Securitas Technology

Versión en español

2027 Global Technology Outlook Report



securitastechnology.com/us-es

Securitas Technology

Contenido

01

Introducción 04-15

P06 | Agradecimientos

P08 | Mensaje de bienvenida y prólogo

P10 | Securitas Technology: visión general

P12 | Descripción general de la plataforma SecureStat HQ

02

Resumen ejecutivo 16-31

P18 | 2027 technology outlook

P24 | Conclusiones clave para los líderes de seguridad

P26 | Información sobre clientes, mercado y socios tecnológicos.

03

Aprovechar la oportunidad que ofrece la IA 32-57

P36 | Mejorando la detección de amenazas con IA

P40 | GenAI para operaciones de seguridad más inteligentes

P46 | La IA agéntica para agilizar las decisiones de seguridad.

P50 | Optimización de la seguridad empresarial impulsada por IA

P56 | Plan de acción para profesionales de la seguridad

04

Soluciones en la nube que transforman la seguridad 58-85

P62 | La base para la seguridad de próxima generación

P68 | Supervisión y mantenimiento del estado del sistema

P72 | Verificación remota y gestión de incidentes

P78 | Gestión centralizada del sistema de seguridad

P84 | Plan de acción para profesionales de la seguridad

05

Drones y robots llevando la seguridad al límite 86-109

P90 | Detección de drones

P96 | Drones para vigilancia

P100 | Robots en seguridad

P108 | Plan de acción para profesionales de la seguridad

06

Salvaguardar el Ecosistema de seguridad física 110-133

P114 | Mejores prácticas de seguridad de datos

P120 | Fiabilidad de los datos

P126 | Sistemas de seguridad resistentes a la computación cuántica

P132 | Plan de acción para profesionales de la seguridad

07

Perfiles de colaboradores 134-173

P136 | Socios tecnológicos destacados

P164 | Securitas destaca

Securitas Technology

01

Introducción

En esta sección

- Agradecimientos
- Mensaje de bienvenida y prólogo
- Securitas Technology: visión general
- SecureStat HQ Descripción general de la plataforma

Securitas Technology

Gracias a nuestros socios estratégicos de tecnología y expertos de la industria que han contribuido.

Los principales innovadores y tecnólogos en seguridad del mundo.

Gracias a nuestra estrecha colaboración con los principales innovadores, tecnólogos y fabricantes de productos de seguridad, ofrecemos a nuestros clientes un acceso inigualable a las soluciones de seguridad más avanzadas y sostenibles disponibles en la actualidad.

3xLOGIC
AJAX
AMAG TECHNOLOGY An Allied Universal Company
ARITECH
ASSA ABLOY
AXIS COMMUNICATIONS
brivo simply better security
DMP
Genetec
Hanwha Vision
HID
Honeywell | LENEL·S2 by Honeywell
IDIS One Solution. One Company.
INTELLICENE SECURITY. EVOLVED.
IQSIGHT
MARCH networks A Delta Group Company
milestone
MOTOROLA SOLUTIONS
OpenEye
PACOM
radionix
resideo
Software House C·CURE IQ
SONITROL
VERINT
Viakoo

Securitas Technology

Prefacio

El informe más completo del mundo sobre tecnología de seguridad.

La IA, la nube y la robótica impulsan un nuevo ecosistema de seguridad.



Bienvenido al 2027 Global Technology Outlook Report

En primer lugar, quiero expresar mi entusiasmo por presentar la novena edición anual de este informe. Sin duda, es nuestra publicación más esperada cada año, ya que combina datos globales exclusivos, perspectivas e investigaciones de nuestros socios tecnológicos estratégicos, expertos y internos además de la encuesta líder mundial a clientes finales y principales responsables de la toma de decisiones del mercado, ¡todo en uno!

La seguridad está cambiando y las tendencias son importantes. Los riesgos físicos y digitales siguen convergiendo, el ritmo de la innovación, especialmente en inteligencia artificial, se está acelerando, y se les pide a los líderes de seguridad que respondan a desafíos más complejos con mayor rapidez, inteligencia y confianza. En el mundo actual, las tendencias tecnológicas no solo respaldan la seguridad. La están moldeando activamente.

Esa urgencia refleja las razones clave por las que publicamos el informe cada año: para brindar a nuestros clientes una visión clara y práctica de las tendencias de seguridad electrónica que más importarán, y para ayudarlos a tomar decisiones informadas sobre futuras inversiones y sus planes de acción para programas de seguridad.

El informe reúne perspectivas de cuatro fuentes importantes

- **Los clientes finales** utilizan nuestra exclusiva Encuesta Global de Clientes, una de las más grandes del mundo con 16.000 encuestados en 19 países, como referencia para conocer la evolución de sus necesidades, además de los comentarios de los ejecutivos de nuestro prestigioso Consejo Asesor de Clientes, compuesto por profesionales de diversos sectores.
- **Responsables de la toma de decisiones en materia de seguridad electrónica,** con una amplia investigación realizada de forma independiente por NewtonX en los sectores comerciales y empresariales de todo el mundo.
- **Nuestros socios tecnológicos estratégicos,** que representan a las marcas líderes mundiales en productos de seguridad, cuyas hojas de ruta de innovación, investigación y desarrollo contribuyen a definir hacia dónde se dirige la industria con nuevos productos, software y otras tecnologías.
- **Un equipo especializado de líderes tecnológicos globales internos y expertos en la materia,** que representan a más de 15 países y mercados locales en todo el mundo, y están dedicados a la investigación, el análisis, la evaluación, la comparación y las pruebas de tecnología.

En conjunto, estas perspectivas nos brindan **la visión más completa del mundo sobre las tendencias tecnológicas** , las expectativas cambiantes y las oportunidades que se presentan.

Temas que marcarán el año 2027 y la nueva frontera del ecosistema de seguridad...

De cara al futuro, destacan varias tendencias cruciales que analizamos en profundidad a lo largo de este informe:

- **La inteligencia artificial** está teniendo un impacto en todos los aspectos de la tecnología y la gestión de la seguridad, ayudando a los equipos a detectar amenazas, gestionar incidentes y trabajar de forma más eficiente.
- **Las soluciones basadas en la nube** son cada vez más comunes y permiten operaciones de seguridad más flexibles, conectadas y resilientes.
- **Los drones y robots** están ampliando las posibilidades de visualización y actuación de los equipos de seguridad, ofreciendo nuevas formas de monitorizar ubicaciones y responder a incidentes a medida que se integran en el ecosistema de seguridad del futuro.
- A medida que los sistemas se vuelven más interconectados, **salvaguardar el propio ecosistema de seguridad física** — desde la integridad de los datos, la sostenibilidad y la higiene cibernética hasta la preparación para los riesgos de la era de la computación cuántica que se vislumbran en el horizonte — se ha vuelto esencial para los programas de seguridad de todo tipo y tamaño.

En Securitas Technology, estamos comprometidos a ayudar a nuestros clientes a afrontar estas tendencias en constante evolución con confianza, basándonos en décadas de experiencia en diversas disciplinas e industrias, y en estrechas colaboraciones con los principales fabricantes e innovadores de tecnología de seguridad del mundo.

Nuestra inversión en nuestra plataforma de gestión de seguridad SecureStat HQ ® refuerza ese compromiso. Al combinar datos, IA y experiencia humana, estamos sentando las bases para **una seguridad verdaderamente basada en la inteligencia**. En todo el Grupo Securitas, seguimos fortaleciendo nuestras capacidades y experiencia en inteligencia de riesgos y servicios especializados para poder satisfacer tus necesidades hoy y ayudarte a prepararte para el mañana.

Espero que este informe líder del sector te brinde información útil, te inspire nuevas ideas, respalde tu plan de inversión y te ayude a planificar el futuro. Gracias por tu continua colaboración y por la confianza que depositas en Securitas Technology como tu asesor de confianza.

Tony Byerly
Presidente Global y Director General
Securitas Technology

Sigue a Tony en LinkedIn

Securitas Technology

Acerca de Securitas Technology

Tu asesor de confianza en un panorama de seguridad en constante evolución.

Simplificando la complejidad para la seguridad de tu negocio.

- **Encontrar la tecnología adecuada para ti.** Trabajamos como tu asesor de confianza para ayudarte a identificar la mejor solución de seguridad para tus necesidades específicas.
- **Creamos tu solución completa y personalizada.** Diseñamos, integramos, instalamos, supervisamos, mantenemos y brindamos soporte integral para tu solución de seguridad electrónica.
- **Optimización de tus sistemas de seguridad.** Te ayudamos a optimizar y gestionar tus sistemas de seguridad mediante una extensa red de profesionales de seguridad altamente cualificados y certificados, y servicios remotos.



Obtenga más información sobre nuestras tecnologías, servicios y experiencia en el sector en **securitastechnology.com/us-es**



Un socio tecnológico global centrado exclusivamente en seguridad y protección.

40+

Países con capacidades y presencia en tecnología de seguridad

- Cobertura en **6** continentes
- **Empresa líder mundial** en seguridad electrónica comercial.

1M+

Sitios de clientes en todo el mundo

- **Más de 1,6 millones** de conexiones monitorizadas
- **Más de 1 millón** de llamadas de mantenimiento, inspección y servicio realizadas anualmente

12,000+

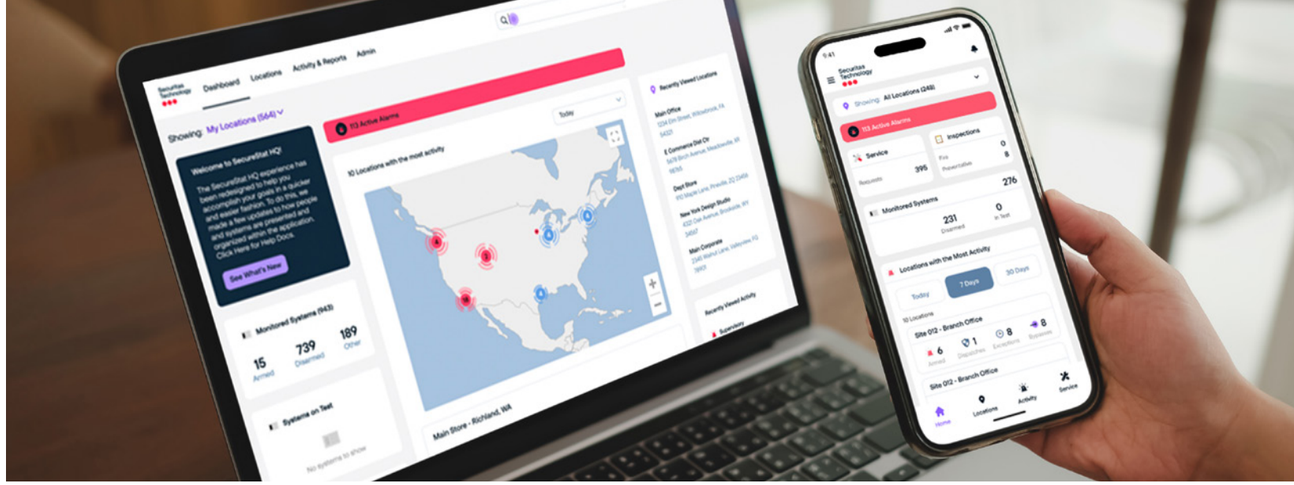
Empleados en todo el mundo

- **Más de 5000** técnicos
- **Más de 500** ingenieros/diseñadores arquitectos / Innovadores

Securitas Technology

SecureStat HQ®

La plataforma todo en uno para una seguridad optimizada



Ayudar a los clientes a tomar decisiones más inteligentes.

SecureStat HQ es una plataforma líder en la industria para la gestión de la seguridad. , combinando el control a nivel de sitio, la gestión de eventos en toda la organización, datos para optimizar la seguridad y un acceso sin interrupciones a nuestros servicios.

Proporciona a las organizaciones una comprensión clara de su entorno para que puedan tomar decisiones mejor fundamentadas y pasar de respuestas reactivas a operaciones basadas en la inteligencia.

A medida que los sistemas se vuelven más interconectados y las amenazas más dinámicas, SecureStat HQ actúa como la columna vertebral que unifica las alertas de seguridad empresarial, los análisis, los servicios y la información en todas las ubicaciones.

Comience con SecureStat HQ

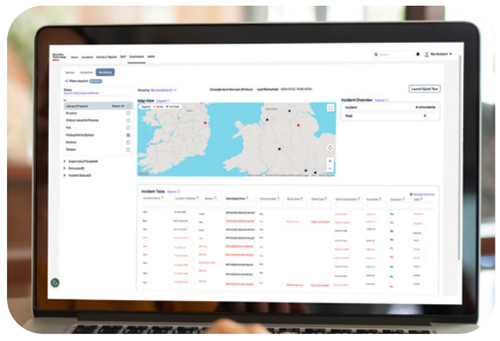
SecureStat HQ está disponible para tlos clientes de Securitas Technology en algunos mercados. Escanee el código QR ahora para solicitar una cuenta.

Unificar sistemas, sitios y datos en un solo lugar.

La inteligencia artificial generativa avanzada está transformando la forma en que trabajan los equipos de seguridad, pero su valor depende de contar con la plataforma adecuada. **SecureStat HQ proporciona a sus clientes esa base.**

Al centralizar la información procedente de sensores, cámaras y servicios de monitorización, ofrece **potentes herramientas** para ayudar a los clientes a comprender su postura de seguridad, identificar patrones y proporcionar información valiosa que permita tomar medidas de seguridad más rápidas y seguras.

SecureStat HQ es compatible con una **amplia gama de sistemas de las marcas líderes del sector,** integrando videovigilancia, control de acceso, sistemas de detección de intrusiones y mucho más.



Convertir los datos de seguridad en inteligencia empresarial.

SecureStat HQ conecta los sistemas de seguridad, los flujos de datos y los procesos automatizados más importantes, aportando **inteligencia proactiva** a las operaciones diarias de los clientes.

Con SecureStat HQ al alcance de la mano, los clientes pueden identificar dónde existen vulnerabilidades y dónde la tecnología puede ofrecer beneficios operativos significativos que respalden la mejora continua del negocio.

Ofrece una visión de 360 grados de los activos de seguridad.

También forma parte de la plataforma SecureStat HQ, **SecureStat 360** ® que permite una gestión proactiva del ciclo de vida de los sistemas y activos de seguridad física, respaldada por la excelencia operativa y de servicio. SecureStat 360 permite a los clientes:

- Maximizar la vida útil de los equipos
- Planificar las actualizaciones de manera más eficiente.
- Reducir la exposición a vulnerabilidades conocidas.
- Documentar las emisiones de CO2

Visualice y controle su seguridad con los paneles vde control de SecureStat HQ.

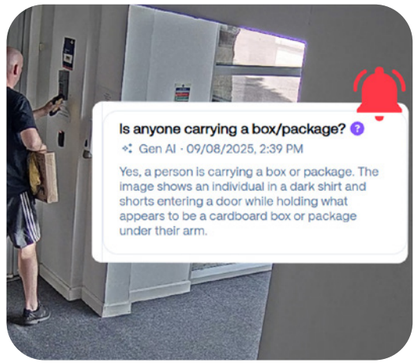
Los potentes paneles de control le permiten ver, explorar y compartir datos sobre aspectos críticos de sus operaciones de seguridad.

- **Panel de instalación:** Obtenga visibilidad en tiempo real del estado de los proyectos de instalación para que los equipos de operaciones, ventas y proyectos puedan supervisar el progreso, identificar retrasos y garantizar su finalización a tiempo.
- **Panel de control de monitoreo:** Centralice, gestione y analice la actividad de las alarmas en todas sus ubicaciones con eventos de las últimas 24 horas. Disponible como parte de las suscripciones Advanced y Premium.
- **Panel de servicio:** Acceda a un registro completo de su historial de servicio para ayudarle a realizar un seguimiento de las incidencias activas, comprender las tendencias e informar sobre la actividad del servicio.

Securitas Technology

Presentamos SecureStat® Cumulus™

SecureStat Cumulus amplía las capacidades de SecureStat HQ con una solución de vídeo basada en la nube que utiliza inteligencia artificial generativa (GenAI).



Con SecureStat Cumulus, las organizaciones obtienen controles visuales intuitivos, acceso desde cualquier lugar y notificaciones para eventos importantes. Ofrece flexibilidad de conexión de la cámara a la nube y una plataforma abierta compatible con una amplia gama de cámaras IP y routers. Sus funciones de IA generativa comprenden el lenguaje natural, interpretan el contexto y ayudan a los equipos a supervisar prácticamente cualquier cosa, desde la seguridad en el lugar de trabajo hasta la experiencia del cliente y las amenazas a la seguridad, simplemente describiendo lo que quieren ver.

Adéntrate en una nueva era de videovigilancia en la nube con IA.

Con paquetes flexibles de nube e inteligencia artificial que se adaptan a su negocio, SecureStat Cumulus es increíblemente fácil de implementar, usar y administrar. Escanea el código QR para obtener más información.

SecureStat Cumulus

Vídeo de cámara a la nube transformado por IA generativa.



Securitas Technology

02

Resumen Ejecutivo

En esta sección

- Perspectivas tecnológicas para 2027
- Información sobre clientes, mercado y socios tecnológicos.
- Conclusiones clave para los líderes de seguridad

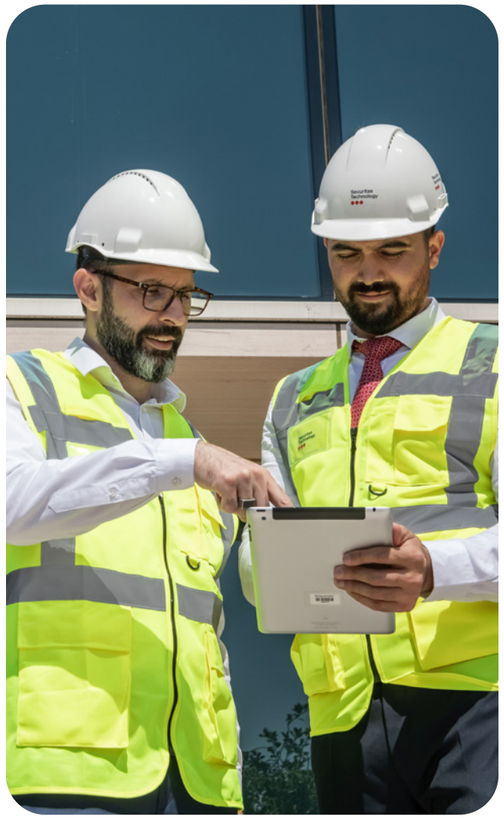
Securitas Technology

Perspectivas tecnológicas para 2027

La era de la seguridad conectada, basada en datos y automatizada



En los próximos años se observará una aceleración de los programas de seguridad multicapa altamente integrados, a medida que las organizaciones se adapten a un entorno en el que las amenazas físicas y digitales continúan convergiendo.



Según nuestros clientes [1], **los robos, el vandalismo, la seguridad de los empleados y el cumplimiento normativo** se encuentran entre las principales preocupaciones que impulsan las prioridades de sus programas de seguridad, lo que lleva a las organizaciones a centrarse en tecnologías y servicios de seguridad que les ayuden a anticipar mejor los riesgos, prevenir interrupciones y mejorar la respuesta ante incidentes.

Las 5 principales preocupaciones que impulsan las prioridades de seguridad de nuestros clientes [1]

01 Robos/ allanamiento

02 Intrusión/ vandalismo

03 Acceso no autorizado/ limitación de acceso

04 Seguridad de los empleados

05 Cumplimiento normativo

El uso de la inteligencia artificial está pasando de aplicaciones limitadas a un uso cotidiano. Los avances en la tecnología de IA generativa influirán en la forma en que los equipos de seguridad detectan amenazas, gestionan incidentes y manejan la creciente carga de trabajo operativa.

Al mismo tiempo, **la inversión en soluciones basadas en la nube y servicios remotos está aumentando** para fortalecer la resiliencia y mejorar la eficiencia en entornos distribuidos.

Existe **interés en el creciente potencial de los drones y las tecnologías robóticas** para ampliar la visibilidad, automatizar tareas rutinarias y proporcionar nuevas formas de mejorar la monitorización en tiempo real y el conocimiento de la situación.

Como fundamento de todo lo anterior, **cobra cada vez mayor importancia garantizar la integridad de las redes de seguridad física, ante el aumento de las amenazas ciberfísicas y la necesidad de contar con sistemas cada vez más conectados y automatizados en los que se pueda confiar.**

En todos los sectores, los líderes buscan soluciones proactivas y orientación práctica de socios de seguridad que puedan ayudarles a prever riesgos potenciales y a desarrollar programas de seguridad basados en inteligencia y preparados para el futuro.

1. Encuesta interna realizada a clientes de Securitas Technology en Australia, Bélgica, Canadá, Dinamarca, Finlandia, Francia, Alemania, Irlanda, México, Países Bajos, Noruega, Portugal, Singapur, España, Suecia, Suiza, Turquía, Reino Unido y Estados Unidos. Los datos mostrados reflejan únicamente las respuestas de los clientes comerciales. Realizado en noviembre de 2025.

Securitas Technology

Principales tendencias para 2027

01

Inteligencia artificial
La IA es ahora una parte fundamental del trabajo diario de seguridad, ya que reduce las falsas alarmas, mejora la detección de amenazas y automatiza tareas que requieren mucho esfuerzo en ámbitos como la videovigilancia, el control de accesos y las operaciones diarias.

02

Soluciones en la nube
Las soluciones basadas en la nube y los servicios remotos están haciendo que la seguridad sea más flexible, escalable y resistente gracias al acceso en cualquier momento y lugar, las actualizaciones automatizadas y los controles intuitivos.

03

Drones y robots
Estas tecnologías están ampliando el alcance de las operaciones de seguridad, brindando a los equipos visibilidad en tiempo real y capacidades de patrullaje cada vez más automatizadas.

04

Protección del ecosistema de seguridad física
Las organizaciones están dando prioridad a la integridad de los datos, la higiene cibernética y el uso responsable de la IA a medida que los sistemas se vuelven más interconectados y surgen nuevas amenazas, incluidos los riesgos cuánticos y los deepfakes.



Securitas Technology

Nuestras fuentes de datos

Encuesta global a clientes

16.000+

Clientes en 19 países

Investigación de mercado

575

Profesionales de la seguridad que representan a organizaciones de todo el mundo

Consultoría con socios tecnológicos

26

Líderes mundiales en innovación en tecnología de seguridad

Fuerzas globales que aceleran el cambio

- **La presión económica** está impulsando a las organizaciones a lograr más con menos recursos.
- **Las amenazas cibernéticas y físicas** continúan convergiendo de maneras que exigen respuestas coordinadas.
- **Las exigencias regulatorias** en materia de gobernanza de datos y prácticas responsables de IA están aumentando en diversas industrias.
- **La adopción de la nube** se está acelerando a medida que las organizaciones modernizan su infraestructura tecnológica.
- **La escasez de mano de obra** está impulsando la demanda de automatización y servicios remotos.



Perspectivas basadas en datos de mercado, amplia experiencia, y comentarios de los clientes

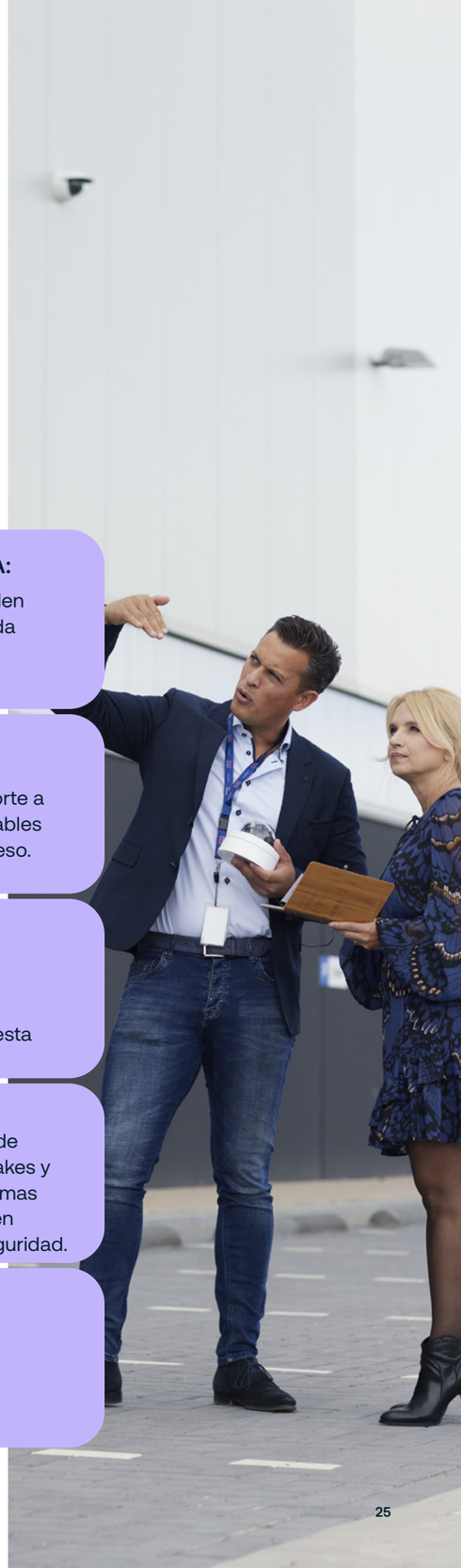
- **Encuesta global a clientes y comentarios del consejo asesor de 2025:**
  Un proceso de encuesta gestionado por Securitas Technology con respuestas de más de 16.000 clientes en 19 países. La encuesta global a clientes incluyó preguntas sobre la adopción prevista de tecnologías de seguridad y las inversiones realizadas en ellas. También se recabaron opiniones de los miembros del Consejo Asesor de Clientes de Securitas Technology, un grupo diverso de altos ejecutivos que representan a clientes usuarios finales de multitud de sectores y que proporcionan a Securitas Technology información sobre sus retos y necesidades en materia de tecnología de seguridad.
- **Investigación de mercado:**
  Un estudio de mercado externo encargado por Securitas Technology recabó respuestas de 575 profesionales de seguridad verificados que representan a organizaciones de Norteamérica, Europa y Asia-Pacífico. Dirigido a los responsables de la toma de decisiones directamente involucrados en las inversiones en tecnología, el estudio independiente se centró en la utilización actual, la adopción futura y la inversión planificada en materia de seguridad electrónica.
- **Consultoría con socios tecnológicos:** Un proceso consultivo gestionado por Securitas Technology para recopilar datos e información de 26 socios tecnológicos estratégicos que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de productos de seguridad del sector.
- **Expertos internos en la materia:**
  Una serie de entrevistas internas e investigaciones realizadas para recabar información de líderes tecnológicos internos y expertos en la materia de Securitas Technology en todo el mundo. Esto incluyó a miembros del equipo de Estrategia e Innovación Tecnológica de Securitas, el Comité Global de Revisión Tecnológica (GTRC) y el Consejo Global de Innovación Tecnológica (GTIC), en representación de más de 15 países y mercados locales.



Securitas Technology

Conclusiones clave para los líderes de seguridad

	Qué debes saber ahora	Cómo planificar con anticipación
→ 01	**La IA se está integrando en las operaciones de seguridad fundamentales...** ...ayudando a los equipos a detectar amenazas, abordar las falsas alarmas y agilizar las investigaciones con mayor precisión y rapidez.	**Crea una hoja de ruta práctica para la adopción de la IA:** Comienza con casos de uso específicos y de alto valor que te ayuden a seleccionar e invertir en infraestructura preparada para la IA. Valida la exactitud e integridad de las fuentes de datos e implementa directrices claras para su uso responsable.
→ 02	**Las soluciones en la nube y capacidades remotas...** ...son habituales y están transformando la prestación de servicios de seguridad, haciendo que las operaciones sean más escalables, resilientes y consistentes en múltiples ubicaciones.	**Construye sobre tu base en la nube:** Continua integrando la infraestructura en la nube para brindar soporte a la monitorización remota, la verificación remota y soluciones escalables para aplicaciones clave como la videovigilancia y el control de acceso.
→ 03	**Los sistemas autónomos están ganando terreno...** ...con drones y robots que apoyan a los equipos ampliando la visibilidad, mejorando la capacidad de respuesta y ayudando a automatizar tareas rutinarias, sentando las bases para la nueva frontera del ecosistema de seguridad.	**Evalúa la automatización para ampliar la capacidad del equipo:** Considera la posibilidad de implementar herramientas que ayuden a reducir la carga de trabajo manual, desde drones y robots hasta sistemas de monitoreo automatizados, para contribuir a una respuesta más rápida y eficiente ante incidentes.
→ 04	**La integridad de los datos y la higiene cibernética son fundamentales...** ...impulsados por la convergencia de riesgos físicos y digitales, y la necesidad de mantener la confianza en sistemas cada vez más automatizados.	**Invierte en la resiliencia de los ecosistemas:** Prioriza la higiene cibernética, refuerza las prácticas de integridad de datos y prepárate para las amenazas emergentes, como los deepfakes y los ataques habilitados por computación cuántica. Investiga las últimas directrices sobre resistencia cuántica y capacita a los empleados en inteligencia artificial y concienciación sobre los riesgos de ciberseguridad.
→ 05	**Los líderes buscan orientación en medio del rápido cambio tecnológico...** ...buscando socios de seguridad que puedan ayudarles a evaluar, adoptar y gestionar las soluciones adecuadas para su entorno.	**Prioriza los resultados, no las tecnologías:** Basa tus decisiones en los riesgos, desafíos y oportunidades más importantes para tu organización, y adopta nuevas tecnologías cuando respalden tu programa de seguridad.



Securitas Technology

Lo que nuestros clientes están priorizando

Conclusiones clave de nuestro proceso anual de consulta con clientes [1]

Tecnologías más adoptadas

Principales tecnologías de seguridad que utilizan actualmente nuestros clientes:



80% Detección de intrusiones

59% Detección de incendios

51% Videovigilancia

49% Control de acceso



Servicios basados en suscripción más adoptados

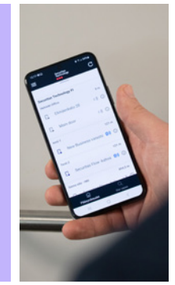
Principales servicios recurrentes de seguridad electrónica que utilizan actualmente nuestros clientes:

1. **74%** Monitoreo de alarmas de intrusión
2. **54%** Monitoreo de alarmas contra incendios
3. **45%** Videovigilancia
4. **45%** Contrato de servicios de reparación
5. **34%** Mantenimiento preventivo

Las 5 tecnologías más populares

Las tecnologías de seguridad que nuestros clientes están interesados en adoptar en los próximos 18 meses:

1. Inteligencia artificial — **26%**
2. Credenciales móviles en smartphones — **21%**
3. Protección móvil contra la coacción / trabajadores en solitario. — **19%**
4. Gestión de visitantes — **18%**
5. Biometría sin contacto — **18%**

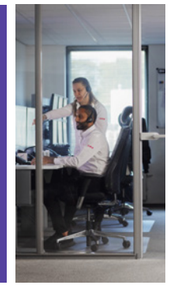




Los 5 servicios de suscripción más populares

Servicios de seguridad electrónica recurrentes que nuestros clientes están interesados en adoptar en los próximos 18 meses:

1. Servicios remotos basados en vídeo — **22%**
2. Gestión del ciclo de vida de activos/ equipos — **20%**
3. Inteligencia de riesgos — **19%**
4. Capacitación en seguridad contra incendios y preparación para emergencias — **18%**
5. Gestión remota de visitantes — **17%**





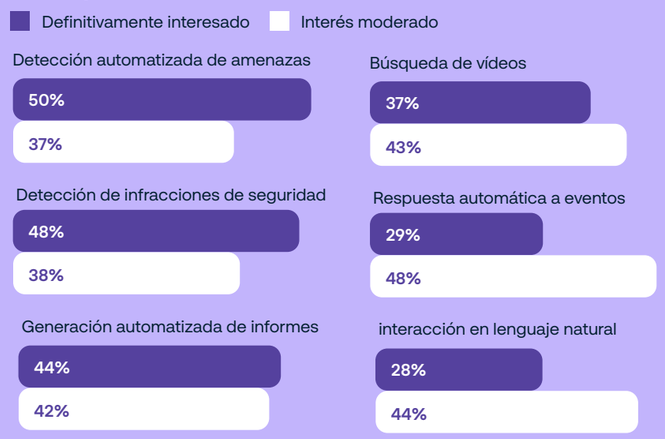
1. Encuesta interna realizada a clientes de Securitas Technology en Australia, Bélgica, Canadá, Dinamarca, Finlandia, Francia, Alemania, Irlanda, México, Países Bajos, Noruega, Portugal, Singapur, España, Suecia, Suiza, Turquía, Reino Unido y Estados Unidos. Los datos mostrados reflejan únicamente las respuestas de los clientes comerciales. Realizado en noviembre de 2025.

Securitas Technology

Tendencias del mercado de la tecnología de seguridad

Perspectivas globales de los responsables de la toma de decisiones y las personas influyentes en la seguridad electrónica comercial [1]

Principales casos de uso futuros de AI Generativa

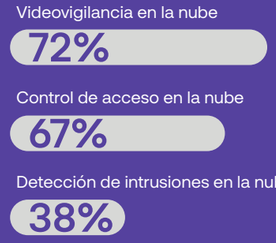


Los 3 principales desafíos en la implementación de la IA

1. **48%** Retorno de la inversión incierto
2. **47%** Preocupaciones sobre el cumplimiento normativo y la privacidad
3. **41%** Falta de conocimiento interno

44% Planean aumentar el uso de servicios remotos basados en la nube.

Las mejores soluciones en la nube utilizadas actualmente



Los 3 principales factores que impulsan la adopción de servicios remotos.

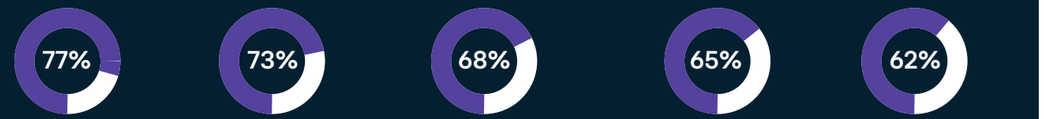
1. **61%** Ahorro de costes
2. **58%** Respuesta más rápida ante incidentes
3. **46%** Mayor disponibilidad

Drones, detección de drones y robots

Detección de drones	Vigilancia con drones	Robots
3.8% → 9.7%	5.4% → 9.9%	7.3% → 9.9%
Uso actual → Uso previsto	Uso actual → Uso previsto	Uso actual → Uso previsto

5.7% de las organizaciones reportan un incidente relacionado con drones en el último año

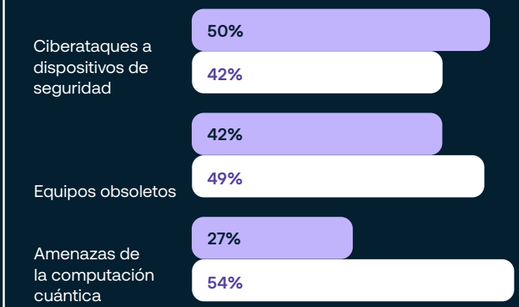
Prácticas actuales de ciberseguridad física



Prácticas ciberfísicas previstas

29% Pruebas realizadas por terceros	**25%** Segmentación de red	**18%** Plan de respuesta ante incidentes
15% Monitoreo de red	**15%** Acceso basado en roles	

Principales preocupaciones ciberfísicas



Sostenibilidad

54% Consideran la sostenibilidad como algo importante o muy importante en la selección de tecnología de seguridad.

+ del 6% con respecto a 2025

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Securitas Technology

Perspectivas de los socios tecnológicos

Perspectivas de nuestros socios tecnológicos en la vanguardia de la innovación en seguridad [1]

95% de nuestros socios han experimentado un aumento en la adopción de la nube.

→ **43%**
Aumento significativo

→ **52%**
Aumento moderado



100% AI
de nuestros socios tecnológicos están incorporando activamente la IA a sus soluciones.

Las 3 principales tendencias que impactan en el sector de la seguridad (en los próximos 3-5 años)

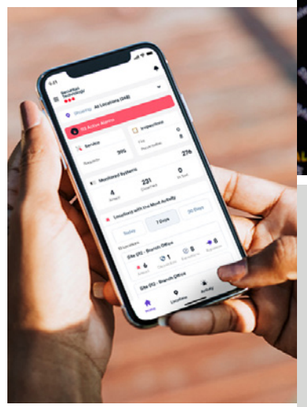
1. IA
2. Integración en la nube
3. Integración

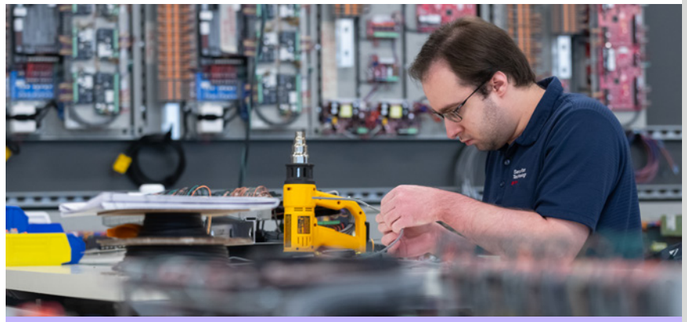
→ **62%**
de nuestros socios clasificaron a la IA como su opción número 1



Las 3 principales prioridades estratégicas de desarrollo de productos

1. Experiencia de usuario
2. Tecnología en la nube
3. IA





Las 3 principales aplicaciones de IA que influyen en el desarrollo de productos

1. Análisis en el perímetro.
2. Interacción en lenguaje natural
3. IA generativa

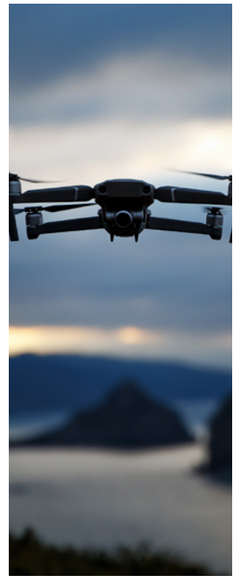


Socios tecnológicos que actualmente integran o planean integrar drones y robots.

48% Detección de drones

43% Drones de vigilancia

38% Robots





Cómo perciben nuestros socios el impacto de los drones y los robots en las futuras operaciones de seguridad.

10% → Impacto transformador

38% → Impacto significativo

48% → Impacto moderado

Las 3 principales iniciativas de sostenibilidad

1. Abastecimiento local y logística optimizada
2. Empaquetado
3. Diseño de productos energéticamente eficientes

1. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.

Securitas Technology

03

Aprovechar la oportunidad que ofrece la IA

En esta sección

- Mejorando la detección de amenazas con la IA
- IA generativa para operaciones de seguridad más inteligentes
- La IA agéntica optimiza las decisiones de seguridad.
- Optimización de la seguridad empresarial impulsada por la IA
- Plan de acción para profesionales de la seguridad

Securitas Technology

La IA pasa de ser una tecnología de nicho a convertirse en esencial

La IA ya no es una mejora incremental de los procesos establecidos. Está diseñada para transformar todos los aspectos de las operaciones diarias, ayudando a los equipos a detectar problemas con mayor precisión, actuar con más rapidez y tomar decisiones con mayor certeza.

Esto es importante porque la mayoría de los profesionales de la seguridad se enfrentan a una creciente complejidad y a expectativas cada vez mayores, mientras que los recursos siguen siendo limitados. El problema es que la IA todavía puede parecer un objetivo en constante movimiento. Están sucediendo muchas cosas a la vez: nuevas herramientas, nuevos modelos, nuevos casos de uso, y es fácil que los líderes se pregunten por dónde empezar o cómo enfocar sus esfuerzos de una manera práctica en lugar de abrumadora.

En nuestra encuesta de mercado, la incertidumbre sobre el retorno de la inversión (citada por el 48% [1] **de los encuestados) encabezó la lista de razones por las que la implementación de la IA en los programas de seguridad sigue siendo un desafío para las organizaciones,** seguido de cerca por las preocupaciones sobre la privacidad, la falta de conocimiento interno y la incertidumbre sobre en qué casos de uso centrarse.

Sin embargo, existen fuertes indicios de que la creciente madurez de las tecnologías de IA y los modelos generativos está generando confianza entre los líderes de seguridad globales, quienes colocaron **el análisis de vídeo impulsado por IA como la principal prioridad de inversión tecnológica para los próximos 12-18 meses (21 %** [1] **).**

100%

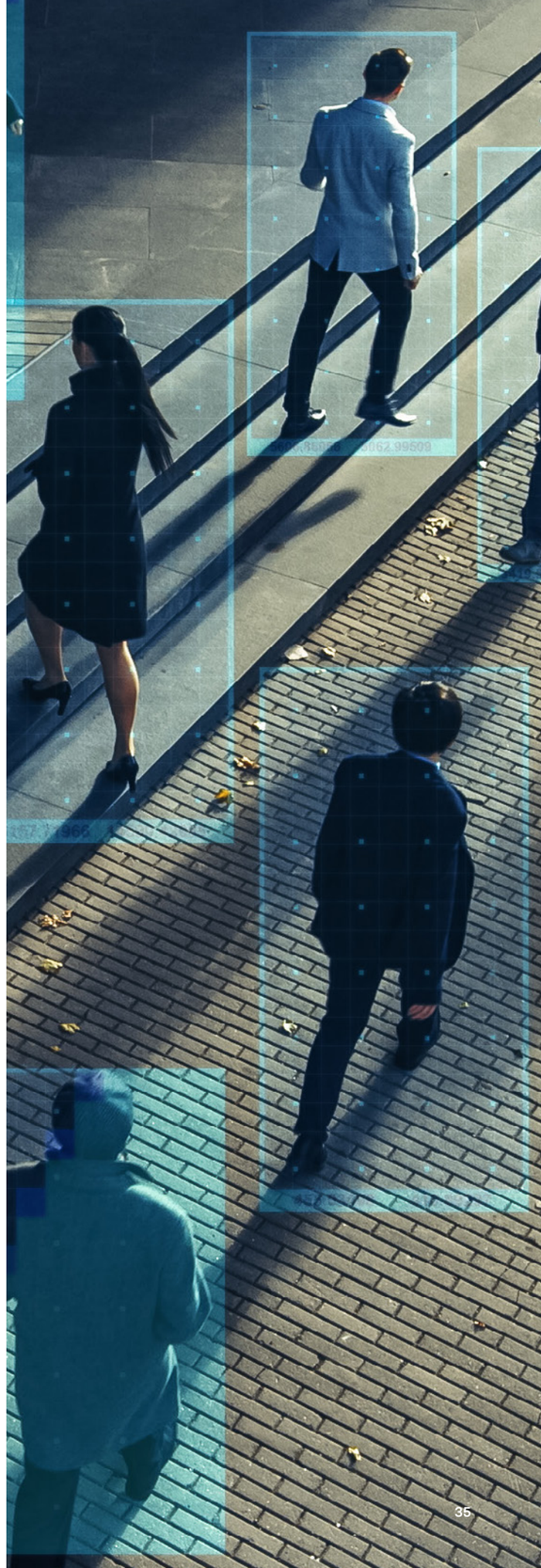
[2] de nuestros socios tecnológicos están invirtiendo en IA hoy en día.

Las perspectivas:

- **La detección de amenazas mediante IA** está ayudando a solucionar el problema de las falsas alarmas y a mejorar la precisión de la detección tanto en los sistemas de videovigilancia como en los de intrusión. Los modelos de IA reducen la necesidad de supervisión manual y proporcionan a los operadores humanos más contexto que nunca.
- **La IA generativa está cambiando la forma en que los operadores encuentran y comparten información.** , lo que hace que las búsquedas de vídeo, los resúmenes y la comunicación sean más rápidas e intuitivas.
- **La IA agéntica está emergiendo como una nueva forma de apoyar la toma de decisiones en tiempo real,** ofreciendo una guía coherente en todos los flujos de trabajo.
- **La IA está ayudando a las organizaciones a mejorar la salud de sus sistemas,** prever los riesgos potenciales y fortalecer el desempeño operativo general.
- **Las plataformas de seguridad basadas en la nube facilitan la adopción y la escalabilidad de la IA.** Al proporcionar la estructura necesaria para una implementación coherente y transformar los dispositivos de seguridad existentes en sensores inteligentes con tecnología de IA.
- **Una gobernanza sólida, la integración de datos, y los planes de implementación por fases son esenciales** para un uso responsable y eficaz de la IA.

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

2. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.



Securitas Technology

Mejorando la detección de amenazas con la IA

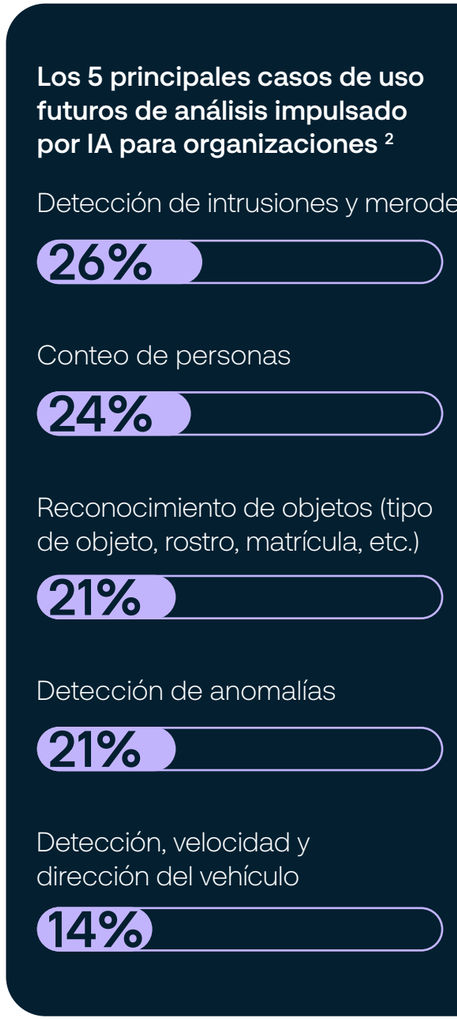
Mejorar la precisión y abordar las falsas alarmas

Tradicionalmente, el análisis de vídeo se ha centrado principalmente en el reconocimiento de objetos o la detección de movimiento como activadores, lo que puede generar falsas alarmas debido a su configuración amplia y basada en reglas. La IA hace que la detección de amenazas sea más precisa, consistente y sensible al contexto. Tanto si el análisis se realiza en la nube como en el dispositivo (en una cámara, por ejemplo), la IA separa la actividad relevante del movimiento cotidiano para que los operadores puedan centrarse en lo importante, lo que permite un filtrado más preciso y da como resultado menos envíos innecesarios y más tiempo para trabajos de mayor valor. **El análisis perimetral es, con diferencia, el principal enfoque en IA para nuestros socios tecnológicos estratégicos, con un 48 %** [1] **que lo consideran su máxima prioridad.**

Comprender el contexto, no solo el movimiento

Los modelos de IA modernos van más allá de las formas o el movimiento y evalúan el contexto de la escena. Detectan situaciones que podrían suponer una amenaza, como movimientos inusuales, merodeo o intentos de acceso que no se ajustan a la norma, para alertar con antelación sobre un riesgo elevado. Existe un gran interés en la detección de anomalías basada en el comportamiento, ya que estos análisis avanzados pueden ayudar a los equipos a obtener una ventaja inicial y una mayor confianza, lo que permite una respuesta más proactiva.

Los 5 principales casos de uso futuros de análisis impulsado por IA para organizaciones [2]



Fortalecimiento de la conciencia situacional

El uso de la IA puede ayudar a los responsables de seguridad a obtener una visión más clara de lo que ocurre en una instalación, al identificar sucesos clave a partir de vídeos en directo. En entornos concurridos o extensos, nadie puede supervisar todas las transmisiones; la IA resalta los momentos que merecen atención y los detalles que los operadores podrían pasar por alto. Esa visión más precisa y contextualizada es lo que puede ayudar a los equipos a anticiparse a los acontecimientos y a responder con mayor certeza en el futuro.



1. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.

2. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Información del socio tecnológico

Seguridad más inteligente: Cómo la IA ayuda a eliminar las falsas alarmas

Los sensores de seguridad convencionales reaccionan al movimiento sin comprender qué lo causó: una persona, un gato, el faro de un coche, la rama de un árbol. El resultado es una avalancha de alertas sin contexto, lo que provoca fatiga por exceso de alarmas y que se pasen por alto amenazas reales.

Las cámaras Ajax utilizan inteligencia artificial integrada en el dispositivo para detectar, clasificar y rastrear objetos en tiempo real. Esto por sí solo elimina la fuente más común de falsas alarmas. Pero como el sistema entiende qué se mueve y hacia dónde se dirige, permite establecer reglas más específicas, como activar alertas solo cuando una persona cruza un perímetro definido, filtrando todo lo demás.

La IA generativa abre la siguiente frontera: ir más allá del reconocimiento de clases de objetos predefinidos para comprender lo que sucede en una escena. Esto posibilita funciones como la detección de armas y la descripción de eventos en lenguaje natural. Mientras que los sistemas actuales se limitan a detectar aquello para lo que han sido programados explícitamente, la IA generativa tiene el potencial de identificar amenazas para las que nadie pensó en definir una regla.

En conjunto, estas capacidades transforman las cámaras, pasando de ser grabadoras de movimiento pasivas a sistemas que comprenden el contexto y que solo intensifican la información cuando realmente importa.

AJAX

Los análisis impulsados por IA están redefiniendo lo que puede hacer la detección de intrusiones.

El mercado de la seguridad está atravesando un momento crucial a medida que la industria evoluciona del hardware al software, a la nube y ahora a la IA en la nube.

Los sistemas de alarma y sensores están convergiendo con las plataformas de videovigilancia, convirtiendo cada cámara y sensor en parte de un sistema basado en el comportamiento que genera alarmas y, próximamente, alertas predictivas sobre la actividad dentro y alrededor de una instalación. El "análisis de intenciones" influirá cada vez más en la innovación, llevando a la industria hacia una IA con capacidad de gestión que utiliza análisis de vídeo y sensores basados en aprendizaje automático para determinar rápidamente qué es una amenaza real y qué no lo es.

Históricamente, la coordinación con las autoridades ha sido difícil porque los sistemas tradicionales se basan en interruptores de contacto binarios y reactivos y sensores de movimiento que no pueden evaluar lo que realmente está sucediendo en su entorno. La confianza en en los despliegues de personal generados por sistemas automáticos aumentará significativamente a medida que los sistemas equipados con inteligencia artificial reemplacen la tecnología tradicional.

Soluciones como Intruder AI de Actuate y XV Gateways con AlarmVision® de DMP transforman las cámaras IP estándar en dispositivos inteligentes de detección de alarmas. AI mejorar la detección de movimiento con análisis avanzados e integrar los eventos de vídeo directamente con los paneles de intrusión, las organizaciones obtienen notificaciones instantáneas, una mayor conciencia situacional y una reducción drástica de las falsas alarmas.

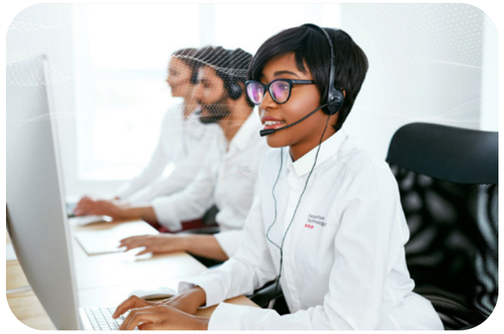
Securitas Technology

Mejorar la eficiencia del operador

La monitorización de alarmas de seguridad es el servicio de seguridad por suscripción más adoptado, con más de la mitad de las organizaciones (55% [1]) que dependen de la monitorización de terceros para la seguridad empresarial diaria . Y es aquí donde la IA también puede tener un impacto considerablemente positivo. Al ayudar a reducir el ruido, sacar a la luz detalles clave y disminuir el esfuerzo necesario para verificar las alarmas, la IA está capacitando tanto a los gerentes de seguridad como a los operadores de monitoreo de alarmas para validar las alarmas, obtener las pruebas que necesitan y escalar los problemas con menos fricción, lo que mejora la eficiencia al tiempo que reduce la carga cognitiva y la fatiga.

55%

de las organizaciones utilizan actualmente servicios de monitoreo de alarmas en sus programas de seguridad [1]



Funcionando a la perfección con plataformas digitales

La detección basada en inteligencia artificial resulta mucho más eficaz cuando se integra en el ecosistema de seguridad más amplio. Mediante las plataformas de gestión de seguridad digital, las alertas, los vídeos y los datos del sistema se integran en una única vista, lo que facilita a los operadores el uso de la IA para comprender lo que está sucediendo y actuar con rapidez. Esta configuración unificada ayuda a conectar los conocimientos generados por la IA con otros sistemas y agiliza los flujos de trabajo de respuesta. También proporciona la gobernanza, la coherencia de los datos y la estructura necesarias para expandir la IA a través de múltiples sitios
con confianza.

Un primer paso práctico Adéntrate en la IA

Para muchas organizaciones, el análisis tradicional basado en reglas es una herramienta de detección de amenazas familiar y bien establecida. Sin embargo, a medida que las analíticas basadas en IA más potentes y contextualizadas, como la detección de intrusiones, merodeo y vehículos, se vuelven más accesibles y fáciles de usar, representan el siguiente paso lógico. Estas aplicaciones ofrecen una forma sencilla y eficaz de empezar a adoptar la IA. Ofrecen beneficios claros e inmediatos, como una mayor precisión, una mejor detección de anomalías y tiempos de respuesta más rápidos, sin necesidad de realizar cambios operativos importantes. También respaldan un enfoque con intervención humana, lo que permite a los operadores validar o refinar los resultados de la IA y mantener la supervisión donde más importa. Comenzar aquí ayuda a los equipos a familiarizarse con la IA y a ganar confianza, creando una base sólida para expandirse hacia capacidades de IA generativa más avanzadas.

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Información del socio tecnológico

El borde de la inteligencia

La inteligencia artificial está redefiniendo el ámbito de la detección de intrusiones al trasladar la capacidad de procesamiento al "borde".

Este cambio representa uno de los avances tecnológicos más significativos en la seguridad moderna, ya que permite tomar decisiones críticas directamente en los dispositivos en lugar de depender únicamente de sistemas centralizados.

Como resultado, las organizaciones se benefician de una mayor rapidez en la obtención de información, una menor latencia y una arquitectura de seguridad más resistente que sigue funcionando incluso cuando se interrumpe la conectividad.

Esta evolución mejora tanto la seguridad como la eficiencia operativa. Por ejemplo, los clasificadores de IA ahora proporcionan una verificación de alarmas avanzada, lo que permite a los centros de monitoreo distinguir las emergencias que ponen en peligro la vida de los eventos de menor prioridad de forma instantánea y con mucha mayor confianza. Estas capacidades ayudan a reducir las falsas alarmas, agilizar los flujos de trabajo de los operadores y garantizar que las amenazas reales reciban atención inmediata.

Más allá de las mejoras en seguridad, la IA hace que los sistemas sean "más inteligentes" y más fáciles de implementar. El control inteligente de puertas, por ejemplo, simplifica la instalación, reduce los costes laborales y aumenta la rentabilidad para los integradores.

Si bien el sector comercial se vio ralentizado en el pasado por un hardware poco fiable, Radionix está superando esa brecha al respaldar una tecnología robusta que ofrece un alcance superior y un rendimiento fiable incluso en las aplicaciones comerciales más complejas.

Securitas Technology

IA Generativa para operaciones de seguridad más inteligentes

Transformando la forma en que los equipos interactúan con la información

La IA generativa está transformando la forma en que los equipos de seguridad acceden a sus sistemas y trabajan con ellos, eliminando muchos de los pasos manuales que antes los ralentizaban. **Beneficios como la detección automatizada de amenazas [1] encabezan la lista de aplicaciones de AI generativa en las que las organizaciones muestran interés, junto con la detección de violaciones de seguridad y la generación de informes del sistema, ya que ofrecen eficiencias operativas tangibles.**

Mientras tanto, los operadores pueden disfrutar de una experiencia de usuario simplificada gracias a la posibilidad de conversar con los sistemas mediante mensajes en lenguaje natural basados en chat. Esto refleja el objetivo de IA generativa de ayudar a reducir el tiempo dedicado a tareas rutinarias y permitir que los equipos se centren en evaluar riesgos, coordinar la respuesta y apoyar las actividades sobre el terreno. Crea una forma más fluida e intuitiva de interactuar con los datos, que se adapta al ritmo y la presión de las operaciones de seguridad modernas. **La IA generativa es una de las tres principales prioridades de desarrollo de productos de IA para el 60 % [2] de nuestros socios tecnológicos estratégicos.**

Interés de las organizaciones en las aplicaciones de IA generativa para sistemas de seguridad electrónica [1]

Detección automatizada de amenazas
87%

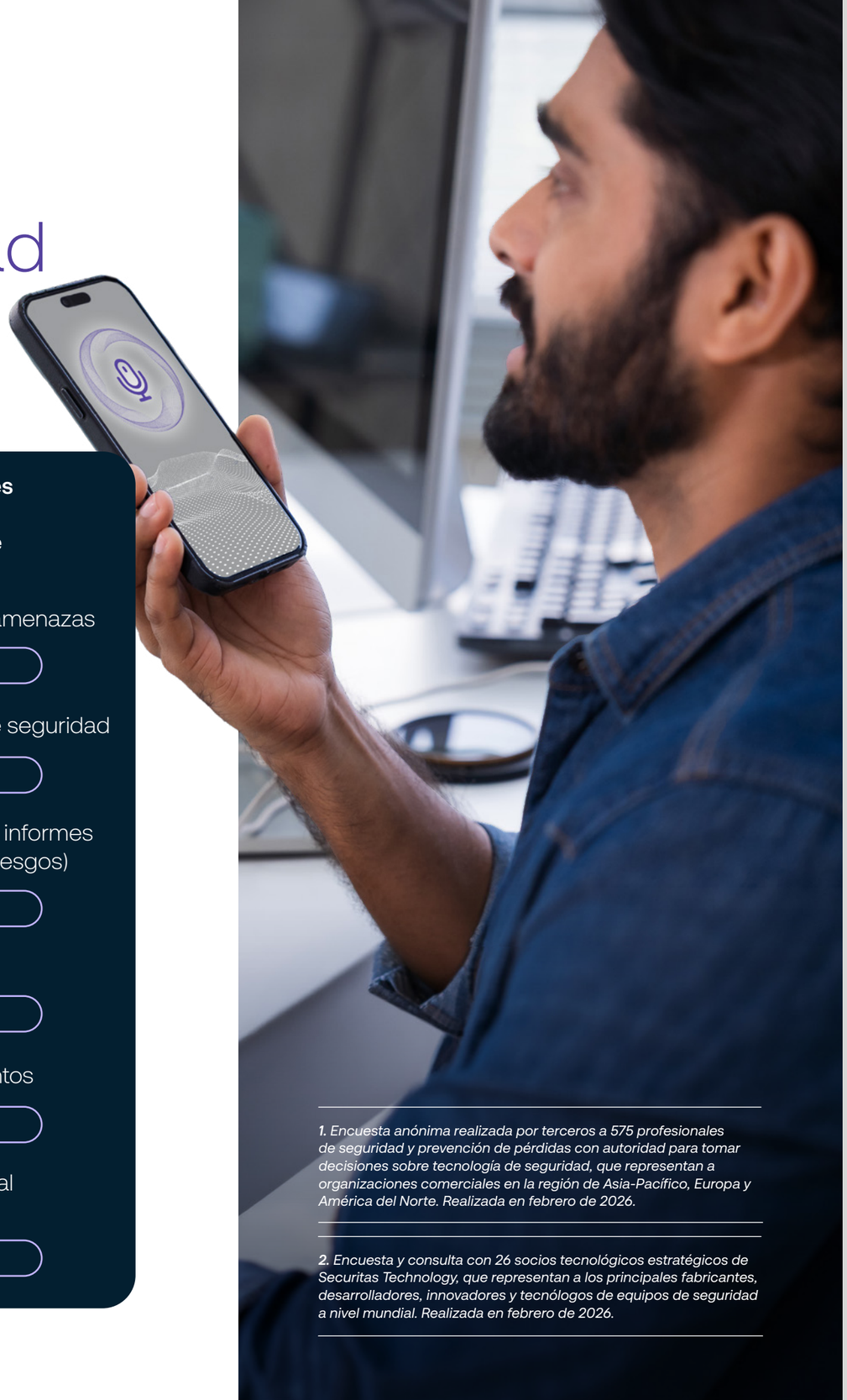
Detección de infracciones de seguridad
86%

Generación automatizada de informes (resúmenes de amenazas y riesgos)
86%

Búsqueda de vídeos
80%

Respuesta automática a eventos
77%

Interacción en lenguaje natural con sistemas
72%



1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

2. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.

Información del socio tecnológico

Comprender la IA Generativa

La IA generativa es muy eficaz para identificar patrones en grandes volúmenes de datos de seguridad que pueden indicar riesgos emergentes, pero sus conclusiones aún requieren el juicio y el contexto humanos.

Todavía necesitamos validarlo probando el sistema con datos que ya conocemos, datos que sabemos que son buenos y datos que sabemos que son malos.

Necesitamos ver cómo se comporta cuando se le proporciona información errónea o contradictoria. ¿Qué ocurre si etiquetamos a alguien como de alto riesgo, pero los datos no respaldan esa conclusión? ¿Qué ocurre si clasificamos a alguien como de bajo riesgo, pero los datos sugieren lo contrario?

Dado que no existe un estándar de referencia absoluto para la IA, las pruebas de estrés son esenciales. Esto es especialmente cierto para quienes trabajamos en seguridad física y protección de la vida. Es nuestra responsabilidad someter estas tecnologías a pruebas de estrés antes de implementarlas en entornos reales.

Si la IA se utiliza únicamente para evaluar algo con un riesgo mínimo, las consecuencias de equivocarse pueden ser relativamente menores. Pero si se utiliza para decidir quién puede acceder a determinadas zonas, cuándo desplegar la seguridad o cuándo involucrar a las fuerzas del orden, lo que está en juego es mucho mayor.

ASSA ABLOY
Opening Solutions

Securitas Technology

Hacer que la búsqueda de vídeos sea más rápida e intuitiva

Las búsquedas de vídeo tradicionales pueden ser lentas y manuales, y a menudo requieren que los operadores revisen clips largos o dependan de filtros de palabras clave muy específicos. Por eso, las organizaciones recurren a GenAI para agilizar sus procesos de revisión. Estos modelos pueden comprender la intención detrás de una solicitud, lo que significa que un operador simplemente puede describir el momento que busca, como cuando llegó un camión de reparto o cuando alguien entró por una puerta lateral, y el sistema encuentra rápidamente las imágenes relevantes. Esto reduce el tiempo de revisión, mejora la recopilación de pruebas y ayuda a los equipos a avanzar en las investigaciones con mucha menos fricción.

Automatización de informes y flujos de trabajo operativos

La IA generativa se está aplicando en la elaboración de resúmenes de alarmas, incidentes o actividad de turnos basados en datos operativos reales, lo que ayuda a que los traspasos de información sean más coherentes, a satisfacer las necesidades de cumplimiento normativo y a reducir las tareas de documentación manual. **El 86% [1] de las organizaciones que encuestamos muestran un gran interés en este tipo de generación automatizada de informes.** Por ejemplo, un responsable de seguridad podría subir su documento de procedimiento operativo estándar (POE) a su plataforma de seguridad con inteligencia artificial; la IA crearía automáticamente los mensajes de alarma en lenguaje natural para que GenAI los programe y supervise. Al asumir esta carga de trabajo administrativa, GenAI puede liberar a los operadores para que dediquen más tiempo a la monitorización activa y a las situaciones en las que su criterio aporta mayor valor.



86%

de organizaciones están interesadas en la generación automatizada de informes [1]



1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Aprender más sobre inteligencia artificial

La continua evolución de las nuevas cámaras que combinan la IA con el análisis de audio y vídeo integrado está dando como resultado una detección y clasificación de objetos de gran precisión.

En los últimos años, las empresas de todo el sector de la seguridad y la vigilancia han ampliado el uso de la IA, haciendo mucho más que mejorar el rendimiento de las imágenes de las cámaras. Además de reducir las falsas alarmas, los clientes obtienen datos útiles que permiten implementar una monitorización inteligente para mejorar la eficiencia operativa y generar información empresarial basada en datos. Seguiremos viendo nuevos tipos de dispositivos y una fusión de la IA para aportar mayor inteligencia a las cámaras y sistemas de vigilancia.

El siguiente paso consiste en una continua transición hacia la IA generativa combinada con el procesamiento del lenguaje natural, satisfaciendo la demanda de los clientes de simplicidad, personalización y búsqueda por voz, que pronto se convertirá en la norma en la seguridad empresarial. El mercado seguirá viendo surgir plataformas abiertas e inteligencia artificial generativa, que permitirán capacidades más específicas para un seguimiento preciso y la detección de objetos.

Los usuarios pueden realizar búsquedas utilizando lenguaje natural. En lugar de revisar los datos manualmente, bastaría con pedirle al sistema que identifique a una persona que haya entrado entre la 1:00 p. m. y las 2:00 p. m. vistiendo una camisa roja, gafas azules y un sombrero. Del mismo modo que hablan con Siri o Alexa en casa, los clientes ahora esperan comunicarse con los sistemas de seguridad de la misma manera. Los sistemas modernos son cada vez más inteligentes y capaces de gestionar este tipo de solicitudes, y los clientes están valorando esta sencillez.

Hanwha Vision

Securitas Technology

Comprensión visual y contexto de audio

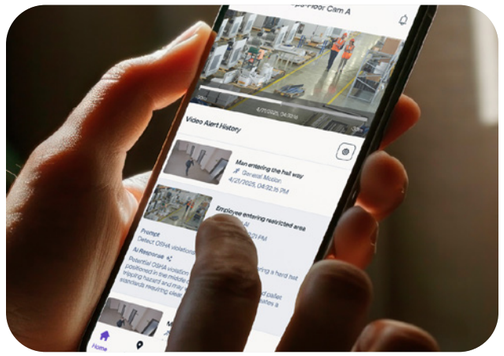
A diferencia del análisis de vídeo tradicional, GenAI puede interpretar lo que sucede en una imagen de vídeo, lo que permite a los operadores estar al tanto de riesgos o situaciones específicas, desde amenazas a la seguridad hasta infracciones en materia de salud y seguridad. Puede leer el texto que aparece en las imágenes y reconocer objetos o patrones que puedan ser relevantes para la solicitud del operador. Estas solicitudes pueden realizarse mediante consultas sencillas en lenguaje natural, tanto para configurar alertas para eventos futuros como para buscar eventos pasados. Esta capacidad multimodal ayuda a los equipos a supervisar entornos complejos o con mucha actividad de forma más eficaz, reuniendo detalles que de otro modo tardarían mucho más tiempo en recopilarse. Amplía el abanico de información disponible y facilita una toma de decisiones más rápida y mejor fundamentada.

86%

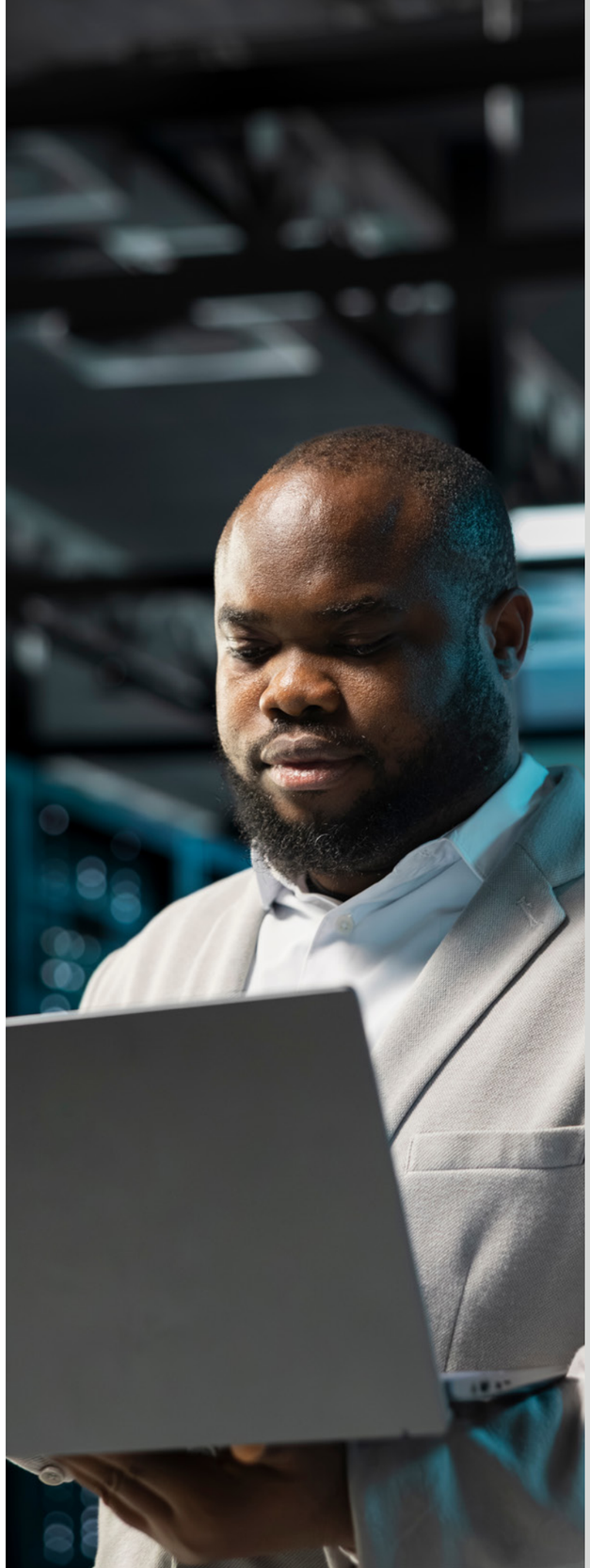
de organizaciones están interesadas en utilizar GenAI para señalar violaciones de seguridad [1]

La llave para operaciones más eficientes y resilientes

La IA generativa tiene el potencial de mejorar radicalmente la eficiencia y la eficacia al liberar a los equipos de seguridad de tareas manuales de bajo valor y proporcionarles información útil para la toma de decisiones. Cuando los operadores pueden obtener rápidamente la información correcta, ya sea un resumen de un incidente, un vídeo que necesita revisión o una alerta que requiere atención, dedican menos tiempo a tareas administrativas y más tiempo a gestionar situaciones activas. La generación automatizada de informes de incidentes resulta especialmente valiosa cuando el volumen de datos es elevado o las operaciones se realizan las 24 horas del día. Al simplificar las tareas rutinarias y mejorar el flujo de información, la IA generativa contribuye a unas operaciones de seguridad más eficientes, estables y resilientes.



1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.



Información del socio tecnológico

Transformación de las operaciones de seguridad

La IA generativa puede optimizar significativamente los flujos de trabajo de seguridad al automatizar la detección, la investigación y la respuesta ante amenazas.

Identifica anomalías hasta **100 veces más rápido** [2] que los métodos tradicionales, reduce los falsos positivos en aproximadamente un **50 %** [3] **y** reduce la carga de trabajo de los analistas a través del análisis automatizado de registros, la clasificación de alertas y la orientación para la solución rápida de incidentes. También mejora la gestión de vulnerabilidades mediante la realización de revisiones de código automatizadas y la detección de hasta el **90 %** [4] de los errores antes de la producción, lo que ayuda a los equipos de seguridad a adelantarse a los atacantes.

Para el análisis predictivo de riesgos, la IA generativa permite la modelización proactiva de amenazas mediante el análisis de grandes conjuntos de datos, incluidos patrones de comportamiento, actividad de red e inteligencia global sobre amenazas, para anticipar las rutas de ataque y los riesgos emergentes. Las organizaciones que utilizan seguridad predictiva basada en IA logran una detección de amenazas **un 60 %** [5] **más** rápida y costes derivados de brechas de seguridad significativamente menores. A medida que los ataques basados en IA se vuelven más sofisticados y adaptables, la IA generativa ayuda a predecir la evolución de las amenazas y a contrarrestar tácticas avanzadas como el ransomware automatizado por IA o las campañas de phishing dinámicas.

En conjunto, estas capacidades transforman las operaciones de seguridad, pasando de un enfoque reactivo a uno predictivo, lo que permite una toma de decisiones más rápida, una menor carga operativa y una mayor resistencia frente a las ciberamenazas de próxima generación.

2. *Seguridad de Microsoft. Investigación sobre IA en ciberseguridad/Security Copilot. microsoft.com/security.*

3. *Instituto de Investigación Capgemini. Reinventando la ciberseguridad con inteligencia artificial: La nueva frontera en seguridad digital. capgemini.com/research/reinventing-cybersecurity-with-artificial-intelligence.*

4. *Sinopsis. Informe sobre el estado de la seguridad del software (SOSS). synopsys.com/software-integrity/resources/analyst-reports.*

5. *Seguridad de IBM. Informe sobre el coste de una filtración de datos (2023). ibm.com/reports/data-breach.*

IDIS One Solution. One Company.

Securitas Technology

La IA agéntica optimiza las decisiones de seguridad.

Transición de la IA de asistencia a la inteligencia colaborativa

Aunque se encuentra en una fase temprana de adopción, la IA con capacidad de gestión de agentes representa la siguiente etapa en la forma en que la inteligencia artificial puede respaldar las operaciones de seguridad. En lugar de centrarse únicamente en el análisis o la detección, estos modelos pueden desempeñar un papel más activo ayudando a los operadores a interpretar una situación, cómo podría evolucionar y cuál es la mejor manera de responder. **Casi la mitad (48% [1]) de nuestros socios tecnológicos estratégicos clasificaron la IA agéntica como una de las tres principales prioridades de desarrollo en sus productors, y un 16% la sitúo en primer lugar.**

Es importante tener en cuenta que los agentes de IA no pretenden reemplazar el juicio humano, pero pueden ayudar a reforzarlo organizando la información y a ver destacando lo importante y ofreciendo opciones basadas en procedimientos operativos estándar. **Con más de tres cuartas partes de las organizaciones mostrando interés en la respuesta automatizada a eventos** [2], existe una demanda real de tecnología que ayude a los equipos de seguridad a dedicar menos tiempo a reaccionar a alertas individuales y más tiempo a gestionar eventos con una idea más clara de las circunstancias y la prioridad.

77%

Muchas organizaciones están interesadas en la respuesta automatizada a eventos por agentes de IA [2]

Ayudar a tomar decisiones con intención, en tiempo real

Los sistemas de IA con capacidad de gestión de agentes están diseñados no solo para seguir reglas preestablecidas, sino para evaluar activamente los eventos y responder en consecuencia. Combinan información procedente de vídeos, sensores, datos sobre el estado del sistema y patrones históricos para ofrecer recomendaciones fundamentadas en situaciones que cambian rápidamente. Si aparecen varias alertas en la misma zona, por ejemplo, la IA puede ayudar a determinar cuál necesita atención primero, sugerir pasos de verificación o mostrar las imágenes de las cámaras más relevantes. Este nivel de asistencia permite a los operadores mantenerse concentrados y responder con mayor eficacia, especialmente cuando la actividad se dispara.

Reducir la carga cognitiva de los equipos de seguridad

Los equipos de seguridad a menudo tienen que gestionar un gran volumen de información bajo presión de tiempo. La IA activa ayuda a aliviar esa carga filtrando el ruido y destacando lo que realmente necesita atención. Organiza las tareas, realiza un seguimiento de los incidentes en evolución y revela información que los operadores podrían no detectar de inmediato. Este apoyo ayuda a los equipos a mantener la conciencia situacional, reduce la fatiga y promueve una gestión más coherente de los incidentes en todos los turnos y ubicaciones.



1. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.

2. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Inteligencia artificial agéntica en seguridad crítica: Una nueva oportunidad

La IA agéntica ofrece muchas oportunidades en materia de seguridad crítica.

Principalmente, simplifica la gestión de las operaciones de seguridad. Un proceso de detección y respuesta más rápido, mediante agentes orientados a objetivos que perciben, razonan, planifican y actúan, ahorra tiempo y dinero al automatizar la respuesta de inmediato. Ofrece una mayor calidad de alarma gracias al uso de múltiples tecnologías (vídeo, audio, acceso, intrusión y entorno) para comprender mejor lo que ocurre sobre el terreno.

Ayuda a brindar una mejor asistencia tecnológica mediante el seguimiento automático de panorámica, inclinación y zoom, la comunicación por voz, el control de iluminación y barreras, la retención y el bloqueo de puertas, y es escalable en diferentes ubicaciones, lo que la convierte en una solución flexible que crece junto con las empresas.

Por supuesto, existen consideraciones en torno al uso de la IA con capacidad de gestión de agentes en la seguridad crítica. Siempre será necesario un ser humano: Algunas acciones deben permanecer configuradas como "nunca automáticas" para evitar errores. También pueden surgir dificultades relacionadas con la complejidad de la integración vinculada a los sistemas heredados.

Lo más importante es que la rendición de cuentas por las acciones autónomas debe ser visible para evitar problemas de responsabilidad y de acuerdo de nivel de servicio (SLA). Deben establecerse límites claros y mecanismos de desactivación de emergencia

Las organizaciones deberían adoptar un enfoque por etapas para obtener los mejores resultados, comenzando con una autonomía limitada de bajo riesgo y expandiéndose a medida que mejora la confianza, equilibrando la velocidad y la escala con la seguridad, la explicabilidad y el cumplimiento normativo.

3xLOGIC



Permitiendo operaciones más proactivas y coordinadas

A medida que la IA agéntica siga madurando, creemos que desempeñará un papel más importante en la coordinación de actividades entre sistemas y equipos de seguridad. Los agentes pueden automatizar los primeros pasos de la evaluación inicial, activar acciones de seguimiento o notificar a los operadores cuando se alcanzan ciertos umbrales. Cuando se conectan a plataformas de seguridad centralizadas, estas capacidades pueden funcionar como parte de un ecosistema unificado donde la detección, el análisis y la respuesta trabajan juntos de manera más fluida. Se trata de un nivel de integración que respalda la transición de una gestión reactiva de incidentes a operaciones más proactivas, basadas en la inteligencia, en múltiples ubicaciones.

¿Qué deben tener en cuenta los responsables de seguridad a medida que evoluciona la tecnología?

La IA agéntica es una novedad en el ámbito de la seguridad, y las mejores prácticas aún están en desarrollo. El soporte a la toma de decisiones, donde el agente de IA recopila información y presenta opciones a un operador humano, es un punto de partida probable para la mayoría de las organizaciones, pero los profesionales de la seguridad deberían prepararse para un futuro en el que los agentes de IA desempeñen un papel más activo en la respuesta a incidentes. Entre las consideraciones clave para este tipo de aplicación se incluyen el grado de autonomía que las organizaciones están dispuestas a otorgar a un agente de IA para la toma de decisiones, y cómo se mantendrá la participación humana para garantizar tanto la rendición de cuentas como la reversibilidad. A medida que aumente la fiabilidad y se consoliden las mejores prácticas de gobernanza, la IA con capacidad de gestión ofrecerá nuevas formas de acelerar la toma de decisiones y mejorar la respuesta ante incidentes.

Información del socio tecnológico

La rendición de cuentas comienza con cómo se diseña el flujo de trabajo

La IA agéntica está pasando del ciclo del hype a la realidad operativa, y la cuestión no es si desplegar agentes autónomos, sino cómo mantener el control humano de los resultados críticos.

La IA agéntica ahora se encarga de la coordinación en todos los sistemas de seguridad: procesa vídeos, correlaciona registros de acceso, detecta desviaciones y activa acciones de seguimiento. Pero la rendición de cuentas debe estar integrada en el propio flujo de trabajo, no añadida a posteriori.

Consideremos agentes de investigación autónomos que reciben una alarma, recopilan 30 minutos de evidencia multimodal y proponen medidas de mitigación inmediatas para que un operador las apruebe. Este modelo de intervención humana es clave: El agente se encarga de la velocidad y la recopilación de datos, mientras que la responsabilidad de las decisiones recae en las personas.

La transparencia proviene de la arquitectura. Las plataformas que exponen interfaces de programación de aplicaciones (API) seguras y auditables para agentes permiten rastrear, explicar y revisar cada acción iniciada por la IA. Medir el desempeño de los agentes en función de indicadores clave de rendimiento (KPI) definidos —tiempo de clasificación de incidentes, precisión de las pruebas, tasas de falsos positivos— convierte la confianza de un principio abstracto en algo medible.

A medida que las organizaciones implementen la IA con agentes en sus flujos de trabajo de seguridad a gran escala, los ganadores serán aquellos que consideren la rendición de cuentas no como una limitación, sino como un requisito de diseño desde el primer día.

Securitas Technology

Optimización de la seguridad empresarial impulsada por IA

La integración de datos es clave para obtener información valiosa de la IA

El 40% [1] de las organizaciones encuestadas nos indicó que la falta de integración de datos entre los sistemas de seguridad les impide implementar la IA en su programa de seguridad. Esto pone de manifiesto la importancia de un ecosistema de datos integrado como clave para liberar el enorme potencial de la IA a la hora de optimizar la seguridad y generar un valor empresarial real. Cada vez más organizaciones están trabajando en esa dirección. **Nuestra encuesta también destacó que la capacidad de integrar sistemas es uno de los tres criterios principales [1] para seleccionar un proveedor de tecnología de seguridad electrónica para organizaciones** de todos los tamaños y en todas las geografías.

Cómo la IA está ayudando a impulsar la eficiencia operativa

Para las organizaciones con altos niveles de integración, la IA les está ayudando a comprender sus entornos de maneras que los procesos manuales rara vez permiten. Mediante el análisis de patrones en vídeo, sensores, datos de rendimiento del sistema e historial de incidentes, la IA destaca las tendencias importantes, ya sean cuellos de botella recurrentes, cambios de comportamiento o indicadores tempranos de un mayor riesgo. Estos conocimientos pueden proporcionar a los responsables de seguridad una base más clara para la toma de decisiones sobre flujos de trabajo e inversiones en tecnología, mejorando el rendimiento diario y, al mismo tiempo, facilitando la planificación a largo plazo.



La inteligencia artificial es la #1

tecnología de vanguardia que nuestros clientes están interesados en adoptar en los próximos 12-18 meses [2]

Mejorar la eficiencia de la fuerza laboral y la asignación de recursos

La IA ayuda a los equipos a trabajar de forma más eficiente al encargarse de tareas repetitivas y de bajo valor, y al resaltar la información que requiere el juicio humano. Ofrece a los líderes una visión más clara de cómo se está empleando el tiempo, con qué eficacia se están gestionando los incidentes y dónde se pueden mejorar los procesos. Con el tiempo, estos conocimientos ayudarán a tomar mejores decisiones en materia de personal, a lograr estructuras de turnos más equilibradas y a distribuir las responsabilidades de forma más inteligente entre los diferentes centros.

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

2. Encuesta interna realizada a clientes de Securitas Technology en Australia, Bélgica, Canadá, Dinamarca, Finlandia, Francia, Alemania, Irlanda, México, Países Bajos, Noruega, Portugal, Singapur, España, Suecia, Suiza, Turquía, Reino Unido y Estados Unidos. Los datos mostrados reflejan únicamente las respuestas de los clientes comerciales. Realizado en noviembre de 2025.

Información del socio tecnológico

Soluciones más inteligentes para ayudar a ofrecer mejores procesos de seguridad

La optimización impulsada por IA permite a las organizaciones mejorar la eficacia de la seguridad al tiempo que optimizan la eficiencia operativa mediante la automatización de la inteligencia y la toma de decisiones en todos los sistemas.

Por ejemplo, el filtrado inteligente de alarmas reduce las falsas alarmas y las molestias, lo que permite a los operadores priorizar los eventos de alto riesgo y acelerar las decisiones de despacho.

En el control de acceso, la IA supervisa el uso inusual de credenciales, los patrones de acceso no autorizado y las secuencias atípicas, lo que previene el uso indebido y reduce la necesidad de una supervisión manual constante.

La verificación por vídeo también se acelera mediante análisis de IA, que pueden detectar personas, vehículos y comportamientos inusuales, lo que permite a los operadores remotos confirmar incidentes rápidamente y responder de forma proactiva.

Más allá de la respuesta a incidentes, la IA supervisa continuamente el estado del sistema, detectando fallos en los dispositivos, problemas de comunicación o desviaciones en la configuración antes de que afecten al servicio, lo que ayuda a mantener las operaciones sin interrupciones.

El mantenimiento predictivo mejora aún más la eficiencia al anticipar fallos en el controlador o los periféricos y programar un servicio proactivo, minimizando así el tiempo de inactividad y las interrupciones operativas.

Al combinar la detección inteligente de amenazas, la monitorización automatizada y los análisis predictivos, la optimización impulsada por la IA equilibra una seguridad sólida con la eficiencia de los recursos, lo que permite a las organizaciones responder con mayor rapidez, prevenir incidentes antes de que se agraven y mantener operaciones fiables en entornos complejos y distribuidos.

PACOM VIGIL CORE™

Securitas Technology

Mejorar el cumplimiento, la presentación de informes y la supervisión operativa

Las organizaciones necesitan cada vez más demostrar el cumplimiento tanto de las políticas internas como de las normativas externas. La IA tiene el potencial de respaldar esto al monitorear el cumplimiento de manera más consistente que la supervisión manual y al resaltar dónde pueden estar disminuyendo los estándares. Puede ayudar a realizar un seguimiento de los indicadores clave de rendimiento, respaldar una documentación más clara y generar resúmenes que brinden a los líderes una mejor visibilidad en todas las ubicaciones. Este nivel de conocimiento no solo mejorará el control, sino que también ayudará a mantener procesos consistentes y repetibles que resistan las auditorías y las revisiones internas.

Fortalecimiento de la gestión estratégica de riesgos

Al combinar las tendencias históricas con la información en tiempo real, la IA ayuda a las organizaciones a detectar riesgos potenciales con antelación y a tomar medidas antes de que los problemas se agraven. Puede poner de manifiesto patrones emergentes, como cambios en la actividad de robos, alteraciones en el comportamiento fuera del horario laboral o condiciones ambientales inusuales, que pueden indicar una mayor exposición. Cuando estos conocimientos se integran en plataformas integrales de gestión de seguridad, pasan a formar parte de un panorama de riesgos más amplio que respalda una toma de decisiones más proactiva e informada en todos los sitios.

Construyendo un camino hacia la mejora continua

La optimización impulsada por IA no es una actualización puntual, sino un proceso continuo. A medida que se recopilen más datos y los modelos sigan madurando, las organizaciones obtendrán una visión más clara de lo que sucede en sus operaciones de seguridad y sobre dónde se pueden realizar mejoras. Con el tiempo, esto ayuda a crear un ciclo de aprendizaje y perfeccionamiento constante que fortalece la resiliencia, mejora el rendimiento y garantiza que el programa de seguridad mantenga el ritmo de las necesidades del negocio.



Información del socio tecnológico

Mejorar la eficacia de la seguridad con IA

La inteligencia artificial tiene el potencial de mejorar enormemente la eficacia de las operaciones de seguridad al acelerar los tiempos de respuesta, añadir información contextual a los incidentes, identificar eventos que de otro modo pasarían desapercibidos y, en algunos casos, resolver incidentes de forma autónoma.

Sin embargo, la IA debe implementarse con cuidado para garantizar que los resultados sean precisos, fiables y estén en consonancia con las expectativas de la organización.

La planificación debe comenzar con objetivos operativos claramente definidos. En lugar de centrarse únicamente en lo que un modelo de IA puede detectar, hay que determinar el flujo de trabajo deseado completo. Por ejemplo, detectar las caídas de pacientes en un hospital es solo el punto de partida. El resultado operativo debe incluir la presentación de vídeo en directo y grabado del incidente, la identificación de la ubicación y de la gravedad, el ofrecimiento de opciones de actuación adecuadas y el registro de los resultados para perfeccionar continuamente las normas y reducir las falsas alarmas.

Unos controles de gobernanza sólidos son esenciales para cualquier implementación de IA. Las organizaciones deben definir qué funciones tiene permitidas realizar la IA, las condiciones necesarias para que la automatización pueda actuar, cómo se almacenarán y protegerán los datos y durante cuánto tiempo se conservará la información. Estas políticas deben gestionarse activamente a lo largo de todo el ciclo de vida del sistema.

Por último, los sistemas eficaces requieren un diseño cuidadoso que involucre la intervención humana. En entornos de seguridad y protección de la vida, la IA debería resaltar los eventos importantes, organizar la información y recomendar acciones, mientras que los humanos conservan la responsabilidad de aprobar o escalar las decisiones, garantizando así que la

Securitas Technology

> La IA es más potente cuando se basa en problemas reales, datos fiables y en el juicio humano. La oportunidad para los líderes de seguridad no reside en perseguir todas las nuevas herramientas, sino en centrarse en los casos de uso donde la IA puede hacer que sus equipos sean más eficaces, más resilientes y estén mejor preparados para lo que venga después.

Dr. Serdar İnce
Vicepresidente sénior de Innovación Global e Inteligencia Artificial
Securitas Technology



Securitas Technology

Plan de acción para profesionales de la seguridad



Implementación de la IA en tu programa de seguridad

01

Comienza con un propósito claro.

Define qué quieres que la IA te ayude a lograr. Ya sea el objetivo reducir las falsas alarmas, acelerar las respuestas, mejorar los flujos de trabajo de los operadores u obtener información más clara a partir de los datos, los objetivos específicos facilitan la elección de las herramientas de IA adecuadas y la medición de su impacto a lo largo del tiempo.

02

Construir una base sólida de datos y gobernanza.

La IA depende de datos fiables, una configuración coherente y una buena higiene cibernética. Revisa cómo están configurados tus sistemas, quién puede acceder a qué información y cómo se almacenan y protegen los datos. Una gobernanza clara y sencilla contribuye a que las implementaciones de IA funcionen mejor y sean más escalables.

03

Céntrate primero en los casos de uso de alto valor y bajo riesgo.

Empieza con aplicaciones de IA que estén probadas, sean medibles y fáciles de adoptar para los equipos. Entre los primeros pasos habituales se incluyen la detección basada en IA, la búsqueda de vídeos en lenguaje natural, la generación de informes automatizados y la obtención de información sobre el estado del sistema. Los pequeños triunfos iniciales ayudan a generar impulso y a demostrar valor a las partes interesadas.

04

Integra la IA en los flujos de trabajo existentes.

La IA funciona mejor cuando mejora la forma en que los equipos ya operan. Diseña tus flujos de trabajo principales, desde la gestión de alarmas hasta las investigaciones, e identifica dónde la IA puede automatizar pasos, ofrecer recomendaciones o reducir el esfuerzo manual. La integración con plataformas de gestión de seguridad garantiza que la información valiosa llegue a las personas adecuadas en el momento oportuno.

05

Realiza pilotos con un propósito y escala basados en evidencia

Pon en marcha proyectos piloto específicos con criterios de éxito claros. Realice un seguimiento de métricas como la reducción de alarmas, el tiempo de verificación, la carga de trabajo del operador o las tasas de resolución de incidentes. Utiliza los resultados y los comentarios de tu equipo para perfeccionar tu enfoque y escala solo cuando el valor sea consistente y repetible.

06

Prepara a tu equipo y elige a los socios adecuados.

La IA está cambiando la forma en que trabajamos, por lo que la comunicación y la formación son esenciales. Explica cómo la IA apoya, en lugar de reemplazar, el juicio humano y brinda a los equipos orientación práctica sobre el uso de las nuevas herramientas. Colabora con socios que comprendan tanto la IA como las operaciones de seguridad y que puedan respaldar una adopción responsable y transparente a lo largo del tiempo.

Securitas Technology

04

Las soluciones en la nube están transformando la seguridad

En esta sección

- La base de la seguridad de próxima generación
- Monitoreo y mantenimiento del estado de los sistemas
- Verificación remota y gestión de incidentes
- Gestión centralizada del sistema de seguridad
- Plan de acción para profesionales de la seguridad

Securitas Technology

El cambio hacia operaciones de seguridad flexibles y conectadas

La creciente adopción de plataformas de seguridad basadas en la nube está cambiando la forma en que las organizaciones gestionan los incidentes y mantienen su tecnología de seguridad.

Ahora que la nube se ha consolidado como la base para la escalabilidad de los sistemas y la gestión de riesgos ciberfísicos, las organizaciones se centran cada vez más en aprovechar las ventajas operativas de una mayor conectividad y una gestión de seguridad centralizada. Estas capacidades basadas en la nube ayudan a los equipos de seguridad a trabajar de manera más eficiente, mantener estándares consistentes en todas las ubicaciones y mejorar la resiliencia, al tiempo que reducen los requisitos de hardware en las instalaciones y mejoran la redundancia de datos.

Nuestro estudio de mercado muestra una fuerte demanda de funcionalidades remotas en todos los sectores, y el 44 % [1] **de las organizaciones planea aumentar su inversión en servicios remotos.** Los servicios remotos ofrecen a los responsables de seguridad una mayor visibilidad en todas las instalaciones y permiten respuestas más rápidas y coordinadas, incluso cuando los recursos in situ son limitados. **Nuestros socios tecnológicos estratégicos también identificaron la funcionalidad remota como el segundo factor** [2] **determinante en la adopción de tecnología basada en la nube.**

44%

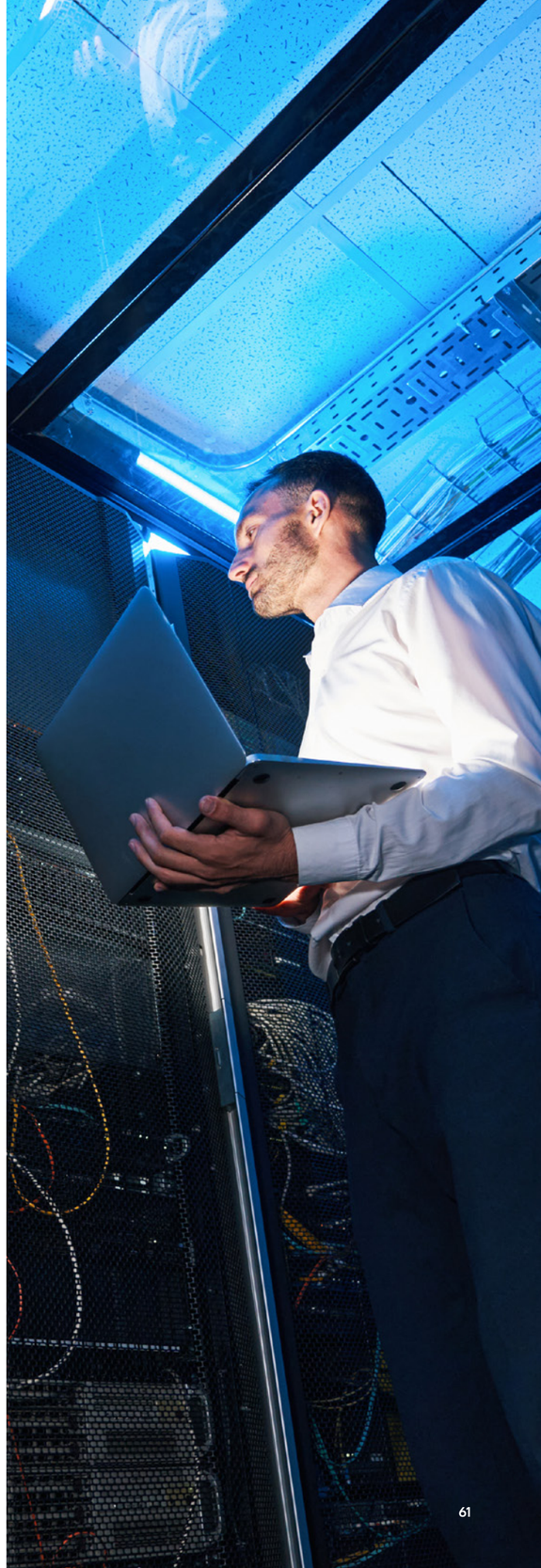
de las organizaciones prevén aumentar su uso de servicios remotos durante los próximos 18 meses [1]

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

2. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.

Las perspectivas:

- **La infraestructura en la nube y la nube híbrida se está convirtiendo en la configuración estándar, lo que permite programas de seguridad escalables, flexibles y preparados para la IA** que evolucionan con las demandas operativas.
- **Los servicios remotos están ayudando a las organizaciones a mantener una sólida protección** en múltiples ubicaciones, incluso cuando los recursos presenciales son limitados.
- **La monitorización y el mantenimiento remotos del estado de los sistemas refuerzan la fiabilidad** al identificar los problemas con antelación y minimizar el tiempo de inactividad.
- **La verificación centralizada y la gestión de incidentes pueden mejorar la precisión y la velocidad** al proporcionar a los equipos una visión más clara y unificada de la actividad.
- **La administración remota del sistema simplifica las actualizaciones** , los permisos y la implementación de políticas en diferentes ubicaciones.
- **En conjunto, estas capacidades respaldarán una operación de seguridad más proactiva y basada en la inteligencia** .



Securitas Technology

La base de la seguridad de próxima generación

Por qué la nube es importante para la seguridad moderna

La adopción de plataformas de seguridad basadas en la nube continúa en aumento. **Nuestra encuesta a clientes reveló que casi una cuarta parte[1] de las empresas ya están aprovechando esta tecnología, siendo la videovigilancia en la nube y el control de acceso algunas de las soluciones más adoptadas.** La tecnología en la nube se está convirtiendo en la columna vertebral de las operaciones de seguridad modernas y en la base de las capacidades avanzadas de IA, evitando la sustitución completa del hardware y permitiendo una mayor agilidad en las actualizaciones y la configuración.

Si bien el costo de los equipos y el riesgo de pérdida de datos confidenciales siguen siendo las principales preocupaciones para aquellas organizaciones que aún no han adoptado la nube, un número creciente considera que las ventajas superan las posibles desventajas. **Nuestros socios tecnológicos estratégicos también están notando esta tendencia, y el 92 %[2] ha observado un aumento en la adopción durante el último año.**

Las configuraciones híbridas seguirán ofreciendo a las organizaciones una vía para aprovechar la flexibilidad de las plataformas en la nube y alejarse progresivamente de la dependencia exclusiva de la infraestructura local, que puede consumir muchos recursos y ser lenta para escalar.

24%

de nuestros clientes ya han implementado sistemas de seguridad electrónica basados en la nube [1]

1. Encuesta interna realizada a clientes de Securitas Technology en Australia, Bélgica, Canadá, Dinamarca, Finlandia, Francia, Alemania, Irlanda, México, Países Bajos, Noruega, Portugal, Singapur, España, Suecia, Suiza, Turquía, Reino Unido y Estados Unidos. Los datos mostrados reflejan únicamente las respuestas de los clientes comerciales. Realizado en noviembre de 2025.

2. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.



Información del socio tecnológico

IA en la nube como valor predeterminado operativo

La videovigilancia ha experimentado una transformación fundamental. Hemos dejado atrás la era de "rebobinar y revisar" para entrar en una era de inteligencia empresarial proactiva. Este cambio se sustenta en el dominio sostenido de la nube como motor indispensable para la innovación en seguridad.

Una infraestructura en la nube garantiza que su sistema esté siempre actualizado. Las mejoras en la interfaz y las actualizaciones de firmware se aplican de forma transparente a todas las cámaras y paneles de control conectados, lo que elimina la carga de mantenimiento del hardware antiguo. Cuando se diseña adecuadamente, la nube sirve como un motor extensible para nuevas capacidades a través de API abiertas y formatos de datos flexibles.

La IA ya no se limita a la detección de movimiento; ahora es una herramienta esencial para crear flujos de trabajo completamente nuevos. Al aprovechar los modelos de lenguaje a gran escala (LLM, por sus siglas en inglés), quienes toman las decisiones pueden definir búsquedas personalizadas e informes comerciales utilizando un lenguaje sencillo, sin necesidad de programación.

- "Muéstrame todos los vehículos de reparto que entraron después de las 7:00 p. m."
- "Avísenme si los trabajadores no llevan equipo de protección personal en la obra."

Esta potencia centralizada en la nube transforma los datos brutos en información útil, convirtiendo la seguridad inteligente en la estrategia predeterminada para todas las organizaciones.

brivo
simply better security



Desbloqueando el poder de la analítica avanzada y la IA

La nube es esencial para que las organizaciones puedan aprovechar las capacidades avanzadas de IA que combinan datos de múltiples sistemas para obtener una verdadera inteligencia operativa. El análisis del comportamiento, la búsqueda impulsada por GenAI y la inteligencia automatizada sobre el estado del sistema dependen de la potencia informática y el acceso a los datos que proporcionan las plataformas en la nube. Desde la detección de intrusiones hasta el vídeo y el control de acceso, las organizaciones pueden aprovechar información en tiempo real, útiles herramientas de IA y mejoras continuas mediante actualizaciones automáticas. De esta forma, la nube se convierte en algo más que una capa de almacenamiento: se convierte en una capa de inteligencia que eleva todo el ecosistema de seguridad.

Tipos de tecnologías de seguridad basadas en la nube que utilizan actualmente las organizaciones [1]

Videovigilancia en la nube

72%

Control de acceso en la nube

67%

Detección de intrusiones en la nube

38%

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Construyendo seguridad remota escalable y resiliente con la nube

La nube está cambiando la forma en que se crean y se prestan los servicios de seguridad remota.

No se trata solo de trasladar los sistemas y los vídeos a un lugar externo. Se trata de brindar a los equipos de seguridad la flexibilidad necesaria para crecer y adaptarse sin tener que reconstruir constantemente su infraestructura.

En el pasado, ampliar un sistema de vigilancia significaba añadir más servidores, almacenamiento y hardware en cada ubicación. Si bien este enfoque es eficaz, se vuelve costoso y complejo a medida que las organizaciones se expanden. Las arquitecturas basadas en la nube cambian ese modelo al permitir que los proveedores de seguridad incorporen nuevos sitios, cámaras y análisis rápidamente, a menudo sin necesidad de implementar infraestructura adicional en las instalaciones. Esta escalabilidad es esencial a medida que las empresas crecen y las operaciones de seguridad se vuelven más distribuidas.

La resiliencia es igualmente importante. Los entornos en la nube están diseñados con redundancia y conmutación por error integradas, de modo que si un componente falla, otro toma el relevo. En el caso de los servicios de seguridad remota, esto significa que el vídeo, las alertas y el acceso al sistema permanecen disponibles cuando más se necesitan.

Hoy en día, muchas organizaciones están adoptando arquitecturas híbridas que combinan lo mejor de ambos mundos. La grabación y el procesamiento pueden realizarse cerca de las cámaras en las instalaciones, mientras que la nube se encarga de la gestión centralizada, el análisis y el almacenamiento a largo plazo. El resultado es un modelo flexible que permite a los proveedores supervisar múltiples ubicaciones desde una única plataforma y ampliar los servicios a medida que crece la clientela.

MARCH networks
A Delta Group Company

Conectando sitios, sistemas y equipos a través de una única plataforma

Las plataformas digitales basadas en la nube son ahora una parte esencial del conjunto de herramientas del responsable de seguridad. Ayudan a unificar la visibilidad y el control en todas las ubicaciones, permitiendo el acceso remoto para ver vídeo en directo, comprobar el estado del sistema, ajustar la configuración y verificar las alertas desde cualquier lugar, utilizando una única interfaz coherente. Este nivel de centralización es muy valorado por las organizaciones porque ayuda a eliminar los flujos de trabajo aislados y fomenta una toma de decisiones más coordinada. Para las organizaciones con múltiples sedes, la capacidad de gestionar permisos, integrar nuevos dispositivos y supervisar el rendimiento en todas las ubicaciones supone una ventaja significativa, ya que ayuda a impulsar una seguridad coherente en todas las sedes y proporciona claridad para mejorar la seguridad en general.

La gestión centralizada de la seguridad es el principal motor de la adopción de la nube.

según nuestros socios tecnológicos estratégicos [1]

Equilibrando la flexibilidad con la seguridad y la privacidad

La adopción de soluciones en la nube permite a las organizaciones beneficiarse de una mayor flexibilidad. Pero también deben considerar cuidadosamente la seguridad, la privacidad y la gobernanza de los datos. Si bien los proveedores de servicios en la nube actuales ofrecen una sólida protección, desde el cifrado seguro hasta los estrictos controles de acceso y los robustos marcos de cumplimiento, sigue siendo importante comprender cómo se manejan los datos de seguridad, dónde se almacenan y quién puede acceder a ellos. Las organizaciones también tienen la responsabilidad de garantizar que las redes internas a las que están conectadas las plataformas en la nube estén bien protegidas y mantenidas. Consulta **la sección 6** para obtener más información sobre las mejores prácticas de seguridad de datos.

1. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.



Las arquitecturas de seguridad basadas en la nube redefinen la escalabilidad y la resiliencia

Las arquitecturas basadas en la nube están cambiando la forma en que los servicios de seguridad remota se escalan y operan.

En lugar de planificar para una capacidad fija, las plataformas modernas en la nube se ajustan automáticamente a las demandas de carga de trabajo, incluidas las visualizaciones simultáneas de vídeo en directo, las altas tasas de ingesta de datos, las alarmas en cola y las exportaciones de casos. Los diseños multiusuario permiten supervisar de forma eficiente múltiples ubicaciones y clientes sin que un entorno afecte a otro. A medida que las organizaciones crecen, la incorporación de nuevos clientes se vuelve más sencilla y la planificación de la capacidad resulta mucho menos restrictiva.

Las arquitecturas en la nube también permiten una fuerza laboral más flexible. Los operadores y administradores pueden trabajar desde una única interfaz en cualquier parte del mundo, lo que mejora la colaboración y la coherencia entre los equipos distribuidos.

La resiliencia está integrada en la nube desde su diseño. Las arquitecturas de alta disponibilidad ayudan a mantener un tiempo de actividad constante con una infraestructura mínima en las instalaciones del cliente o en entornos de estación central. Las actualizaciones sin tiempo de inactividad facilitan la introducción de nuevas funcionalidades sin interrupciones, mientras que las características configurables permiten a los operadores trabajar de forma más eficiente.

La adopción de la nube refuerza la seguridad y el cumplimiento normativo mediante la integración de proveedores de identidad, el cifrado de datos en reposo y en tránsito, y arquitecturas que eliminan la necesidad de puertos de firewall abiertos o acceso VPN. Los modelos híbridos reducen aún más el uso del ancho de banda, disminuyen los costos de infraestructura y permiten que los equipos se centren en la prestación de servicios en lugar de en el mantenimiento de los sistemas.

VERINT.

Securitas Technology

Supervisión y mantenimiento del estado del sistema

Fortalecer la confiabilidad del sistema a través de la concienciación proactiva

La fiabilidad del sistema es uno de los tres factores principales [1] Según nuestro estudio de mercado, esto está impulsando un mayor uso de los servicios remotos. Mediante los servicios de monitorización y mantenimiento remotos, las organizaciones buscan obtener una visión más clara y continua del rendimiento de su infraestructura de seguridad. En lugar de detectar problemas solo cuando se informan o cuando algo falla, los equipos de seguridad quieren ser alertados de los posibles problemas con antelación para ayudar a mantener los sistemas funcionando de forma fiable en todas las ubicaciones.

Esta visibilidad proactiva resulta especialmente valiosa para organizaciones con una gran presencia geográfica, recursos técnicos limitados in situ o entornos donde los fallos de los equipos pueden afectar directamente a la seguridad de los empleados o a las operaciones.

46%

de las organizaciones afirman que la necesidad de un mayor tiempo de actividad del sistema está impulsando un mayor uso de los servicios remotos [1]



Identificar problemas a nivel de dispositivo antes de que interrumpan las operaciones

Las plataformas conectadas a la nube permiten a los equipos de seguridad realizar un seguimiento del estado, la conectividad y el rendimiento de los dispositivos en tiempo real. Los socios de servicio también pueden revisar de forma remota las cámaras, los sensores y otros dispositivos conectados a la red para detectar signos tempranos de degradación, interrupciones o inconsistencias en la configuración. Los diagnósticos con soporte de IA ayudan a detectar comportamientos inusuales, como la disminución de la calidad del vídeo, fallos de almacenamiento o componentes defectuosos, para que los equipos puedan actuar antes de que pequeños problemas provoquen interrupciones del servicio.

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Información del socio tecnológico

Minimiza el tiempo de inactividad con una monitorización remota de la salud más inteligente: Mantenimiento proactivo para sistemas de seguridad modernos

Las innovaciones en la monitorización remota que minimizan el tiempo de inactividad comienzan con una visibilidad centralizada y en tiempo real del estado del sistema, no solo con alarmas después de que algo falla.

Los paneles de control del estado del sistema reúnen los indicadores clave del sistema en un solo lugar, incluido el estado en tiempo real de los paneles, los lectores, los servicios del servidor y el uso del disco, para que los equipos puedan detectar la degradación con antelación y actuar antes de que se produzca una interrupción del servicio.

Gracias a las plataformas de seguridad centralizadas y habilitadas para la nube, el cambio más importante está pasando de la resolución de problemas reactiva al mantenimiento proactivo mediante:

- Indicadores de estado codificados por colores y paneles de control configurables que permiten a los operadores identificar rápidamente los problemas (incluso en implementaciones a gran escala).
- Alertas específicas para dispositivos fuera de línea o con funcionamiento deficiente (como un panel o un lector) para reducir las "fallas silenciosas" que, de otro modo, solo se descubren cuando las puertas dejan de funcionar.
- Búsqueda rápida, filtrado e informes exportables para agilizar la clasificación de problemas, documentar las soluciones e identificar patrones recurrentes que indiquen hardware obsoleto o inestabilidad de la red.

A medida que estos paneles de control evolucionan, la próxima frontera son los diagnósticos basados en tendencias, los flujos de trabajo automatizados y los modelos de servicio remoto que permiten a los equipos resolver más problemas sin necesidad de visitas presenciales, manteniendo los sistemas en línea y seguros con menos interrupciones.

AMAG TECHNOLOGY
An Allied Universal Company

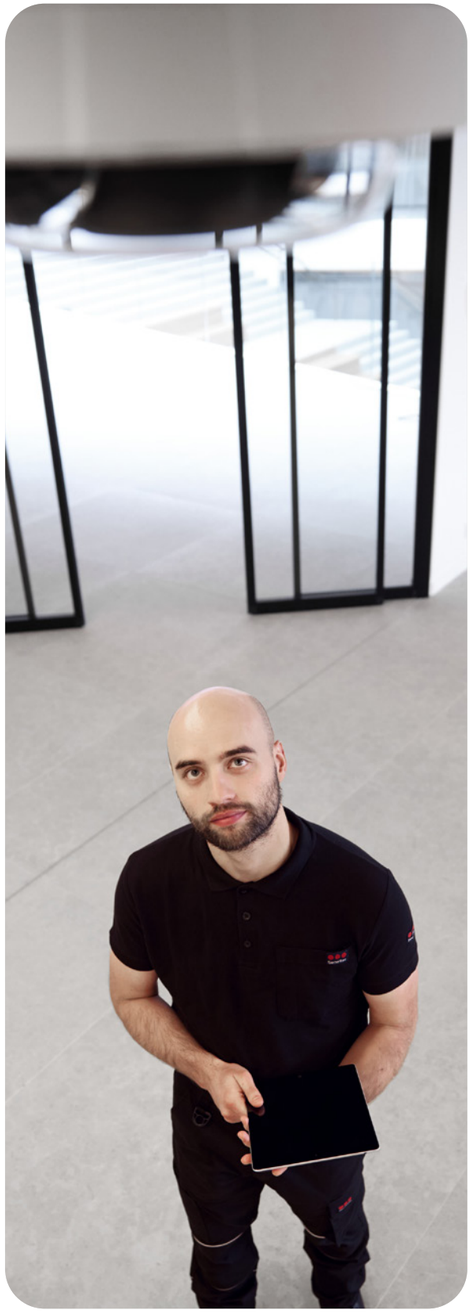
Reducir las visitas innecesarias a las instalaciones y mejorar la sostenibilidad

Cuando los equipos internos o los proveedores de seguridad pueden diagnosticar y resolver problemas de forma remota, dedican menos tiempo a desplazarse a las instalaciones y más tiempo a centrarse en tareas de mayor valor. Muchos problemas comunes, desde cambios de configuración hasta reinicios del sistema, pueden solucionarse sin necesidad de enviar un técnico al lugar. Esto se traduce en menores emisiones de carbono, una resolución más rápida, menores costes operativos y un enfoque más sostenible para brindar soporte técnico en ubicaciones muy dispersas.

Apoyo al mantenimiento predictivo y a la planificación del ciclo de vida

Mediante el seguimiento del rendimiento del sistema y la información de los activos a lo largo del tiempo, las plataformas de monitorización remota del estado y de gestión del ciclo de vida ayudan a las organizaciones a detectar cuándo los dispositivos se acercan al final de su vida útil o cuándo los problemas repetidos apuntan a problemas técnicos más profundos. Estos conocimientos permiten elaborar presupuestos más precisos, planificar actualizaciones de forma más inteligente y reducir las interrupciones inesperadas del servicio.

El mantenimiento predictivo también ayuda a los equipos a priorizar la atención en los sitios que más la necesitan, garantizando que los recursos se dirijan donde tendrán el mayor impacto operativo.



1 de cada 5

Los clientes de Securitas Technology están interesados en adoptar servicios de gestión del ciclo de vida en los próximos 18 meses [1]

Una situación beneficiosa para las organizaciones y sus socios de seguridad

La disponibilidad de servicios basados en la nube, como la monitorización del estado del sistema y el mantenimiento preventivo remoto, se está convirtiendo en una poderosa ventaja tanto para las organizaciones como para sus proveedores de servicios de seguridad. Estos servicios facilitan la detección temprana de problemas del sistema, desde el deterioro de los activos hasta la manipulación indebida, y pueden ayudar a evitar que se agraven y afecten la continuidad del negocio.

Para los proveedores de servicios, la conectividad remota permite una clasificación más rápida de incidencias, respuestas más coordinadas y una mejor alineación entre el personal in situ, los operadores remotos y los especialistas técnicos, lo que ayuda a los clientes a mantener una postura de seguridad más sólida y coherente.

1. Encuesta interna realizada a clientes de Securitas Technology en Australia, Bélgica, Canadá, Dinamarca, Finlandia, Francia, Alemania, Irlanda, México, Países Bajos, Noruega, Portugal, Singapur, España, Suecia, Suiza, Turquía, Reino Unido y Estados Unidos. Los datos mostrados reflejan únicamente las respuestas de los clientes comerciales. Realizado en noviembre de 2025.

Información del socio tecnológico

Evolución de la monitorización remota: Minimizar el tiempo de inactividad y permitir un mantenimiento proactivo

La monitorización remota está evolucionando desde simples comprobaciones de estado hasta convertirse en una potente herramienta para minimizar el tiempo de inactividad y mejorar la fiabilidad del sistema.

Un avance importante en esta evolución es la monitorización del estado del sistema en tiempo real, que realiza un seguimiento continuo del rendimiento de los paneles de intrusión, los sensores, las cámaras, los comunicadores celulares y las conexiones de red.

Los sistemas de diagnóstico remoto basados en la nube, como AlarmNet® 360 de Resideo, respaldan este cambio al identificar problemas como cortes de energía, fallas de comunicación o fallas en los dispositivos, que se detectan de inmediato, a menudo antes de que los clientes noten el problema. Proporciona acceso seguro a los datos y configuraciones del sistema, y permite a los técnicos solucionar muchos problemas de forma remota, lo que reduce la necesidad de desplazamientos de técnicos, acelera los tiempos de respuesta y mejora la experiencia del cliente.

El mantenimiento impulsado por IA reduce aún más el tiempo de inactividad al analizar las tendencias de rendimiento y el estado de los equipos para anticipar posibles fallos del sistema.

En lugar de reaccionar ante las interrupciones del servicio, los equipos de servicio pueden programar el mantenimiento de forma proactiva, mejorando el tiempo de actividad y prolongando la vida útil de los equipos.

resideo

Securitas Technology

Verificación remota y gestión de incidentes

Mejorar la respuesta ante incidentes con una verificación más rápida y clara

La verificación remota de alarmas y vídeos permite a los equipos de seguridad evaluar incidentes de forma rápida y precisa sin necesidad de estar presentes en el lugar. Los resultados de nuestra encuesta a clientes muestran que la demanda de estos servicios por parte de las organizaciones es alta.

Mediante sistemas de vídeo y detección de intrusiones conectados a la nube, los operadores remotos de los centros de monitorización de alarmas pueden revisar las alertas y el vídeo en directo en tiempo real, determinar si es necesario escalar la situación y guiar a los equipos de respuesta con la información adecuada. Este enfoque reduce la incertidumbre, acorta los tiempos de respuesta y ayuda a disminuir las falsas alarmas. Cada vez más, los servicios policiales locales están implementando políticas que implican que no responderán a una alarma sin una verificación visual de una amenaza activa.

Mejorar la gestión de incidentes mediante una supervisión centralizada

Cuando la verificación y la gestión de incidentes se realizan desde una ubicación central, ya sea una sala de control de seguridad interna o a través de un proveedor de monitorización externo, las organizaciones pueden obtener una visión completa de la actividad en todas sus instalaciones. Los operadores de alarmas pueden comparar alertas, detectar patrones, priorizar eventos y coordinar respuestas de manera más eficaz. Esta supervisión centralizada también favorece una toma de decisiones más coherente, garantizando que incidentes similares se gestionen de la misma manera, independientemente de dónde se produzcan o de quién sea el responsable de derivarlos a instancias superiores. Resulta especialmente valioso para organizaciones con ubicaciones diversas o con distintos niveles de experiencia in situ.

Más de la mitad → 57%

de nuestros clientes actualmente utilizan o están interesados en adoptar servicios remotos basados en video en los próximos 18 meses [1]

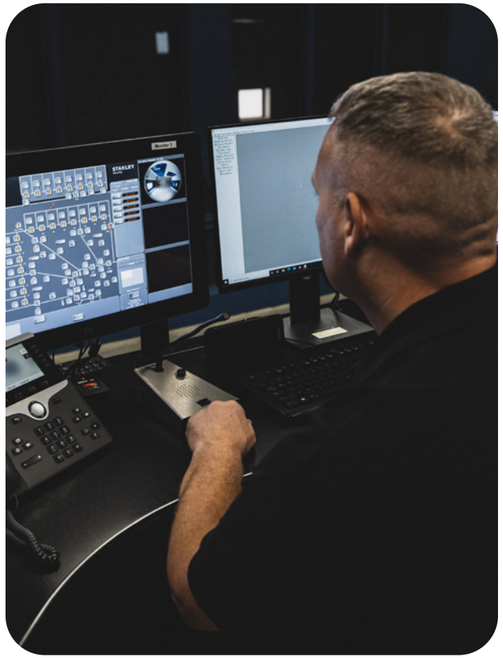
1. Encuesta interna realizada a clientes de Securitas Technology en Australia, Bélgica, Canadá, Dinamarca, Finlandia, Francia, Alemania, Irlanda, México, Países Bajos, Noruega, Portugal, Singapur, España, Suecia, Suiza, Turquía, Reino Unido y Estados Unidos. Los datos mostrados reflejan únicamente las respuestas de los clientes comerciales. Realizado en noviembre de 2025.



Aprovechar la IA y la IA general para dar soporte a los operadores remotos

Como se comenta en **la sección 3** , las herramientas basadas en inteligencia artificial están ayudando a los operadores a revisar vídeos, identificar actividades relevantes y extraer la información más importante durante un incidente. La IA puede recopilar resúmenes, destacar las imágenes clave y agilizar la comunicación con los equipos internos o los servicios de emergencia.

De cara al futuro, las capacidades de la IA con agentes ayudarán a reducir aún más la carga cognitiva, mejorar la precisión y proporcionar a los operadores la claridad que necesitan para actuar con confianza, especialmente cuando gestionan varias alertas al mismo tiempo.



Información del socio tecnológico

Servicios remotos que transforman las operaciones de seguridad

Las plataformas de servicios unificados, como Fusion One de Aritech, aportan mayor visibilidad operativa y eficiencia a las operaciones de seguridad al ofrecer un conjunto integral de servicios remotos que van mucho más allá de la gestión de productos.

Las plataformas digitales unificadas dan soporte a todas las etapas del ciclo de vida de la seguridad, desde la instalación y el mantenimiento hasta la gestión integral de incidentes, abarcando la detección de intrusiones, el control de acceso y la videovigilancia.

Un componente clave de este ecosistema es la gestión remota de incidentes. Nova, el servicio especializado de gestión remota de incidentes de Fusion One, centraliza todas las alarmas y eventos de cada subsistema en un único motor de flujo de trabajo inteligente. Ya sea que se implemente en las instalaciones o en la nube, esto permite a los operadores monitorear, verificar y resolver incidentes de forma remota en entornos de un solo sitio o de múltiples sitios. Admite enfoques basados tanto en la monitorización como en la planificación, lo que garantiza que cada incidente se gestione con coherencia, rapidez y plena visibilidad operativa.

Al permitir la supervisión remota y optimizar los flujos de trabajo, las plataformas digitales basadas en la nube reducen significativamente la necesidad de intervenciones in situ, aceleran la toma de decisiones y garantizan que cada ubicación, por muy dispersa que esté, se beneficie del mismo nivel de capacidad de respuesta.

El resultado es una resolución de incidentes más rápida, una mayor continuidad y un entorno de seguridad más coordinado y resiliente en todo el ecosistema de seguridad física.

ARITECH

Coordinación remota y personal de respuesta en el lugar

La verificación remota refuerza la respuesta in situ en lugar de sustituirla. Al confirmar la naturaleza de una alerta antes de enviar personal, los equipos pueden asegurarse de que los equipos de respuesta lleguen informados y preparados. Los operadores remotos pueden mantenerse involucrados durante todo el incidente, ajustando las vistas de las cámaras, compartiendo actualizaciones y proporcionando nueva información a medida que evoluciona la situación. Esta colaboración mejora el conocimiento de la situación, aumenta la seguridad y conduce a respuestas más eficaces en general. **Nuestra encuesta de mercado descubrió que una respuesta más rápida ante incidentes es una de las principales razones que impulsan un mayor uso de los servicios remotos, citada por el 58 % [1] de los encuestados, y solo superada por el ahorro de costes (61 % [1]).**

Fomentar la resiliencia en diferentes entornos

Para las organizaciones con múltiples sedes, diferentes niveles de personal o que operan fuera del horario habitual, la gestión remota de incidentes proporciona una forma escalable de mantener una protección constante. Contribuye a garantizar altos estándares en todas las ubicaciones, incluso cuando los recursos in situ son limitados. Y cuando se respalda con una plataforma de gestión de seguridad robusta que integra múltiples fuentes de datos, la verificación remota se convierte en parte de un modelo de respuesta coordinado y basado en inteligencia que mantiene a las personas, la tecnología y los datos alineados en tiempo real.



1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Una mejor comprensión equivale a una mejor respuesta

Las herramientas de verificación remota aceleran drásticamente la resolución de incidentes y reducen los tiempos de respuesta al proporcionar información inmediata y útil en entornos distribuidos.

Los clips de audio y vídeo activados por impacto permiten a los operadores verificar las alarmas en cuestión de segundos, distinguiendo rápidamente las amenazas reales de las falsas alarmas o las molestias causadas por ellas. Este triaje rápido elimina las demoras causadas por la incertidumbre y garantiza que la atención se centre donde realmente se necesita.

Las alarmas verificadas también mejoran la eficacia del despacho. Cuando las fuerzas del orden o los servicios de emergencia reciben pruebas confirmadas y detalles contextuales, los incidentes se priorizan adecuadamente, lo que permite una llegada más rápida al lugar de los hechos y respuestas mejor fundamentadas. Al mismo tiempo, las capacidades de control remoto en tiempo real permiten a los equipos de seguridad actuar de inmediato, bloqueando o desbloqueando puertas, iniciando confinamientos o ajustando las vistas de las cámaras para controlar las situaciones antes de que lleguen los servicios de emergencia.

En entornos con múltiples ubicaciones, la verificación remota se adapta sin problemas a cualquier situación. Los incidentes que afectan a múltiples emplazamientos pueden gestionarse desde una plataforma centralizada, con comandos y actualizaciones que se aplican instantáneamente en todas las instalaciones afectadas. Tras un incidente, el acceso centralizado a los vídeos, los historiales de eventos y los registros de auditoría acorta significativamente los ciclos de investigación, lo que permite un análisis más rápido de las causas fundamentales y la adopción de medidas correctivas.

Al reducir las falsas alarmas mediante audio, vídeo y análisis verificados, las herramientas de verificación remota también liberan recursos de emergencia para eventos reales, lo que mejora los tiempos de respuesta generales y el rendimiento del nivel de servicio en las operaciones de seguridad distribuidas.

SONITROL



Securitas Technology

Gestión centralizada del sistema de seguridad

Gestionar los sistemas de forma coherente en todas las ubicaciones

En todos los sectores, las aplicaciones digitales se han convertido en una herramienta fundamental para que las personas accedan a información y servicios de forma sencilla y rápida desde la palma de su mano. Esta misma velocidad y sencillez beneficia también a los profesionales de la seguridad. Los responsables de supervisar la seguridad de las instalaciones buscan plataformas de gestión de seguridad que les permitan actualizar y administrar sus sistemas y ubicaciones desde cualquier lugar, idealmente a través de una única aplicación que integre múltiples productos y marcas. De esta forma, tareas como visualizar las imágenes de las cámaras, ajustar la configuración, actualizar los permisos de usuario o refinar las políticas de control de acceso pueden gestionarse de forma remota a través de un dispositivo móvil. Se trata de un enfoque que ofrece mayor visibilidad, datos consolidados y garantiza que cada sitio se ajuste a los estándares de seguridad generales de la organización.



Las plataformas de gestión de seguridad son un

Los 3 mejores

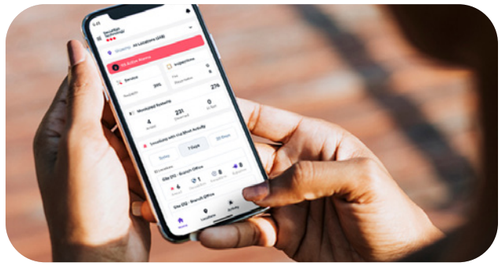
servicio de suscripción que las organizaciones priorizarán en los próximos 12-18 meses [1]



Mejorar la eficiencia mediante la configuración centralizad.

Las actualizaciones del sistema que antes requerían cambios en cada ubicación ahora se pueden completar de forma centralizada en cuestión de minutos. Los equipos pueden ajustar la configuración del sistema, implementar actualizaciones de funciones y aplicar cambios de políticas en múltiples sitios de forma rápida y eficiente. Esto simplifica el trabajo diario, reduce la complejidad operativa y fortalece la gobernanza al garantizar que cada cambio sea coherente y esté documentado.

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.



Información del socio tecnológico

Las capacidades ampliadas de gestión remota están ayudando a reducir costes y complejidad

Históricamente, la actualización de los sistemas de seguridad ha sido un proceso lento y laborioso.

Gestionar los sistemas de seguridad de esta manera tradicional a menudo implica el despliegue de vehículos, trabajar en zonas con conexiones poco fiables y el riesgo de que los clientes pospongan las actualizaciones necesarias.

Estos desafíos se ven agravados a medida que aumenta el tamaño del edificio o campus, lo que conlleva un incremento de los costes a medida que las empresas crecen.

Ante el creciente número de amenazas a la ciberseguridad y los avances como la criptografía postcuántica, garantizar que las actualizaciones de hardware y software se entreguen de forma constante y eficiente se ha vuelto esencial.

Los responsables de seguridad buscan mantener estándares de seguridad rigurosos al tiempo que reducen el tiempo, la mano de obra y los tiempos de inactividad innecesarios. La evolución de los servicios de seguridad remota, posibilitada por la tecnología basada en la nube, está convirtiendo este enfoque de gestión de la seguridad en el modelo moderno a seguir.

Se prefieren las soluciones de control de acceso que facilitan las actualizaciones masivas e incluyen herramientas para reducir las visitas in situ y la duración de las cargas. Por ejemplo, HID Linq proporciona herramientas gratuitas para actualizar varios lectores simultáneamente, incluidas opciones móviles que funcionan sin conexión a Internet.

HID



Apoyamos el crecimiento, la expansión y la apertura de nuevas sedes

La gestión remota de sistemas facilita enormemente la escalabilidad de las organizaciones. Ya sea para inaugurar una nueva instalación, activar una ubicación temporal o adaptarse a las necesidades cambiantes del negocio, los equipos pueden configurar los sistemas de forma remota y poner las instalaciones en línea rápidamente. Esta flexibilidad resulta especialmente valiosa para organizaciones con operaciones estacionales, puntos de venta distribuidos o entornos que necesitan expandirse rápidamente sin largos periodos de instalación in situ.

Unificar todo el ecosistema de seguridad

Las plataformas que permiten la gestión remota de sistemas son la herramienta a través de la cual los profesionales de la seguridad pueden supervisar y comprender su cartera tecnológica. Se trata de un entorno unificado donde la configuración del sistema, la monitorización del estado, el vídeo, el análisis de datos y las alertas trabajan conjuntamente para generar información y claridad que antes no eran accesibles sin una consolidación y un análisis de datos manuales, complicados y que consumían mucho tiempo. Esta visión centralizada ayuda a reducir la fragmentación y a mejorar la coherencia entre los distintos sitios web. También favorece un enfoque más coordinado, donde la información fluye sin problemas entre los sistemas y fortalece el rendimiento operativo general.

Información del socio tecnológico

Ojos por todas partes, control por todas partes

Gestionar entornos de seguridad complejos de forma remota proporciona a los equipos una ventaja práctica.

Con la tecnología adecuada, los operadores pueden ver las transmisiones de vídeo, los eventos del sistema y el estado de los dispositivos en un solo lugar y responder más rápido, en lugar de tener que alternar entre cuatro o cinco paneles de control. Una sola pantalla puede cubrir todo un campus o múltiples sedes en todo el país, lo que facilita la coordinación sin necesidad de contratar más personal.

Las ventajas van más allá de la centralización: si una cámara se desconecta o un enlace de red empieza a fallar, los equipos pueden reaccionar en tiempo real para solucionar el problema sin sacrificar la continuidad operativa. Esto permite que los equipos más pequeños se centren en tareas de alta prioridad en lugar de en una supervisión constante. El acceso móvil permite que el personal se aleje de la sala de control y siga estando al tanto de lo que sucede.

Sin embargo, existe una contrapartida: Conectar más dispositivos en más ubicaciones amplía la superficie de ataque. Las cámaras remotas crean posibles puntos de entrada para los hackers, por lo que los equipos deben considerar la ciberseguridad como algo imprescindible y no como algo deseable pero no esencial.Cuando se implementan esas medidas de seguridad, la gestión remota se convierte en una ventaja: los equipos pueden ampliar la cobertura, mantener la capacidad de respuesta y brindar una protección uniforme en todos los sitios sin agotar los recursos.

INTELLICENE
SECURITY. EVOLVED.

Securitas Technology

> La nube está transformando la seguridad en una disciplina más inteligente, rápida y conectada. La inteligencia artificial, los servicios remotos y la información en tiempo real permiten a los clientes proteger a su personal y sus activos desde cualquier lugar, con mayor precisión y menor complejidad.

Lisa Gutierrez
Vicepresidente de Servicios Avanzados Globales al Cliente y Gestión de Ventas.
Securitas Technology





Plan de acción para profesionales de la seguridad

Aprovechar al máximo las capacidades habilitadas para la nube

01

Establecer una estrategia clara de nube y conectividad.

La seguridad preparada para el futuro depende de una conectividad fiable y una sólida infraestructura en la nube. En colaboración con tus compañeros del departamento de TI, revisa el ancho de banda, la resiliencia y la seguridad de la red, así como las políticas de gestión de datos, para garantizar que tu organización esté preparada para el vídeo, el análisis y la configuración habilitados para la nube. Para algunas organizaciones, un enfoque híbrido como punto de partida para la adopción de la nube puede ser la mejor opción.

02

Identificar dónde las capacidades remotas aportan mayor valor.

Evalúa su programa de seguridad para detectar deficiencias en la cobertura, puntos críticos operativos o limitaciones de recursos. ¿Existen centros con personal limitado, ubicados en zonas remotas o que experimenten problemas técnicos recurrentes? Estos sistemas suelen beneficiarse más de servicios remotos como la verificación de alarmas por vídeo, el mantenimiento o la supervisión del estado del sistema.

03

Estandarizar la monitorización y el mantenimiento del estado del sistema.

Explora la posibilidad de utilizar la monitorización remota del estado del sistema para ayudar a realizar un seguimiento del rendimiento del dispositivo, la coherencia de la configuración y el tiempo de actividad en todas las ubicaciones. Los diagnósticos basados en inteligencia artificial pueden identificar los primeros indicios de fallos, lo que ayuda a los equipos a resolver los problemas con mayor rapidez y a mantener un nivel de protección constante en todas las instalaciones.

04

Definir procedimientos claros para la verificación y la escalada remotas.

Revisa el proceso que sigue para supervisar y verificar las alarmas. ¿Sigues dependiendo del personal in situ para verificar y escalar los incidentes? ¿Sería más eficiente utilizar un servicio remoto? Unos procedimientos claros ayudarán a mejorar la calidad de la respuesta, reducirán los envíos innecesarios y garantizarán que la información crítica llegue a las personas adecuadas de manera oportuna.

05

Centralizar la configuración del sistema y la gestión de políticas.

Si aún no lo has hecho, considere la posibilidad de suscribirse a una plataforma de gestión de seguridad para consolidar alarmas, supervisar la actividad y administrar sistemas de forma remota. La centralización refuerza la gobernanza, reduce los errores y garantiza que todas las sedes operen bajo las mismas políticas, al tiempo que facilita cambios más rápidos durante el crecimiento o las modificaciones operativas.

06

Adopte un enfoque que priorice el trabajo remoto para la monitorización, la optimización y el soporte.

Dar prioridad a los servicios remotos ofrece las ventajas de una supervisión continua, un mantenimiento proactivo y una mayor sostenibilidad. Si bien en muchos casos seguirá dependiendo de la tranquilidad que brindan las visitas físicas a las instalaciones y la experiencia técnica, la adopción de servicios remotos es clave para una experiencia de seguridad más eficiente y basada en la inteligencia.

Securitas Technology

05

Drones y robots que llevan la seguridad al límite

En esta sección

- Detección de drones
- Drones para vigilancia
- Robots en seguridad
- Plan de acción para profesionales de la seguridad

Securitas Technology

Creciente interés en las tecnologías autónomas

La nueva frontera de la seguridad

Los drones y los robots son temas que llevan varios años dando vueltas en el ámbito de la seguridad, pero esta tecnología no era un tema de conversación habitual. Eso está cambiando.

La creciente disponibilidad de drones de uso comercial, combinada con el desarrollo acelerado de robots con inteligencia artificial, significa que su potencial como herramientas de seguridad que amplían la visibilidad, automatizan actividades rutinarias y brindan apoyo a organizaciones que operan en entornos complejos está empezando a hacerse realidad. **El 88% [1] de nuestros socios tecnológicos estratégicos espera que las tecnologías autónomas tengan un impacto moderado o significativo en las operaciones de seguridad durante los próximos 5 a 10 años, y un 8 % considera que tendrán un impacto transformador.**

En lo que respecta a los drones, existen dos aspectos tecnológicos de seguridad específicos.

El primero son **los sistemas de detección de drones** , utilizados para detectar y rastrear drones y vehículos aéreos no tripulados (VANT) que podrían suponer un riesgo para la seguridad y la privacidad de un local comercial. Por el contrario, las organizaciones pueden aprovechar los drones como una **herramienta de seguridad proactiva** para ampliar la cobertura de vigilancia, realizar patrullas automatizadas y ayudar en la gestión de incidentes.

En el ámbito de la **robótica** , ya existen oportunidades para automatizar algunos procesos de seguridad, como la asistencia en la gestión de visitantes y las tareas propias de un servicio de conserjería. A medida que **las aplicaciones robóticas cuadrúpedas y humanoides** se vuelven más probadas, asequibles y aceptadas por el público, es probable que los avances en IA las posicionen como importantes factores disruptivos dentro de la industria de la seguridad.

En los próximos años, el desarrollo de tecnologías autónomas ofrecerá a las organizaciones nuevas formas de reforzar el conocimiento de la situación, mejorar la coherencia y complementar la vigilancia humana en entornos complejos.



Las perspectivas:

- **La detección de drones se está volviendo cada vez más esencial.** a medida que las amenazas aéreas se vuelven más comunes y complejas de gestionar para las organizaciones comerciales.
- **Los drones utilizados con fines de vigilancia pueden ofrecer una visibilidad rápida y flexible.** en entornos extensos o de difícil acceso.
- **Los robots pueden ayudar a automatizar las patrullas rutinarias.** , controles ambientales y vigilancia in situ para apoyar y capacitar a los guardias humanos.
- **Los sistemas autónomos pueden ayudar a aliviar la presión sobre los equipos de primera línea.** y fortalecer la resiliencia operativa.
- **Integración con plataformas de gestión de seguridad** Reúne los datos de drones y robots (telemetría, vídeo y alertas) en una sola vista.
- **A medida que la tecnología madura y las regulaciones evolucionan** Los drones y los robots están en una posición privilegiada para una mayor adopción por parte de la industria.

1. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.

2. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Los drones y los robots entran en la fase de adopción temprana.

Porcentaje de organizaciones que planean adoptar la detección de drones, la vigilancia con drones o los robots en los próximos 12-18 meses [2]

9.7% Detección de drones

9.9% Drones para vigilancia

9.9% Robots

Securitas Technology

Detección de drones: Cómo afrontar la amenaza aérea



Por qué la detección de drones se está volviendo esencial

Los drones no autorizados están creando nuevos desafíos para las organizaciones con perímetros extensos, operaciones delicadas o entornos complejos. La tecnología en sí misma es cada vez más capaz y accesible, lo que introduce nuevos riesgos que van desde intrusiones accidentales hasta vigilancia deliberada o intenciones delictivas. Estas amenazas pueden eludir las defensas tradicionales contra intrusiones perimetrales, lo que convierte la capacidad de detección de drones en un componente cada vez más crítico de las estrategias de seguridad modernas.

5.7%

de organizaciones experimentaron un incidente relacionado con drones en los últimos 12 meses [1]

“Tuvimos un allanamiento en unas instalaciones donde el perpetrador utilizó un dron para reconocer nuestra ubicación.”

Director de Operaciones y participante en la encuesta de mercado, EE. UU. [1]

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Securitas Technology

Principales preocupaciones que impulsan la adopción de sistemas de detección de drones

Adquirir un dron avanzado nunca ha sido tan fácil, lo que los hace tan accesibles para los delincuentes como para los verdaderos aficionados. Independientemente de la intención que motive cada vuelo, la actividad de los drones supone una amenaza para las organizaciones comerciales en términos de seguridad, privacidad, robo, espionaje e interrupción de operaciones.

Ante la dificultad de defenderse de las amenazas aéreas, existe una creciente necesidad de que los equipos de seguridad implementen sistemas eficaces de detección de drones que permitan respuestas más rápidas y mejor informadas ante los incidentes.

Las 3 principales razones por las que las organizaciones están implementando tecnología de detección de drones

01 Mejorar la seguridad en el lugar de trabajo

02 Prevención de interrupciones operativas

03 Prevención del robo de propiedad intelectual



Cómo afrontar los incidentes con drones más allá de la detección

Para la mayoría de las organizaciones, detectar un dron y monitorear sus movimientos es el nivel máximo de mitigación que se puede lograr en el marco legal actual. En la mayoría de las jurisdicciones, las leyes y regulaciones impiden que los equipos de seguridad tomen medidas directas contra la amenaza de los drones, como la neutralización física o electrónica. El objetivo principal de la detección de drones debe ser generar un conocimiento rápido de la situación para poder mitigar el riesgo. En algunas jurisdicciones, una estrecha coordinación con las fuerzas del orden puede ser una vía para mitigar realmente el riesgo de los drones, y esta es un área que puede cambiar rápidamente a corto y medio plazo a medida que aumenta la amenaza de los drones.



1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Información del socio tecnológico

"Los avances en la detección de drones serán esenciales para las futuras estrategias de seguridad perimetral. A medida que los drones se vuelven más comunes y cada vez más económicos, representan un desafío creciente que las medidas de seguridad tradicionales no están diseñadas para abordar.

ASSA ABLOY

"Históricamente, las estrategias de perímetro se han centrado principalmente en las amenazas terrestres. El rápido aumento de la actividad de los drones en los últimos cinco años ha ampliado ese perímetro verticalmente, lo que obliga a los equipos de seguridad a vigilar y responder también a los riesgos procedentes del aire. Detectar drones a una distancia suficiente, con rapidez y precisión, sigue siendo un reto. Sin embargo, la continua innovación en radares, análisis de vídeo e integración de datos está mejorando la fiabilidad y los tiempos de respuesta. Esperamos que esta situación siga mejorando en el futuro, convirtiéndolas en fuentes más fiables dentro de la estrategia de seguridad perimetral integral."

AXIS COMMUNICATIONS

"Prevemos que la seguridad perimetral evolucionará hacia múltiples capas. La intrusión terrestre (vallas, vídeo, control de acceso) es lo habitual hoy en día, pero los drones pueden eludir por completo los controles terrestres. Las cámaras de línea de visión no captan bien el espacio aéreo, y las amenazas pueden aproximarse desde alturas y desde detrás de estructuras. La monitorización del espacio aéreo, la clasificación mediante IA y la respuesta coordinada harán que la seguridad perimetral sea volumétrica, no lineal. Esto cambiará radicalmente la arquitectura de detección y convertirá la detección de drones de un nicho de mercado a un estándar, especialmente en infraestructuras críticas.

Hanwha Vision

Securitas Technology

Comprender la amenaza en tiempo real

La detección eficaz de drones comienza con la concienciación. Las soluciones modernas utilizan diversas técnicas, como la monitorización por radiofrecuencia, el radar, el análisis óptico y los sensores acústicos, para identificar y rastrear drones de terceros en diferentes entornos. Estos sistemas ayudan a los equipos a distinguir entre la actividad de aficionados, el tráfico comercial y el comportamiento sospechoso. Cuando se integran con protocolos de seguridad centralizados, estas alertas pueden ser rastreadas, priorizadas y respaldadas con contexto para guiar la respuesta adecuada. Esta es un área de soluciones que seguirá desarrollándose rápidamente a medida que los ciberdelincuentes se vuelvan más sofisticados y utilicen técnicas como el enmascaramiento de la identificación remota o frecuencias no estándar para intentar evadir la detección.

Reforzar la protección con automatización e IA

A medida que la tecnología continúa evolucionando, la detección de drones se vuelve más precisa y automatizada. Los análisis basados en inteligencia artificial pueden ayudar a identificar patrones de vuelo, clasificar tipos de drones y detectar acciones que puedan indicar un riesgo elevado. Esta mayor automatización puede ayudar a reducir las falsas alarmas, al garantizar que los equipos de seguridad reciban alertas relevantes y que permitan tomar medidas al respecto. También existe la posibilidad de respaldar la respuesta ante amenazas mediante el uso interno de tecnología de drones, ya que los sistemas de detección pueden configurarse para activar verificaciones visuales automatizadas o respuestas de patrullaje mediante drones o robots de vigilancia in situ.



Una solución vital para ampliar la protección perimetral.

La tecnología de detección mediante drones proporciona una capa adicional de protección para las organizaciones que buscan reforzar sus defensas perimetrales y salvaguardar las zonas sensibles. Contribuye a la resiliencia al proporcionar a los equipos una mayor visibilidad, información más clara y más tiempo para reaccionar. A medida que la actividad aérea continúa aumentando en entornos comerciales, industriales y públicos, integrar la detección de drones en el ecosistema de seguridad general será un paso clave para prepararse para el futuro.

Planes de detección de drones entre nuestros socios tecnológicos estratégicos:

12% tienen una integración o asociación

4% lo tienen contemplado en su hoja de ruta de desarrollo de productos

32% lo están explorando actualmente

1. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.

Información del socio tecnológico

"La expansión de las operaciones más allá de la línea de visión (BVLOS, por sus siglas en inglés) obliga a las defensas perimetrales a ampliar las zonas de detección más allá de las vallas, estableciendo redes de seguridad aéreas estratificadas capaces de monitorizar la actividad de drones de largo alcance antes de que alcancen activos críticos. Estas innovaciones están transformando la seguridad perimetral, pasando de sistemas estáticos centrados en tierra a arquitecturas de defensa del espacio aéreo dinámicas, interconectadas y basadas en inteligencia.

IDIS One Solution. One Company.

"Las tecnologías de detección de drones están redefiniendo la seguridad perimetral al ampliar el perímetro más allá de vallas y puertas para incluir el espacio aéreo. Este cambio respalda una evolución más amplia en la seguridad perimetral, pasando de la monitorización reactiva a las operaciones proactivas y conectadas, donde una detección más rápida, un mejor conocimiento de la situación y una respuesta automatizada son clave para adelantarse a las amenazas emergentes.

INTELLICENE SECURITY. EVOLVED.

"Las amenazas de los drones serán la principal preocupación para las organizaciones en el futuro." La tecnología está superando a la regulación en lo que respecta a qué se puede volar y dónde. El fácil acceso a la tecnología de bajo coste crea una brecha de seguridad difícil de cerrar y de contrarrestar.

IQSIGHT

"La detección mediante drones se convertirá en una útil capa complementaria de protección perimetral. A medida que estas tecnologías mejoren y se integren más fácilmente con los sistemas de vídeo, detección de intrusiones y control de acceso existentes, ayudarán a las organizaciones a lograr una mayor comprensión de la situación sin modificar su estrategia de seguridad principal.

PACOM

Securitas Technology

Drones para vigilancia: Proteger desde una perspectiva diferente

Ampliar la visibilidad en entornos complejos

Los drones están llamados a transformar la forma en que las organizaciones supervisan áreas extensas, dispersas o de difícil acceso. Ofrecen una visibilidad rápida y flexible que complementa las cámaras fijas y los guardias de seguridad in situ, mejorando el conocimiento de la situación al proporcionar a los equipos de seguridad una visión más clara de lo que ocurre en todo su entorno. Los sectores con una amplia presencia, desde la logística y los servicios públicos hasta las instalaciones industriales y las operaciones en campus universitarios, son los que tienen más probabilidades de encontrar que los drones son eficaces para reducir las brechas de visibilidad y mejorar los tiempos de respuesta ante incidentes.



Fortalecimiento de la respuesta ante incidentes y la toma de decisiones

Los programas de drones como primera respuesta (DFR, por sus siglas en inglés) ya están siendo probados con éxito por las fuerzas del orden y las autoridades gubernamentales para brindar apoyo al personal en tierra con visibilidad en tiempo real de los incidentes, desde el seguimiento de sospechosos hasta la obtención de pruebas. Se prevé que este enfoque gane terreno en el mercado comercial, y que las organizaciones utilicen drones para ayudar a verificar la activación de una alarma, una intrusión perimetral o un problema medioambiental. **Según nuestra encuesta de mercado, la monitorización de incidentes en tiempo real es la principal aplicación que impulsa la adopción futura de drones para vigilancia** [1] . Esto no solo proporciona a los equipos de respuesta actualizaciones en tiempo real a medida que se desarrollan los incidentes, sino que también puede conducir a decisiones más rápidas sobre el terreno, reducir los envíos innecesarios y proteger mejor al personal.

Las 3 principales aplicaciones que impulsarán la adopción de drones de vigilancia por parte de las organizaciones en los próximos 12-18 meses [1]

Monitoreo de incidentes en tiempo real

29%

Patrullas de seguridad

27%

Verificación de alarma

23%

Una capa móvil de inteligencia

A diferencia de los sistemas de ubicación fija, los drones proporcionan una cobertura dinámica, móvil y basada en inteligencia artificial. Pueden desplazarse directamente al lugar donde se les necesita, seguir rutas de patrulla predefinidas o responder a alertas activadas por sensores, análisis o solicitudes del operador. Gracias a sus capacidades de vídeo de alta resolución, análisis de datos y opciones como imágenes térmicas o multiespectrales, los drones permiten a los equipos de seguridad verificar eventos, evaluar riesgos y recopilar información sobre la situación de forma rápida y segura. Esta movilidad convierte a los drones en una valiosa capa adicional dentro de un ecosistema de seguridad conectado.

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Información del socio tecnológico

"Los drones pueden utilizarse para complementar la vigilancia de seguridad perimetral, permitiendo una verificación visual rápida y eficaz, al tiempo que eliminan la necesidad de enviar a una persona a una situación de peligro."

AMAG TECHNOLOGY
An Allied Universal Company

"El despliegue en tiempo real de drones para videovigilancia es una alternativa viable a las estrategias tradicionales. Creemos que los drones cautivos están siendo poco utilizados y no se habla mucho de ellos. Los drones cautivos pueden permanecer en el aire indefinidamente y requieren menos infraestructura para su despliegue.

DMP

"Nuestro enfoque respecto al uso de drones se centra en integrar las operaciones aéreas directamente en nuestra plataforma de seguridad unificada, de modo que los drones se conviertan en una parte inherente de los flujos de trabajo de seguridad, en lugar de herramientas independientes. Gracias a las alianzas e integraciones, nuestra plataforma puede recibir transmisiones de vídeo en directo de drones, telemetría GPS y datos de misión junto con las señales de las cámaras fijas, lo que permite a los operadores ver, controlar y gestionar los drones desde la misma interfaz que utilizan para CCTV, control de acceso y alarmas.

Genetec™

"Al proporcionar acceso instantáneo de vídeo y audio al lugar de un evento, los drones pueden ayudar a lograr tiempos de respuesta más rápidos sin poner a los recursos humanos en situaciones peligrosas."

Honeywell | LENEL·S2 by Honeywell

Integrando drones en un ecosistema de seguridad conectado

Los drones se vuelven mucho más potentes cuando se integran en una plataforma de seguridad centralizada. Al consolidar los vídeos, la telemetría y las alertas de los drones junto con los datos de las cámaras, el control de acceso y otros sistemas, los operadores pueden obtener una visión operativa más unificada. Esta integración también admite flujos de trabajo automatizados. Por ejemplo, activar el lanzamiento de un dron cuando se activa un sensor perimetral o cuando las alertas de estado del sistema indican un posible problema.

Desbloquear la eficiencia operativa y la escalabilidad

A medida que la tecnología de drones se vuelve más accesible e inteligente, y a medida que las regulaciones continúan evolucionando, las organizaciones están explorando cómo los drones pueden respaldar no solo la seguridad, sino también las tareas operativas. Además de brindar apoyo con patrullas de seguridad rutinarias, estas incluyen el monitoreo de entregas, el apoyo a los controles de salud, seguridad y medio ambiente (HSE, por sus siglas en inglés) y la inspección de infraestructura crítica, especialmente en áreas de difícil acceso o peligrosas. Por ejemplo, un dron integrado con análisis de vídeo mediante inteligencia artificial podría ayudar a detectar automáticamente corrosión, anomalías u otras vulnerabilidades que supongan un riesgo para la continuidad del negocio. La capacidad de desempeñar múltiples funciones ayuda a las organizaciones a obtener mayor valor de la inversión en drones, al tiempo que reduce la carga de trabajo de los equipos de seguridad.

Planes de vigilancia con drones entre nuestros socios tecnológicos estratégicos [1]

16% tienen una integración o asociación

8% lo tienen contemplado en su hoja de ruta de desarrollo de productos

20% lo están explorando actualmente



1. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.

Avanzando hacia operaciones de seguridad más proactivas

Según la información proporcionada por nuestros socios tecnológicos y los estudios de mercado, los drones utilizados para la vigilancia están permitiendo un cambio de la monitorización reactiva a un enfoque más proactivo y basado en la inteligencia. Gracias a una mejor visibilidad, una confirmación más rápida y una mayor certeza situacional, los drones están bien posicionados para convertirse en herramientas prácticas que permitan reforzar la resiliencia y respaldar operaciones más eficientes en entornos complejos.



Información del socio tecnológico

"Creemos que los drones desempeñarán un papel fundamental en el futuro de la seguridad. La adopción de drones se está produciendo a un ritmo sin precedentes, y el sector de la seguridad no tardará en aprovechar esta tendencia.

milestone

"El riesgo de enviar un dron a una misión crítica o a un escenario peligroso es prácticamente nulo. Gracias a los drones, podemos recopilar datos inmediatos para facilitar una mejor respuesta ante incidentes, monitorizar lugares a los que los humanos no pueden acceder y ayudar a tomar decisiones que podrían salvar vidas.

MOTOROLA SOLUTIONS

"La capacidad de desplegar rápidamente la vigilancia con drones para la protección del perímetro permitirá una respuesta más rápida ante incidentes y una mayor conciencia situacional. Aunque no desarrollamos directamente tecnología de drones, somos capaces de integrar información de vídeo y eventos procedentes de soluciones con drones en nuestra plataforma para la monitorización remota de vídeo en directo.

OpenEye

"Los drones ayudarán a proporcionar una mayor conciencia situacional en escenarios que hacen que sea peligroso o geográficamente imposible obtener información visual. Por ello, consideramos que los drones desempeñarán un papel fundamental en la respuesta a incidentes.

VERINT

Securitas Technology

Robots en seguridad: Mejorar la eficiencia y la experiencia humanas.

Encontrar aplicaciones para respaldar las operaciones de seguridad

La robótica es un tema de gran actualidad entre los profesionales de la seguridad y la sociedad global en su conjunto. Año tras año, los innovadores tecnológicos de todo el mundo muestran las últimas capacidades de los robots impulsadas por inteligencia artificial, ya sea en el hogar, en lugares públicos o en entornos comerciales como plantas de fabricación e instalaciones de infraestructura crítica.

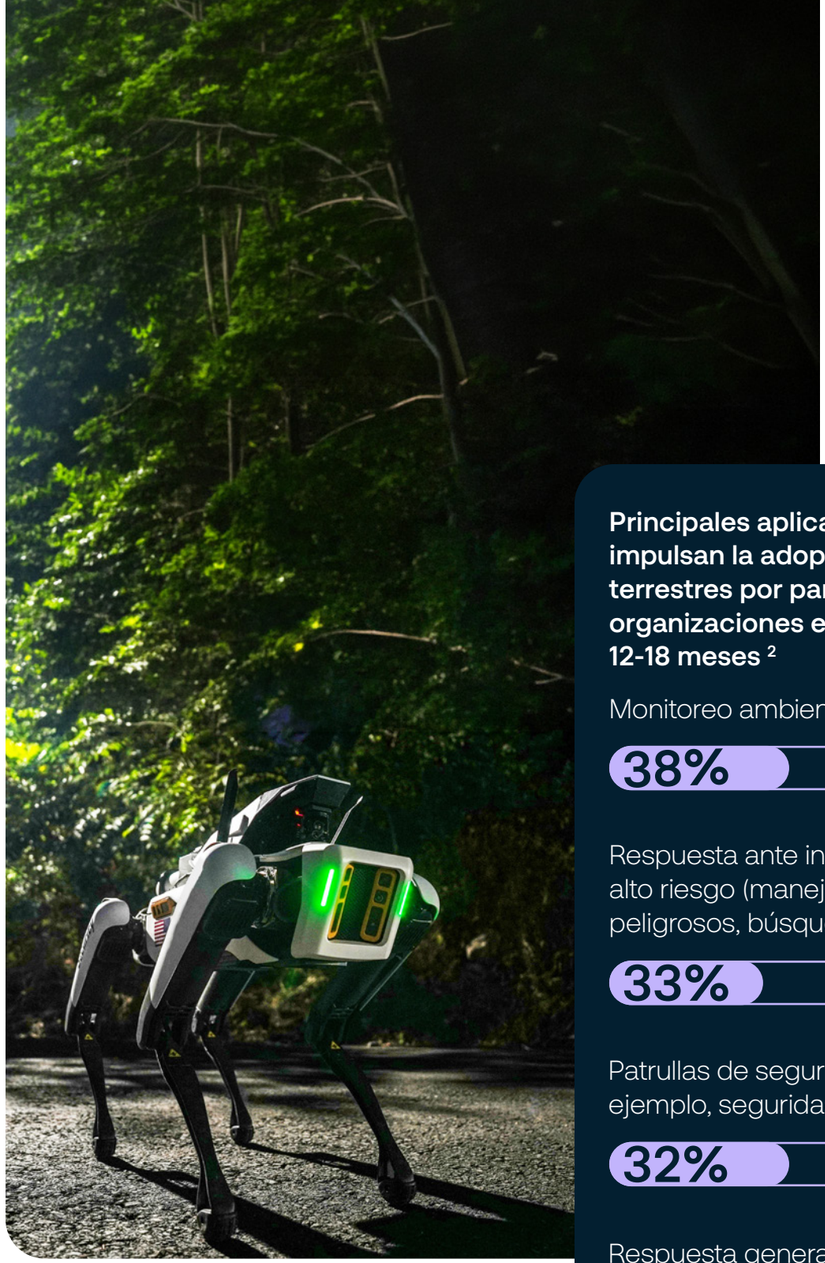
Los robots también están encontrando aplicaciones en la seguridad, principalmente en forma de dispositivos con ruedas y robots cuadrúpedos que pueden ayudar con la gestión de visitantes y las patrullas de seguridad automatizadas. El interés futuro se centra en tareas más sofisticadas, como la monitorización ambiental, la respuesta a incidentes de alto riesgo y el suministro de una presencia más ágil y sólida sobre el terreno. Si bien no fueron diseñados específicamente para fines de seguridad, la adaptación de robots humanoides para estas aplicaciones de seguridad y protección resulta cada vez más prometedora.

Planes de robótica entre nuestros socios tecnológicos estratégicos [1]

4% tienen una integración o asociación

12% lo tienen contemplado en su hoja de ruta de desarrollo de productos

24% lo están explorando actualmente



Principales aplicaciones que impulsan la adopción de robots terrestres por parte de las organizaciones en los próximos 12-18 meses [2]

Monitoreo ambiental
38%

Respuesta ante incidentes de alto riesgo (manejo de materiales peligrosos, búsqueda y rescate, etc.)
33%

Patrullas de seguridad (por ejemplo, seguridad perimetral)
32%

Respuesta general ante incidentes
28%

Gestión de visitantes
22%

1. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.

2. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.





Apoyar a los equipos de primera línea en entornos difíciles

Muchas organizaciones operan en entornos complejos o de alto riesgo donde la monitorización continua es esencial, pero físicamente exigente. Los robots son idóneos para estas tareas, ya que pueden patrullar grandes espacios interiores, vigilar puntos de acceso, desplazarse por aparcamientos o supervisar zonas exteriores sin fatigarse. Mediante el uso de cámaras integradas y diversos sensores, pueden detectar movimientos, cambios de temperatura, derrames u otras anomalías que requieran atención, lo que ayuda a los equipos de seguridad a mantenerse informados y, al mismo tiempo, limita la exposición del personal a las zonas más peligrosas de las instalaciones.

Información del socio tecnológico

“Observamos cómo la robótica está transformando la seguridad, pasando de un modelo dependiente de la mano de obra a una arquitectura que prioriza la automatización. Más allá de la vigilancia tradicional, los robots permiten realizar patrullajes constantes y de alta frecuencia, así como la detección de elementos ambientales (como gases peligrosos o detección térmica) en áreas que son inseguras o difíciles de monitorear para los humanos.

AJAX

“Es probable que los robots complementen las operaciones de seguridad tradicionales al brindar apoyo en la cobertura rutinaria, proporcionar visibilidad adicional durante los incidentes y permitir evaluaciones iniciales más seguras antes del despliegue del personal. Con el tiempo, pueden ayudar a las organizaciones a mantener una supervisión más consistente en todas las ubicaciones y a mejorar la coordinación de la respuesta al aportar información oportuna y localizada a los flujos de trabajo de seguridad existentes.

brivo
simply better security

“Los robots transformarán las operaciones de seguridad física al automatizar las patrullas y la vigilancia, mejorando la eficiencia, liberando al personal para tareas de mayor valor y aumentando la seguridad de los trabajadores humanos. También permiten el análisis en tiempo real y la vigilancia remota, lo que amplía la eficacia y el impacto de las soluciones de seguridad en todo el sector.

MARCH networks
A Delta Group Company

“A medida que el coste de la robótica siga disminuyendo, la demanda de esta tecnología aumentará, con el potencial de sustituir algunos servicios de vigilancia tradicionales por capacidades autónomas.”

radionix

Securitas Technology

La capacidad de vídeo y el funcionamiento autónomo son características importantes

La capacidad de grabación de vídeo, el funcionamiento autónomo y la capacidad de operar en cualquier condición climática se consideran los factores más importantes para las organizaciones que implementan robots terrestres. Otras características clave incluyen la movilidad, la duración de la batería y la capacidad de audio; todas ellas fundamentales para garantizar la fiabilidad y el rendimiento que generan confianza en la tecnología, de modo que más organizaciones tengan la seguridad necesaria para invertir.

44%

de las organizaciones clasificaron la capacidad de video como la característica más importante de la tecnología robótica [1]



Mejorar la eficiencia operativa y la capacidad de respuesta

Se obtendrá un valor tangible al utilizar robots para realizar tareas repetitivas que requieren atención pero no un juicio humano constante. La realización de patrullas programadas, el monitoreo de las condiciones ambientales y el envío de alertas directamente a los operadores permitirán al personal de seguridad concentrarse en tareas de mayor valor y fortalecer los niveles generales de servicio. Los robots también pueden enviarse para verificar alarmas o investigar perturbaciones, lo que proporciona a los equipos una visibilidad rápida con mínimas interrupciones.

Una opción cada vez más realista para los profesionales de la seguridad

Los robots están avanzando progresivamente hacia una mayor adopción, pero su implementación a gran escala en entornos de seguridad dependerá de varios factores: la aceptación cultural, la disminución de los costes, la fiabilidad demostrada, la preparación operativa y casos de uso claros con un retorno de la inversión definido. A corto plazo, los robots tienen el potencial de complementar a los equipos de seguridad humanos, aliviando la carga de trabajo rutinario y mejorando la forma en que se detectan, analizan y gestionan los riesgos.

Sectores como la logística, la fabricación, la atención médica y las operaciones en grandes instalaciones se encuentran entre los que tienen más probabilidades de ver cómo los robots se convierten en un componente estándar del ecosistema de seguridad. Los robots cuadrúpedos y humanoides, en particular, están llamados a ser uno de los factores de disrupción más importantes de la industria a medida que sus capacidades sigan evolucionando. En última instancia, la adopción a gran escala dependerá de un rendimiento fiable, datos de alta calidad y un impacto operativo medible.



1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Información del socio tecnológico

"Prevemos que los robots se convertirán en dispositivos de seguridad híbridos que combinan las funciones tradicionales de vigilancia, gestión de visitantes, conserjería y servicios de mantenimiento con capacidades de detección avanzadas para una mayor visibilidad y el cumplimiento de la normativa."

Software House C•CURE IQ

"Los robots actuarán como multiplicadores de fuerza, encargándose de patrullas repetitivas y de la monitorización mediante sensores para que los agentes humanos puedan centrarse en la toma de decisiones. A medida que aumenten las capacidades (mejor navegación, análisis integrados, comunicación móvil), se extenderá el alcance de las operaciones de seguridad más allá de lo que pueden abarcar las funciones de vigilancia tradicionales.

SONITROL

"Creemos que el principal uso de los robots en los futuros programas de seguridad será como complemento de los servicios de vigilancia tradicionales."

resideo

"Estamos en las primeras etapas del uso de robots para apoyar las operaciones de vigilancia humana, y esto seguirá desarrollándose durante los próximos años. Si bien se están logrando avances, aún faltan algunos años para que los robots puedan realizar acciones autónomas de forma segura en un entorno empresarial.

VIAKOO

Securitas Technology

> Aunque las tecnologías autónomas aún están en desarrollo, los drones y los robots están ganando terreno como valiosas incorporaciones a los programas de seguridad modernos. En lugar de sustituir a las personas, estas herramientas amplifican lo que los equipos de seguridad pueden ver, comprender y sobre lo que pueden actuar, lo que ayuda a los clientes a mejorar el conocimiento de la situación, fortalecer la respuesta y avanzar en nuestra misión compartida de hacer del mundo un lugar más seguro.

Doug Walsh
Vicepresidente de Estrategia Tecnológica Global
Securitas Technology



Securitas Technology

Plan de acción para profesionales de la seguridad

Evaluación de aplicaciones para tecnología autónoma

01

Comienza con un planteamiento claro del problema

Antes de explorar cualquier sistema autónomo, identifica los desafíos operativos específicos que debe abordar, ya sean puntos ciegos en el perímetro, lagunas en la cobertura de grandes instalaciones, requisitos de patrullaje repetitivos o problemas de seguridad para los equipos de primera línea. Una descripción clara del problema ayuda a determinar dónde los drones o los robots pueden aportar un valor significativo.

02

Mapea los casos de uso a su entorno

Elige tecnologías basadas en aplicaciones prácticas, no en su novedad. Los drones son idóneos para grandes áreas al aire libre, rutas de patrullaje flexibles y verificación rápida de incidentes, mientras que los robots permiten la monitorización continua en interiores o exteriores, la detección ambiental y las patrullas rutinarias que exigen consistencia. Adaptar las capacidades al contexto es clave para el éxito.

03

Incorpora la integración en tu proceso de toma de decisiones

La conectividad es un factor importante a la hora de evaluar nuevas tecnologías de seguridad. Asegúrate de que cualquier solución de drones o robots pueda integrarse con tu ecosistema de seguridad existente, de modo que las alertas, la telemetría y las transmisiones de vídeo se gestionen junto con otros sistemas. La integración mejora la eficiencia y reduce la compartimentación operativa.

04

Considera la normativa, el sitio, y los requisitos de seguridad

Las operaciones con drones requieren una atención meticulosa a las normas locales del espacio aéreo, las restricciones de vuelo y las obligaciones de cumplimiento. Los robots pueden necesitar rutas definidas, planes de seguridad y la concienciación del personal. Abordar los requisitos normativos y específicos de cada emplazamiento desde el principio agilizará la implementación y reducirá los riesgos.

05

Realiza pilotos con un propósito claro y escala con base en la evidencia

Los proyectos piloto específicos ayudan a validar el rendimiento, generar confianza interna y descubrir aspectos prácticos antes de su implementación a mayor escala. Realiza un seguimiento de los resultados medibles: tiempos de respuesta, consistencia en las patrullas, reducción de la carga de trabajo o mejora del conocimiento de la situación. Escala la tecnología cuando demuestre un valor consistente y repetible.

06

Prepara a su equipo para la colaboración entre personas y tecnología

El éxito de los drones y los robots depende de la eficacia con la que ayuden a las personas que los utilizan. Proporcionar capacitación que abarque los flujos de trabajo, la respuesta a incidentes, las transferencias de sistemas y el papel de la automatización. Ayudar a los equipos a comprender cómo estas tecnologías amplían sus capacidades fomenta su adopción y maximiza su impacto.









Securitas Technology

06

Salvaguardar el ecosistema de seguridad física

En esta sección

- mejores prácticas de seguridad de datos
- Fiabilidad de los datos
- Sistemas de seguridad resistentes a la computación cuántica
- Plan de acción para profesionales de la seguridad

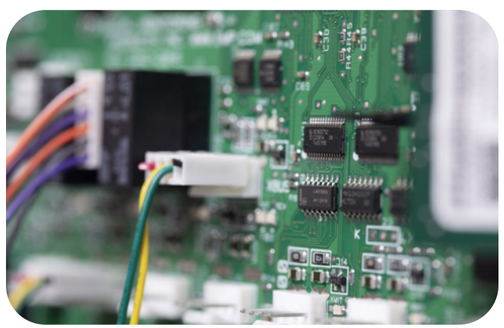
Securitas Technology

Infraestructura resiliente para programas de seguridad física



A medida que los sistemas de seguridad física se vuelven cada vez más conectados e inteligentes, proteger la infraestructura que los respalda se ha convertido en una prioridad fundamental para ayudar a mantener un rendimiento óptimo y protegerse contra futuras amenazas de ciberseguridad.

Las organizaciones ya no se centran únicamente en la funcionalidad de las soluciones de seguridad. La seguridad de los datos, la fiabilidad y la resiliencia de los dispositivos, el software y las tecnologías de red subyacentes son ahora consideraciones igualmente importantes en la selección de tecnología. Una sólida gobernanza de datos, una higiene cibernética coherente y tecnologías de seguridad ciberresistentes son ahora esenciales para mantener la confianza en un entorno digital que evoluciona rápidamente, incluida la llegada de la computación cuántica en un futuro próximo.



Las 3 principales prácticas ciberfísicas que actualmente llevan a cabo las organizaciones [1]

77%
Gestión de contraseñas

73%
Sensibilización/formación en ciberseguridad

68%
Actualizaciones periódicas del firmware

Las perspectivas:

- **Las redes que albergan sistemas de seguridad física requieren una protección robusta.** como parte de la estrategia general de ciberseguridad de una organización.
- **La higiene cibernética, la gobernanza del acceso y el uso responsable de la IA.** Ahora son elementos fundamentales de un programa de seguridad moderno.
- **Los riesgos emergentes como el vídeo generado por IA y el engaño mediante deepfakes** están provocando que las organizaciones adapten la forma en que verifican, validan y confían en los datos de seguridad.
- **La preparación cuántica** se está convirtiendo en una importante prioridad futura a medida que las amenazas de "recolectar ahora, descifrar después" ganan terreno.
- **Salvaguardar el ecosistema será clave** para permitir la adopción segura de la IA, la automatización y una seguridad preparada para el futuro a gran escala.

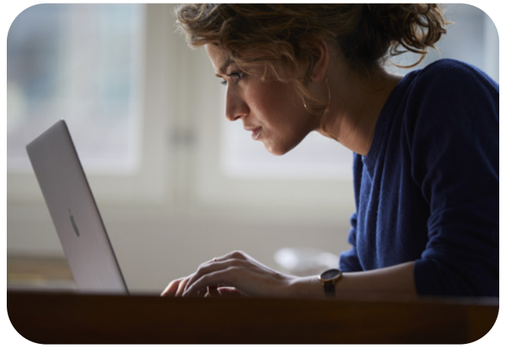
1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Securitas Technology

Mejores prácticas de seguridad de datos

Colocar una sólida gobernanza de datos en el centro de la seguridad moderna

A medida que la seguridad física se vuelve más digital e interconectada, los datos se han convertido rápidamente en uno de los activos más valiosos y vulnerables. Las organizaciones dependen del vídeo, los registros de acceso, el estado de los dispositivos y la telemetría del sistema para tomar decisiones informadas, pero esos datos deben ser precisos, estar bien gestionados y protegidos. Una gobernanza sólida garantiza que la información se mantenga segura, disponible y útil. Esto incluye definir los derechos de acceso, establecer políticas de retención claras y garantizar que los datos confidenciales se manejen de manera responsable en todos los sitios y sistemas.



Fortalecer la ciberhigiene en todos los dispositivos y plataformas de seguridad

La ciberhigiene es ahora un requisito básico para mantener operaciones de seguridad física seguras y fiables. **Los estándares consistentes de administración de contraseñas (77% [1]), la capacitación en concientización sobre ciberseguridad (73% [1]) y las actualizaciones regulares de firmware (68% [1]) son prácticas recomendadas bien establecidas entre las organizaciones que encuestamos, mientras que las inversiones futuras se centran en pruebas de terceros (29% [1]), segmentación de red (25% [1]) y planes de respuesta a incidentes (18% [1]) para mejorar aún más la resiliencia digital.**

En conjunto, estos controles ayudan a minimizar la exposición a accesos no autorizados o intentos de intrusión. Incluso un solo dispositivo mal configurado puede generar riesgos innecesarios. La integración de prácticas de higiene estandarizadas en todos los aspectos del entorno de seguridad física crea una base más sólida para que la IA, la automatización y las operaciones remotas se desarrollen de forma segura.

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Las 3 principales prácticas ciberfísicas planificadas para las organizaciones en 2027 [1]

Pruebas de terceros

29%

Segmentación de red

25%

Planes de respuesta ante incidentes

18%







Crear coherencia en todos los dispositivos y sitios web

Las organizaciones están respondiendo a las amenazas ciberfísicas impulsando la uniformidad en la forma en que se implementan los dispositivos de seguridad en múltiples ubicaciones. Las plantillas de configuración estandarizadas, los calendarios de actualización centralizados y las estructuras de permisos unificadas contribuyen a mantener los sistemas seguros, alineados y funcionando sin problemas. Esto reduce el riesgo operativo, simplifica el mantenimiento y garantiza que las organizaciones puedan confiar en los datos procedentes de cualquier ubicación. Al eliminar la variabilidad, las organizaciones crean un entorno más predecible y manejable, lo cual es especialmente importante al adoptar la nube, los servicios remotos y las capacidades mejoradas con IA.

92%

de las organizaciones están extremadamente o moderadamente preocupadas por el pirateo de dispositivos de seguridad [1]

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

Información del socio tecnológico

Garantizar la integridad en los programas de seguridad física digital

A medida que los sistemas de seguridad física se vuelven más digitales, interconectados y gestionados en la nube, garantizar la integridad de los datos de seguridad requiere un enfoque disciplinado y proactivo.

Los vídeos, los registros del sistema y los datos de acceso son tan fiables como las prácticas utilizadas para protegerlos. Uno de los riesgos más importantes para la integridad de los datos en la actualidad no es un fallo tecnológico, sino un error humano, que abarca desde contraseñas débiles hasta actualizaciones de software retrasadas y acceso inadecuado al sistema.

Una gestión sólida de identidades y accesos es fundamental. Las organizaciones deben implementar cuentas de usuario únicas, controles de acceso basados en roles y autenticación multifactor para reducir el acceso no autorizado y mejorar la rendición de cuentas. La gestión centralizada de usuarios y el registro de auditorías refuerzan aún más la supervisión al proporcionar una visibilidad clara sobre quién accedió a los datos y cuándo.

Igualmente importante es mantener la higiene del sistema. Mantener actualizados el software de grabación, los sistemas operativos, el firmware y las aplicaciones cliente garantiza que las vulnerabilidades conocidas se corrijan antes de que puedan ser explotadas. Evitar el uso de soportes extraíbles, proteger el hardware en ubicaciones con acceso controlado y aislar las redes de cámaras también ayudan a prevenir la manipulación y la pérdida de datos.

Por último, las plataformas gestionadas en la nube desempeñan un papel importante al permitir el acceso remoto seguro, configuraciones estandarizadas y la aplicación coherente de las políticas de seguridad en todas las ubicaciones. Al combinar una gobernanza sólida, un diseño de sistema seguro y un mantenimiento continuo, las organizaciones pueden preservar la integridad de sus datos de seguridad física y mantener la confianza a largo plazo en sus programas de seguridad.

OpenEye

Securitas Technology

Establecer una clara propiedad y responsabilidad sobre los datos

Una gobernanza de datos eficaz depende de la clara definición de roles y responsabilidades. Los responsables de seguridad colaboran cada vez más estrechamente con sus homólogos de TI y operaciones para definir quién es propietario de qué conjuntos de datos, quién gestiona el acceso y quién es responsable de hacer cumplir las políticas. Sin esta claridad, pueden surgir lagunas que den lugar a fallos de supervisión o a una gestión deficiente de la información. Definir la responsabilidad desde el principio ayuda a las organizaciones a mantener la visibilidad en todos sus entornos, fortalecer la colaboración y responder de manera más eficaz a los incidentes que involucran datos sensibles o de alto valor.

Apoyar la IA y la automatización con datos más limpios

Los sistemas basados en inteligencia artificial funcionan mejor cuando los datos que reciben están estructurados, son consistentes y precisos. Los datos de seguridad limpios y bien mantenidos pueden mejorar el análisis, potenciar la automatización y aumentar la fiabilidad de las capacidades generales. Por el contrario, los datos de mala calidad pueden dar lugar a falsos positivos, clasificaciones erróneas y una carga de trabajo adicional innecesaria. Las organizaciones están tomando medidas para fortalecer la calidad de los datos ahora, con miras a una adopción más avanzada de la IA en el futuro, lo que crea un camino más fluido para la escalabilidad y la mejora del rendimiento general del sistema de seguridad.





Alinear las prácticas de datos con la privacidad y el cumplimiento normativo.

A medida que las expectativas en materia de privacidad y las normativas de ciberseguridad se vuelven más complejas, los responsables de seguridad están tomando medidas para garantizar que las prácticas de recopilación, retención, acceso y eliminación de datos se ajusten a las políticas internas, las directrices del sector y los requisitos legales. Mantener una documentación clara y procesos transparentes contribuirá a generar confianza con los empleados, los clientes y los socios, al tiempo que integra las consideraciones de privacidad en los flujos de trabajo cotidianos. En definitiva, esto ayuda a reducir el riesgo de incumplimiento normativo, fortalece la integridad operativa y refuerza la confianza en la forma en que se gestionan los datos.

La integridad de los datos requiere prácticas de ciberseguridad eficaces

En el centro de la seguridad física se encuentra el concepto de integridad de los datos; ¿se han gestionado las pruebas de vídeo para crear una cadena de custodia fiable o se está verificando la autenticidad de la identidad antes de conceder el acceso?

Así como los procesos digitales han reemplazado a los analógicos en materia de seguridad, también lo ha hecho el concepto de gestión de la integridad de los datos. Es fundamental centrarse en contar con procesos que garanticen la ciberseguridad tanto de los datos que fluyen a través de un sistema de seguridad física como de la identidad de los participantes (tanto humanos como no humanos).

Casi todas las organizaciones cuentan con políticas de seguridad de la información para proteger los datos, pero no siempre se utilizan fuera del departamento de TI. Comience por implementar su política de seguridad de la información en todos los sistemas de seguridad física, por ejemplo, con políticas de rotación de contraseñas y manteniendo el firmware actualizado.

A esto hay que combinarlo con la gestión de identidades para dispositivos no humanos, como todos los dispositivos de cámara y los sistemas de control de acceso, mediante el uso de certificados en todos los dispositivos para garantizar que sean quienes dicen ser.

El uso de una plataforma automatizada como Viakoo no solo facilita la gestión de estas funciones en grandes flotas de dispositivos, sino que también proporciona los datos históricos necesarios para cumplir con los requisitos de cumplimiento y auditoría.

VIAKOO

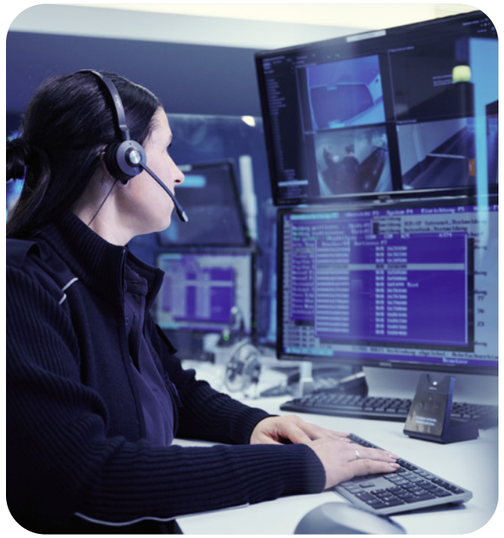
Securitas Technology

Fiabilidad de los datos

Abordar los riesgos emergentes: Deepfakes y contenido manipulado

Los vídeos generados por IA y los medios sintéticos plantean retos que los procesos de seguridad electrónica tradicionales nunca fueron diseñados para afrontar. Los deepfakes, en los que la IA manipula imágenes o grabaciones de vídeo para crear contenido falso, pueden ocultar hechos y socavar la confianza en las pruebas visuales, o utilizarse para intentar engañar a los sistemas de reconocimiento facial.

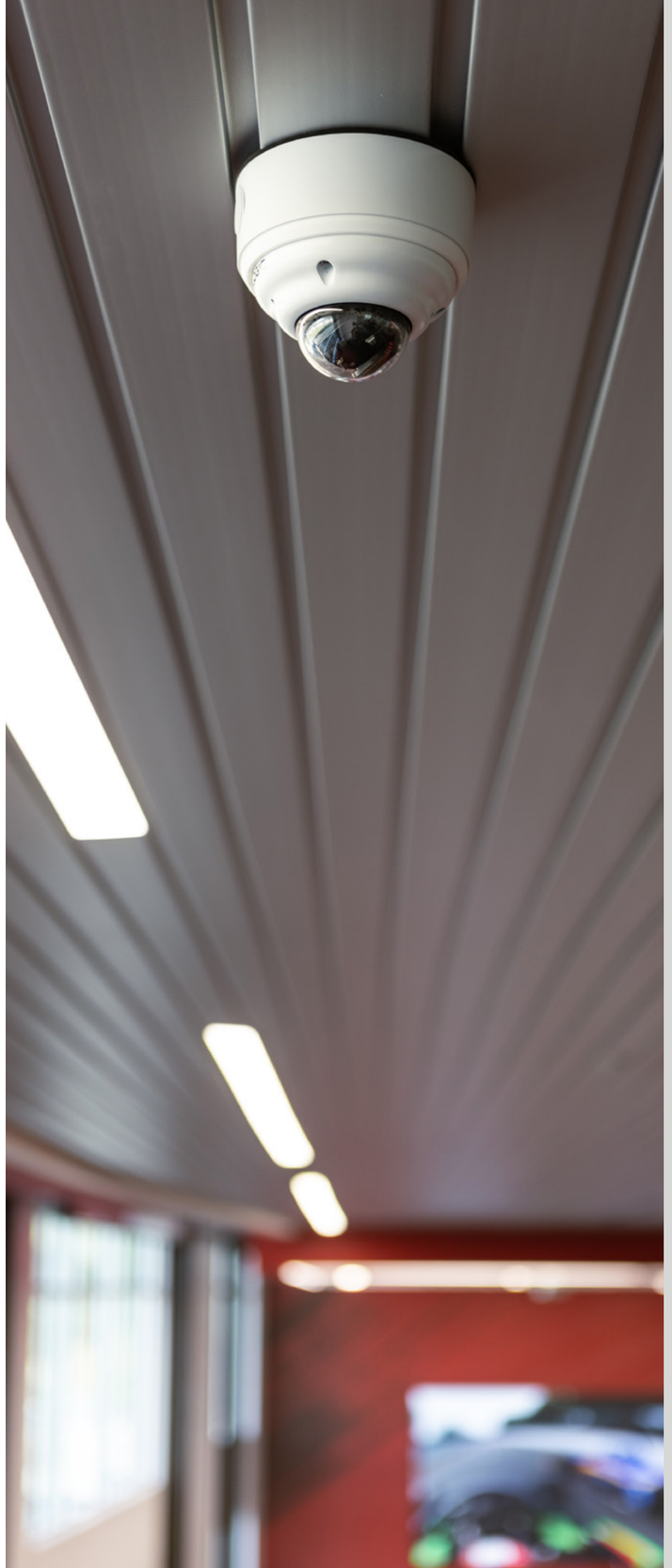
A medida que estas herramientas se vuelven más accesibles, las organizaciones deben asumir que la amenaza aumentará. **Nuestro estudio de mercado revela una conciencia aguda de la vulnerabilidad de los equipos de seguridad existentes a los ciberataques y otros riesgos (91% [1])** . Actualizar el firmware de los dispositivos y garantizar que se implementen medidas de seguridad para verificar la autenticidad, como la marca de agua digital, puede ayudar a los equipos de seguridad a adelantarse a la manipulación de contenido de vídeo. Se trata de tener la tranquilidad de que las pruebas en las que se basan siguen siendo creíbles, incluso en situaciones complejas.



91%

de las organizaciones están preocupadas por los equipos obsoletos que causan vulnerabilidad [1]

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.



Información del socio tecnológico

Garantizar la fiabilidad de los datos de seguridad: El papel de los líderes tecnológicos como Axis

En una era de IA, deepfakes y contenido sintético, garantizar la fiabilidad de los datos de seguridad es primordial.

Como líder en la industria de la seguridad, Axis Communications se compromete a proporcionar soluciones que protejan la integridad de los datos frente a las amenazas en constante evolución.

Integramos cifrado avanzado, protocolos de autenticación y funciones de ciberseguridad integradas, como vídeo firmado, arranque seguro y firmware de confianza, para garantizar la autenticidad de las grabaciones de vigilancia y evitar alteraciones no autorizadas. Estas técnicas criptográficas y protecciones basadas en hardware garantizan que los datos sean a prueba de manipulaciones, preservando la integridad probatoria a lo largo de todo su ciclo de vida.

Emplear análisis basados en inteligencia artificial para detectar inconsistencias sutiles en los medios que puedan indicar manipulación, como los deepfakes. Los algoritmos de IA evolucionan continuamente para adelantarse a las amenazas emergentes, garantizando así la fiabilidad de las soluciones de seguridad.

Para cumplir con los estrictos estándares y las mejores prácticas de la industria, debe realizar auditorías periódicas y colaborar con expertos en ciberseguridad para fortalecer las estrategias de defensa. Este enfoque proactivo y multicapa, que combina cifrado, análisis basados en IA, protecciones de hardware y estándares de la industria, garantiza que las soluciones sigan siendo resistentes frente a riesgos cada vez más sofisticados.

AXIS COMMUNICATIONS

Securitas Technology

Verificación de autenticidad en el punto de captura

La confianza en los datos comienza con la confianza en los dispositivos. Las cámaras y los sensores que utilizan firmware actualizado, transmisiones encriptadas y otras funciones de seguridad integradas proporcionan una mayor protección contra la piratería informática o la manipulación. Garantizar que los dispositivos sean legítimos y no hayan sido manipulados durante la instalación crea una base más fiable para los análisis de IA, las evaluaciones de los operadores y los flujos de trabajo posteriores. Esta verificación a nivel de origen está adquiriendo cada vez más importancia a medida que los sistemas se vuelven más inteligentes e interconectados.





Principales medidas de ciberresiliencia para nuestros socios tecnológicos [1]

Porcentaje de socios clasificados entre las tres principales prioridades:

96%

Fortalecimiento de la arquitectura del sistema

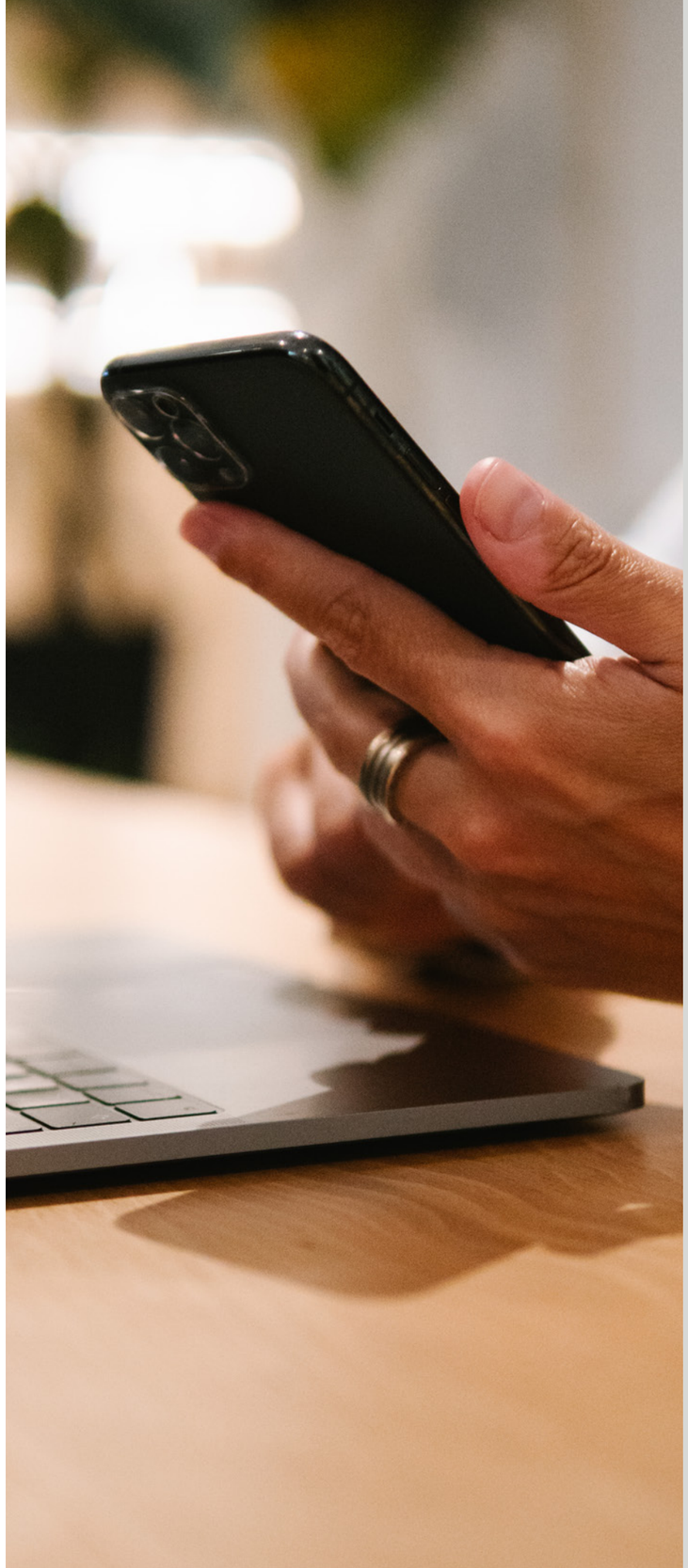
92%

Aumentar la seguridad a nivel de dispositivo

80%

Gestión de identidades y accesos

1. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.



Información del socio tecnológico

Construir una base de controles cibernéticos sólidos

En la era de la IA, los responsables de seguridad no pueden prometer una verdad absoluta, pero sí pueden esforzarse por lograr que los datos de seguridad sean auténticos, inalterados y atribuibles.

Comienza con los controles cibernéticos básicos: Autenticación robusta para demostrar quién o qué se conecta, autorización para limitar sus acciones y cifrado tanto en tránsito como en reposo, con una gestión de claves rigurosa.

A continuación, hablaremos de la integridad y la procedencia de las pruebas. La detección de manipulaciones en el momento de la captura utiliza firmas digitales criptográficas integradas en las grabaciones y validadas al exportarlas. Por otro lado, la marca de agua vincula al usuario, la estación de trabajo y el contexto de la cámara a cada fotograma para disuadir la divulgación no autorizada.

Por último, los líderes necesitan una cadena de custodia auditable. Registros de auditoría inmutables e informes de actividad del usuario que muestran quién accedió a los datos, cuándo y qué se modificó. Cualquier alteración no autorizada sería detectada por los controles de integridad, independientemente de lo convincente que pueda parecer el deepfake o el contenido sintético resultante.

Genetec™



Protección de vídeo y pruebas mediante flujos de trabajo seguros

Las pruebas deben gestionarse con cuidado para que sigan siendo fiables. **El primer paso esencial, priorizado por los profesionales de la seguridad (77% [1]) y los fabricantes (80% [2)] , es el siguiente.) según nuestras encuestas – está gestionando adecuadamente el acceso a la información.** Además, el almacenamiento cifrado, los registros a prueba de manipulaciones, las grabaciones con marca de agua y los procedimientos documentados de cadena de custodia pueden ayudar a preservar la integridad de los datos registrados. Estos flujos de trabajo garantizan que se pueda confiar en los vídeos y los registros durante auditorías, investigaciones o procesos legales. Unos estándares de manejo claros y repetibles reducen la ambigüedad, refuerzan la responsabilidad y fomentan la coherencia entre las distintas sedes y equipos.

Utilizar integraciones de fuentes confiables para validar la inteligencia

Muchas organizaciones complementan los datos de sus propios sistemas con información de terceros, desde informes de situación hasta sensores ambientales. Verificar el origen y la fiabilidad de estas fuentes ayuda a garantizar que las opiniones externas no distorsionen la toma de decisiones. Trabajar únicamente con proveedores verificados y de confianza reduce el riesgo de que la desinformación o los datos corruptos influyan en las operaciones. Las integraciones en la capa de confianza se están convirtiendo en un sello distintivo de los programas de seguridad maduros y basados en inteligencia.

Concienciación sobre los medios de comunicación engañosos

Incluso con las medidas de seguridad más avanzadas, el juicio humano sigue siendo esencial. **La concienciación sobre ciberseguridad es la segunda mejor práctica para contrarrestar los riesgos ciberfísicos, citada por el 73 % [1] de los líderes de seguridad en nuestra encuesta de mercado.** Capacitar a los equipos para detectar señales de manipulación, cuestionar grabaciones sospechosas y reportar anomalías fortalece la capacidad de una organización para detectar contenido multimedia engañoso de forma temprana. La formación en sensibilización reduce la posibilidad de interpretaciones erróneas, facilita una respuesta más precisa ante incidentes y aumenta la confianza del operador. Esta capa humana refuerza una cultura más amplia de vigilancia y confianza en todo el ecosistema de seguridad.



1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

2. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.

Información del socio tecnológico

Datos y ciberseguridad para un sistema de vídeo fiable

A medida que los sistemas de vídeo se vuelven más conectados y la inteligencia se acerca al extremo de la red, la confianza debe diseñarse desde el principio. Los proveedores de tecnología deben adoptar un enfoque de seguridad desde el diseño en todo lo relacionado con el hardware, el software y las integraciones. Eso significa proteger los datos en cada etapa, desde su captura hasta su análisis y entrega. El enfoque debe salvaguardar los datos y gestionar el acceso de los usuarios para cumplir con los estándares de confiabilidad más estrictos.

Una arquitectura verdaderamente segura tiene en cuenta todos los componentes del ecosistema de seguridad de vídeo: cámaras, dispositivos de almacenamiento, comunicación de red, infraestructura de clave pública (PKI) y software de gestión de vídeo. Las certificaciones independientes, como las que cumplen con la serie de normas UL 2900, ayudan a validar que las medidas de seguridad de un proveedor están actualizadas.

Igualmente importante es trabajar en estrecha colaboración con los clientes para garantizar que los sistemas se integren en sus estrategias generales de seguridad y TI. Cuando las organizaciones dependen del vídeo para tomar decisiones críticas, la seguridad y la fiabilidad deben ser innegociables.

IQSIGHT

Securitas Technology

Sistemas de seguridad resistentes a la computación cuántica

Preparación para futuros riesgos criptográficos

La computación cuántica es todavía un área en desarrollo de la tecnología de la información, pero las organizaciones deben prepararse desde ahora para el impacto altamente disruptivo que puede tener en las prácticas actuales de cifrado de datos. Aunque todavía no domina el debate sobre la ciberseguridad, está en el punto de mira tanto de los profesionales de la seguridad como de los proveedores de tecnología. **En nuestra encuesta de mercado, el 27%** [1] **de las organizaciones lo clasificaron como una de las principales preocupaciones ciberfísicas, mientras que la resistencia cuántica es una de las cinco principales prioridades de desarrollo para nuestros socios tecnológicos** [2] **.**

La amenaza más inmediata es la estrategia de "recolectar ahora, descifrar después", en la que los ciberdelincuentes capturan archivos cifrados hoy con la esperanza de descifrarlos una vez que las herramientas cuánticas estén lo suficientemente desarrolladas.

Para las organizaciones que almacenan vídeos de larga duración, registros de identidad o registros de acceso, prepararse con antelación ayudará a reducir el riesgo a largo plazo y a evitar adaptaciones disruptivas cuando evolucionen los estándares criptográficos.

27%

Las organizaciones están extremadamente preocupadas por las amenazas cuánticas al cifrado de los sistemas de seguridad electrónica [1]



Comprender el cronograma del segundo trimestre del año y por qué es importante

Y2Q (años para la era cuántica), el punto en el que las computadoras cuánticas podrían ser capaces de romper el cifrado de uso generalizado, se está convirtiendo en un hito de planificación para los líderes de seguridad. Aunque se desconoce el momento exacto, la dirección es clara: Los datos cifrados de larga duración almacenados hoy en día podrían volverse vulnerables en los próximos años. Las organizaciones con períodos de retención prolongados deben asumir que sus archivos podrían estar en riesgo en el futuro. Considerar Y2Q (años para la era cuántica) como un horizonte estratégico ayudará a orientar las prioridades de cifrado y las conversaciones con los proveedores.

Identificar los datos de larga duración que corren mayor riesgo

No todos los conjuntos de datos necesitan protección cuántica inmediata. La prioridad son los datos de larga duración, como los archivos de vídeo y las credenciales de control de acceso, ya que estos registros siguen siendo confidenciales durante años. Mapear dónde reside esta información y cómo está cifrada actualmente ayuda a las organizaciones a comprender su nivel de exposición e identificar qué sistemas requieren actualizaciones más tempranas. Esta claridad reduce la posibilidad de pasar por alto conjuntos de datos de alto riesgo y facilita una planificación de la transición más específica.

1. Encuesta anónima realizada por terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para tomar decisiones sobre tecnología de seguridad, que representan a organizaciones comerciales en la región de Asia-Pacífico, Europa y América del Norte. Realizada en febrero de 2026.

2. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.

Información del socio tecnológico

La preparación es clave a medida que avanzan las tecnologías cuánticas.

La implementación de controles sólidos es esencial para salvaguardar las fuentes de datos encriptadas, garantizando que no puedan copiarse ni descifrarse posteriormente a medida que avanzan las tecnologías cuánticas.

Las organizaciones deben tomar medidas proactivas para prepararse para los sistemas de seguridad resistentes a la computación cuántica y para garantizar la vigencia de sus estrategias de cifrado a largo plazo.

El primer paso consiste en comprender las áreas de vulnerabilidad mediante una evaluación exhaustiva y la creación de un inventario completo de las aplicaciones, bases de datos y servicios que utilizan criptografía de cifrado de clave pública. Este inventario también debería incluir productos de terceros integrados en la solución general, ya que representan posibles puntos de entrada para futuras capacidades cuánticas.

Una vez que se haya elaborado un inventario completo, las organizaciones deben establecer planes de migración para la transición a la criptografía postcuántica (PQC) aprobada por el NIST, que son algoritmos diseñados específicamente para ser resistentes a los ataques cuánticos.

Además, la adopción de técnicas de diseño criptoágil es crucial, ya que permite a las organizaciones cambiar rápidamente los algoritmos de cifrado sin necesidad de realizar modificaciones de ingeniería fundamentales. Esta flexibilidad permite una postura de seguridad más ágil y adaptable ante la evolución de las amenazas.

Como líder en el avance de las tecnologías cuánticas, la división Quantinuum, propiedad de Honeywell, desarrolló Quantum Origin, que proporciona claves criptográficas resistentes a la computación cuántica. Esto sitúa a la empresa a la vanguardia en el desarrollo de soluciones innovadoras para abordar estos desafíos, mejorando aún más el panorama de seguridad para las empresas a medida que afrontan la transición hacia la resistencia cuántica.

Honeywell | LENEL·S2 by Honeywell

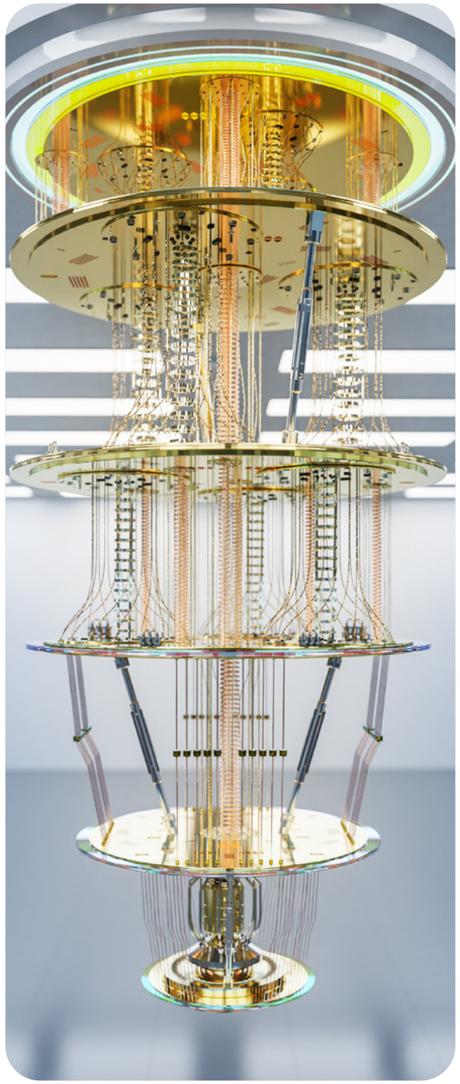
Securitas Technology

Evaluación de la preparación cuántica en todo tu ecosistema

La transición gradual a la computación cuántica afectará a todos los actores de la cadena de suministro de tecnología de seguridad, desde los usuarios finales hasta los proveedores de cuyas tecnologías y servicios dependen. Si bien estos proveedores avanzarán hacia estándares criptográficos resistentes a la computación cuántica en diferentes plazos, los comentarios de nuestros socios tecnológicos estratégicos muestran que el nivel de concienciación es alto. Muchos socios ya están trazando sus propias hojas de ruta, conscientes de que una planificación temprana ayudará a tranquilizar a los usuarios finales, evitará lagunas en la cobertura y garantizará la preparación para adaptarse a medida que se acelera la transición cuántica.

La resistencia cuántica es una de las 5 principales

prioridades de desarrollo para nuestros socios tecnológicos [1]



1. Encuesta y consulta con 26 socios tecnológicos estratégicos de Securitas Technology, que representan a los principales fabricantes, desarrolladores, innovadores y tecnólogos de equipos de seguridad a nivel mundial. Realizada en febrero de 2026.

2. NIST. Criptografía postcuántica. nist.gov/pqc

Integración de consideraciones cuánticas en la planificación del ciclo de vida

La integración del cifrado resistente a la computación cuántica en los ciclos de actualización tecnológica en curso ayudará a que la transición sea más manejable. A medida que los dispositivos llegan al final de su vida útil o los sistemas se someten a actualizaciones importantes, las organizaciones pueden trabajar con sus proveedores de seguridad para introducir reemplazos resistentes a la computación cuántica sin el riesgo de una interrupción importante. Este enfoque gradual distribuye la inversión a lo largo del tiempo y garantiza que las organizaciones permanezcan protegidas a medida que evolucionan los estándares criptográficos.

Mantenerse a la vanguardia de los estándares y el cumplimiento emergentes

Los organismos reguladores y de normalización, como el Instituto Nacional de Estándares y Tecnología (NIST [2]), comparten activamente directrices sobre el cifrado seguro frente a la computación cuántica. El seguimiento de estos avances puede ayudar a las organizaciones a anticipar las necesidades futuras y evitar cambios reactivos de última hora. La adopción temprana de marcos de mejores prácticas demuestra una gobernanza proactiva y fortalece la resiliencia del ecosistema. Mantenerse a la vanguardia de los estándares en constante evolución garantiza que los programas de seguridad sigan preparados a medida que se acerca Y2Q (años para la era cuántica) y las expectativas de cifrado cambian en toda la industria.

Información del socio tecnológico

Garantizar la confianza digital a largo plazo mediante infraestructuras integradas

La seguridad resistente a la computación cuántica es el próximo baluarte de la confianza digital.

Es lógico suponer que los métodos y estándares que utilizamos hoy para proteger los datos digitales no resistirán ni protegerán contra la tecnología superpotente del mañana.

Una de las principales razones de esta percepción es la expectativa de una ruptura definitiva con las normas de cifrado estándar actuales. Para estar preparados para el futuro, es necesario pasar de sistemas de seguridad aislados y rígidos a un ecosistema modular e integrado, diseñado para ofrecer agilidad criptográfica.

Motorola Solutions aborda este cambio unificando tecnologías que antes estaban dispares en un marco de seguridad coherente. Nuestra experiencia en comunicaciones de misión crítica y seguridad de vídeo basada en IA nos permite implementar arquitecturas definidas por software que se pueden actualizar a medida que evolucionan los estándares del Instituto Nacional de Estándares y Tecnología (NIST), evitando así la obsolescencia de la infraestructura.

Nuestra fortaleza reside en la respuesta asistida: Un ecosistema donde la IA aplicada analiza vastos flujos de datos para proporcionar a los operadores humanos información útil para la toma de decisiones. Mediante la integración de análisis de vídeo, control de acceso y software de centro de mando, vamos más allá del cifrado pasivo para adoptar una defensa activa e inteligente.

Esta convergencia garantiza que, a medida que avanzan las amenazas criptográficas, nuestros clientes mantengan una postura sólida mediante flujos de trabajo automatizados y la detección de anomalías en tiempo real.

En definitiva, Motorola Solutions proporciona una base preparada para el futuro donde la conectividad segura y autenticada, junto con las capacidades de respuesta inteligente, garantizan la continuidad operativa en un panorama de amenazas en constante evolución.

MOTOROLA SOLUTIONS

Securitas Technology

> La seguridad física y la ciberseguridad son ahora inseparables. En un ecosistema moderno e interconectado, la protección de la red no es solo una cuestión técnica, sino la base sobre la que se sustenta todo lo demás. Por eso, una buena higiene cibernética ya no es opcional; es la disciplina esencial que mantiene la resiliencia y la fiabilidad de las plataformas de seguridad actuales.

Mike Beattie
Director de Sistemas de Información y Vicepresidente Sénior de Tecnologías de la Información Globales
Securitas Technology



Securitas Technology

Acción para los profesionales de la seguridad





Creación de un ecosistema de seguridad física ciberseguro

01 **Trata los datos de seguridad como un activo crítico**
Revisa cómo funciona el video y el control de acceso. Los registros y la información de los dispositivos se recopilan, almacenan y consultan en toda tu organización. Establece una clara responsabilidad y prácticas de retención coherentes para que cada decisión esté respaldada por datos fiables y bien gestionados.

02 **Estandariza las prácticas de ciberhigiene en toda la organización.**
Aplica prácticas de ciberhigiene coherentes en todos los sitios web y dispositivos. Implemente capacitación periódica, autenticación estricta, segmentación de red y permisos controlados. La estandarización reduce las vulnerabilidades, mejora la resiliencia y garantiza que el ecosistema de seguridad en general siga siendo fiable a medida que crece y se vuelve más interconectado.

03 **Construye procesos que verifiquen la autenticidad**
A medida que el contenido manipulado se vuelve más común, implementa tecnologías y prácticas que evalúen su autenticidad desde el momento de la captura y en etapas posteriores, cuando la información se almacena o se utiliza para tomar acciones. Utiliza transmisiones encriptadas, exportaciones seguras y procedimientos documentados de cadena de custodia para mantener la confianza en los vídeos, los registros y los resultados del sistema.

04 **Identifica datos de larga duración vulnerables a amenazas cuánticas**
Localiza los archivos y los registros de acceso almacenados durante períodos prolongados y evalúa cómo están cifrados y almacenados. Comprende qué sistemas almacenan datos de larga duración y priorízalos para una planificación segura frente a la computación cuántica.
Una evaluación temprana ayuda a las organizaciones a evitar transiciones disruptivas y de alta presión en el futuro.

05 **Alinea esfuerzos con proveedores que estén preparando soluciones de cifrado resistentes a la computación cuántica.**
Colabora con los proveedores para comprender tus planes de trabajo para la seguridad cuántica y sus plazos de encriptación. Selecciona socios con estrategias claras y compromisos con los estándares emergentes. Esto garantiza que tu ecosistema evolucione de forma coherente y evita la fragmentación a medida que las tecnologías resistentes a la computación cuántica se convierten en expectativas del sector.

06 **Construye una gobernanza adaptativa que evolucione con el riesgo**
Revisa periódicamente las políticas que rigen el manejo de datos, el uso de la IA, el control de acceso al sistema y la protección de pruebas. Asegúrate de que los equipos comprendan sus responsabilidades y ten canales claros para escalar problemas. La gobernanza adaptativa mantiene la infraestructura tecnológica alineada con las mejores prácticas y reduce la probabilidad de que nuevas vulnerabilidades pasen desapercibidas.





Securitas Technology

07

Contribuciones destacadas

En esta sección

- Socios tecnológicos destacados
- Securitas destaca

Securitas Technology

Contribuciones destacadas de socios tecnológicos

3xLOGIC™ es un innovador líder y proveedor de hardware, software y soluciones basadas en la nube que impulsan la inteligencia empresarial para clientes de todo el mundo. Las soluciones de 3xLOGIC van más allá de la seguridad para ofrecer un valor empresarial transformador, mediante la extracción de datos y su conversión en información útil, lo que proporciona una mayor visibilidad y una perspectiva novedosa sobre problemas que las empresas ni siquiera sabían que tenían.



Más información

Gestiona tus vídeos de forma más inteligente con 3xLOGIC VIGIL 13

VIGIL 13 de 3xLOGIC es la última versión de software y cámara para su solución de gestión de vídeo, que añade potentes análisis de aprendizaje profundo basados en el dispositivo para mejorar los tiempos de respuesta, el conocimiento de la situación y las investigaciones.

Entre sus características principales se incluyen el reconocimiento automático de matrículas (ANPR), la protección perimetral y contra la intrusión, la compatibilidad con la configuración de análisis remotos y capacidades ampliadas de aprendizaje profundo basado en el borde.

El sistema ANPR captura las matrículas desde una distancia de hasta 18 metros (60 pies) a velocidades de 120 km/h (75 mph), reconociendo la marca, el modelo y el color del vehículo, lo que lo hace ideal para la seguridad, el control de acceso, la gestión de aparcamientos y la automatización del comercio minorista.

Los sistemas de protección perimetral y contra la vagancia detectan comportamientos no autorizados como la vagancia, la intrusión o el vertido ilegal de residuos, y proporcionan alertas en tiempo real para una actuación rápida. Esta solución refuerza las medidas de seguridad y prevención de pérdidas en tiendas de conveniencia, escuelas, comercios minoristas, almacenes y centros de distribución.

VIGIL 13 ofrece alertas en tiempo real, gestión de alarmas personalizable y seguimiento avanzado de objetos, personas y vehículos en el Edge, lo que reduce las necesidades de almacenamiento y ancho de banda. Su configuración flexible de zonas e interacción direccional mejora la identificación y las notificaciones, lo que aumenta la eficiencia del operador.

Sus excepcionales características lo convierten en la opción perfecta para la seguridad empresarial y organizacional, ya que ofrece información valiosa sobre seguridad envuelta en un producto diseñado para ser flexible, intuitivo y rentable.

Ajax Systems es una empresa tecnológica internacional y el mayor fabricante de sistemas de seguridad de Europa, con más de 4,5 millones de usuarios finales y 330.000 usuarios PRO en más de 180 países de todo el mundo. La empresa ofrece soluciones integrales para la protección de hogares y negocios de cualquier tamaño. Hasta la fecha, la cartera de productos de Ajax incluye 280 dispositivos para protección contra intrusiones, videovigilancia, seguridad contra incendios y protección de la vida, así como para confort y automatización.



Más información

Ecosistema de seguridad Ajax para cualquier proyecto

Ajax Systems ofrece un sistema de seguridad integral todo en uno diseñado para proteger instalaciones residenciales, comerciales y de alto riesgo contra robos, incendios y otras amenazas. Al combinar protección contra intrusiones, videovigilancia, seguridad contra incendios y protección de la vida, así como confort y automatización, el sistema se puede adaptar a necesidades específicas y gestionarse a través de una única interfaz.

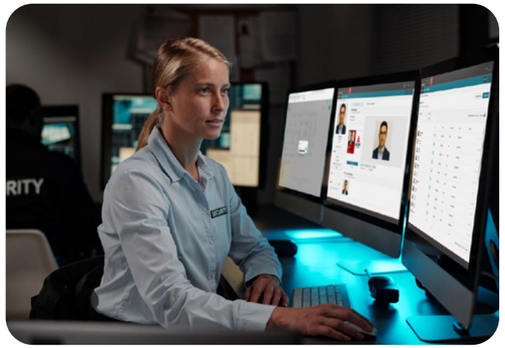
Para la protección contra intrusiones, Ajax ofrece soluciones inalámbricas **Baseline** certificadas según la norma EN 50131 Grado 2, adecuadas para una amplia gama de proyectos. Se ofrecen dispositivos de intrusión **de alta calidad** para instalaciones de alto riesgo, tanto en versiones cableadas como inalámbricas, que proporcionan una mayor resistencia al sabotaje y cumplen con los requisitos de la norma EN 50131 **Grado 3** . Ajax Systems presentó la **primera solución inalámbrica de detección de intrusiones de grado 3 del mundo** , diseñada para una instalación rápida, reduciendo la complejidad del cableado y disminuyendo los costos de mano de obra para los proyectos.

En materia de seguridad contra incendios y protección de la vida, Ajax establece un nuevo referente con su **sistema de detección de incendios totalmente inalámbrico y certificado según la norma EN54** para instalaciones comerciales y municipales. La línea EN54 permite una protección contra incendios fiable sin necesidad de un cableado complejo, mientras que el **concentrador contra incendios EN54 Fire Hub Jeweller** garantiza el control centralizado y la gestión remota. Hub también es compatible con dispositivos de protección contra intrusiones, videovigilancia y automatización que cumplen con la norma EN 50131 Grado 2, lo que lo convierte en una solución unificada. La línea EN54 ofrece una interfaz de aplicación móvil para una experiencia de usuario intuitiva, una gestión de instalaciones más sencilla y un servicio remoto eficiente.

Las soluciones de videovigilancia, disponibles en las líneas de productos **Baseline** y **Superior** , ofrecen opciones escalables con funciones basadas en inteligencia artificial. Los dispositivos ofrecen transmisiones instantáneas y fotos para una verificación rápida, mientras que la integración con el ecosistema Ajax permite escenarios de automatización. Las soluciones de vídeo ofrecen aplicaciones sincronizadas, notificaciones instantáneas y monitorización segura basada en la nube con sólidas protecciones de privacidad.

En AMAG Technology, damos prioridad a la identidad, protegiendo su activo más importante: las personas. Como fabricante global de soluciones de seguridad, ofrecemos la suite de soluciones Symmetry, fiable y escalable, que proporciona un sistema de seguridad integral que se adapta a las necesidades de su programa de seguridad.

Con una mentalidad centrada en el cliente, adoptamos un enfoque de afuera hacia adentro para resolver los desafíos de hoy, anticipándonos a los del mañana: incorporamos resiliencia a nuestros productos y operaciones y ofrecemos soluciones fáciles de usar, eficientes y efectivas. Actuamos como un socio transparente y accesible, comunicándonos de forma proactiva, centrándonos en lo que mejor sabemos hacer e invitando a los clientes a unirse a nosotros en este camino. Finalmente, al fabricar nuestros propios productos y controlar nuestra cadena de suministro, nos mantenemos ágiles, flexibles y confiables para que usted obtenga la capacidad de respuesta que necesita y pueda planificar con confianza para el futuro.



Más información

AMAG Technology anuncia la gestión de identidades Symmetry CONNECT 2.0

Gestiona las identidades en múltiples sistemas de acceso y automatiza los procesos manuales para optimizar las operaciones comerciales.

AMAG Technology™ ha anunciado el lanzamiento de **Symmetry CONNECT 2.0** , una solución de gestión de acceso e identidad física diseñada para empresas que operan con múltiples sistemas de control de acceso mixtos.

Actualmente, las organizaciones rara vez utilizan una única plataforma de acceso. Las fusiones, adquisiciones, la expansión global y las operaciones descentralizadas suelen crear un mosaico de sistemas que pueden ser difíciles de gestionar, aumentar el riesgo y ralentizar la respuesta.

Para hacer frente a esta realidad, AMAG Technology se asoció con **SwiftConnect** , proveedor de la red de acceso conectado para lugares y espacios, para ofrecer un enfoque dinámico para la gestión de identidades en entornos de control de acceso físico dispares.

Symmetry CONNECT 2.0 ayuda a los clientes a unificar una única identidad en múltiples sistemas, preservando la infraestructura existente y minimizando las interrupciones. Los equipos de seguridad pueden gestionar una única identidad y escalarla a través de diferentes edificios e instalaciones, sin necesidad de proyectos de sustitución completa.

CONNECT proporciona una interfaz de usuario moderna y optimizada para gestionar el ciclo de vida completo de la identidad. Desde una única pantalla, los operadores pueden gestionar las credenciales, los derechos de acceso y los roles, la incorporación y la desvinculación de empleados, y las aprobaciones. Las actualizaciones se aplican a todos los sistemas conectados, lo que reduce los errores y mejora la eficiencia.

Symmetry CONNECT se centra en cinco procesos clave: incorporación/desvinculación de empleados, aplicación centralizada de políticas, solicitudes de acceso de autoservicio, experiencia de usuario optimizada y auditoría y cumplimiento, sustituyendo los flujos de trabajo manuales y desconectados que dependen de correos electrónicos, hojas de cálculo, llamadas telefónicas y la memoria institucional.

Aritech es un proveedor global de soluciones inteligentes de detección de intrusiones, vídeo y seguridad integrada, en el que confían profesionales de todo el mundo desde hace casi medio siglo. En el centro de nuestra tecnología se encuentra la inteligencia humana: La experiencia, el compromiso y la presencia sobre el terreno de nuestro personal, que trabaja codo con codo con clientes y socios cada día.

En Aritech, creemos que la fortaleza no proviene de productos aislados, sino de soluciones inteligentes y conectadas. Con una cartera de productos impulsada por la tecnología digital que abarca la detección de intrusiones, la videovigilancia, el control de acceso y las tecnologías integradas, Aritech reúne la seguridad en un potente ecosistema.

En el centro de esta evolución se encuentra la Fusión: Nuestra plataforma digital permite una gestión más inteligente, una mayor visibilidad y una integración perfecta entre sistemas y ubicaciones.

A medida que la seguridad trasciende el hardware y se adentra en entornos IP y celulares conectados, la protección debe ir más allá. Aritech lidera esta transformación con soluciones ciberseguras y escalables diseñadas para los riesgos actuales y los desafíos del futuro.

Estamos preparados para cualquier desafío de seguridad,
En cualquier momento y en cualquier lugar.

Adelante, aceptamos el reto.

Más información



Fusión: Transformando la forma en que se entrega el valor de la seguridad

Fusion es la solución de seguridad unificada de Aritech, que funciona tanto en las instalaciones del cliente como en la nube, y se ofrece a través de un conjunto modular de servicios digitales escalables. Más que una plataforma tecnológica, representa una transformación en la forma en que deben ofrecerse las soluciones de seguridad y en cómo deben generarse valor a largo plazo para los usuarios. En un mercado definido por la complejidad, la fragmentación y el cambio rápido, Fusion desplaza el enfoque de los productos aislados a los ecosistemas integrados y orientados a los servicios.

En organizaciones cada vez más dispersas, las infraestructuras de seguridad fragmentadas crean puntos ciegos operativos, ralentizan los ciclos de toma de decisiones y elevan los costes del ciclo de vida. El cambio hacia plataformas unificadas se ha convertido en una necesidad operativa.

Al unificar la detección de intrusiones, el control de acceso, el vídeo y la conectividad en un entorno modular basado en la nube, Fusion simplifica la gobernanza del sistema al tiempo que permite la escalabilidad en ubicaciones individuales y operaciones globales complejas. Y lo que es más importante, cambia el modelo de entrega: La seguridad ya no es una instalación estática, sino un servicio en constante evolución.

Esta transformación también redefine nuestra forma de trabajar con socios y clientes. La visibilidad centralizada del ciclo de vida, la gobernanza remota del sistema y el control unificado permiten a las organizaciones pasar de una respuesta reactiva a los incidentes a una gestión proactiva de los riesgos. Los responsables de seguridad obtienen visibilidad en toda la empresa, control operativo e inteligencia basada en datos para fundamentar las estrategias de inversión, cumplimiento y resiliencia.

El verdadero valor de Fusion reside en alinear la seguridad con el rendimiento operativo. Al conectar sistemas y habilitar flujos de trabajo automatizados, reduce la complejidad, mejora la resiliencia y transforma los datos de seguridad en información útil que respalda la toma de decisiones estratégicas.

En definitiva, Fusion refleja una evolución más amplia del sector, que va desde el despliegue de hardware hasta la orquestación de servicios, desde las relaciones transaccionales hasta las asociaciones a largo plazo, y desde el suministro de tecnología hasta la creación de valor.

El Grupo ASSA ABLOY es el líder mundial en soluciones de acceso. Cada día, ayudamos a miles de millones de personas a experimentar un mundo más abierto. ASSA ABLOY Opening Solutions lidera el desarrollo de sistemas de apertura de puertas y productos para soluciones de acceso en hogares, empresas e instituciones. Nuestra oferta incluye puertas, herrajes para puertas y ventanas, cerraduras mecánicas e inteligentes, control de acceso y servicio técnico.

ASSA ABLOY Door Security Solutions combina la experiencia de los expertos en apertura de puertas más reconocidos del sector con la amplia gama de productos de las principales marcas de puertas y herrajes para ofrecer soluciones completas a socios y usuarios finales en instalaciones comerciales, minoristas, multifamiliares, gubernamentales e institucionales. Combinando tecnologías innovadoras con un profundo conocimiento de las especificaciones, el diseño, el soporte, la capacitación y el cumplimiento de los códigos, ASSA ABLOY Door Security Solutions trabaja en estrecha colaboración con las comunidades de arquitectos, seguridad, gestión de instalaciones e integradores para abordar los numerosos desafíos que enfrentan al brindar servicio y seguridad a sus clientes.



Más información

Actualiza cualquier sistema de acceso de forma inalámbrica o instala cerraduras inalámbricas desde cero

Los dispositivos inalámbricos Aperio son la forma más sencilla de **ampliar el alcance de su sistema de control de acceso** o de sustituir sus cerraduras mecánicas por un control de acceso inteligente. Gracias a su funcionamiento **inalámbrico y a que funcionan con baterías,** los dispositivos Aperio son rápidos y económicos de instalar, y le permiten ahorrar dinero en costes de funcionamiento y mantenimiento.

La **gama de productos** Aperio incluye cilindros, escudos y cerraduras completas alimentadas por batería para puertas de seguridad. La galardonada manilla Aperio integra una potente funcionalidad de control de acceso en una manilla de puerta de diseño estilizado.

Gracias a que Aperio está **construido con una arquitectura abierta** , la integración perfecta permite controlar cualquier puerta cableada existente y los dispositivos Aperio alimentados por batería desde la misma interfaz de control de acceso.

Control de acceso en más puertas, de forma sencilla y a bajo coste.

Aperio está construido sobre una plataforma abierta para una integración rápida y de bajo coste con su sistema de control de acceso y gestión de seguridad existente, o con uno completamente nuevo. Aperio permite programar los derechos de usuario y generar registros de auditoría instantáneos para más puertas, llevando la gestión de la seguridad al siguiente nivel.

Acceso a la puerta sin llave que le ahorra tiempo y dinero.

La vida es más cómoda cuando se sustituyen las llaves mecánicas por credenciales RFID. Es fácil revocar electrónicamente cualquier credencial extraviada, por lo que no perderá tiempo ni dinero cambiando cerraduras. Aperio funciona con todas las principales tecnologías RFID de baja y alta frecuencia, incluidas las que ya utiliza, y con tecnologías móviles como la comunicación de campo cercano (NFC) y BLE (Bluetooth de baja energía).

Axis permite un mundo más inteligente y seguro al mejorar la seguridad, la protección, la eficiencia operativa y la inteligencia empresarial. Como empresa de tecnología de redes y líder del sector, Axis ofrece soluciones de videovigilancia, control de acceso, intercomunicadores y audio. Estas funcionalidades se ven mejoradas por aplicaciones de análisis inteligente y respaldadas por una formación de alta calidad.

Axis cuenta con alrededor de 5.000 empleados dedicados en más de 50 países y colabora con socios de integración de sistemas y tecnología en todo el mundo para ofrecer soluciones a sus clientes. Axis fue fundada en 1984 y su sede central se encuentra en Lund, Suecia.



Más información

Axis y ARTPEC-9: Avances en vídeo inteligente con AV1

Axis Communications sigue dando forma al futuro del vídeo inteligente con la introducción de la codificación AV1 en cámaras que incorporan su último sistema en chip (SoC), **el ARTPEC-9** . Al ser la primera empresa del sector en integrar AV1 directamente en un sistema en chip diseñado específicamente para vídeo en red, Axis está estableciendo un nuevo referente en eficiencia, rendimiento y escalabilidad de vídeo.

AV1, desarrollado por la Alliance de Open Media, es un códec abierto y libre de regalías diseñado para ofrecer vídeo de alta calidad con tasas de bits significativamente más bajas. En combinación con ARTPEC-9, permite una compresión hasta un 40 % superior a la de H.264 y aproximadamente un 20 % superior a la de H.265, sin sacrificar el detalle de la imagen. Para los clientes, esto se traduce en un menor consumo de ancho de banda, menores costes de almacenamiento y tiempos de retención de vídeo más prolongados.

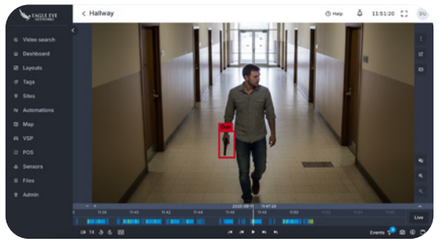
Basado en décadas de experiencia de Axis en procesamiento de imágenes y diseño de sistemas, ARTPEC-9 admite capacidades de transmisión múltiple y mantiene la compatibilidad con H.264, H.265 y MJPEG, lo que garantiza una integración perfecta en los sistemas existentes y prepara a las organizaciones para el futuro. Las mejoras en la eficiencia también hacen que AV1 sea especialmente adecuado para implementaciones híbridas y conectadas a la nube, donde la optimización del ancho de banda y la escalabilidad son esenciales.

Brivo es la empresa innovadora en inteligencia artificial y líder mundial en seguridad física nativa en la nube, con más de 2 millones de dispositivos desplegados en más de 100.000 ubicaciones en 80 países.

El producto estrella, Brivo Security Suite, unifica el control de acceso, la inteligencia de vídeo, la gestión de visitantes y la detección de intrusiones en una única interfaz para centralizar la seguridad en toda la empresa. Las empresas utilizan la plataforma de seguridad unificada con tecnología de IA de Brivo para detectar y prevenir amenazas de forma proactiva, mejorar las operaciones, reducir la responsabilidad, cumplir con las normativas, aumentar las ventas y maximizar los beneficios.

Brivo, pionera en control de acceso nativo en la nube y videovigilancia, cuenta con la confianza de más de 25 millones de usuarios en todo el mundo para proteger a personas, propiedades y activos digitales. Con sede principal en Bethesda, Maryland, y Austin, Texas, Brivo cuenta con oficinas adicionales en Lehi, Utah, Amsterdam, Bangalore y Tokio.

Brivo se fusionó recientemente con Eagle Eye Networks. Visite **brivo.com** para obtener más información sobre el sistema de gestión de vídeo (VMS) Eagle Eye AI y sus capacidades de inteligencia de vídeo basadas en IA.



Más información

Protección proactiva para identificar armas antes de que la amenaza se intensifique

En un mundo donde las armas de fuego están cada vez más presentes, la rapidez con la que se reconoce una amenaza es la delgada línea que separa la seguridad de la tragedia. La mayoría de los delitos relacionados con armas de fuego, como los robos a bancos, terminan en menos de tres minutos. Para alterar esta cronología, la seguridad debe ir más allá del registro de antecedentes y centrarse en la detección de amenazas en el momento en que se blande un arma.

Los sistemas tradicionales a menudo dependen de sensores acústicos que se activan solo *después de* que se efectúa un disparo. **El sistema Brivo Eagle Eye Gun Detection** centra su atención en identificar un arma blandida en el mismo instante en que se desenfunda.

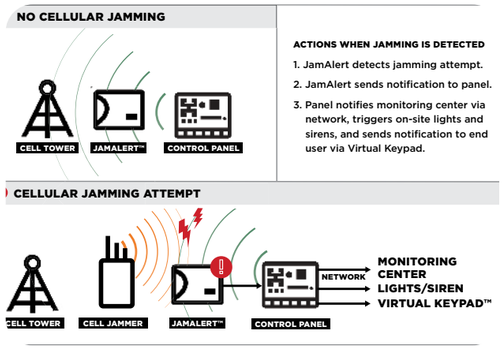
La precisión es fundamental para evitar el caos de las falsas alarmas y el trauma de los confinamientos. Para garantizar la máxima precisión, Brivo diseñó un sistema de verificación de triple capa:

- **Rapid Edge AI:** El sistema Eagle Eye AI Bridge, ubicado en la escuela o el negocio, analiza continuamente los vídeos de seguridad en busca de armas de fuego exhibidas.
- **IA en la nube:** Verificación secundaria mediante un modelo de IA Eagle Eye a gran escala en la nube.
- **Revisión humana:** Verificación experta las 24 horas del día, los 7 días de la semana, para confirmar la amenaza antes de activar su plan de respuesta ante emergencias.

Ya sea en escuelas, hospitales o centros comerciales, una visión más rápida salva vidas. Al combinar inteligencia artificial de vanguardia con supervisión humana, proporcionamos la información instantánea necesaria para cerrar las instalaciones y alertar a los servicios de emergencia.

DMP es un fabricante independiente de propiedad familiar de soluciones de alarma contra intrusiones, incendios, control de acceso, vídeo y telefonía móvil. Los productos DMP están diseñados, desarrollados y fabricados en Estados Unidos con componentes estadounidenses e internacionales. Nuestra fábrica, centro de atención telefónica, departamento de ingeniería y distribución están ubicados en Springfield, Missouri, justo donde comenzó el negocio hace 50 años.





Más información

Detector de interferencias celulares JamAlert™

La amenaza ya no es teórica. Grupos transnacionales de delincuencia sudamericana —que ahora son objeto de advertencias del FBI y alertas emitidas tanto por la NFL como por la NBA— han estado desplegando dispositivos de interferencia de señales como parte de robos coordinados de alta tecnología dirigidos a atletas profesionales y otras personas con alto poder adquisitivo en todo Estados Unidos. Cuando un inhibidor de señal está activo, las señales de alarma de los teléfonos celulares nunca llegan al centro de monitoreo, no se envía a las autoridades y los delincuentes entran sin ser detectados.

Esta no es una preocupación minoritaria. Se trata de un patrón que, según las fuerzas del orden, se observa en casi todos los estados, y el sector de la seguridad comercial en general está tomando nota. Las aseguradoras reconocidas internacionalmente ahora exigen dispositivos de detección de interferencias celulares, específicamente **JamAlert** , como requisito para la cobertura en sectores de alto riesgo, incluidas las instituciones financieras, el comercio minorista de alta gama y las propiedades residenciales de lujo.

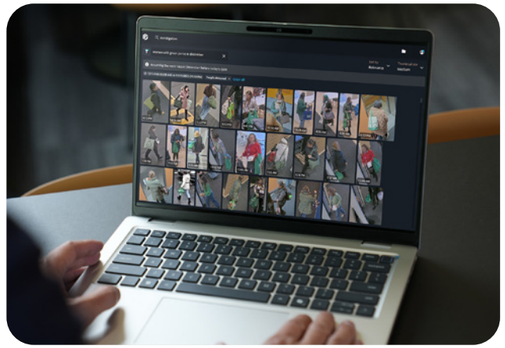
JamAlert aborda la amenaza directamente. El dispositivo monitoriza continuamente las frecuencias celulares y alerta instantáneamente al panel de control en el momento en que se detecta actividad de interferencia, lo que proporciona a los profesionales de la seguridad una ventana de tiempo crucial para responder antes de que se produzca una brecha de seguridad. Es compatible con versiones anteriores y posteriores de los paneles DMP y universalmente compatible con sistemas que no son DMP, lo que lo convierte en un complemento práctico para prácticamente cualquier infraestructura de seguridad existente.

A medida que los grupos de robo organizados se vuelven más sofisticados y las compañías de seguros elevan los estándares de protección requeridos, la pregunta ya no es si la detección de interferencias celulares debe formar parte de un sistema de seguridad, sino si uno puede permitirse el lujo de prescindir de ella.

Genetec Inc. es una empresa tecnológica global que lleva más de 25 años transformando el sector de la seguridad física. La cartera de soluciones de la compañía permite a empresas, gobiernos y comunidades de todo el mundo proteger a las personas y los activos, al tiempo que mejora la eficiencia operativa y respeta la privacidad individual.

Genetec ofrece los productos líderes a nivel mundial para la gestión de vídeo, el control de acceso y el reconocimiento automático de matrículas (ALPR), todos ellos basados en una arquitectura abierta y diseñados con la ciberseguridad como pilar fundamental. La cartera de productos de la empresa también incluye soluciones de detección de intrusiones, intercomunicadores y gestión de pruebas digitales.

Con sede en Montreal, Canadá, Genetec presta sus servicios a más de 42.500 clientes a través de una extensa red de socios de canal y consultores acreditados en más de 159 países.



Más información

Nuevas capacidades de investigación en Genetec™ Security Center SaaS

Las nuevas capacidades de investigación de **Security Center SaaS** ayudan a los equipos de seguridad a realizar investigaciones más rápidas y efectivas en entornos grandes y distribuidos. Diseñada para adaptarse al desarrollo de las investigaciones, la solución permite a los operadores comenzar con información limitada y localizar rápidamente las grabaciones relevantes en múltiples ubicaciones y cámaras.

Los profesionales de la seguridad pueden aprovechar las capacidades de búsqueda inteligente para obtener la información más relevante, como la detección de personas o objetos similares que entran o salen de las escenas. Los operadores pueden visualizar el movimiento de un sospechoso o vehículo a través de diferentes ubicaciones, creando una visión completa del incidente mediante el uso de trayectorias para reconstruir rápidamente las conexiones sin tener que revisar horas de vídeo.

A medida que avanzan los casos, las pruebas se organizan automáticamente en una narración clara y cronológica, lo que facilita la validación de los hallazgos, la documentación de las secuencias de eventos, el intercambio de resultados y el cierre eficiente de los casos.

Hanwha Vision ayuda a las organizaciones a obtener más seguridad, gestionar menos y operar de forma más inteligente. Al ofrecer constantemente innovaciones en videovigilancia que combinan protección las 24 horas del día, los 7 días de la semana, inteligencia artificial y plataformas basadas en la nube, ayudamos a mejorar la experiencia de seguridad y a transformar las operaciones generales de una organización.

Nuestro ecosistema híbrido y en la nube, impulsado por OnCloud VSaaS directo a la nube y OnCAFE control de acceso nativo en la nube, simplifica la seguridad al tiempo que proporciona mayor visibilidad y control. Integrado con análisis de IA, cámaras IP, dispositivos de almacenamiento, software de gestión de vídeo y grabadoras, codificadores/decodificadores, monitores y accesorios, e inteligencia empresarial, Hanwha Vision convierte los sistemas de seguridad en información útil que mejora la seguridad, la eficiencia y la toma de decisiones en toda la organización.

Las tecnologías de Hanwha Vision satisfacen todas las necesidades de cualquier aplicación de vigilancia: comercio minorista, transporte, educación, servicios financieros, atención médica, hostelería, aeropuertos, instalaciones deportivas y agencias gubernamentales. Nuestra visión es optimizar la gestión de la seguridad proporcionando una protección de vigilancia potente, inteligente y escalable.



Más información

Opciones de vigilancia... a tu medida.

Las tecnologías de Hanwha Vision conforman un ecosistema conectado, lo que permite a los clientes elegir la arquitectura que mejor se adapte a sus necesidades, presupuestos y planes futuros. Un ejemplo perfecto es nuestro ecosistema de soluciones de vigilancia basadas en la nube:

- **OnCloud** , nuestra plataforma completa de software de gestión de vídeo como servicio (VSaaS) con conexión directa a la nube, optimiza las operaciones de vigilancia con una experiencia de usuario potente y flexible, combinando la velocidad y la escalabilidad de la nube con las ventajas de la grabación en el borde y el análisis mediante IA.
- **OnCAFE** , nuestro sistema de control de acceso nativo en la nube que integra a la perfección la videovigilancia y el control de acceso. OnCAFE unifica las herramientas de seguridad, vigilancia y gestión de instalaciones para los usuarios desde una única fuente. La capacidad de conectar vídeo, acceso, alarmas y mucho más, todo bajo la misma arquitectura, ofrece simplicidad operativa y una mayor conciencia situacional.

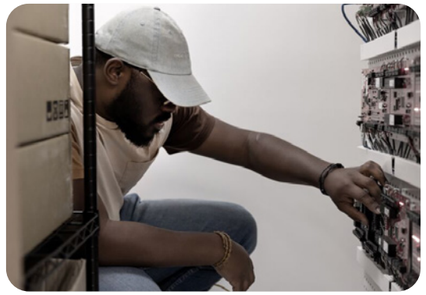
Al combinar OnCAFE con la gestión de vídeo OnCloud, los integradores y los usuarios finales obtienen un panel de control centralizado. OnCAFE y OnCloud ofrecen todas las características de los sistemas tradicionales locales, además de escalabilidad, facilidad de uso y control de acceso y vídeo integrados en una única plataforma. En lugar de largas instalaciones de servidores y licencias complejas, la configuración es tan sencilla como registrar los dispositivos en la nube.

Cada una de ellas es potente por sí sola, pero juntas ofrecen a los clientes una flexibilidad de gestión completa y transparente sobre sus sistemas de vigilancia. Tanto OnCAFE (control de acceso) como OnCloud (gestión de vídeo) funcionan en la plataforma unificada en la nube de Hanwa Vision, con un conjunto común de credenciales y una integración perfecta entre el vídeo y el control de acceso.

HID Global impulsa las identidades confiables de las personas, los lugares y las cosas del mundo. Hacemos posible que las personas realicen transacciones de forma segura, trabajen de manera productiva y viajen libremente. Nuestras soluciones de identidad de confianza brindan a las personas un acceso cómodo a espacios físicos y digitales, y conectan elementos que pueden identificarse, verificarse y rastrearse digitalmente.

Millones de personas en todo el mundo utilizan productos y servicios HID para desenvolverse en su vida cotidiana, y más de 2.000 millones de objetos están conectados a través de la tecnología HID. Trabajamos con gobiernos, instituciones educativas, hospitales, instituciones financieras, empresas industriales y algunas de las compañías más innovadoras del planeta.

Con sede en Austin, Texas, HID Global cuenta con más de 3.000 empleados en todo el mundo y opera oficinas internacionales que dan soporte a más de 100 países. HID Global ® es una marca del Grupo ASSA ABLOY.



Más información

Mercury está diseñado para un crecimiento seguro

La aplicación integrada **de Mercury** amplía las funcionalidades de los controladores de acceso. La plataforma, ahora disponible comercialmente, amplía la arquitectura abierta de Mercury al permitir que las aplicaciones aprobadas se ejecuten directamente en el extremo de la red. Al integrar la lógica empresarial y las integraciones en el propio controlador, las organizaciones pueden acelerar la innovación, reforzar la seguridad y escalar la funcionalidad sin necesidad de rediseñar su infraestructura principal.

Los controladores diseñados según estándares abiertos permiten a los socios integrarse de forma más eficiente, al tiempo que ofrecen a los usuarios finales la flexibilidad necesaria para adaptarse con el tiempo. A medida que evolucionan los requisitos normativos y se amplían las necesidades de integración, el entorno de las aplicaciones admite una modernización por fases en lugar de una sustitución completa.

Contamos con una comunidad cada vez mayor de fabricantes de equipos originales (OEM) y desarrolladores que crean proyectos sobre la plataforma de Mercury. Al proporcionar un entorno seguro y abierto en el controlador, Mercury permite a sus socios crear nuevas capacidades que operan directamente en el extremo de la red.

La innovación ya no se limita a los sistemas iniciales. Ahora, las aplicaciones pueden mejorar la integración, el análisis y la orquestación dentro del propio controlador. Este enfoque de ecosistema permite a los socios diferenciar sus ofertas al tiempo que aportan valor añadido a los usuarios finales.

Con el apoyo de un programa estructurado para desarrolladores, los socios tecnológicos siguen un proceso de incorporación de cuatro pasos que incluye la presentación de propuestas, la colaboración con Mercury en la evaluación técnica, el acceso a las herramientas de desarrollo y la realización de una revisión de seguridad antes de la distribución. Este marco garantiza que las aplicaciones cumplan con las expectativas de rendimiento y ciberseguridad, al tiempo que ayuda a los socios a lanzar soluciones al mercado con mayor rapidez.

Con más de 30 años de experiencia y un firme compromiso con la arquitectura abierta, Mercury ha creado una plataforma preparada para el futuro que garantiza una interoperabilidad perfecta entre las principales soluciones técnicas y de software. Mercury cuenta con más de 5 millones de controladores instalados en todo el mundo.

La división de Soluciones de Seguridad y Acceso (SAS) de Honeywell ahora incluye LenelS2 junto con el grupo de Seguridad Comercial de Honeywell. LenelS2 continúa siendo un líder mundial reconocido en el suministro de soluciones avanzadas de seguridad física, que incluyen control de acceso, videovigilancia y credenciales móviles.

La combinación de LenelS2 y Commercial Security eleva aún más las soluciones de gestión de seguridad unificadas, escalables y completas de Honeywell para clientes que van desde empresas globales hasta pequeñas y medianas empresas.

Los operadores de instalaciones y los equipos de seguridad en sectores verticales en constante evolución eligen y confían en las tecnologías móviles y en la nube de Honeywell para obtener soluciones de control de acceso, detección de intrusiones y videovigilancia que les ayudan a crear instalaciones más seguras y eficientes en todo el mundo.



Más información

Integración impulsada por IA para empresas globales

¿Cómo será el Centro de Operaciones de Seguridad (SOC) del futuro? Respuesta ante incidentes mucho más rápida y precisa, menor coste de propiedad y operación, detección acelerada de amenazas, conocimiento de la situación en tiempo real y flujos de trabajo optimizados, todo ello gestionado eficazmente en diversos sistemas y ubicaciones geográficamente dispersas.

La seguridad empresarial necesita transformarse para poder hacer frente a las amenazas en constante evolución. Las configuraciones SOC tradicionales deben volverse más integradas y ágiles. Si bien la industria está ofreciendo innovaciones nuevas y fascinantes gracias a la IA, la nube y las tecnologías móviles, la sustitución completa de los sistemas no es realista debido al coste, el tiempo y el riesgo que implica.

El ciclo típico de ideación, construcción y lanzamiento para sistemas de seguridad complejos a nivel empresarial generalmente solo ofrece avances incrementales a lo largo del tiempo. La clave para lograr una transformación significativa, y no solo una mejora incremental, de manera que se reduzca el riesgo, se maximice el tiempo de actividad y se equilibre el coste total, reside en integrar las capacidades de SOC de próxima generación en las plataformas existentes.

Los usuarios finales necesitan una forma de incorporar innovaciones orientadas al futuro sin tener que reemplazar por completo sus sistemas existentes, que, a nivel empresarial, suelen ser configuraciones personalizadas y perfeccionadas, diseñadas a lo largo de muchos años y con una inversión significativa para satisfacer con precisión las necesidades de la organización. Los clientes no deberían tener que elegir entre innovación y fiabilidad; deberían poder realizar sus actualizaciones a su propio ritmo y obtener los beneficios operativos de las nuevas tecnologías de forma más eficiente y con menos riesgo.

Gracias a su alcance y a su potente cartera de tecnologías de seguridad, IoT e IA, Honeywell, incluidas las plataformas LenelS2 y Forge, está en una posición privilegiada para ofrecer innovación con visión de futuro pero a la vez sólida, a gran escala. Al incorporar capacidades de automatización a plataformas existentes y probadas como **LenelS2 OnGuard** , y al aplicar agentes de IA y aprendizaje automático que tienen en cuenta el contexto, Honeywell ayuda a las empresas de todos los sectores a afrontar las complejidades del panorama de amenazas del futuro, al tiempo que controla los costes y mejora los resultados generales de seguridad.

IDIS Americas, con sede en Coppell, Texas, ofrece una cartera integral de soluciones de vídeo avanzadas y tecnologías basadas en inteligencia artificial para diversas aplicaciones de videovigilancia. Nuestra cartera de productos incluye software de gestión de vídeo (VMS), cámaras de vigilancia, grabadoras de vídeo en red (NVR), análisis avanzados (AA), soluciones en la nube y mucho más, ofreciendo soluciones a medida para las necesidades de nuestros clientes.

IDIS Americas aprovecha las fortalezas y la experiencia combinadas de las empresas Costar e IDIS para ofrecer una selección más amplia de productos, una mayor innovación tecnológica y un nivel de servicio aún más alto que nunca. IDIS Americas diseña, desarrolla y distribuye soluciones de videovigilancia y seguridad con productos de alto rendimiento para satisfacer las necesidades cambiantes del cliente.

Nuestra misión es convertirnos en un socio líder de referencia a través de productos de calidad, precios competitivos y un servicio al cliente inigualable. Descubra IDIS Americas y vea cómo puede marcar la diferencia en su negocio.



Más información

Más inteligentes, más rápidos, más agudos: Las nuevas cámaras IDIS Edge AI lideran el futuro de la vigilancia

La **gama de cámaras IDIS Edge AI Plus de última generación** representa un gran avance en la videovigilancia inteligente, al combinar análisis avanzados de aprendizaje profundo con un rendimiento de imagen excepcional. Diseñadas para ofrecer a las organizaciones vías flexibles y asequibles para modernizar sus sistemas de seguridad, estas cámaras brindan potentes capacidades de IA en el dispositivo, que incluyen **detección de multitudes, detección de objetos abandonados y retirados, detección de caídas y detección de violencia** , todo ello impulsado por el **motor de análisis IDLA Pro** mejorado.

Diseñada para un rendimiento óptimo en condiciones reales, la gama incluye **cámaras domo y tipo bala de 8 MP resistentes al vandalismo y aptas para exteriores** , así como **unidades PTZ de última generación** que ofrecen **zoom óptico de 40x, seguimiento automático mediante IA y visión nocturna de hasta 400 metros** . Estos modelos PTZ ofrecen una cobertura de escena sin precedentes y son ideales para la monitorización de grandes áreas en infraestructuras críticas, espacios públicos, transporte y grandes emplazamientos comerciales.

La innovadora **tecnología A Cut** de IDIS recorta y extrae automáticamente las imágenes más relevantes de los objetos detectados, lo que permite a los operadores identificar rápidamente personas o vehículos y acceder directamente a los momentos clave del vídeo grabado. En combinación con **la búsqueda por IA de IDIS** , los usuarios pueden filtrar las grabaciones por atributos detallados como **el género, el grupo de edad, el color de la ropa, el tipo de vehículo o los accesorios** , lo que reduce drásticamente el tiempo de investigación y mejora el conocimiento de la situación.

Las cámaras Edge AI Plus, basadas en **IDIS DirectIP** , ofrecen una implementación plug and play, configuración con un solo clic, ciberseguridad multicapa y **cero tarifas de licencia** , lo que garantiza un costo total de propiedad líder en la industria. Gracias a una claridad de imagen superior, impulsada por infrarrojos, WDR y un gran **sensor de 1/1,8”** , la nueva generación de IA de borde permite a los equipos de seguridad actuar con mayor rapidez, inteligencia y proactividad que nunca.

Intellicene ha redefinido la seguridad física con un enfoque basado en la inteligencia que va más allá de las operaciones de seguridad tradicionales. Nuestra misión es ayudarle a proteger a su personal, sus bienes y sus operaciones vitales, con la inteligencia como eje central de todo ello. Nuestra plataforma conecta y unifica diversas tecnologías, proporcionando información práctica que mejora la seguridad, optimiza las operaciones e impulsa decisiones empresariales más inteligentes.

Desde aplicaciones móviles y análisis basados en inteligencia artificial hasta software infinitamente escalable y dispositivos inteligentes, estamos creando tecnología avanzada que eleva el nivel y hace que el mundo sea más seguro. Intellicene le permite gestionar de forma eficiente las operaciones comerciales y de seguridad más complejas. Unificamos la seguridad, posibilitamos la acción y le proporcionamos la información necesaria para protegerse.



Más información

Presentamos Intellicene Insight

Información de Intellicene Transforma los sistemas de videovigilancia tradicionales en plataformas de seguridad inteligentes basadas en eventos que ven, comprenden e interpretan la actividad en tiempo real. En realidad, los operadores solo pueden vigilar de forma fiable un número limitado de cámaras a la vez antes de que la precisión disminuya drásticamente.

Insight utiliza inteligencia artificial avanzada para mejorar drásticamente la precisión de la detección, eliminando el ruido. Gracias a la detección de anomalías en tiempo real, el análisis del comportamiento y la IA contextual impulsada por su modelo de lenguaje visual propio, Insight identifica las desviaciones de la actividad normal sin depender únicamente de reglas manuales, lo que permite una respuesta más rápida y una toma de decisiones más segura.

Diseñado para ofrecer escalabilidad y flexibilidad, Insight admite la monitorización de hasta 800 cámaras por estación de trabajo, con mejoras significativas en el rendimiento de detección. Ofrece más de 100 clases de objetos, reconocimiento de poses, búsqueda forense, seguimiento multicámara y compatibilidad con detección de intrusiones, detección de armas y peleas, alertas de incendios y humo, cumplimiento de normativas sobre EPI, análisis de tráfico y mucho más. Diseñado para su implementación en el borde de la red, híbrida o centralizada, Insight se integra a la perfección con las cámaras existentes y las plataformas Intellicene, lo que lo convierte en una solución eficiente en cuanto a hardware y lista para la empresa que responde a los desafíos modernos de seguridad, protección y operaciones.

IQSIGHT

Anteriormente conocida como Bosch Video Systems, IQSIGHT cuenta con más de 60 años de experiencia en ingeniería. IQSIGHT ofrece seguridad de vídeo basada en inteligencia que ayuda a las organizaciones a ver con claridad, comprender el contexto en tiempo real y actuar con confianza, transformando el vídeo en información útil para que los líderes puedan tomar mejores decisiones con mayor rapidez.

IQSIGHT ofrece una cartera probada de soluciones de vídeo que cumplen con las normativas NDAA y TAA, incluidas las cámaras FLEXIDOME, AUTODOME y MIC, respaldadas por más de 600 patentes y diseñadas para funcionar de forma fiable a largo plazo.



Más información

Videovigilancia basada en la inteligencia

La IA está transformando la seguridad por vídeo, pasando de la vigilancia tradicional a la inteligencia visual, lo que permite a las organizaciones reconocer patrones y anticipar lo que pueda suceder a continuación. Con previsión, pueden detectar los riesgos antes, tomar decisiones más rápidas y operar con mayor confianza para abordar los problemas antes de que se agraven.

La inteligencia en el extremo de la red permite que las cámaras actúen como sensores, alertando sobre situaciones como intrusiones en el perímetro, exhibición de armas, falta de equipos de protección personal (EPP), entre otras. Los análisis específicos para cada aplicación utilizan algoritmos entrenados para entornos definidos con el fin de proporcionar detecciones fiables y precisas, minimizando al mismo tiempo los falsos positivos.

Para sitios críticos, la incorporación de la verificación de alarmas mediante IA basada en la nube añade un segundo par de ojos para comprobar las alertas dudosas. Al igual que la repetición instantánea en los deportes, la detección basada en los bordes toma la decisión en el campo y envía un breve videoclip a la nube para su revisión. La verificación de alarmas mediante IA confirma una amenaza potencial o anula la llamada; además, anula o intensifica rápidamente las alarmas para reducir aún más los falsos positivos y ayudar a prevenir la fatiga por alarmas.

Una alta precisión de detección también es esencial cuando las cámaras se integran con otros sistemas, lo que permite que las alarmas activen acciones automatizadas. Las cámaras inteligentes pueden publicar temas de transporte de telemetría de cola de mensajes (MQTT), como eventos activados por el motor de reglas de la cámara, valores de conteo y más. La compatibilidad con MQTT facilita la conexión con software de terceros para aprovechar al máximo los eventos analíticos y ampliar los usos de los dispositivos periféricos con IA más allá de la seguridad.

Si bien la seguridad seguirá siendo fundamental, la inteligencia visual desempeñará un papel cada vez más importante en la expansión del vídeo a usos operativos en numerosos entornos.

MARCH networks
A Delta Group Company

March Networks ofrece soluciones de vídeo inteligentes, seguras y basadas en la nube, diseñadas para mejorar la seguridad, mitigar los riesgos y optimizar la eficiencia operativa. Nuestros sistemas de análisis basados en inteligencia artificial se integran con el control de acceso, las alarmas, los sistemas de punto de venta y los cajeros automáticos para ir más allá de la vigilancia tradicional, ofreciendo información en tiempo real que ayuda a las empresas a prevenir el fraude, detectar amenazas y optimizar el rendimiento.

Con décadas de experiencia y alcance global, somos un socio de confianza para organizaciones preocupadas por la seguridad en todo el mundo, incluidas más de 1500 instituciones financieras, más de 600 minoristas y más de 900 empresas comerciales e industriales en más de 75 países.

Gracias al respaldo de nuestra red de socios certificados, March Networks puede diseñar y ofrecer soluciones de videovigilancia personalizadas, adaptadas a las necesidades operativas y de seguridad únicas de los clientes de Securitas, garantizando el máximo nivel de protección y la continuidad del negocio.



Más información

Almacenamiento en la nube a largo plazo de March Networks

Almacenamiento en la nube a largo plazo de March Networks Ofrece una solución de retención de vídeo segura, escalable y rentable, basada en la infraestructura de Amazon Web Services (AWS). Mediante un modelo de almacenamiento flexible y por niveles, impulsado por Amazon S3 Glacier, las organizaciones pueden archivar vídeos de vigilancia durante años sin necesidad de ampliar su hardware local ni aumentar la complejidad de sus sistemas informáticos.

Diseñado para empresas con estrictos requisitos de cumplimiento y retención de datos, este servicio ayuda a las empresas a reducir los costes de almacenamiento a largo plazo hasta en un 80 %, manteniendo al mismo tiempo altos niveles de durabilidad, resistencia y seguridad. El vídeo se cifra y protege automáticamente dentro de la arquitectura de nube altamente robusta de AWS, lo que garantiza la preservación fiable de pruebas críticas y grabaciones operativas.

March Networks Cloud Storage se integra directamente con la plataforma de gestión de vídeo de March Networks, lo que permite a las organizaciones gestionar el vídeo archivado y el almacenado en sus propias instalaciones desde una única interfaz. Los clientes pueden conservar los vídeos recientes en grabadoras locales para realizar investigaciones rápidas, al tiempo que archivan sin problemas las grabaciones más antiguas en la nube. Los vídeos archivados pueden buscarse, recuperarse y exportarse cuando sea necesario sin interrumpir las operaciones diarias.

Este enfoque híbrido proporciona la flexibilidad necesaria para ampliar el almacenamiento a medida que aumentan los volúmenes de vídeo en múltiples ubicaciones. Además, elimina la necesidad de grandes ampliaciones de almacenamiento local, simplifica la gestión de TI y ayuda a las organizaciones a mantener políticas de retención de vídeo a largo plazo, al tiempo que mantiene predecibles los costes de infraestructura.

Milestone Systems es líder mundial en tecnología de vídeo basada en datos, utilizada en sectores tan diversos como la fabricación, los aeropuertos, las fuerzas del orden, el comercio minorista y la gestión del tráfico. Ofrecemos una visión clara de cómo crear un mundo más seguro, mejor y más próspero.

Nuestra suite de productos incluye el software de gestión de vídeo XProtect, el análisis basado en IA BriefCam y la plataforma VSaaS en la nube Arcules. Ayuda a nuestros clientes a aprender del pasado, comprender el presente y predecir el futuro.

Milestone también está impulsando la IA de visión responsable a través del Proyecto Hafnia, la biblioteca de datos de vídeo que cumple con la normativa más grande del mundo, y la tecnología de anonimización BrighterAI.

Fundada en 1998 y con sede en Copenhague, Milestone emplea a más de 1.500 personas en todo el mundo y es una empresa independiente dentro del Grupo Canon desde 2014.



Más información

Vídeo inteligente, diseñado de forma responsable

Milestone Systems está impulsando la tecnología de vídeo con tres nuevas funcionalidades basadas en inteligencia artificial, diseñadas para ayudar a los operadores a trabajar más rápido, investigar de forma más inteligente y cumplir con la normativa.

Resumen de vídeo de XProtect Utiliza un modelo de visión-lenguaje (VLM) para resumir e interpretar automáticamente el contenido de vídeo. Desarrollado con tecnología NVIDIA y perfeccionado con más de 75 000 horas de datos de vídeo reales, obtenidos de forma ética del Proyecto Hafnia, el VLM permite a los operadores enviar clips directamente desde el XProtect Smart Client y recibir resúmenes de texto estructurados, lo que facilita la evaluación de situaciones urgentes, reduce las falsas alarmas y estandariza la documentación de incidentes.

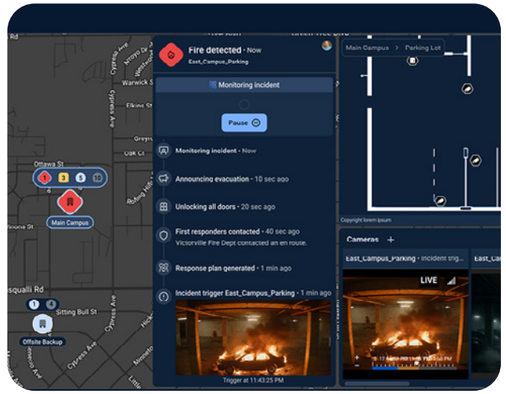
La anonimización de vídeo, con tecnología de BrighterAI , incorpora la protección automatizada de la privacidad directamente en los flujos de trabajo de vídeo de Milestone. Con tan solo unos clics, los usuarios pueden eliminar rostros, matrículas y cuerpos de los vídeos, garantizando así el cumplimiento del RGPD, la Ley de IA de la UE y otras normativas mundiales de privacidad antes de compartir las grabaciones con terceros.

La búsqueda mediante IA introduce la búsqueda en lenguaje natural en toda la gama de productos de Milestone, lo que permite a los operadores encontrar momentos de vídeo relevantes simplemente describiendo lo que buscan, sin necesidad de búsqueda manual ni filtros complejos. Es una forma más rápida e intuitiva de encontrar lo que importa en las grabaciones de vídeo.

En conjunto, estas capacidades representan una nueva generación de inteligencia de vídeo responsable e impulsada por IA, basada en los más de 25 años de confianza de Milestone como la plataforma VMS más abierta del sector.

La seguridad es la base de todo lo que hacemos en Motorola Solutions. Desarrollamos y conectamos tecnologías para ayudar a proteger a las personas, la propiedad y los lugares. Nuestras soluciones fomentan la colaboración, que es fundamental para lograr comunidades más seguras, escuelas más seguras, hospitales más seguros, empresas más seguras y, en última instancia, naciones más seguras.

Escanee el código QR a continuación para visitar nuestro sitio web y obtener más información sobre nuestro compromiso con la innovación para un futuro más seguro para todos.



Más información

Operador: Resiliencia empresarial mediante orquestación inteligente

Operador Revoluciona los centros de operaciones de seguridad con automatización impulsada por IA. Esta plataforma nativa de la nube clasifica proactivamente las amenazas, minimiza los falsos positivos y automatiza las respuestas, ahorrando tiempo y esfuerzo y reduciendo los tiempos de respuesta. Operator actúa como un multiplicador de fuerza para los profesionales de la seguridad al sintetizar datos de sistemas de video, control de acceso, sensores y radio en una única vista práctica. Utiliza la agrupación de eventos para filtrar el ruido, identificando el incidente principal entre cientos de señales dispares. Su agente de respuesta automatiza los planes de respuesta, como cerrar puertas o notificar a los servicios de emergencia, transformando así las operaciones de seguridad en una defensa proactiva e inteligente.

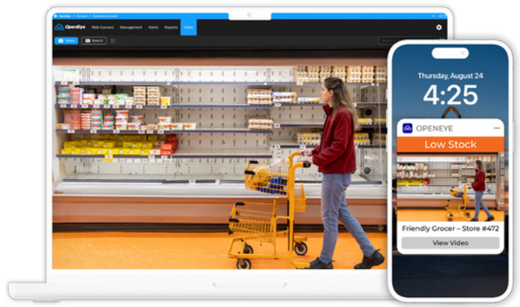
Sus características y capacidades habilitadas por IA incluyen:

- **Clasificación de eventos:** Verifica y combina automáticamente las señales para filtrar el ruido de las falsas alarmas, ofreciendo una visión clara de solo las amenazas de alta gravedad.
- **Planificación de respuesta dinámica:** Genera planes de respuesta en tiempo real, paso a paso, que guían a los operadores con confianza a través de desafíos nuevos o complejos.
- **Interfaz operativa unificada:** Proporciona una interfaz única e intuitiva para la visibilidad en tiempo real de vídeo, control de acceso y radios, eliminando la necesidad de alternar entre múltiples aplicaciones.
- **Ejecución automatizada:** Ejecuta manuales de procedimientos predefinidos para garantizar una contención y acción rápidas y consistentes, actuando como operador de seguridad digital junto con el personal de recursos humanos.

Para descubrir cómo Operator puede revolucionar sus operaciones de seguridad, visite la página oficial del producto en **motorolasolutions.com/inform** o explore el portal de documentación del operador.

Con sede en Liberty Lake, Washington, OpenEye es un proveedor líder de soluciones inteligentes en la nube para seguridad de vídeo, inteligencia empresarial y prevención de pérdidas. Nuestros productos, fáciles de usar, están diseñados para ayudar a los clientes a optimizar sus operaciones y reducir la carga de trabajo del departamento de TI, facilitando la gestión de implementaciones e integraciones de videovigilancia de todos los tamaños con un enfoque proactivo.

OpenEye es una subsidiaria de Alarm.com (Nasdaq: ALARM). Con más de 2000 empleados y más de 900 miembros en nuestro equipo de I+D en Norteamérica, ofrecemos servicios a millones de ubicaciones con soluciones de vídeo, control de acceso y detección de intrusiones basadas en la nube que hacen que las propiedades sean más inteligentes y seguras.



Más información

Búsqueda y alertas con tecnología de IA en los servicios web de OpenEye

OpenEye continúa expandiendo OpenEye Web Services (OWS) con **AI Visual Search** y **AI Visual Check** , dos funcionalidades basadas en inteligencia artificial diseñadas para ayudar a los equipos a localizar momentos clave más rápidamente y mantenerse informados sin necesidad de una revisión manual constante.

La búsqueda visual mediante IA ayuda a los usuarios a localizar los momentos más importantes. En lugar de revisar manualmente horas de grabaciones o dedicar tiempo a configurar filtros de búsqueda, los usuarios pueden simplemente describir lo que buscan, como por ejemplo "una persona que llevaba una caja en el vestíbulo ayer por la tarde", y recibir rápidamente resultados relevantes. AI combinar análisis avanzados e inteligencia en la nube, la búsqueda visual con IA convierte la revisión de vídeos complejos en una experiencia rápida e intuitiva que cualquier usuario puede dominar. AI eliminar el tiempo de revisión manual y proporcionar información clara y práctica, permite a los equipos tomar decisiones más rápidas y seguras al verificar eventos de seguridad, realizar un seguimiento de las tendencias operativas o descubrir momentos clave.

AI Visual Check permite a los equipos trabajar de forma más inteligente gracias a la verificación visual basada en inteligencia artificial. En lugar de vigilar constantemente los vídeos o realizar inspecciones rutinarias, OWS evalúa las imágenes de las cámaras en nombre de los usuarios y solo les avisa cuando algo requiere atención. Las organizaciones definen lo que más importa, como un vestíbulo limpio, estantes surtidos o puntos de acceso seguros, y AI Visual Check valida continuamente esas condiciones. Cada alerta incluye un contexto claro, resúmenes breves generados por IA e imágenes de referencia que facilitan la comprensión de lo sucedido y permiten actuar con rapidez. AI automatizar la verificación visual rutinaria, los equipos ahorran tiempo, reducen las alertas innecesarias y obtienen información más valiosa en todas las ubicaciones sin necesidad de estar continuamente sentados frente a una pantalla.

Con más de 40 años de éxito a nivel mundial, PACOM destaca por integrar a la perfección soluciones de hardware y software para lograr una seguridad fiable y la excelencia empresarial. Como expertos en integración de seguridad, ofrecemos soluciones modulares y rentables con control de acceso multinivel, fiabilidad propia e integración perfecta con terceros a través de una API abierta.



Más información

Solución PACOM VIGIL CORE para cajeros automáticos con inteligencia de sensores remotos

Los cajeros automáticos están en lugares remotos, sin vigilancia y son vulnerables. Cuando un cajero automático es atacado, trasladado o robado, el impacto va más allá del simple robo. Puede provocar interrupciones en el servicio, riesgos regulatorios y costosas respuestas de emergencia. La seguridad tradicional de los cajeros automáticos suele basarse en alarmas fragmentadas que reaccionan demasiado tarde. **PACOM VIGIL CORE** aborda este desafío al transformar la protección de cajeros automáticos, pasando de alertas reactivas a una inteligencia proactiva basada en sensores que ayuda a los equipos a detectar riesgos con anticipación y actuar con mayor rapidez.

PACOM VIGIL CORE mejora la seguridad de los cajeros automáticos mediante un sistema de monitorización integrado y sensores remotos inteligentes. El sensor monitoriza la luz ambiental, la temperatura, la humedad, las vibraciones, el movimiento y la actividad de la puerta, identificando condiciones anormales que pueden indicar manipulación, entrada forzada o riesgo ambiental. Si se retira físicamente un cajero automático, VIGIL CORE también puede rastrear su ubicación, lo que facilita una recuperación e investigación más rápidas. Los umbrales de alarma se pueden configurar y ajustar de forma remota, lo que permite un control centralizado sin necesidad de visitas frecuentes al sitio.

Los datos de los sensores se gestionan a través de la plataforma VIGIL CORE, lo que proporciona a los operadores una visión unificada de las alarmas, los diagnósticos y el estado de las instalaciones en un cajero automático o en toda la red. Para facilitar la verificación rápida, VIGIL CORE integra una minicámara OSDP que captura instantáneas basadas en eventos vinculados a alarmas y actividad de sensores. Esto permite a los operadores confirmar incidentes rápidamente, reducir las falsas alarmas y enviar personal de respuesta con confianza.

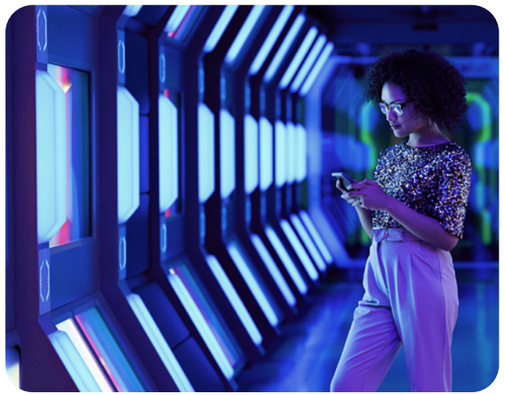
El resultado es una solución de seguridad escalable para cajeros automáticos que protege el tiempo de actividad, reduce los costos operativos y brinda a las instituciones financieras un mayor control sobre sus redes de cajeros automáticos.

radionix

La transición del negocio de sistemas de intrusión y acceso de Bosch a Radionix se ha completado. Como empresa independiente, avanzamos con mayor rapidez y nos centramos más en lo esencial, combinando nuestra tradición con la agilidad necesaria para satisfacer sus necesidades cambiantes.

Radionix proporciona un "centro de control" para su seguridad, unificando la detección de intrusiones, el control de acceso y la seguridad contra incendios en una red integrada y siempre activa. Ya sea en persona o de forma remota, usted obtiene el poder de gestionar el acceso y tomar decisiones al instante, mientras nuestra tecnología trabaja discretamente para proteger a su personal y sus bienes.

Esto es más que un nuevo nombre; es una nueva era de innovación construida sobre una base de confianza.



Más información

El ecosistema de próxima generación

El futuro ecosistema de Radionix modernizará nuestros **paneles de las series B y G,** en los que ya hemos confiado, manteniendo al mismo tiempo su característica fiabilidad, versatilidad y facilidad de uso.

“La instalación será más rápida gracias a una interfaz unificada y a la integración mediante API”, explica Greg Mora, director de producto de Radionix. “Estamos avanzando hacia una plataforma local conectada a la nube que garantiza que los dispositivos IoT permanezcan en línea con datos instantáneos y en tiempo real.”

Al reducir el tiempo de instalación, Radionix permite a los técnicos trabajar de forma más eficiente, abordando directamente los problemas relacionados con la mano de obra. Además, somos pioneros en la innovación inalámbrica segura para empresas.

Si bien la tecnología inalámbrica tradicionalmente se ha reservado para las pequeñas empresas, Radionix está llevando esa facilidad de configuración al sector comercial a gran escala sin comprometer los rigurosos estándares de seguridad que exigen nuestros clientes.

resideo

Resideo es un fabricante y desarrollador líder de productos y soluciones de control, detección y automatización basados en tecnología, presentes en más de 150 millones de espacios residenciales y comerciales en todo el mundo, con decenas de millones de nuevos dispositivos vendidos anualmente.

La reconocida marca First Alert ® de Resideo ofrece soluciones de seguridad, protección y detección de fugas de agua. Con más de un siglo de experiencia demostrada, los termostatos inteligentes Honeywell Home de la compañía ayudan a equilibrar la calidad del aire interior y ofrecen ahorro de energía.



Más información

Serie de cámaras First Alert® CX4: Vigilancia avanzada para Pymes

Las cámaras de vídeo First Alert ® CX4 ofrecen seguridad de ultra alta definición para hogares y pequeñas y medianas empresas (pymes) con una claridad y un análisis avanzados. Compatibles tanto con el sistema de seguridad Resideo ProSeries como con el sistema de seguridad híbrido First Alert ® VISTA ® , las cámaras ofrecen grabación continua y análisis mejorados para proporcionar una detección integral en entornos empresariales.

Las cámaras CX4 ofrecen una nitidez 4K y una resolución de 8 megapíxeles con un sensor de imagen de alto rendimiento, capturando detalles cruciales con una claridad que facilita la identificación de rostros, matrículas y otra información importante; una ventaja clave para la seguridad de las pequeñas empresas, la prevención de pérdidas y el conocimiento de la situación.

Las pequeñas empresas pueden elegir entre tres modelos para cubrir una amplia gama de aplicaciones:

- **Cámara tipo bala CX4B** Para vigilancia perimetral, almacenes o aplicaciones minoristas.
- **Cámara tipo torreta CX4T** Para vestíbulos, escaleras y zonas comerciales.
- **Cámara domo CX4D** Para entradas, salidas, oficinas o aplicaciones de servicio de alimentos.

Las cámaras también ofrecen almacenamiento de vídeo local, que mantiene los datos de vídeo en las instalaciones para reducir los requisitos y costes de red, y almacenamiento de eventos de vídeo basado en la nube, que envía el vídeo del evento importante a la nube, reduciendo el impacto del robo o la manipulación del hardware al tiempo que protege la información importante.

La visualización integrada a través de la experiencia familiar **de Total Connect ® 2.0** permite a los usuarios ver transmisiones en vivo de varias cámaras en una sola pantalla, mientras que el análisis inteligente identifica personas, vehículos, animales y paquetes para reducir las notificaciones innecesarias y ofrecer las alertas prácticas más importantes.

Con imágenes de alta definición, formatos flexibles y funciones inteligentes integradas, las cámaras de vídeo First Alert CX4 ofrecen una videovigilancia avanzada y escalable para los propietarios de pequeñas empresas.

El apasionado equipo de expertos de Software House ofrece soluciones de seguridad física que responden a los desafíos en constante evolución de las empresas modernas de hoy en día. Durante más de 30 años, muchas de las organizaciones y entidades gubernamentales más grandes del mundo han confiado en nosotros para ofrecer soluciones seguras, flexibles y que cumplen con la normativa.

Nuestro objetivo es simple: Capacitar a las organizaciones para que protejan a su personal y sus bienes, al tiempo que les proporcionamos las herramientas necesarias para ser más productivas.

- **Software:** C•CURE 9000 permite a nuestros clientes tomar el control total de sus sistemas de control de acceso, vídeo, intrusión, incendios y automatización de edificios.

- **Hardware:** Los controladores de puertas de Software House ofrecen un rendimiento de primera clase con opciones de implementación flexibles para arquitecturas tanto centralizadas como distribuidas.

- **Cibernético:** Seguimos marcando la pauta en ciberseguridad y nos dedicamos incansablemente a garantizar que sus datos estén protegidos y sus redes sean seguras.

- **Integraciones:** Nuestra solución se vuelve más potente gracias a su integración con los sistemas que nuestros clientes ya utilizan.

Software House es una marca de Johnson Controls Security Products, una división de Johnson Controls Inc.

Más información

Análisis basado en inteligencia artificial para la seguridad

C•CURE IQ Security Intelligence está diseñado para ayudar a las organizaciones a gestionar volúmenes de alarmas abrumadores mediante la identificación de eventos significativos dentro de grandes conjuntos de datos. Las empresas suelen experimentar millones de alarmas al año, muchas de las cuales son incidentes menores que enmascaran sucesos críticos. La plataforma prioriza las alarmas esenciales a través de**Alarm Intelligence** , que utiliza un motor de reglas personalizable para reducir el ruido, clasificar las alarmas y aplicar una puntuación de riesgo dinámica en tiempo real que se adapta a medida que evolucionan las situaciones. Esto garantiza que los equipos de seguridad se centren en los incidentes más urgentes y respondan con mayor eficacia.

Algunos ejemplos de reglas automatizadas incluyen el filtrado de falsas alarmas causadas por actividad válida de la tarjeta, la escalada de eventos de acceso forzado que ocurren en grupos y la identificación de comportamientos sospechosos, como intentos de acceso rechazados repetidamente. Los paneles de control ofrecen una visualización en tiempo real de las tendencias de las alarmas, el estado y la actividad de automatización, lo que permite unas operaciones más ágiles.

La solución también incluye potentes**capacidades de**Spatial Intelligence. Estas funciones ofrecen una visión integral del uso de las instalaciones, el movimiento del personal y las tendencias de ocupación. Herramientas como la última ubicación conocida, el recuento virtual de personal (para el control de acceso), las métricas de acceso mediante tarjeta y los paneles de control de ocupación proporcionan visibilidad en tiempo real sobre dónde se encuentran las personas, cómo se utilizan los espacios y cómo se pueden optimizar las instalaciones para garantizar la seguridad y la eficiencia. El análisis de la asistencia contribuye a la gestión de la plantilla al destacar tendencias e identificar posibles problemas.

Diseñado para ofrecer un rendimiento a escala empresarial, el sistema recomienda configuraciones robustas de CPU, memoria y SQL Server. Los distintos niveles de licencia (SM, MD, LG y XL) ofrecen diferentes capacidades, y todas las versiones incluyen Alarm Intelligence con múltiples reglas y las funciones principales de Spatial Intelligence.

SONITROL es líder en seguridad electrónica verificada, proporcionando soluciones de seguridad innovadoras y personalizadas (detección de intrusiones, control de acceso y vídeo integrados) en toda Norteamérica.

Mediante el uso de un sistema patentado de detección de intrusiones por audio activado por impacto y alarmas verificadas, SONITROL ha liderado la industria en detenciones documentadas, más de 188.000 y en aumento.



Más información

Integración inalámbrica SONITROL CORE+ PowerG

SONITROL CORE sigue elevando el listón de la seguridad profesional con la integración de **la tecnología inalámbrica PowerG.** , aportando protección inalámbrica rápida, flexible y altamente fiable a la plataforma unificada CORE.

Esta integración combina los sensores inalámbricos de largo alcance y bajo consumo de batería de PowerG con el sistema patentado y verificado de detección de intrusiones de audio y vídeo de SONITROL. El resultado es una solución potente que simplifica las instalaciones a la vez que mantiene el rendimiento probado por el que SONITROL es conocido. Al eliminar el cableado complejo, los distribuidores pueden reducir significativamente el tiempo y el coste de instalación, a la vez que adaptan fácilmente los sistemas a grandes instalaciones, propiedades con múltiples ubicaciones o entornos donde el cableado no es práctico.

La tecnología inalámbrica PowerG ofrece un rendimiento líder en la industria, que incluye comunicación cifrada por salto de frecuencia con un alcance de hasta 2 kilómetros en línea de visión y una gestión de energía adaptativa que permite una duración de la batería de hasta 8 años por dispositivo. El cifrado AES de 128 bits de grado militar, la comunicación bidireccional y el funcionamiento resistente a las interferencias garantizan una protección fiable para aplicaciones comerciales y de tipo universitario.

Los sensores PowerG homologados, como los contactos inalámbricos para puertas y ventanas, los detectores de movimiento, los sensores de rotura de cristales y los botones de pánico, se integran a la perfección con el transceptor principal PowerG y los paneles de seguridad CORE, todo ello gestionado a través de una única plataforma. Los instaladores se benefician de una rápida implementación y una fácil expansión, mientras que los usuarios finales obtienen una menor complejidad del sistema, menores costos y una respuesta policial más rápida gracias a la tecnología de alarma de audio y video verificada de SONITROL.

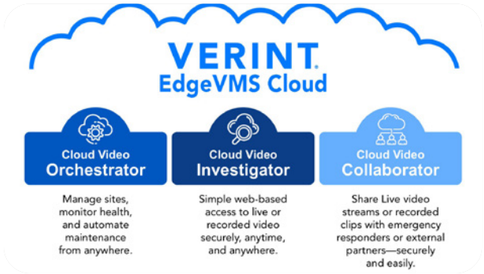
Próximamente se incorporarán sensores adicionales homologados, lo que ampliará aún más la flexibilidad del ecosistema CORE.

VERINT®

Verint es un proveedor líder de soluciones de seguridad y prevención de fraude para instituciones financieras, en el que confían más de 3000 bancos y cooperativas de crédito, incluidos 8 de los 10 principales bancos de EE. UU. Con más de dos décadas de experiencia, Verint ayuda a las organizaciones a mitigar el fraude, reducir el riesgo y mantener el cumplimiento normativo en un entorno en constante evolución.

Nuestras soluciones de seguridad avanzadas permiten a los clientes identificar riesgos, agilizar las investigaciones y responder con rapidez gracias a información útil. Las instituciones financieras de todo el mundo confían en la tecnología y los conocimientos de Verint para adelantarse a las amenazas emergentes, desde ataques a cajeros automáticos y fraudes hasta actividades internas y vulnerabilidades en las sucursales. Al combinar los datos de las transacciones con la inteligencia de vídeo, Verint mejora la visibilidad, la precisión y los tiempos de respuesta.

Las soluciones de Verint, escalables y preparadas para la nube, admiten entornos grandes y geográficamente dispersos. Gracias a su amplia experiencia en el sector y a su constante innovación, Verint se asocia con instituciones financieras para mejorar la eficiencia, proteger los activos y fortalecer el ecosistema de seguridad.



Más información

Aproveche el valor de la arquitectura híbrida con Verint EdgeVMS Cloud Suite

A medida que las instituciones financieras definen sus estrategias en la nube, muchas optan por un camino deliberado en lugar de precipitarse a una migración completa. Los responsables de seguridad están buscando el equilibrio entre la flexibilidad que ofrece la tecnología en la nube y el rendimiento y la fiabilidad de los que dependen sus operaciones. Un modelo híbrido favorece ese equilibrio, permitiendo a las organizaciones ampliar sus capacidades en la nube al tiempo que siguen aprovechando la infraestructura existente.

La **suite Verint EdgeVMS Cloud** refleja este enfoque al combinar la funcionalidad flexible de la nube con la seguridad y el rendimiento que esperan las instituciones financieras.

Con **Cloud Video Orchestrator** , los equipos pueden supervisar la gestión de dispositivos en toda la empresa mediante la monitorización del estado en tiempo real, la emisión inteligente de incidencias y la generación de informes de rendimiento desde prácticamente cualquier lugar.

Cloud Video Inspector permite a los usuarios autorizados acceder rápidamente a vídeos en directo y grabados desde un navegador, eliminando la necesidad de software adicional.

Cuando es necesario compartir vídeos, **Cloud Video Collaborator** permite un acceso seguro y temporal para equipos internos o socios externos autorizados, manteniendo la cadena de custodia.

Diseñada para entornos híbridos, la Cloud Suite permite a las organizaciones modernizarse a su propio ritmo, mejorando la visibilidad en todas las ubicaciones y escalando estratégicamente sin interrumpir las operaciones de seguridad diarias.

VIAKOO

Viakoo permite a sus clientes garantizar el rendimiento continuo de sus sistemas de seguridad física y de tecnología operativa (OT), al tiempo que protege su superficie de ataque OT con soluciones avanzadas de detección y corrección de vulnerabilidades. La visión de Viakoo es que cada dispositivo empresarial conectado sea 100% visible, operativo y seguro.

La plataforma Viakoo Action Platform, que no requiere agentes, mantiene los entornos OT distribuidos y no gestionados seguros y en funcionamiento continuo con el menor riesgo y coste posibles. La ciberhigiene automatizada de los dispositivos se actualiza de forma fiable y a gran escala con firmware, contraseñas y certificados para elevar la postura de seguridad y el rendimiento del sistema a las expectativas de TI empresariales.

Viakoo Inc. es líder en ciberseguridad y garantía de servicio para dispositivos conectados. Todas las soluciones de Viakoo se conciben y desarrollan íntegramente en EE. UU.



Más información

Viakoo DFM-AutoMode reduce drásticamente el tiempo de remediación de seguridad física de meses a minutos

Con el lanzamiento de **Device Firmware Manager AutoMode™ (DFM-AutoMode)** , Viakoo ha mejorado su **plataforma insignia Viakoo Action Platform** con una solución de remediación autónoma impulsada por IA. Esta nueva capacidad reduce la superficie de ataque cibernético de la seguridad física y de la tecnología operativa (OT) de una organización más rápidamente que cualquier otra solución de seguridad, al acelerar drásticamente el tiempo necesario para corregir las vulnerabilidades conocidas.

La función AutoMode de Viakoo mejora la seguridad de la tecnología operativa (OT) al proporcionar operaciones autónomas para encontrar vulnerabilidades en el inventario de dispositivos, determinar si hay nuevo firmware disponible y, a continuación, configurar una tarea de actualización para corregir las vulnerabilidades. La acción solo se lleva a cabo tras la aprobación humana, mediante un solo clic. La remediación tradicional puede tardar días o semanas; DFM-AutoMode lo hace en segundos.

La estrategia de Viakoo en torno a las funcionalidades de AutoMode aprovecha la información obtenida de más de 2.000 millones de horas de uso del producto en la plataforma de Viakoo, beneficiándose de la experiencia real en todos los sectores verticales principales. Esta amplia experiencia, combinada con la cartera de patentes de Viakoo en gestión de OT e IoT, constituye la base de AutoMode.

Viakoo tiene previsto extender la tecnología AutoMode a todas las funcionalidades de remediación dentro de la plataforma Viakoo Action Platform.

Securitas Technology

Securitas destaca



Securitas

Liderando el cambio de la industria hacia la seguridad basada en la inteligencia

Descubre cómo el enfoque basado en la inteligencia de Securitas está empoderando a sus clientes en una nueva era de seguridad global.

Más información

Ver un mundo diferente

En un contexto de un mundo en rápida evolución y un entorno de riesgos cada vez más complejo, las organizaciones de todos los sectores se enfrentan al reto de desenvolverse en un panorama donde las amenazas aumentan tanto en frecuencia como en complejidad. Las amenazas a la seguridad moderna se desarrollan más rápido que nunca y afectan tanto a los entornos físicos como a los digitales.

En Securitas lo vemos todos los días. La tecnología que da poder a las empresas también abre nuevas puertas a los ciberdelincuentes. “El modelo tradicional de reaccionar después de que algo sucede sigue vigente, pero para anticiparse mejor a los riesgos y prevenirlos, las organizaciones necesitan señales más tempranas, una visión más precisa y la capacidad de actuar antes de que una situación se convierta en un problema.

Cuando preguntamos a nuestros clientes sobre su socio de seguridad ideal, su visión coincidió con la nuestra: Tecnología integrada y avanzada, resolución proactiva de problemas y un enfoque integral de la seguridad y la gestión de riesgos.

Aquí es donde Securitas está centrando su atención: Transformar la incertidumbre en certeza, ofrecer un socio de confianza cuando el panorama está cambiando y brindar seguridad a los clientes cuando más la necesitan. Al transformar la forma en que recopilamos, analizamos y actuamos en función de la información de inteligencia, estamos redefiniendo el papel de la seguridad como un motor estratégico de la resiliencia y la continuidad del negocio.

Mejorar la seguridad mediante la innovación basada en la inteligencia

En toda nuestra organización global, este cambio hacia una seguridad basada en la inteligencia ya está en marcha. Mediante la monitorización continua de los acontecimientos mundiales, la detección temprana de indicadores y el análisis contextual en tiempo real, permitimos a nuestros clientes detectar las amenazas emergentes con mayor antelación y comprender su relevancia para las operaciones diarias.

Convertirnos en una organización basada en la inteligencia significa conectar el riesgo, las operaciones y la toma de decisiones de una manera que refleje cómo se desarrollan realmente las amenazas. Significa pasar de la reacción a la anticipación, potenciar las capacidades humanas con datos y tecnología, y ofrecer una visión única y conectada de lo que realmente importa.

Desde la gestión de riesgos y los servicios de seguridad hasta la tecnología avanzada y las soluciones digitales, la transformación de Securitas está respaldada por un amplio ecosistema de capacidades operativas y de inteligencia.

Transformar los datos en visión de futuro, no solo en información valiosa

Los datos pueden permitir tomar medidas significativas. Nuestro objetivo es ayudar a los clientes a filtrar la información irrelevante y concentrarse en las señales que realmente importan.

Nuestros servicios de inteligencia digital y de riesgos brindan a las organizaciones una visión más completa de su entorno de riesgos, ya sea que esto implique el seguimiento de los acontecimientos mundiales, la identificación de patrones emergentes o el apoyo a través de investigaciones complejas y escenarios de crisis. Además, estamos reforzando nuestra capacidad para interpretar señales de inteligencia digital y de código abierto a gran escala en la gestión de riesgos de seguridad, la tecnología y los servicios de seguridad, transformándolas en directrices claras y prácticas adaptadas al perfil de riesgo de cada cliente.

Empoderando a nuestra gente y a nuestros clientes

A pesar del ritmo del cambio tecnológico, un principio permanece constante: Las personas son el centro de todo lo que hacemos.

En lo que respecta a los servicios de primera línea, nuestros agentes utilizan información en tiempo real, herramientas con soporte de IA y asistentes digitales como **MyConnect** y **MySecuritas** para responder con mayor rapidez y ofrecer un servicio de mayor calidad a los clientes.

Para los clientes que utilizan nuestras soluciones tecnológicas, plataformas como **SecureStat HQ** y **SecureStat Cumulus** les permiten centralizar las alarmas, visualizar el rendimiento del sistema de seguridad y recibir alertas basadas en información estratégica, con el apoyo de la IA generativa. En entornos sanitarios especializados, la integración de la seguridad electrónica con **sistemas de localización en tiempo real (RTLS)** proporciona información contextual continua sobre personas, activos y movimientos.

Utilizando IA y tecnología avanzada

La inteligencia artificial (IA), las plataformas en la nube, la robótica, los drones y la automatización se han convertido en elementos fundamentales del funcionamiento de la seguridad moderna en la actualidad. La IA filtra las distracciones, acelera el análisis y saca a la luz la información que merece la atención humana.

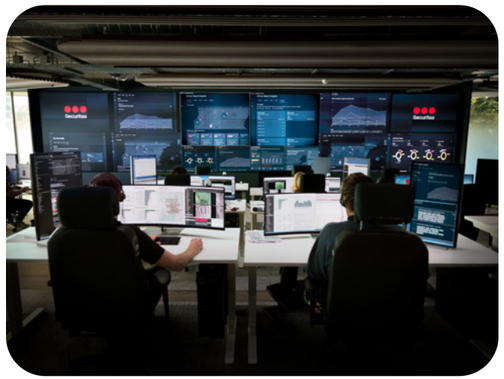
Para complementar nuestros servicios tecnológicos, los analistas humanos de nuestros centros de monitorización e inteligencia de riesgos se aseguran de que la información automatizada se valide y se contextualice.

A medida que se conecten más sistemas y la inteligencia sea más precisa, la seguridad se percibirá menos como una postura defensiva y más como una capacidad estratégica e informada.

Mantenerse a la vanguardia en un mundo diferente

Ese es el papel que Securitas se compromete a desempeñar: Ser el socio de confianza en seguridad basada en inteligencia.

Al fortalecer nuestro enfoque basado en la inteligencia, Securitas está elevando el estándar de la seguridad moderna, ayudando a nuestros clientes a desenvolverse en un entorno de incertidumbre con mayor claridad, mayor resiliencia y una postura de seguridad más inteligente y conectada.



Servicios de inteligencia

Ofrecemos soluciones de seguridad proactivas y basadas en inteligencia que permiten a nuestros clientes proteger sus organizaciones con confianza.

Más información

La era de la inteligencia en seguridad ha llegado.

Estamos impulsando un futuro donde la inteligencia transforma la seguridad en una ventaja estratégica. Gracias a nuestra visión sin precedentes, las organizaciones pueden afrontar con confianza y resiliencia las complejidades del mañana.

Nuestro equipo de analistas y expertos integra a la perfección capacidades digitales y soluciones innovadoras con seguridad basada en inteligencia, ofreciendo a nuestros clientes una protección personalizada, cada vez más predictiva y proactiva.

Como nuestro servicio estrella, nuestra gestión de inteligencia de riesgos integra información basada en datos y tecnología con análisis de expertos para proporcionar a las organizaciones información precisa, oportuna, relevante y práctica. Estos conocimientos ayudan a los clientes a comprender los riesgos que plantean los actores criminales y terroristas, los cambios geopolíticos, las amenazas a la ciberseguridad, los desafíos ambientales y mucho más.

Inteligencia en su máxima expresión

Nuestra **inteligencia de riesgos** va más allá de simplemente identificar lo que está sucediendo. Explica por qué es importante, qué podría suceder a continuación y, lo que es más importante, qué medidas se pueden tomar. Con cinco niveles de servicios premium, ofrecemos herramientas digitales, servicios gestionados y experiencia especializada integrada, todo ello personalizable para crear una solución a medida que satisfaga las necesidades únicas de nuestros clientes.



Concietización

Manténte a la vanguardia con un conocimiento actualizado de la situación y de los últimos acontecimientos en el panorama mundial de la seguridad y las amenazas. Recibe más de 350 informes anuales, que incluyen actualizaciones diarias, semanales, mensuales y puntuales sobre eventos globales importantes. Este servicio es adecuado para organizaciones de todos los tamaños y sectores, garantizando que los clientes dispongan de la información necesaria para tomar decisiones fundamentadas.

Alertamiento

Recibe alertas dirigidas para incidentes y amenazas cerca de las ubicaciones de los clientes con nuestro servicio de alertas altamente personalizado. Protege a las personas, propiedades y activos manteniéndose informado con notificaciones en tiempo real y alertas tempranas sobre amenazas emergentes.

Asesoramiento

Accede a servicios de inteligencia especializados para proteger a las organizaciones. Nuestro completo paquete de inteligencia sobre protección, amenazas y riesgos aprovecha la estrategia de inteligencia de fuentes múltiples de Securitas, que combina la inteligencia humana experta (HUMINT) con tecnología de vanguardia para la inteligencia de fuentes abiertas (OSINT).

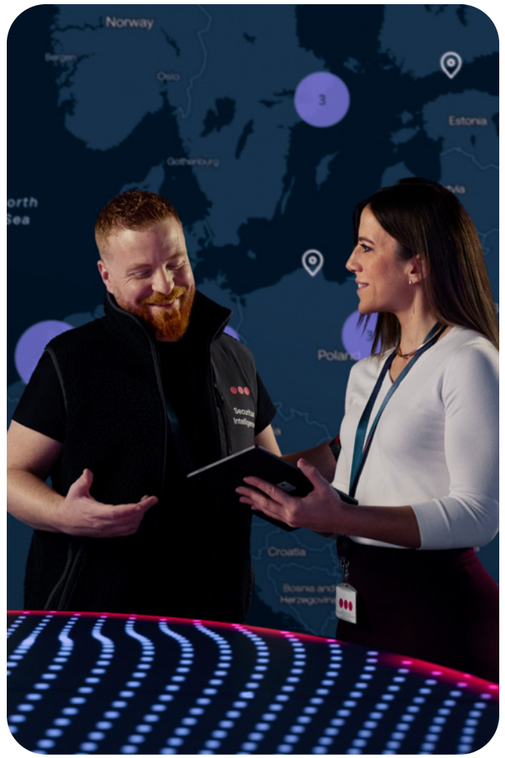
Análisis

Integra recursos especializados de inteligencia y gestión de riesgos directamente en la organización. Nuestros analistas y expertos, con el apoyo de la comunidad de inteligencia global de Securitas, proporcionan acceso a una red mundial de especialistas en la materia y a información local.

Inteligencia ad hoc

Ofrecemos servicios personalizados de inteligencia de riesgos y consultoría para satisfacer las necesidades específicas de nuestros clientes. Ya sea que necesiten actualizaciones inmediatas sobre un evento, informes puntuales, proyectos especializados o colaboraciones ad hoc, estamos aquí para ayudarles.





PINKERTON®

Pinkerton es líder mundial en servicios, soluciones y programas de seguridad y gestión de riesgos. Nuestras capacidades incluyen expertos integrados en la materia, protección, investigaciones y consultoría. Desde 1850, Pinkerton ha forjado un legado de conocimiento institucional incomparable, con una visión perspicaz de los riesgos futuros. En todo lo que hacemos, aplicamos una perspectiva integral del riesgo, un diseño basado en el conocimiento y una entrega de principio a fin.

Con nuestro enfoque integral, evaluamos los factores de riesgo a los que se enfrenta hoy, diseñamos una solución eficaz que se adapta a sus necesidades específicas y le brindamos servicios tácticos para ayudarle con la ejecución, ya sea de forma puntual o a largo plazo. Como socio de confianza, usted puede contar con nuestra red de miles de empleados y socios conectados en más de 100 países para satisfacer sus necesidades de gestión de riesgos y seguridad.

Más información

Inteligencia protectora: SCOUT en acción

Información útil para líderes, eventos y operaciones.
Las motivaciones para cometer robos y fraudes no han cambiado; sin embargo, los avances tecnológicos actuales proporcionan a los delincuentes los medios para cometer delitos a la velocidad de internet.
En Pinkerton, la organización de seguridad y gestión de riesgos más antigua de EE. UU., respondimos con SCOUT, inteligencia de protección e informes de diligencia debida, transformando las señales de código abierto en información verificada. El resultado es una alerta temprana y decisiones claras que protegen la continuidad, la confianza y el valor.

Por qué es importante la inteligencia de protección

La inteligencia protectora es fundamental para la seguridad organizacional, ya que ayuda a salvaguardar a las personas, los lugares, los datos y la marca. Muchos riesgos se originan o se propagan en línea: publicaciones en redes sociales, activismo, divulgación de información personal, fraude y acontecimientos globales que se desarrollan con rapidez. Ante tanto ruido, las organizaciones necesitan señales claras y tempranas, además de contexto. La inteligencia de protección aporta esa claridad, sirviendo de apoyo a la planificación de emplazamientos y eventos, la seguridad en viajes y residencias, la protección de la plantilla, la supervisión de proveedores y la reputación. Reduce la incertidumbre y ayuda a los líderes a tomar medidas mesuradas y basadas en evidencia.



EXPLORADOR : Inteligencia de fuentes abiertas + debida diligencia

Los informes de SCOUT Inteligencia protectora + Due Diligence son una innovadora herramienta estratégica de apoyo a la toma de decisiones que combina la experiencia en investigación con la inteligencia para ofrecer información crucial sobre personas de interés (POI) y grupos de interés (GOI). Esto reduce los puntos ciegos y las falsas alarmas, y acelera la toma de decisiones. Nos alineamos con los objetivos del cliente, establecemos umbrales de decisión, informamos a las partes interesadas, coordinamos las medidas con los equipos internos y realizamos revisiones posteriores a la acción para mejorar el próximo ciclo.

SCOUT Investigative

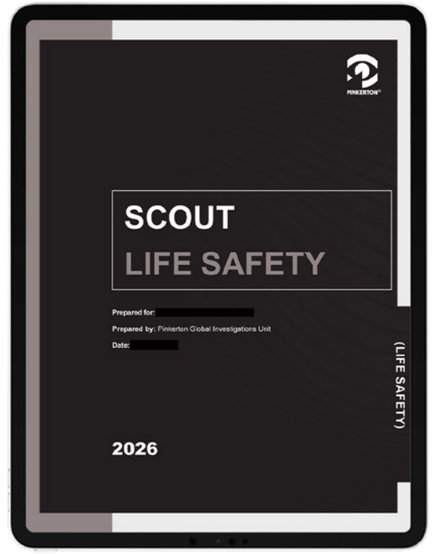
SCOUT Investigative ofrece perfiles verificados. de personas y empresas: registros verificados por los tribunales, información negativa en los medios, datos financieros, activos, licencias y actividad social; yendo más allá de los controles convencionales para ofrecer una debida diligencia basada en una metodología de investigación estructurada, exhaustiva y diseñada para sacar a la luz lo que pasan por alto las comprobaciones estándar.

SCOUT Workplace Violence

SCOUT Workplace Violence proporciona una evaluación rápida e informativa de las amenazas individuales: instantáneas OSINT de 24 horas, informes de amenazas OSINT de 48 horas con la participación de un gestor de amenazas certificado e informes exhaustivos sobre seguridad vital con comprobaciones judiciales presenciales, que ponen de manifiesto comportamientos, exposición legal y recomendaciones para determinar la gravedad.

SCOUT Protective Intelligence SCOUT

Protective Intelligence mapea los riesgos digitalesmediante redes sociales, fuentes abiertas y análisis de la dark web —incluyendo búsquedas generales de amenazas, evaluaciones de exposición y monitoreo configurable— para identificar menciones negativas y amenazas emergentes, reducir la exposición y apoyar una protección proactiva de las personas, eventos, ejecutivos y marca.



Desde informes independientes hasta la integración en los servicios EPIC de Pinkerton (PYMES, protección, investigaciones y consultoría y asesoramiento en materia de riesgos), los informes de inteligencia protectora y diligencia debida de SCOUT son un recurso para ayudar a las organizaciones a tomar decisiones claras, fiables y defendibles en materia de seguridad.

Securitas Healthcare

Mejorar la seguridad y eficiencia en el ámbito sanitario

Empoderarando a los cuidadores, mejorarando la atención.

Securitas Healthcare colabora con más de 15.000 hospitales y residencias para personas mayores en todo el mundo para crear entornos de atención seguros, protegidos y eficientes. Con más de 40 años de experiencia en el sector sanitario, ofrecemos soluciones integradas que protegen a las personas, fortalecen las operaciones y proporcionan información práctica a los líderes en todo el proceso asistencial.

Más información

Nuestra visión es sencilla

Los cuidadores deberían poder centrarse en cuidar a las personas, no en gestionar la complejidad operativa. Al combinar tecnologías de protección, visibilidad en tiempo real e inteligencia basada en datos, ayudamos a las organizaciones a mejorar la seguridad, aumentar la capacidad de respuesta y reducir la carga administrativa.



Presta servicios a hospitales y residencias de ancianos

Ofrecemos a hospitales, clínicas y residencias para personas mayores soluciones adaptadas a sus necesidades clínicas, operativas y normativas específicas. En los hospitales, Securitas Healthcare refuerza la seguridad de los pacientes y del personal al tiempo que mejora la eficiencia. Las soluciones líderes en el sector · como **Hugs®** Infant Protection, protegen a los recién nacidos y facilitan los flujos de trabajo de maternidad, mientras que Staff Protection, Asset Management y Environmental Monitoring mejoran la seguridad, el cumplimiento normativo y la productividad en todos los departamentos.

En las residencias para personas mayores, ayudamos a replantear la seguridad de los residentes y la sostenibilidad operativa. **WanderGuard** ® proporciona una protección fiable contra fugas, diseñada para preservar la dignidad de los residentes al tiempo que fomenta la vigilancia de los cuidadores. Combinado con llamadas de emergencia y de enfermería y gestión de caídas, nuestra cartera permite tiempos de respuesta más rápidos, mejor comunicación, y un entorno de vida más seguro.



Asociación integral durante todo el ciclo de vida

Securitas Healthcare ofrece un enfoque integral, desde la consultoría y el diseño de soluciones hasta la instalación, la formación, los servicios gestionados y el soporte a largo plazo.

Medimos el éxito por los resultados de nuestros clientes: instalaciones más seguras, operaciones más eficientes y equipos de atención capacitados. Al alinear la innovación con los desafíos reales de la atención médica, Securitas Healthcare ayuda a las organizaciones a construir entornos seguros e inteligentes donde una atención excepcional pueda prosperar.



Conéctate con Securitas Technology en las redes sociales

Securitas Technology

2027 Global Technology Outlook Report

Acerca de Securitas Technology

Securitas Technology, que forma parte de Securitas, es un proveedor líder mundial de soluciones de seguridad integradas que protegen, conectan y optimizan empresas de todo tipo y tamaño.

Más de 12.000 miembros de nuestro equipo en 40 países se centran a diario en nuestro propósito de ayudar a que su mundo sea un lugar más seguro y en nuestro compromiso de ofrecer una experiencia al cliente inigualable.

Con los clientes como eje central de todo lo que hacemos, nuestro equipo humano, nuestros conocimientos y nuestra tecnología impulsan nuestro ecosistema conectado de soluciones de salud, seguridad y protección.

Securitas Technology

See a different world

Calle Entrepeñas, 27
28051 Madrid

© 2026 Securitas Technology Corporation

Algunas de las soluciones y servicios referidos en este informe están sujetas a disponibilidad en determinados mercados.