integradas con sistemas de seguridad más amplios.
- El personal de seguridad cuenta con acceso on-premise y/o remoto a las transmisiones en vivo y grabadas en todo momento.
- El personal de seguridad recibe alertas cuando las cámaras detectan actividad sospechosa.
- El personal de seguridad realiza mantenimiento, limpieza e inspecciones periódicas de las cámaras para detectar daños.
- El personal de seguridad mantiene y revisa regularmente los registros de mantenimiento de las cámaras.

- Las grabaciones de las cámaras se almacenan y registran en un VMS ciberseguro.
- Las grabaciones de las cámaras se conservan hasta por 6 meses, de acuerdo con los estándares del sector.
- El sistema de cámaras es inspeccionado por un técnico calificado dos veces al año.

Control de acceso

- Todos los puntos de acceso exteriores están asegurados mediante cerraduras resistentes a manipulaciones.
- Todas las entradas y salidas están protegidas por sistemas de control de acceso.
- Todas las áreas internas de alto riesgo están protegidas por sistemas de control de acceso.
- Los sistemas de control de acceso están integrados con sistemas de seguridad más amplios.
- Los empleados reciben credenciales de acceso rastreables.
- A los empleados solo se les concede acceso a las áreas necesarias para el desempeño de sus funciones.
- Se pueden emitir credenciales temporales para contratistas, visitantes y fuerzas del orden.
- Se utilizan MFA y biometría para proteger áreas de alto riesgo (salas de servidores, bóvedas, etc.).
- Todos los eventos de acceso se registran automáticamente en un sistema digital de gestión de seguridad.
- El personal de seguridad revisa periódicamente los registros de acceso.
- El personal de seguridad puede ajustar y revocar permisos de forma remota.
- El sistema de control de acceso es inspeccionado por un técnico calificado dos veces al año.





Sensores y alarmas

- Todos los puntos de acceso están cubiertos por alarmas activadas por sensores.
- Se instalan botones de pánico en áreas de alto riesgo, como cajas y bóvedas.
- Sensores de sonido, presión y movimiento activan las alarmas correspondientes, como disparos y rotura de vidrios.
- El personal de seguridad y la policía reciben alertas remotas cuando se activan las alarmas.
- Los sensores y las alarmas están integrados con sistemas de seguridad más amplios.
- Las alarmas activadas pueden bloquear puntos de acceso y marcar grabaciones de cámaras para su revisión.
- Los sistemas de alarma son probados mensualmente por el personal de seguridad.
- Los sensores y sistemas de alarma son inspeccionados por un técnico calificado dos veces al año.

Ciberseguridad

- Se implementan firewalls para proteger contra accesos no autorizados a la red.
- Se implementan sistemas NIDS para monitorear el tráfico de red.
- Se implementan soluciones DLP para mitigar eventos de pérdida de datos.
- Se implementa autenticación multifactor para proteger todos los sistemas digitales.
- Ninguna credencial se utiliza para acceder a más de un sistema digital.
- Todos los sistemas de seguridad y gestión reciben actualizaciones de software periódicas.
- Se realizan auditorías de ciberseguridad y pruebas de penetración al menos una vez al año.

Capacitación de empleados

- Se realizan capacitaciones en seguridad física y ciberseguridad cada seis meses.
- Se utilizan reportes de incidentes y registros delictivos locales para identificar amenazas comunes.
- Los empleados saben cómo responder de forma segura ante las amenazas identificadas.
- Los empleados saben cómo utilizar y trabajar de acuerdo con los sistemas de seguridad activos.
- Los empleados saben cómo reportar actividades sospechosas y activar alarmas.
- Los empleados saben que no deben acceder a datos sensibles desde dispositivos personales.
- Los empleados saben cómo cumplir con las normativas de privacidad y protección de datos.
- Los empleados reciben capacitaciones periódicas en gestión de contraseñas.
- Los empleados reciben capacitaciones periódicas sobre concientización en ingeniería social.
- Los recursos y materiales de capacitación están disponibles para todos los empleados.
- Los planes de respuesta ante emergencias y evacuación están disponibles para todos los empleados.



Recursos adicionales

[Guía de analítica de video](#)

Explore la analítica de video, cómo funciona la tecnología, los diferentes tipos, sus beneficios y los aspectos a considerar al adoptarla.

[Diferentes tipos de cámaras de seguridad](#)

Esta guía completa explora los diferentes tipos de cámaras de seguridad, sus ventajas y desventajas, y las características específicas para diversas aplicaciones.

[Guía de sistemas de alarma contra intrusión](#)

Conozca cómo los sistemas de alarma contra intrusión combinan analítica de video y audio con IA, control de acceso y datos de sensores para detectar y responder a actividades sospechosas.



Empiece hoy mismo a trabajar en su seguridad



AVIGILON™

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com

© 2025, Avigilon Corporation. Todos los derechos reservados. MOTOROLA, MOTO, MOTOROLA SOLUTIONS y el logotipo estilizado M son marcas comerciales o marcas registradas de Motorola Trademark Holdings, LLC y se utilizan bajo licencia. Todas las demás marcas son propiedad de sus respectivos dueños. 07-2025 [JMS02]