Securitas Technology

Informe de Perspectivas Tecnológicas Globales **2026**

securitastechnology.com

Contenido

Agradecimiento a nuestros socios estratégicos

Los principales fabricantes e innovadores de tecnología del mundo.

Bienvenida y agradecimiento

Presentación del Informe de Perspectivas Tecnológicas Globales 2026

En nombre de todos los asociados de Securitas Technology en todo el mundo, me complace darle la bienvenida a este, nuestro octavo Informe Anual de Perspectivas Tecnológicas Globales.

Quiero comenzar agradeciendo a nuestros clientes por su continua confianza y colaboración, y por las perspectivas que han dado forma al informe de este año. También me gustaría agradecer a nuestros socios estratégicos y expertos del sector por su vital contribución; su experiencia y pasión por la innovación, son un motor clave para este informe.

Nuestro informe de 2025 tuvo una excelente acogida por parte de nuestros clientes y del sector, lo que complementa otro año histórico para Securitas Technology. Mientras entregamos decenas de miles de proyectos de seguridad integrales de alta calidad para organizaciones de todo el mundo, seguimos innovando, aportando nuevas tecnologías, servicios y beneficios a nuestros clientes. A continuación, algunos puntos destacados:

1. Lanzamos nuestra innovadora iniciativa de sostenibilidad, que documenta datos sobre el consumo energético de los sistemas de seguridad y las emisiones equivalentes de gases de efecto invernadero, fomentando la concienciación y ofreciendo a los clientes opciones de seguridad más sostenibles.

2. Invertimos continuamente en nuestra plataforma digital de gestión de seguridad líder en la industria, SecureStat® HQ™, añadiendo nuevas funciones e innovaciones para brindar a los clientes mayor claridad y control sobre su programa de seguridad.

3. Presentamos nuestro nuevo Programa de Aprendices Técnicos, desarrollado en colaboración con la Asociación de la Industria de la Seguridad (SIA), lo que demuestra nuestra dedicación a la formación de la próxima generación de profesionales de la seguridad.

De vuelta con información actualizada para 2026, esta nueva edición de nuestro Informe de Perspectivas está repleta de información del mercado, nuestros socios tecnológicos estratégicos, tecnólogos de la industria y expertos en seguridad interna de toda nuestra organización global.

En Securitas Technology, consideramos nuestra relación con nuestros clientes como algo más que un simple proveedor de servicios. Actuamos como asesores de confianza en tecnología de seguridad, ayudando a nuestros clientes a mantenerse a la vanguardia de las tendencias y los temas en evolución que definen el futuro de la industria.

Nos enorgullece que nuestro informe se haya convertido en una referencia clave en el calendario del sector, valorado por su enfoque específico en las tendencias tecnológicas dentro del ámbito de la seguridad electrónica. Su contenido está diseñado para ayudarle a evaluar las tendencias actuales y futuras del mercado, anticipar las amenazas emergentes, comprender las tecnologías emergentes y planificar con confianza la hoja de ruta de seguridad y las inversiones tecnológicas de su organización.

Le invito a explorar cada sección del informe, incluyendo información basada en datos de nuestro estudio de mercado, las principales tendencias tecnológicas a tener en cuenta, las últimas innovaciones de nuestros socios estratégicos y el asesoramiento de expertos sobre cómo su organización puede prepararse eficazmente para el futuro de la seguridad.

Tony Byerly, Presidente Global y Director Ejecutivo de Securitas Technology

Acerca de Securitas Technology

Un socio tecnológico global centrado exclusivamente en la seguridad

En seis continentes, ofrecemos una sólida infraestructura global para brindar excelencia operativa y de servicio, impulsada por una profunda innovación y experiencia especializada en seguridad electrónica.

+ de 40

países con capacidades y presencia en tecnología de seguridad

- → 6 continentes
- → #2 en seguridad electrónica comercial a nivel mundial

1+ millón

Sitios de clientes en todo el mundo

- → + de 1.6M de conexiones monitoreadas
- → + de 1M de llamadas de mantenimiento, inspección y servicio realizadas anualmente

+ de 13,000

Empleados en todo el mundo

- → + de 5,000 técnicos
- → + de 500 ingenieros, arquitectos de diseño e innovadores

Conozca más sobre nuestras tecnologías, servicios y experiencia en el sector en securitastechnology.com

Simplificando la complejidad para empresas de todo el mundo

Con miles de productos, sistemas y servicios de seguridad electrónica para elegir, ayudamos a nuestros clientes a distinguirse del resto y a comprender sus necesidades con claridad. La tecnología avanza más rápido que nunca; nuestros expertos se mantienen a la vanguardia de las últimas innovaciones en intrusión, video, control de acceso, detección de incendios, sistemas integrados y más, para que nuestros clientes puedan incorporar las tecnologías futuras en su estrategia de seguridad.

Un asesor de confianza para una seguridad integrada a medida

Trabajando en estrecha colaboración con las empresas, no solo somos su proveedor de tecnología de seguridad, sino también un asesor de confianza y un socio comprometido para una experiencia del cliente a medida, personalizada y con visión de futuro a largo plazo.

Conectando a nuestros clientes con la tecnología de seguridad líder a nivel mundial

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

Impulsando el Valor de la Seguridad Empresarial

Nos integramos a la perfección con el equipo de seguridad de cada cliente, brindando servicios integrales en todos los aspectos de la tecnología de seguridad, desde el diseño, la instalación y la integración de sistemas hasta la monitorización proactiva, el mantenimiento preventivo y los servicios remotos inteligentes.

Securitas Technology

Nuestro Enfoque de Innovación

Forjando juntos el Futuro de la Seguridad

Este informe es solo uno de los resultados de un enfoque probado de innovación en tecnología de seguridad, perfeccionado durante décadas; un enfoque que ha dado lugar a algunos de los proyectos de seguridad más avanzados y complejos del mundo y ha ayudado a miles de organizaciones de todos los tamaños a optimizar continuamente su seguridad.

Activación Centrada en el Cliente

Ante todo, nuestra agenda de innovación se basa en una estrecha colaboración con nuestros clientes y un profundo conocimiento de la seguridad en todos los sectores y regiones. Nuestros Simposios de Seguridad, el Consejo Asesor de Clientes, la colaboración con los principales fabricantes y tecnólogos del mundo, y la participación activa en toda la industria inspiran e informan nuestra búsqueda de mejores tecnologías. Nuestros Centros de Atención al Cliente y Laboratorios de Evaluación Tecnológica permiten a clientes actuales y potenciales conocer las últimas tecnologías de primera mano y comprender qué tecnología lidera la industria.

Asociaciones Estratégicas Globales

Reconocemos que la innovación en tecnología de seguridad es el resultado de un ecosistema de proveedores a nivel mundial que buscan nuevas ideas y lanzan nuevos productos. Nos enorgullece asociarnos con los principales proveedores mundiales de hardware, software, análisis e infraestructura en la nube de seguridad.

Evaluación Interna Sólida

Nuestro equipo global de Estrategia e Innovación Tecnológica, compuesto por expertos en seguridad de todo el mundo, siempre está a la vanguardia para satisfacer las necesidades futuras de nuestros clientes. Trabajan en estrecha colaboración con nuestros líderes empresariales y socios estratégicos para identificar y evaluar los beneficios de las nuevas tecnologías y comprender sus aplicaciones más adecuadas. El equipo también evalúa nuevos productos para garantizar su solidez técnica y viabilidad comercial, con el fin de mejorar nuestra gama de soluciones y servicios.

Excelencia en Personas y Procesos

Por último, hemos desarrollado experiencia en diversas funciones y regiones para ofrecer estas innovaciones a nuestros clientes. Nuestra capacidad para diseñar, instalar, supervisar, mantener y actualizar continuamente nuestra tecnología de seguridad integrada nos ha convertido en un asesor de confianza para organizaciones grandes y pequeñas.

Nuestro Programa de Clientes Globales está especializado para ofrecer estos beneficios incluso a las empresas más grandes del mundo, cuyas necesidades de seguridad abarcan todo el mundo.

Más información sobre el Programa de Clientes Globales de Securitas Technology en securitastechnology.com/global-clients-program

Plataforma de Gestión de Seguridad SecureStat® HQ™

Obtenga claridad y control sobre las operaciones de seguridad para facilitar la mejora continua.

SecureStat® HQ™ es una plataforma integral de gestión de seguridad digital que simplifica la gestión de la seguridad, conecta a los usuarios con sus sistemas de seguridad y los servicios de Securitas Technology, y genera información para optimizar la seguridad y el rendimiento empresarial.

Control de Sitios a Nivel Empresarial

- Organice y visualice las ubicaciones en toda la empresa.
- Establezca horarios de los sitios para garantizar la coherencia.
- Edite contactos y listas de llamadas para mantener los sitios actualizados.

Gestión eficiente de sistemas

- Controle múltiples sistemas: acceso, vídeo, incendio, intrusión, etc.
- Gestione el acceso de usuarios en todos los sistemas.
- Pruebe los sistemas desde cualquier lugar con acceso a internet.

Gestión de eventos en tiempo real

- Messenger de actividad para ver la actividad en diferentes ubicaciones.
- Messenger de alarmas para ver y responder a las alarmas.
- Service Messenger™ para actualizaciones de solicitudes de servicio.
- Messenger de instalación para supervisar proyectos de instalación (próximamente).

Puerta de enlace directa con el cliente

- Abra tickets de servicio y conéctese con el equipo de soporte.
- Consulte y pague facturas.
- Vea videos en vivo y grabados.

Información inteligente sobre datos

- Informes dinámicos y personalizados
- Informes de excepciones y eventos
- Suscripciones a informes para impulsar informes estandarizados.

Planes de suscripción fáciles de elegir

- Planes Básico, Avanzado y Premium disponibles.
- Personalizable según las necesidades de cada organización.
- Acceso a potentes servicios avanzados proporcionados a través de SecureStat® HQ™, incluyendo SecureStat 360® Lifecycle Management.

Otras funciones de SecureStat® HQ™ para optimizar el rendimiento y la tecnología de seguridad

SecureStat 360® Security Technology Lifecycle Management

Ofrezca mayor seguridad y valor organizacional mediante una gestión eficaz del ciclo de vida de los activos de seguridad.

Maximice la vida útil de sus equipos:
Sepa exactamente cuándo se instaló el equipo, su historial de servicio y cuándo se recomienda su reemplazo.

Planificación de actualizaciones rentable:
Vea qué equipos necesitan reemplazo para planificar las actualizaciones de forma eficiente y basar sus decisiones de inversión en datos.

Reduzca la exposición a vulnerabilidadesconocidas:
Supervise fácilmente las versiones de software y firmware, así como su estado de fin de vida útil, para abordar proactivamente el firmware obsoleto o los dispositivos que se están descontinuando.

Documente las emisiones de CO2e:
Consulte las emisiones de CO2e por dispositivo derivadas del consumo de energía y tome decisiones informadas para alinear las inversiones en seguridad con los objetivos de sostenibilidad.

SecureStat® Video

Vea videos en vivo y grabados asociados a un evento.

SecureStat® Access

Gestione remotamente los sistemas de control de acceso.

SecureStat® Alarm

Gestione remotamente los sistemas de detección de intrusiones.

1 Resumen ejecutivo

En el horizonte de la industria de la seguridad en 2026

Las principales tendencias, desafíos y oportunidades que enfrentan los profesionales de la seguridad en 2026 y en adelante.

Acerca del informe

Elaborado por profesionales de la seguridad para profesionales de la seguridad, el Informe de Perspectivas Tecnológicas Globales 2026 combina un conjunto exclusivo de fuentes de datos con una profunda experiencia en el sector, extrayendo información práctica sobre tecnologías, estrategias e innovaciones que influyen en el mercado de la seguridad comercial, tanto en la actualidad como en el futuro.

Estas fuentes de datos y experiencia incluyen:

Encuesta de Mercado: Una encuesta de mercado externa encargada por Securitas Technology, con 575 respuestas de profesionales de la seguridad verificados en Estados Unidos, Francia, Reino Unido, Alemania, Suecia y Australia. La encuesta, dirigida a responsables de la toma de decisiones en tecnología de seguridad electrónica y profesionales con participación directa en inversiones tecnológicas, se centró en el uso actual de la tecnología, su adopción futura y la inversión prevista.

Encuesta a Clientes y Comentarios del Consejo Asesor de 2024: Un proceso de encuesta gestionado por Securitas Technology con respuestas de más de 4500 clientes en 17 países. La Encuesta Global a Clientes 2024 incluyó preguntas relacionadas con la adopción e inversión previstas en tecnología de seguridad. También se recopilaron perspectivas de los miembros del Consejo Asesor de Clientes de Securitas Technology, un grupo diverso de clientes que proporcionan a Securitas Technology retroalimentación sobre sus desafíos y necesidades en tecnología de seguridad, representando a diferentes industrias.

Proceso de Consulta con Socios Tecnológicos: Un proceso consultivo gestionado por Securitas Technology para recopilar datos de encuestas y perspectivas del sector de 24 socios tecnológicos estratégicos participantes. Estos socios incluyen a los principales fabricantes, desarrolladores, innovadores y tecnólogos de productos de seguridad del sector.

Expertos Internos en la Materia: Una serie de entrevistas e investigaciones internas realizadas para recopilar perspectivas de líderes tecnológicos internos y expertos en la materia de Securitas Technology a nivel mundial. Esto incluyó a miembros del equipo de Estrategia e Innovación de Securitas Technology, el Comité de Revisión Tecnológica Global (GTRC) y el Consejo Global de Innovación Tecnológica (GTIC).

Perspectivas para 2026: Lo que Observan los Profesionales de la Seguridad

Nuestro informe de 2025 destacó la creciente importancia de los datos en la seguridad electrónica y exploró cómo están transformando la industria, generando nuevo valor, pero también requiriendo nuevos conocimientos en tecnología de la nube, inteligencia artificial (IA), analítica, privacidad de datos y ciberseguridad.

Estas tendencias se han acelerado en el último año. A nivel mundial, el crecimiento explosivo en el desarrollo de modelos de IA y su uso en la vida diaria está impulsando fuertes inversiones para mejorar la conectividad de datos y la infraestructura de los centros de datos.

Si bien la tecnología de seguridad ha aprovechado la infraestructura de la nube, la analítica y la IA durante varios años, ahora vemos que los fabricantes y desarrolladores de seguridad están profundizando en las funciones de sus productos y soluciones, en áreas como video, detección de intrusiones, control de acceso y más.

Las perspectivas para 2026 muestran el protagonismo sostenido de tres tendencias clave en tecnología de seguridad que ya están teniendo un impacto transformador en la industria: IA, aplicaciones en la nube y sensores avanzados.

Una mayor sofisticación y disponibilidad de estas tecnologías conducirá a una mayor adopción, con un mayor enfoque en el aprovechamiento de los datos recopilados por los dispositivos y aplicaciones de seguridad para generar valor en otras áreas.

Los datos de la encuesta incluidos en este informe revelaron que una mayor seguridad de los empleados es el principal impulsor de las futuras inversiones en seguridad de las organizaciones. Además, el informe profundiza en varios desafíos empresariales crecientes que se prevé que sean prioritarios para los profesionales de la seguridad en 2026. Estos incluyen:

- **Proteger a las personas en entornos empresariales cada vez más volátiles**
- **Adoptar estrategias de gestión de incidentes proactivas y en tiempo real**
- **Impulsar el valor y el impacto organizacional mediante implementaciones de seguridad**

Estas tendencias, el ritmo cada vez más rápido de los cambios tecnológicos y el entorno de amenazas exigen que las organizaciones incorporen una evaluación tecnológica continua en sus programas de seguridad. Un enfoque gradual para la adopción de nuevas tecnologías, con el apoyo de un socio experimentado, puede ayudar a los profesionales de la seguridad a planificar eficazmente la integración fluida de la tecnología en el programa de seguridad de su organización.

Lo que es cierto es que quedarse inactivo no es una opción. Planificar con antelación es la mejor garantía contra tener que ponerse al día en el futuro.

Conclusiones clave

1

El panorama de la IA seguirá evolucionando, impulsado por el desarrollo de casos de uso de la IA generativa (GenAI), como la búsqueda en lenguaje natural, y el aumento de la potencia de procesamiento. La IA ayudará a transformar la integración de sistemas, combinando conjuntos de datos de sistemas dispares para generar seguridad e inteligencia empresarial integradas.

Leer más: Sección 2, página 22

2

La tecnología basada en la nube es la nueva normalidad y se convertirá en la base de muchas nuevas implementaciones de sistemas de seguridad. La migración de la infraestructura local a las configuraciones en la nube continuará, primero mediante un enfoque híbrido, a medida que las organizaciones buscan beneficios como la gestión centralizada y una mayor escalabilidad.

Leer más: Sección 2, página 26

3

La integración de sensores avanzados se expandirá gracias a la creciente compatibilidad con los sistemas de seguridad. Al aprovechar más datos de los sensores, las organizaciones buscarán garantizar el cumplimiento normativo, mejorar la eficiencia y optimizar las experiencias de clientes y empleados.

Leer más: Sección 2, página 30

4

El aumento de la tensión y la volatilidad globales son preocupaciones importantes para las organizaciones. Observamos la priorización de las tecnologías para ayudar a mejorar la seguridad de los empleados y las comunicaciones en caso de crisis, junto con estrategias para mejorar la inteligencia de riesgos, la preparación para emergencias y la recuperación ante desastres.

Leer más: Sección 3, página 36

5

La respuesta reactiva a incidentes está cambiando a la detección proactiva de amenazas. La integración de herramientas de gestión de alarmas con múltiples fuentes de datos y agentes virtuales de IA aumentará la automatización y la precisión, lo que ayudará a los agentes humanos a ser más eficientes y a anticipar mejor las amenazas.

Leer más: Sección 4, página 54

6

Las organizaciones ven el potencial de la tecnología de seguridad como un generador de valor. Desde la mejora de la experiencia de los empleados y clientes hasta el apoyo a los objetivos de sostenibilidad, la tecnología de seguridad está ganando reconocimiento en las juntas directivas como una herramienta para impulsar la eficiencia y ayudar a optimizar las operaciones comerciales de múltiples maneras.

Leer más: Sección 5, página 72

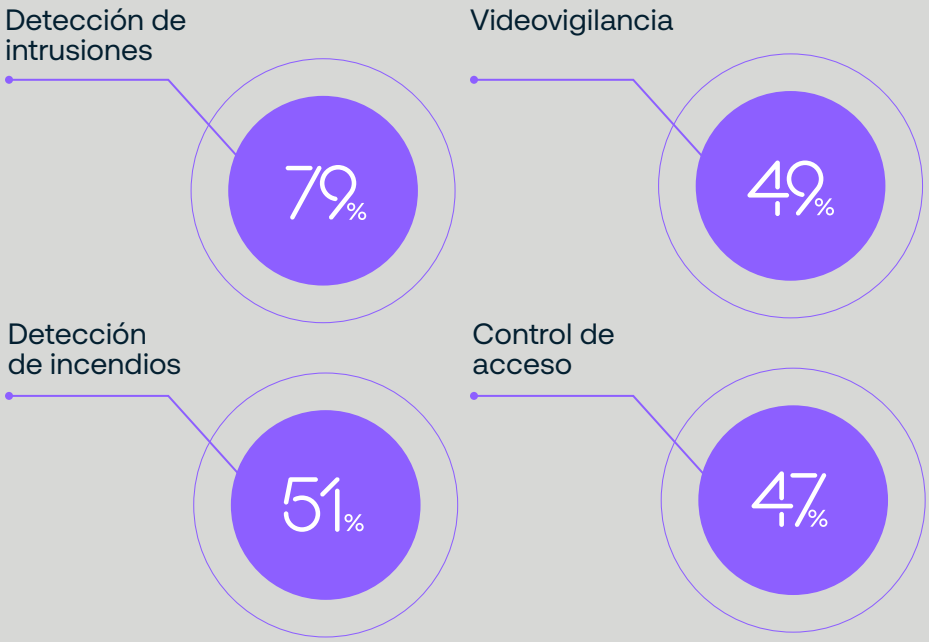
Tendencias e información de datos

Tendencias de los clientes

En diciembre de 2024, encuestamos a nuestros clientes sobre su uso actual de la tecnología y sus planes para su futura adopción.

Tecnologías más adoptadas[1]

Porcentaje que afirma utilizar actualmente:



1 Encuesta interna de marca a 4540 clientes de Securitas Technology en Australia, Bélgica, Canadá, Dinamarca, Finlandia, Francia, Alemania, Irlanda, México, Países Bajos, Noruega, España, Suecia, Suiza, Turquía, Reino Unido y Estados Unidos. Realizado en noviembre de 2024.

Tecnologías en tendencia[1]

	Actualmente se utilizan:	Planean adoptar en los próximos 12 a 18 meses:
1	**29%** Credenciales de teléfonos móviles	**30%** Inteligencia artificial
2	**28%** Soluciones y almacenamiento en la nube	**27%** Credenciales de teléfonos móviles
3	**26%** Gestión de visitantes	**25%** Gestión de visitantes
4	**11%** Inteligencia artificial	**24%** Análisis predictivo
5	**8%** Biometría sin contacto	**20%** Biometría sin contacto
6	**7%** Análisis predictivo	**20%** Soluciones y almacenamiento en la nube

Principales tecnologías basadas en suscripción[1]

	Actualmente se utilizan:	Plan de adopción en los próximos 12 a 18 meses:
1	**43%** Control de acceso gestionado y alojado	**27%** Verificación de alarmas por vídeo
2	**43%** Formación en preparación para incendios y emergencias	**20%** Vídeo gestionado y alojado
3	**39%** Vídeo gestionado y alojado	**16%** Portales de gestión de clientes en línea
4	**37%** Vigilancia de respuesta móvil	**15%** Formación en preparación para incendios y emergencias
5	**25%** Verificación de alarmas por vídeo	**15%** Control de acceso gestionado y alojado
6	**24%** Portales de gestión de clientes en línea	**11%** Vigilancia de respuesta móvil

Tendencias e información de datos

Tendencias del mercado

Realizamos una encuesta exhaustiva a profesionales de seguridad y prevención de pérdidas en varios mercados para identificar las tendencias clave y los casos de uso en tecnología de seguridad.

Adopción y planes de tecnología en la nube[2]

Los sistemas basados en la nube son ahora la regla.

Adopción de la nube en aumento

Uso de tecnología de seguridad electrónica basada en la nube en todas las organizaciones:

18%
Totalmente en la nube

34%
Prevén estar totalmente en nube dentro de 5 años

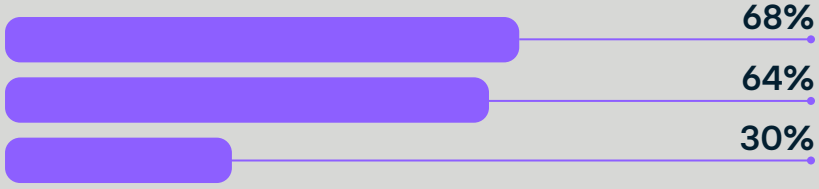
Aumento de la eficiencia impulsando la adopción de la nube

Razones para adoptar sistemas basados en la nube:

- #1 – Gestión de seguridad centralizada
- #2 – Mayor eficiencia
- #3 – Mayor facilidad de uso y gestión

Principales sistemas basados en la nube

Adopción de sistemas por parte de organizaciones que utilizan soluciones en la nube:



Participación en sostenibilidad[2]

Participa directamente en actividades de sostenibilidad

Considera la sostenibilidad importante o muy importante en la selección de tecnología

Adopción y planes de IA[2]

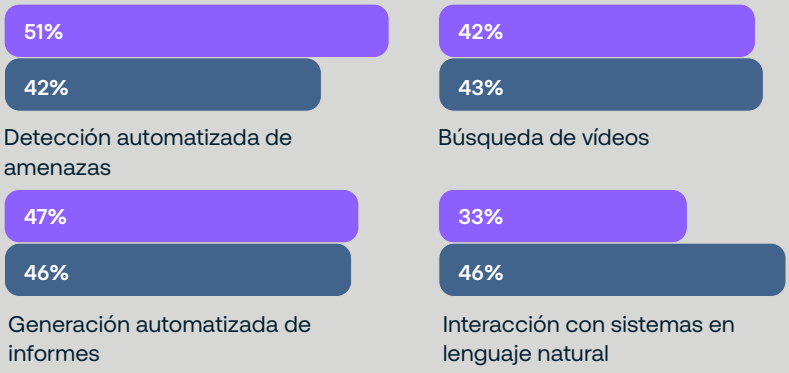
La IA es una parte integral de la tecnología de seguridad, con un gran interés en nuevos casos de uso.

Principales casos de uso actuales de IA

- 36% Reconocimiento de objetos
- 35% Detección de intrusiones y merodeo
- 27% Conteo de personas
- 26% Detección de anomalías
- 24% Detección, velocidad y dirección de vehículos

Principales casos de uso de GenAI del futuro

● "Definitivamente" o
● "Algo" interesado:



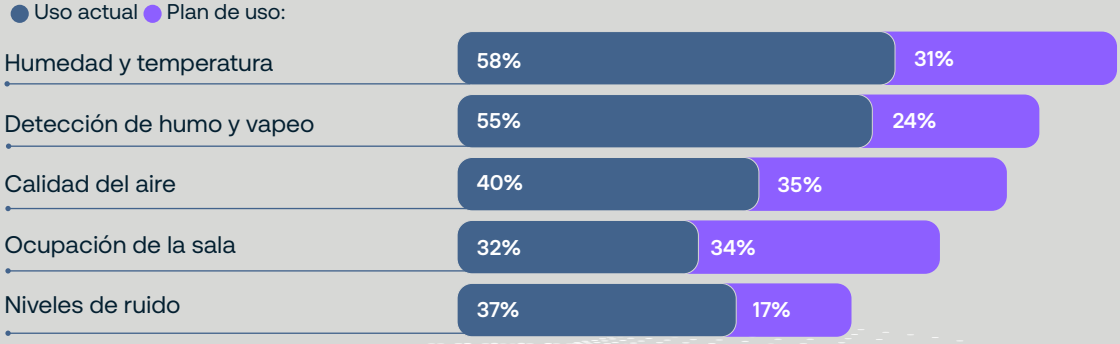
Adopción y planes de tecnología de sensores avanzados[2]

Los sensores avanzados se utilizan ampliamente en seguridad, y la mayoría de las organizaciones buscan expandirse aún más.

Adopción de sensores avanzados en seguridad

- 9% Uso extensivo
- 39% Uso parcial
- 35% Planificación de implementación
- 16% Sin uso

Principales casos de uso de sensores avanzados



[2]Encuesta ciega de terceros a 575 profesionales de seguridad y prevención de pérdidas con autoridad para la toma de decisiones sobre tecnología de seguridad en Australia, Francia, Alemania, Suecia, Reino Unido y Estados Unidos. Realizada en febrero y marzo de 2025.

Perspectivas de los Socios

Encuestamos a nuestros socios tecnológicos estratégicos para conocer su perspectiva sobre la dirección de la tecnología de seguridad y sus planes de innovación.

50% calificó la IA como la principal tendencia en la industria.

3 Principales Tendencias en Tecnología de Seguridad

1

Aplicaciones de IA

"Todos, desde el CSO y el CEO hasta el nivel inferior, intentan identificar cómo su organización puede usar la IA para aprovechar las cámaras que ya tienen."

Hanwha Vision

"Agentics: Agentes de IA como sistemas autónomos capaces de comprender contextos, tomar decisiones y actuar de forma independiente."

milestone

2

Tecnología en la Nube

"Hay un aumento masivo en el interés por las soluciones en la nube que permiten el uso de modelos de IA Generativa para buscar videos grabados."

VERINT

"Prevemos que las pequeñas y medianas empresas, así como las empresas distribuidas, serán las que adopten la tecnología más rápidamente."

MOTOROLA SOLUTIONS

3

Integración de Sistemas

"Modernizar los sistemas de seguridad también libera el valor de la centralización, integrando varios componentes en una sola plataforma."

brivo
simply better security

Las nuevas integraciones en el mercado simplifican la implementación del software de monitoreo de la estación central, lo que facilita la instalación de un VMS multisitio.

EAGLE EYE NETWORKS

Pasos para impulsar la sostenibilidad

1

Diseño del producto

La sostenibilidad guía nuestro proceso de diseño, garantizando longevidad, eficiencia y reciclabilidad, lo que le ayuda a reducir su huella de carbono.

resideo

Nuestro conjunto de herramientas de desarrollo se centra en ocho áreas: materias primas, agua, material virgen, reutilización al final de su vida útil, reciclabilidad, consumo de energía durante su vida útil, huella de carbono y coste financiero.

ASSA ABLOY
Opening Solutions

2

Consumo de energía del equipo

Estamos desarrollando sistemas de vigilancia energéticamente eficientes que reducen el consumo de energía y la huella de carbono.

MARCH networks
A Delta Group Company

Un área clave es nuestro apoyo a arquitecturas híbridas y basadas en la nube, que permiten a las organizaciones optimizar su huella de hardware, reducir el consumo de energía y escalar de forma más eficiente.

INTELLICENE
UNIFYING SECURITY. ENABLING ACTION

3

Prácticas operativas

Nos hemos fijado el objetivo de minimizar el uso de agua en nuestra fabricación y seleccionar únicamente materiales clasificados como seguros, eliminando así los materiales peligrosos.

AXIS COMMUNICATIONS

IDIS América se compromete a impulsar la sostenibilidad en la tecnología de seguridad con productos duraderos que minimizan el desperdicio y reducen la necesidad de reemplazos frecuentes.

IDIS One Solution. One Company.

Principales Prioridades de Desarrollo de Productos

1

Integración de IA y Analítica

"Análisis impulsado por IA para proporcionar detección de incidentes en tiempo real, reconocimiento de anomalías y mitigación proactiva de amenazas."

MARCH networks
A Delta Group Company

"Uso de IA para mejorar la experiencia del usuario, la velocidad y la escalabilidad de las operaciones."

VIAKOO

2

Soluciones en la Nube

"Soluciones basadas en la nube para permitir mayor escalabilidad, flexibilidad y administración remota."

MOTOROLA SOLUTIONS

"Soluciones de nube y movilidad de nivel empresarial."

Honeywell

3

Integración e Interoperabilidad

"Modernizar los sistemas de seguridad también aprovecha el valor de la centralización, integrando varios componentes en una sola plataforma."

Software House C•CURE IQ

"API más abiertas en el ecosistema DMP para una mayor compatibilidad con sistemas dispares."

DMP

4

Mejoras en la Experiencia del Usuario y la Interfaz

"Simplificar la visualización y el análisis de datos de eventos para ayudar a identificar anomalías, detectar tendencias o patrones y correlacionar eventos."

OpenEye

"Aplicaciones modulares, diseñadas específicamente para dispositivos móviles que resuelven los problemas de los clientes."

AMAG TECHNOLOGY
An Allied Universal Company

5

Sostenibilidad y Eficiencia

"Un fuerte énfasis en soluciones energéticamente eficientes y respetuosas con el medio ambiente."

SONITROL

"Obtener más materias primas y componentes cerca de su lugar de producción... nos permite alcanzar nuestros objetivos de reducción de emisiones de carbono."

ASSA ABLOY
Opening Solutions

> "Estas perspectivas de nuestros socios estratégicos líderes en la industria provienen directamente de la vanguardia de la innovación en seguridad global, ofreciendo a nuestros clientes la perspectiva de un desarrollador tecnológico sobre el futuro."

Doug Walsh | Vicepresidente Global de Estrategia Tecnológica de Securitas Technology

2

Tendencias tecnológicas a tener en cuenta **en 2026**

El rápido ritmo de innovación en inteligencia artificial (IA), computación en la nube y sensores avanzados está teniendo un profundo impacto en la tecnología de seguridad, no solo en las tecnologías en sí, sino también en las estrategias de implementación, mantenimiento y uso.

En todo el mundo, la creciente accesibilidad a estas tecnologías innovadoras está transformando nuestra forma de vivir, trabajar y progresar. Para la industria de la seguridad, las oportunidades son inmensas. Los principales fabricantes, desarrolladores de software e innovadores del mundo están adoptando estas tecnologías para crear nuevas funciones mejoradas en videovigilancia, detección de intrusiones, control de acceso y más.

Para los profesionales de la seguridad, esto significa mayor integración, mayor protección y una gestión de la seguridad más eficiente.

La IA lo está acelerando todo

Hoy en día, el uso de la IA se ha generalizado, pero sus capacidades transformadoras siguen impulsando el sector tecnológico global. La inversión sustancial en liberar el inmenso potencial de la IA está permitiendo el rápido desarrollo de capacidades previamente inimaginables que no solo la mantienen en los titulares, sino que impactan prácticamente en todos los sectores de la economía y la sociedad.

La IA tampoco es nueva en la tecnología de seguridad. De hecho, lleva tiempo encontrando aplicaciones en seguridad, ya sea en aprendizaje automático y análisis de datos en soluciones de videovigilancia y detección de amenazas, o en casos de uso impulsados por IA para el reconocimiento de matrículas, la gestión de ocupación, el reconocimiento facial, la detección y el seguimiento de objetos, entre otros.

Estas y otras aplicaciones de la IA se sofisticarán y alcanzarán un mayor alcance, y nuestro estudio de mercado muestra que la IA se considera ahora una tecnología clave en el sector de la seguridad.

Según nuestro estudio de mercado, el 70 % de las organizaciones ya están aprovechando la IA en sus programas de seguridad.[1]

> La IA y los agentes de IA, en particular, están transformando la industria de la seguridad con aplicaciones en control de acceso, gestión de identidades y plataformas de gestión de seguridad, al ofrecer mayor eficiencia y una toma de decisiones basada en datos.
>
> **HID**

Surge una nueva generación de IA

AI entrar en 2026, la IA está superando la fase de aprendizaje automático (ML) para permitir una mayor automatización y generación de información. Aquí es donde entra en juego la IA generativa (GenAI).

Según nuestro estudio de mercado, la mayoría de las organizaciones en todos los mercados están interesadas en los casos de uso de GenAI.

Un estudio reciente de McKinsey2 también muestra que GenAI es una tecnología muy accesible, con la mayoría de los usuarios en roles no técnicos. Esto tiene un gran potencial para la industria de la seguridad.

Una aplicación inmediata que ofrece mayor eficiencia y seguridad es la detección de anomalías (o excepciones). Esta tecnología está evolucionando de la programación basada en reglas al aprendizaje profundo, aprovechando GenAI. En videovigilancia, los algoritmos GenAI pueden implementarse para comprender una escena “normal” e identificar variaciones específicas que contextualizan lo que sucede en tiempo real; por ejemplo, una persona con ropa oscura entra en una zona restringida. Estos algoritmos pueden ser ajustados sin conexión por agentes humanos y luego reimplementados en una o varias cámaras con capacidades edge. Una evolución similar se está produciendo con la detección de audio. La capacidad de detectar audio anormal existe desde hace algunos años; ahora es posible que los agentes virtuales de IA identifiquen la anomalía (un coche, un equipo, etc.), proporcionando a los agentes humanos información procesable de inmediato.

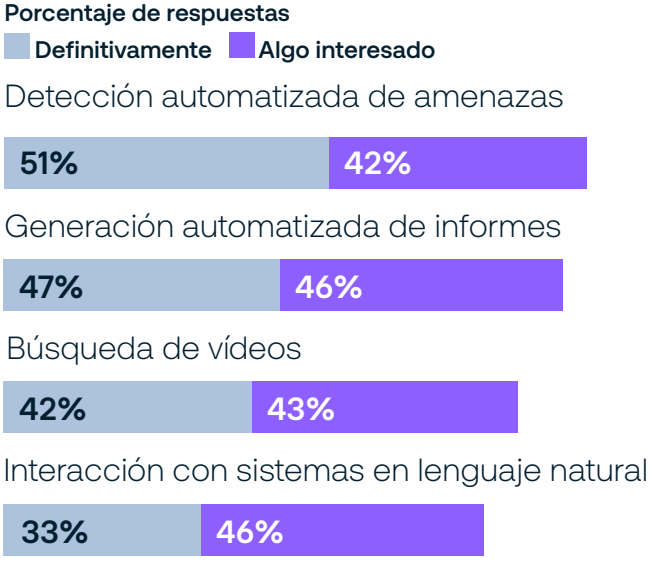
Impacto de la IA en las aplicaciones de seguridad

Incluso los casos de uso de seguridad consolidados se están viendo mejorados por la IA. Por ejemplo, la tecnología de reconocimiento facial para el control de acceso biométrico existe desde hace muchos años; sin embargo, la IA mejora la precisión y la fiabilidad de la autenticación al observar y aprender continuamente los cambios en la apariencia de las personas.

El mismo efecto se observa en la gestión integrada de la seguridad. La capacidad de la IA para integrar y analizar datos de múltiples fuentes permite reconocer tendencias o patrones en los datos que podrían señalar un posible problema. Como ejemplo general, la IA puede sugerir que las falsas alarmas ocurren con mayor frecuencia en un día determinado de la semana y a una hora específica. O, en el sector minorista, identificar transacciones inusuales en el punto de venta durante el turno de un empleado. Estos ejemplos proporcionan a los responsables de seguridad datos reales para abordar diversos desafíos, desde la gestión de falsas alarmas hasta la prevención de robos internos.

Si bien la IA está abriendo nuevas y emocionantes oportunidades para los profesionales de la seguridad, y su importancia sin duda aumentará con el tiempo, todas las organizaciones deben elegir cuidadosamente los casos de uso de la IA al buscar maneras de mejorar la seguridad y el valor comercial. También será importante estar al tanto de la evolución de los requisitos éticos y regulatorios relacionados con la IA.

Las organizaciones están preparadas para GenAI[1]



[1]Encuesta ciega de terceros a 575 profesionales de seguridad con autoridad para la toma de decisiones en tecnología de seguridad en Australia, Francia, Alemania, Suecia, Reino Unido y Estados Unidos. Realizada en febrero y marzo de 2025.

[2]“El lado humano de la IA generativa: Creando un camino hacia la productividad”. McKinsey Quarterly, 18 de marzo de 2024. https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-human-side-of-generative-ai-creating-a-path-to-productivity

Perspectivas de los socios

Avanzando en inteligencia artificial

No es una afirmación arriesgada predecir que la IA seguirá transformando la seguridad y la vigilancia. La tecnología de IA ya es un elemento vital en las estrategias de vigilancia de muchas organizaciones. La combinación de IA con análisis de audio y video integrados permite una detección y clasificación de objetos altamente precisa con menos falsas alarmas, además de ayudar a los clientes a recibir datos útiles que pueden impulsar la monitorización inteligente, mejorar la eficiencia operativa y generar información empresarial basada en datos.

Pero ahora que la IA ha dejado de ser una tecnología emergente, la pregunta que nuestra industria debe plantearse es: "¿Cómo podemos usar la IA de nuevas maneras para ir más allá de la seguridad e influir en el futuro de nuestra organización?".

La pregunta que nuestra industria debe plantearse es: "¿Cómo podemos usar la IA de nuevas maneras para ir más allá de la seguridad e influir en el futuro de nuestra organización?".

Seguiremos viendo surgir plataformas abiertas y modelos de IA generativa, que admiten capacidades más granulares, como la capacidad de "hablar" con un dispositivo y decirle: "Detecta al hombre de la camisa roja entre la 1:00 y las 2:00 a. m. en la cámara del vestíbulo". Además, es probable que el mercado del video esté creciendo con más fuerza que otras categorías de seguridad. Un factor importante es el avance de la tecnología de IA, que está impulsando a los fabricantes a replantear su ruta de acción para la inclusión de la IA en la mayoría de sus líneas de productos.

Nuestra industria debe unirse y crear directrices y estándares de referencia en torno a la IA, determinando qué nivel de precisión es generalmente aceptable para la mayoría de las aplicaciones de seguridad y vigilancia. Es beneficioso para todos (usuarios finales, distribuidores y fabricantes) cumplir con un estándar. Tenemos especificaciones y estándares para cámaras. No hay razón para no tener un estándar para la precisión de la IA.

La combinación de IA y análisis inteligente permite a los profesionales de la seguridad diseñar y construir entornos de vigilancia más seguros y eficientes, especialmente a medida que las tecnologías inteligentes integrales basadas en IA continúan evolucionando hacia soluciones empresariales integrales.

Perspectivas de los socios

Honeywell

Aplicaciones de IA en el control de acceso

Varios sectores verticales lideran la adopción de sistemas de seguridad basados en IA, en respuesta a las necesidades específicas de cada sector y a los avances tecnológicos. La atención médica, el comercio minorista, la manufactura y los centros de datos se encuentran entre los sectores donde observamos la integración más rápida de soluciones de IA para la seguridad.

Por ejemplo, hospitales e instalaciones médicas utilizan sistemas de seguridad basados en IA para mejorar la seguridad de los pacientes y supervisar mejor el acceso a las instalaciones. En los centros de datos se utilizan sistemas de mantenimiento predictivo y monitorización de seguridad basados en IA, así como controles de acceso electrónicos, biometría y cámaras de seguridad con IA para ayudar a mantener la seguridad en las instalaciones físicas.

Hemos observado una mayor sofisticación en las soluciones basadas en IA para mejorar la monitorización de la seguridad y la respuesta a incidentes. En nuestra reciente encuesta*, la seguridad y la protección de los ocupantes es uno de los principales casos de uso de la IA en los edificios actuales.

Más del 60% implementa IA para monitorear comportamientos inusuales, más de la mitad la utiliza para el rastreo de ubicación y el 45% menciona el uso de sistemas de control de acceso basados en biometría.

Adopción de casos de uso de IA por parte de las organizaciones para la seguridad de edificios*

Comportamiento inusual: → más del **60%+**

Rastreo de ubicación: → más del **50%+**

Control de acceso basado en biometría: → **45%**

Además, la IA puede utilizarse para agregar y extraer datos de diversas fuentes, como eventos de acceso, eventos visuales y alarmas.

La IA puede utilizarse para encontrar relaciones no obvias que predigan posibles vulnerabilidades de seguridad, permitiendo a los profesionales de seguridad ser más proactivos y preventivos.

De esta manera, la IA ayuda a los equipos de seguridad a anticiparse al cambiante panorama de amenazas. De igual manera, las vulnerabilidades del sistema pueden detectarse y mitigarse para evitar interrupciones mediante la gestión automatizada de parches.

Honeywell encargó a Wakefield Research la Encuesta de Investigación de Administradores de Edificios de Honeywell, en la que se encuestó a 250 administradores de edificios y altos responsables de la toma de decisiones de EE. UU. de diversos tipos de edificios, como oficinas, hospitales, aeropuertos, escuelas, universidades, hoteles y centros de datos. Para participar en la investigación, los encuestados debían utilizar sistemas de gestión de propiedades con IA en edificios con más de 250 ocupantes.

•mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-human-side-of-generative-ai-creating-a-path-to-productivity

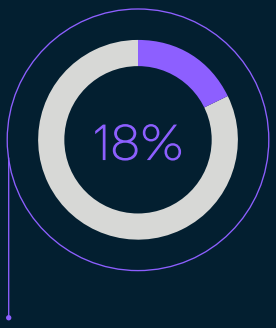
Aplicaciones en la nube: la nueva normalidad

La industria de la seguridad electrónica ha obtenido importantes beneficios en los últimos años gracias al rápido auge de las soluciones basadas en la nube: escalabilidad, implementación más sencilla, mantenimiento más sencillo y ciberseguridad. El crecimiento global de la infraestructura de los centros de datos también implica que las soluciones ahora son ampliamente aplicables a organizaciones de todo tipo y para diversos casos de uso de seguridad.

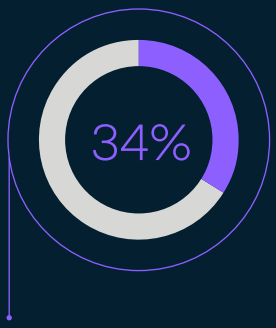
Podemos afirmar con certeza que la tecnología de seguridad basada en la nube está plenamente desarrollada y ya forma parte de los planes futuros de muchas organizaciones. **Según nuestro estudio de mercado, el 18 % de las organizaciones ya están completamente basadas en la nube.**

La adopción de la nube sigue en aumento[1]

Uso de tecnología de seguridad electrónica basada en la nube en todas las organizaciones:



está completamente basada en la nube actualmente



prevé estar completamente basada en la nube dentro de 5 años

[1]Encuesta ciega de terceros a 575 profesionales de seguridad con autoridad para la toma de decisiones en tecnología de seguridad en Australia, Francia, Alemania, Suecia, Reino Unido y Estados Unidos. Realizada en febrero y marzo de 2025.

La demanda impulsa la eficiencia de datos y costos

Las verdaderas soluciones en la nube a nivel empresarial ya están aquí, y nuestros socios tecnológicos estratégicos están realizando importantes inversiones en su infraestructura de datos en la nube, igualando la sofisticación de otros sectores tecnológicos. Esto significa que incluso las organizaciones que gestionan la tecnología de seguridad a nivel global pueden aprovechar la nube como opción predeterminada para sus aplicaciones de seguridad física, con una nube privada como opción. Además, cada vez hay más aplicaciones de seguridad disponibles en la nube: videovigilancia, control de acceso, intrusión y otras.

Además, cada vez hay más aplicaciones de seguridad disponibles en la nube: videovigilancia, control de acceso, intrusión y otras.

A medida que aumenta la demanda de datos junto con la inversión en la nube, el coste del ancho de banda para el almacenamiento y procesamiento de datos comienza a disminuir. Paralelamente, esto allana el camino para la innovación en áreas como la videovigilancia, una de las tecnologías que más datos consume. Los fabricantes de cámaras se están centrando en algoritmos de compresión de vídeo mejorados. Al reducir significativamente la tasa de bits de vídeo y los costes de almacenamiento, estos avances ayudarán a acelerar la adopción de plataformas de vídeo alojadas en la nube e impulsadas por IA.

Nube híbrida: un trampolín sólido

A medida que las soluciones en la nube se generalizan, un enfoque híbrido ofrece un trampolín sólido para las organizaciones en su transición hacia una tecnología de seguridad totalmente basada en la nube. Estas organizaciones pueden ampliar progresivamente sus sistemas en la nube mientras continúan utilizando sistemas locales hasta el final de su ciclo de vida o porque algunas aplicaciones y entornos lo requieren.

Sin embargo, observamos una mayor concienciación entre las organizaciones sobre la carga de mantenimiento y el cumplimiento normativo que conlleva la gestión de una infraestructura local. Al incluir estos costos en su totalidad, el costo total de propiedad de las soluciones en la nube se vuelve mucho más atractivo.

> “La tecnología en la nube permite a las organizaciones gestionar la seguridad de forma remota, escalar su infraestructura según sea necesario e integrar múltiples funciones de seguridad en una única plataforma.”
>
> 3xLOGIC

Nuestro estudio de mercado revela que los factores clave que impulsan la adopción de la nube son la facilidad de mantenimiento, la gestión centralizada, la reducción de los costos operativos y el aumento de la eficiencia. Estos son beneficios convincentes que son difíciles de ignorar.

Para quienes adoptan la nube tardíamente, la buena noticia es que existe un sólido conjunto de buenas prácticas para las soluciones en la nube que ayudan a garantizar la seguridad de los datos, la protección adecuada de la información personal identificable (PII) y la resiliencia del sistema. Como ocurre en Securitas Technology, los integradores de seguridad desempeñarán un papel importante a la hora de ayudar a las organizaciones a crear un plan claro para la adopción de la tecnología basada en la nube, ya que cada empresa debe considerar sus propios requisitos para lograr una transición fluida.

Si bien algunas organizaciones optarán por mantener la tecnología local y muchas optarán por la vía híbrida, la tendencia es clara. Las tecnologías en la nube serán fundamentales para la futura evolución de la seguridad.

Perspectivas de los socios

El camino hacia los sistemas de seguridad en la nube

Las organizaciones están migrando rápidamente sus sistemas a la nube por una buena razón. Las tecnologías de seguridad en la nube ofrecen acceso y gestión remotos, lo que permite a las empresas supervisar y controlar las instalaciones desde cualquier lugar.

Escalar y conectar nuevas tecnologías es más sencillo con las soluciones nativas de la nube, y las empresas pueden reducir los gastos relacionados con servidores locales, mantenimiento y soporte de TI, lo que permite a los equipos centrarse en las prioridades principales del negocio en lugar del mantenimiento del sistema.

A pesar de las claras ventajas, la migración sigue siendo un obstáculo para muchas organizaciones. Les preocupan sus inversiones en hardware: ¿qué ocurre con los paneles de control locales y los dispositivos posteriores? Productos como Brivo Mercury abordan estas preocupaciones al migrar de forma sencilla y económica los paneles de control Mercury existentes para que funcionen en la nube, con mínimas interrupciones.

> Las soluciones VMS híbridas están diseñadas con medidas de ciberseguridad integradas, lo que garantiza el cumplimiento normativo, la resiliencia y la protección de datos.

Este enfoque elimina la necesidad de costosas actualizaciones de "desinstalación y reemplazo", a la vez que ofrece las ventajas de la nube y un sistema de seguridad moderno.

La modernización de los sistemas de seguridad también aprovecha el valor de la centralización, integrando diversos componentes en una sola plataforma. Por ejemplo, una plataforma de seguridad unificada, como Brivo Security Suite, integra el control de acceso, la inteligencia de video, la gestión de visitantes y la detección de intrusiones en un único panel.

Una plataforma centralizada en la nube funciona como un único destino para todas las necesidades de seguridad, proporcionando la codiciada vista panorámica de cada ubicación. Esto reduce la necesidad de gestionar múltiples plataformas y herramientas de seguridad, a la vez que refuerza la ciberseguridad. Además, con la seguridad en la nube, obtiene acceso a métricas e información de seguridad en tiempo real integradas e integradas en sus sistemas empresariales para tomar decisiones empresariales más rápidas e informadas.

Perspectivas de los socios

milestone

El futuro de la videovigilancia: Los sistemas VMS híbridos impulsan la escalabilidad y la flexibilidad

En el panorama tecnológico actual, en rápida evolución, las empresas buscan soluciones de vigilancia que ofrezcan escalabilidad y flexibilidad.

Los sistemas de gestión de video (VMS) híbridos representan un avance en la videovigilancia, ya que combinan las mejores implementaciones en la nube y locales para satisfacer diversas necesidades.

Las soluciones VMS híbridas, como la combinación de **XProtect y Arcules de Milestone**, ofrecen una escalabilidad inigualable al aprovechar la infraestructura en la nube. Esto permite a las empresas ampliar sus capacidades de videovigilancia sin problemas, adaptándose a las mayores necesidades de almacenamiento y procesamiento de datos a medida que las organizaciones crecen.

La flexibilidad es otra ventaja. Las empresas pueden adaptar su vigilancia a sus necesidades específicas con diversas opciones de implementación en la nube, incluyendo la nube pura, la nube perimetral y la integración de cámara a nube con los sistemas locales. Los VMS híbridos ofrecen la libertad de adaptarse y evolucionar, tanto si se requiere una seguridad robusta como agilidad en la nube.

Además, las soluciones VMS híbridas están diseñadas con medidas de ciberseguridad integradas, lo que garantiza el cumplimiento normativo, la resiliencia y la protección de datos. Este enfoque de seguridad por diseño proporciona tranquilidad, protegiendo los datos de vídeo contra posibles amenazas.

La integración de sistemas en la nube y locales también mejora la inteligencia empresarial. Aproveche los datos de video, junto con la analítica avanzada y la IA de Arcules, y tome decisiones más rápidas e informadas, mejorando la seguridad y la eficiencia operativa. Esta capacidad de adaptación al futuro garantiza que los sistemas de vigilancia sigan siendo relevantes y eficaces ante las demandas cambiantes.

En conclusión, la escalabilidad y la flexibilidad de los VMS híbridos revolucionan la industria de la videovigilancia. Soluciones como XProtect de Milestone y Arcules allanan el camino hacia un futuro adaptable y resiliente al ofrecer libertad de implementación, seguridad robusta e inteligencia empresarial mejorada.

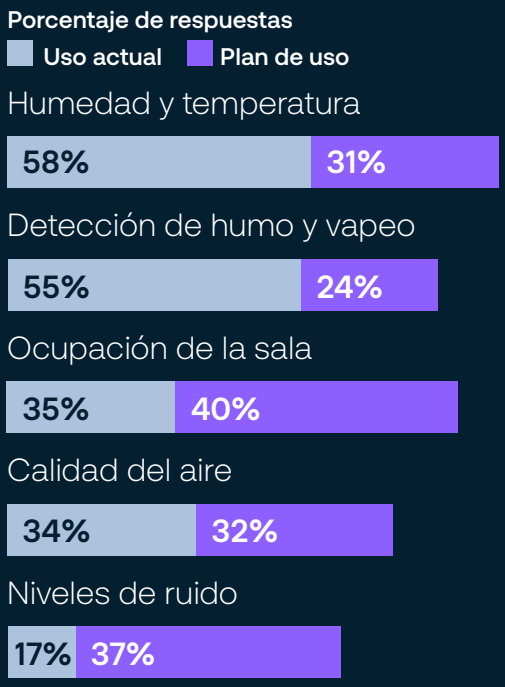
Las aplicaciones avanzadas de sensores están en evolución

El potencial de los sensores avanzados y otros dispositivos conectados (a veces denominados Internet de las cosas o IoT) ha sido un tema muy debatido en la industria de la seguridad durante muchos años.
De hecho, los dispositivos discretos para detectar inundaciones, condiciones de temperatura y luz, calidad del aire, sonido, tabaquismo y vapeo están bien establecidos.

Nuestra encuesta revela que el 48% de las organizaciones han integrado sensores avanzados en sus sistemas de seguridad.[1]

Sin embargo, la industria ha tenido dificultades para ofrecer valor más allá de la simple aplicación de enviar una alerta para mejorar la seguridad o la eficiencia operativa. Ahora, esto está empezando a cambiar.

Monitoreo para más[1]



[1]Encuesta ciega de terceros a 575 profesionales de seguridad con autoridad para la toma de decisiones en tecnología de seguridad en Australia, Francia, Alemania, Suecia, Reino Unido y Estados Unidos. Realizada en febrero y marzo de 2025.

Cámaras de vigilancia: Transformación en Multisensores

Gracias a los avances en IA y análisis de datos, ahora es posible realizar diversas formas de monitorización ambiental de forma proactiva sin necesidad de un sensor independiente. La innovación en tecnología de videovigilancia es un excelente ejemplo de ello. Las cámaras que aprovechan las capacidades de IA, ya sea integradas en el dispositivo (“en el borde”) o conectadas a software de análisis de vídeo, se utilizan como dispositivos multisensor.

Al monitorizar una escena a lo largo del tiempo, los algoritmos de IA pueden ayudar a identificar anomalías; no solo amenazas a la seguridad, sino también cambios ambientales inesperados, como humo, fuego, animales, multitudes e incluso disparos. El uso de sistemas de vídeo como multisensores inteligentes puede ayudar a automatizar la respuesta al proporcionar información precisa a un agente humano.

Desbloqueo de Valor Empresarial mediante la Integración de Sensores

La seguridad y la monitorización ambiental no se limitan a la gestión de amenazas externas. También se puede obtener valor aprovechando los datos capturados mediante la integración de sensores con sistemas de seguridad para optimizar la salud, la seguridad y las operaciones comerciales.

En el sector minorista, los sensores de seguridad y ambientales pueden combinarse para revelar información clave sobre el comportamiento del cliente, desde el seguimiento de la ocupación de las salas hasta el mapeo de la afluencia de clientes; datos valiosos que pueden respaldar futuras estrategias de marketing.

Nuestro estudio de mercado también reveló que más de un tercio (37%) de las organizaciones planean utilizar sensores para monitorizar los niveles de ruido[1]. .Esta aplicación es relevante en muchos sectores donde el ruido puede tener un impacto negativo en empleados y clientes.

En la industria manufacturera, por ejemplo, los sensores pueden ayudar a proteger a los trabajadores del ruido excesivo de la maquinaria industrial. La industria manufacturera también es un buen candidato para la monitorización de la humedad y la temperatura (proporcionada por sensores ambientales, cámaras térmicas y análisis de vídeo) para ayudar a los supervisores de producción a detectar con antelación el sobrecalentamiento de la maquinaria.

Compatibilidad vs. Ciberseguridad

La creciente compatibilidad seguirá impulsando la integración de sensores en las plataformas de seguridad electrónica, una tendencia que permitirá a las organizaciones crear ecosistemas más conectados para la monitorización de su entorno empresarial.

Sin embargo, al considerar qué sensores ambientales o de otro tipo integrar con las redes de seguridad privadas, las organizaciones deben colaborar estrechamente con su proveedor de tecnología de seguridad para evaluar a los proveedores de productos y garantizar que sus dispositivos cumplan con los estándares requeridos de calidad, soporte y ciberseguridad.

Perspectivas de los socios

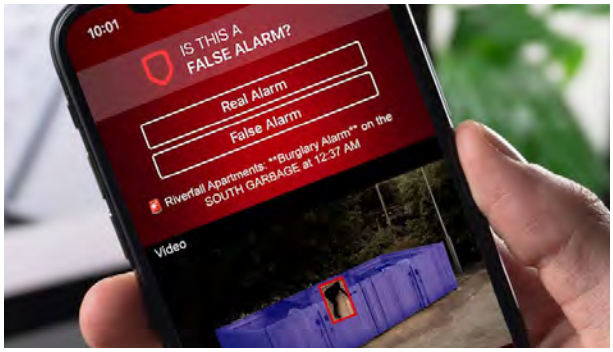
Convierta las cámaras en potentes dispositivos de detección de alarmas

La rápida evolución del software de análisis permite incorporar análisis avanzados a las cámaras de videovigilancia existentes.

Soluciones como las puertas de enlace **XV de DMP** con AlarmVision® convierten las cámaras IP estándar en potentes dispositivos de detección de alarmas. Al mejorar la detección de movimiento con análisis e integrar a la perfección los eventos de vídeo con los paneles de alarma de intrusión, las organizaciones pueden mantenerse al tanto de los eventos mediante notificaciones instantáneas.

Reduzca las falsas alarmas

La comunicación directa entre la cámara y los paneles de intrusión convierte las cámaras en detectores de movimiento inteligentes capaces de activar acciones y alarmas. Mediante el análisis de video del evento, se determina el sujeto del movimiento antes de enviar la alarma, lo que permite a los usuarios finales verificar los videos y mejora la verificación de video del centro de monitoreo.



Reemplazo de haces

Instalar haces para la detección no solo requiere tiempo y recursos, sino que la solución en sí misma suele ser poco confiable y propensa a generar costosas falsas alarmas. Los sistemas de seguridad con cámaras en tándem no solo pueden reemplazar eficazmente los haces de detección, sino que superan con creces sus capacidades. Al integrar las cámaras con el panel de control del sistema de intrusión, las cámaras se convierten en potentes dispositivos de detección de alarmas con zonas específicas; en el caso de AlarmVision, se pueden personalizar hasta cuatro zonas para cada cámara.

Flexibilidad estacional

Otra ventaja es la flexibilidad para adaptarse a las actividades estacionales y a las necesidades cambiantes. En lugar de tener que visitar el sitio y contratar personal adicional para mover haces o cables, las zonas de las cámaras se pueden ajustar rápida y fácilmente. Los cambios estacionales en la actividad y el inventario pueden ser complicados, pero soluciones avanzadas como AlarmVision pueden simplificar enormemente la protección.

Perspectivas de los socios

resideo

Sensores de seguridad conectados: Revolucionando el panorama de la seguridad

En una era donde la tecnología inteligente transforma cada faceta de nuestras vidas, los sistemas de seguridad no son la excepción. Resideo está impulsando el sector de la seguridad con sus sensores de seguridad conectados ProSeries. Estos innovadores dispositivos están transformando la forma en que propietarios de viviendas, empresas y profesionales de la seguridad abordan la seguridad.

Los sensores ProSeries de Resideo integran tecnología de vanguardia para comunicarse fluidamente con el panel principal y los dispositivos móviles. Esta conectividad optimiza el rendimiento de los sensores, ofrece actualizaciones en tiempo real y funciones remotas, a la vez que proporciona a los usuarios un nivel de control sin precedentes sobre sus sistemas de seguridad.

> La conectividad mejora el rendimiento de los sensores, ofrece actualizaciones en tiempo real y capacidades remotas y al mismo tiempo proporciona a los usuarios un nivel de control sin precedentes sobre sus sistemas de seguridad.

Los sensores incluyen una gama de opciones, cada una equipada con funciones avanzadas como cifrado mejorado, reducción superior de falsas alarmas y actualizaciones OTA. Estos sensores se pueden conectar fácilmente a otros dispositivos inteligentes, creando un ecosistema totalmente integrado. Ya sea que el propietario de una vivienda o negocio reciba una alerta en el trabajo o supervise su propiedad a distancia, la tecnología conectada de Resideo permite un enfoque más proactivo y receptivo.

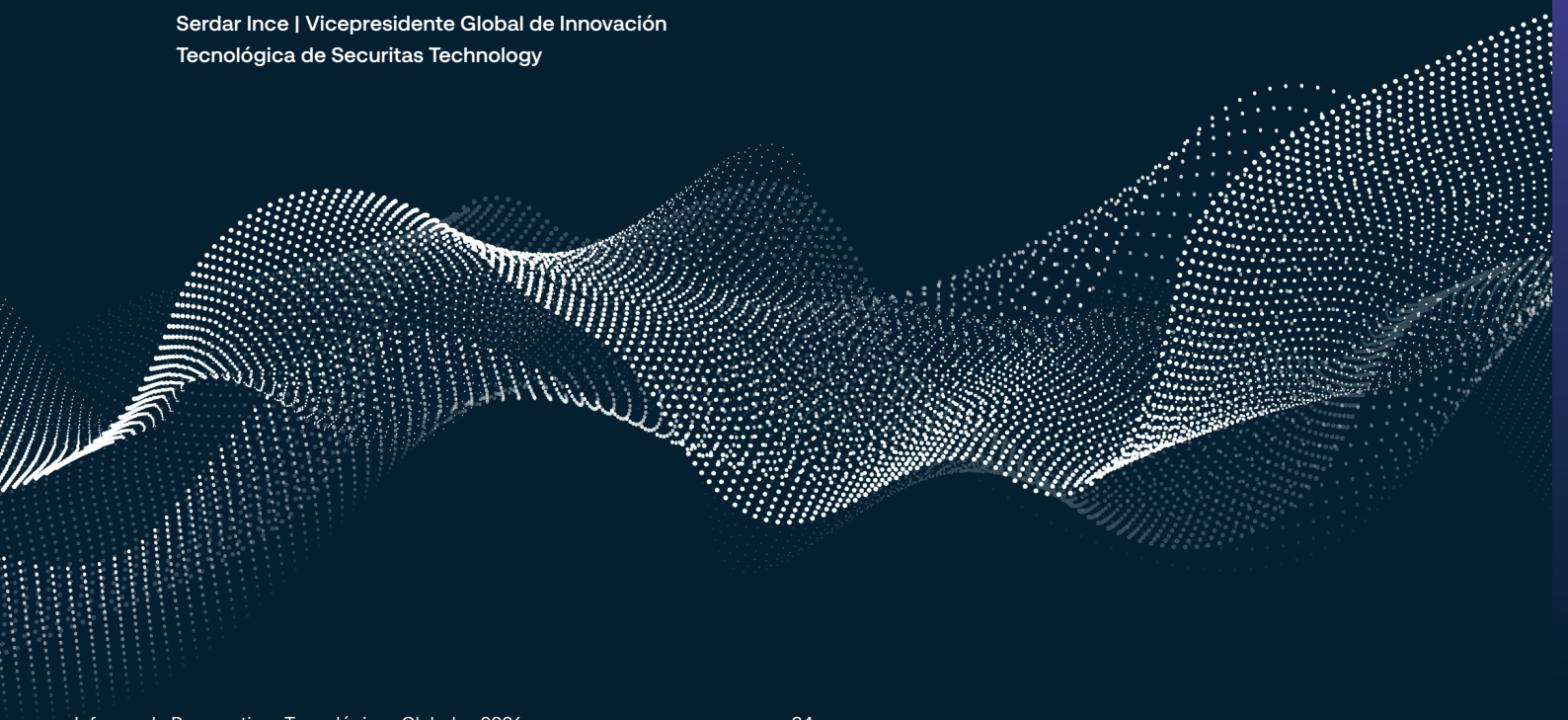
Además, el uso de tecnología basada en la nube en el sistema facilita la gestión y la resolución de problemas, reduciendo el tiempo de inactividad y mejorando la fiabilidad del sistema. Los continuos avances en la comunicación inalámbrica y el cifrado de datos también garantizan que los sensores ProSeries no solo sean eficientes, sino también seguros.

Al adoptar el Internet de las Cosas (IoT) y ofrecer soluciones flexibles y escalables, Resideo está ampliando los límites de lo posible en seguridad. Los sensores conectados ProSeries suponen un gran avance, ya que hacen que los sistemas de seguridad sean más inteligentes, fáciles de usar y mejor equipados para afrontar las cambiantes necesidades del mundo actual.

Plan de Acción para Profesionales de la Seguridad

> GenAI está preparada para transformar el análisis de vídeo. Permitirá a los clientes extraer contexto detallado y generar información instantánea. Al combinar esto con la tecnología en la nube, podemos procesar y gestionar todo de forma más eficiente. Y con la creciente compatibilidad de los sensores avanzados, podemos ampliar la seguridad a través de un ecosistema conectado que impulsa la eficiencia y la inteligencia empresarial.

Serdar Ince | Vicepresidente Global de Innovación Tecnológica de Securitas Technology



Inteligencia Artificial

1

Definir una Estrategia de Datos de IA

Identificar las fuentes de datos y los retos u oportunidades de seguridad que la IA puede ayudar a abordar. Ejemplos específicos pueden incluir la detección y el seguimiento de objetos, el reconocimiento de vehículos o la detección de anomalías. Establecer objetivos claros ayudará a garantizar que el uso de la IA sea intencionado y esté alineado con la estrategia general de seguridad de la organización.

2

Comprender los requisitos regulatorios, legales y éticos

Solicitar la orientación del equipo legal para garantizar que las aplicaciones de IA cumplan con las regulaciones y las leyes de privacidad de datos. Considerar las implicaciones éticas y establecer un proceso de gobernanza para el uso responsable. Esto ayudará a generar confianza y a proteger la información. Un comité de revisión de IA formal y multifuncional puede ayudar a las organizaciones a desarrollar directrices de IA claras y compatibles, y a garantizar su correcta implementación.

Aplicaciones en la nube

3

Desarrollar un modelo y una ruta de acción de migración a la nube

Desarrollar e implementar un modelo y una hoja de ruta de migración claros con hitos y plazos definidos para la transición de las operaciones de seguridad a la nube. Recurrir a un proveedor de tecnología de seguridad para identificar la combinación adecuada de soluciones y servicios basados en la nube para las futuras necesidades de seguridad.

4

Colaborar con equipos de TI especializados

Trabajar en conjunto con el departamento de TI para aprovechar sus conocimientos especializados y crear conjuntamente un plan para implementar un modelo de tecnología de seguridad basado en la nube. Esto incluirá la identificación de los requisitos de infraestructura, la consideración de los riesgos de ciberseguridad y la implementación de procesos de ciberseguridad.

Sensores avanzados

5

Establecer las necesidades de detección

Identificar las aplicaciones específicas de los sensores y las condiciones ambientales que respaldan los objetivos de seguridad y del negocio, como el cumplimiento normativo, la mejora de la eficiencia o la experiencia de los empleados y clientes. Posteriormente, colaborar con un socio tecnológico de seguridad para determinar el mejor enfoque para integrar los sensores avanzados con la infraestructura de tecnología de seguridad existente.

6

Validar la compatibilidad de proveedores y dispositivos

Evaluar exhaustivamente a los posibles proveedores y tecnologías para confirmar que cumplen con los estándares necesarios de calidad, cumplimiento normativo y ciberseguridad. Evaluar aspectos como la seguridad de los endpoints, las vulnerabilidades conocidas y las prácticas de almacenamiento de datos para garantizar una protección robusta y una integración fluida.

3 Soluciones de seguridad para un entorno volátil

La sociedad y los profesionales de la seguridad han estado respondiendo a un aumento en la volatilidad desde los trastornos de la pandemia de COVID-19.

Hoy en día, esta tendencia no muestra signos de desaceleración. En todo caso, la volatilidad, impulsada por la tensión geopolítica, la incertidumbre económica y las condiciones meteorológicas extremas, está aumentando en muchas partes del mundo. Los profesionales de la seguridad deben prepararse para una variedad de eventos de baja probabilidad, pero de gran impacto, desde incidentes laborales hasta disturbios sociales y desastres naturales.

Este también es un tema de preocupación para nuestro Consejo Asesor de Clientes, quienes nos comentaron que mantener la seguridad de sus empleados, instalaciones y activos ante entornos empresariales cada vez más impredecibles se ha vuelto cada vez más difícil.

Tecnología que mejora la seguridad en todos los entornos

Diversas tecnologías nuevas están ayudando a las organizaciones a mejorar la seguridad para todos, ya sean trabajadores en la oficina o en ubicaciones remotas, clientes en un banco o tienda, o niños en una escuela. Aquí, exploramos formas innovadoras en que las organizaciones se aseguran de estar preparadas para cualquier eventualidad.

La seguridad de los empleados es el principal impulsor de la inversión[1]

La mayoría de los encuestados mencionó la seguridad de los empleados como uno de los tres principales impulsores de la inversión en tecnología de seguridad,

Con un **30%** que la clasificó en primer lugar.

Monitoreo de más riesgos

Gracias a los avances en IA, aplicaciones en la nube y sensores avanzados, los profesionales de la seguridad están descubriendo más formas de monitorear el entorno de trabajo de su organización para detectar una multitud de riesgos de seguridad. Estos incluyen:

- **Protección más allá del perímetro:** Tecnologías como la Detección y Alcance por Luz (LiDAR), integradas con los sistemas de detección de intrusiones perimetrales existentes, proporcionan una detección preventiva, en tiempo real y de alta precisión en áreas extensas, ya sea en el límite exterior del sitio o en una instalación interna, como un almacén.
- **Respuesta a sonidos sospechosos:** El análisis de audio integrado en dispositivos multisensor o sistemas de videovigilancia basados en IA ayuda no solo a detectar sonidos, sino también a clasificarlos, mejorando el conocimiento de la situación y la capacidad de respuesta. Por ejemplo, un sistema de video equipado con análisis de audio puede configurarse para filtrar sonidos cotidianos, como el tráfico, pero alertar inmediatamente ante sonidos críticos como disparos o llamadas de socorro humanas como “¡auxilio!”.
- **Detección de las condiciones ambientales:** La integración de sensores ambientales con sistemas de seguridad electrónica ayuda a las organizaciones a identificar y responder a más amenazas o condiciones, como cambios específicos en el entorno. Algunos ejemplos incluyen fumar y vapear sin autorización, la presencia de sustancias químicas nocivas en el aire, cambios repentinos e inesperados de temperatura, el sonido de comportamiento agresivo, etc.

1 Encuesta ciega de terceros a 575 profesionales de seguridad con autoridad para la toma de decisiones sobre tecnología de seguridad en Australia, Francia, Alemania, Suecia, Reino Unido y Estados Unidos. Realizada en febrero y marzo de 2025.

Gestión eficiente de emergencias

Un aspecto fundamental del programa de seguridad de toda organización, la gestión eficaz de incidentes puede marcar la diferencia entre una pequeña interrupción y un desastre mayor. Las organizaciones están recurriendo a aplicaciones tecnológicas para mejorar la gestión de emergencias e incidentes en el momento:

- **Sistemas de notificación masiva:** Común en escuelas y campus universitarios, esta tecnología proporciona comunicaciones rápidas y eficaces sobre incidentes, lo que permite a los profesionales de seguridad alertar a grandes audiencias sobre riesgos de seguridad, como desastres naturales o un tirador activo, en tiempo real. Las notificaciones instantáneas enviadas a través de dispositivos móviles, mensajes de voz y otros canales digitales ayudan a guiar a las personas hacia un lugar seguro con actualizaciones sobre el estado de la situación, protocolos de emergencia, instrucciones de evacuación y escenarios de confinamiento. **La notificación masiva a dispositivos móviles fue una de las 5 tecnologías principales para su futura adopción en nuestra encuesta de mercado, identificada por el 22% de los encuestados[1].**

- **Intercambio de información con el personal de emergencias:** En Norteamérica, es cada vez más común que las organizaciones de alto riesgo compartan grabaciones de vigilancia de seguridad directamente con el personal de primera respuesta. Al proporcionar acceso a las transmisiones de una o más cámaras de alta prioridad (a través de la nube), las organizaciones pueden brindar a las autoridades de respuesta un mayor conocimiento de la situación, lo que les ayuda a responder con mayor eficacia en caso de una llamada a los servicios de emergencia.



Servicios remotos para una seguridad ininterrumpida

Finalmente, observamos que cada vez más organizaciones invierten en servicios gestionados remotamente para garantizar que sus sistemas de seguridad estén optimizados, protegidos y funcionen eficazmente. Algunos ejemplos clave de estos servicios incluyen:

- **Monitoreo preventivo del estado del sistema:** Un servicio gestionado y siempre activo, diseñado para optimizar el estado y el rendimiento de los sistemas de seguridad. Combina herramientas de IA y agentes humanos profesionales para detectar de forma proactiva posibles problemas, como fallos de batería o interferencias en la visión de las cámaras, y reducir el tiempo de inactividad del sistema..

- **Gestión de firmware y contraseñas:** Estos servicios remotos automatizados ayudan a las organizaciones a mantener los sistemas de seguridad conectados a su red de TI actualizados y protegidos contra amenazas externas de ciberseguridad.

- **Protección remota de operaciones:** Los servicios remotos se han vuelto esenciales para proteger las operaciones comerciales, especialmente durante desastres naturales o crisis que restringen el acceso físico a los edificios. Cuando el acceso no es posible, los servicios remotos pueden ayudar a monitorear y proteger las instalaciones. Ayudan a proteger contra problemas como el merodeo y el saqueo, que pueden ser comunes después de desastres naturales como huracanes.

> “Los productos de seguridad ahora utilizan IA, sensores y análisis para identificar amenazas con anticipación. Los sistemas integrados combinan cámaras, control de acceso, alarmas e intercomunicadores para verificar y actuar con rapidez. El resultado es una reducción del retraso entre la detección y la respuesta = un impacto mínimo.”
>
> **Resideo**

Perspectivas de los socios

Estrategias tecnológicas para la continuidad del negocio

Los sistemas de control de acceso físico son cruciales para la seguridad de todas las personas que requieren acceso a las instalaciones de un cliente. Para mantener estos sistemas en funcionamiento y resilientes, es fundamental considerar la planificación de la continuidad del negocio durante el diseño del sistema y gestionarla continuamente durante su vida útil.

Consideraciones de Diseño de Red

Los controladores de acceso a red integrados son independientes por diseño: si la red falla, el controlador continúa tomando decisiones de acceso y almacenando eventos de acceso en el búfer. Sin embargo, durante el fallo, los eventos y las alarmas no se transmiten a los operadores del sistema. Para mejorar la resiliencia, los controladores deben contar con un puerto de red principal y uno de respaldo, enrutados a través de diferentes rutas de red hasta la cabecera del sistema (local o en la nube). Si la red principal falla, el segundo puerto toma el control y continúa enrutando el tráfico, garantizando la entrega de las alarmas.

Para sistemas locales, también se debe considerar la cabecera. Asegúrese de proporcionar una configuración de Alta Disponibilidad con dos servidores o máquinas virtuales que proporcionen una operación de respaldo completa. Mejor aún, ubique el servidor de respaldo en una ubicación diferente pero cercana para proporcionar una conmutación por error instantánea. Para lograr la máxima resiliencia, diseñe un servidor de Recuperación ante Desastres (DR) que proporcione una conmutación por error en caliente en caso de que falle la configuración de HA.

Para sistemas basados en la nube, elija un proveedor que ofrezca múltiples zonas de disponibilidad para protegerse contra fallos en una sola ubicación. Asegúrese de que la estrategia de respaldo de la base de datos del sistema sea sólida: realice copias de seguridad y restauraciones periódicas cada hora como mínimo.

Las redes de confianza cero son una excelente manera de aumentar la fiabilidad y la resiliencia del diseño de su red, especialmente para sistemas basados en la nube. Si bien esto puede requerir dispositivos de red adicionales, el resultado es un sistema más resistente a los ciberataques.

Consideraciones operativas

La continuidad del negocio se mejora al seguir una rigurosa higiene cibernética para mitigar las vulnerabilidades antes de que afecten a su sistema. Mantenga un riguroso proceso de actualización de software tanto para los controladores como para el software de la cabecera, y realice pruebas de penetración periódicas para descubrir y mitigar las vulnerabilidades.

Otra acción importante es supervisar proactivamente el funcionamiento del sistema, predecir posibles fallos y alertar sobre estas condiciones. ¿Está el disco duro del sistema alcanzando su capacidad máxima? ¿El tráfico de red muestra alta latencia o reintentos? ¿Recibe errores en la base de datos? A veces, incluso los indicadores más pequeños son señal de algo más preocupante.

Por último, ¡no olvide las baterías! En serio: supervise y cambie las baterías de respaldo de los controladores de acceso para que sigan funcionando durante un corte de energía de CA.

Perspectivas de los socios

Mejora de la seguridad en el lugar de trabajo con la gestión de acceso digital

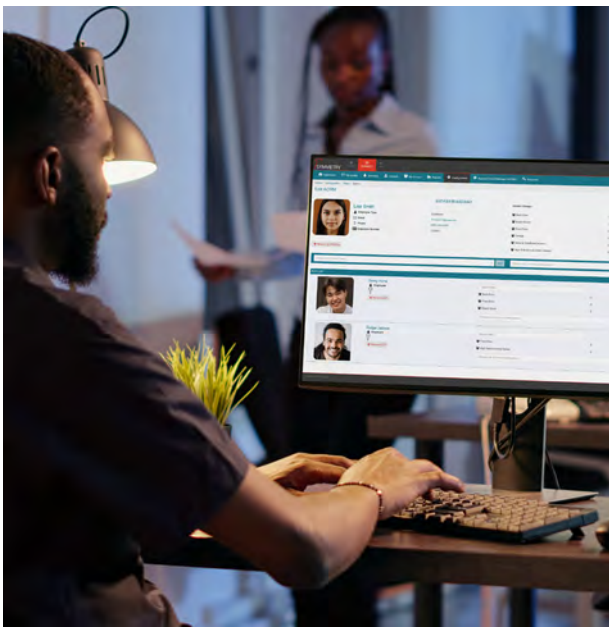
A medida que evolucionan las amenazas a la seguridad en el lugar de trabajo, las organizaciones deben modernizar sus estrategias de gestión de acceso para proteger eficazmente a las personas, los activos y los datos.

Un enfoque digital para la gestión de acceso refuerza la seguridad, mejora la eficiencia y proporciona inteligencia en tiempo real para mitigar los riesgos de forma proactiva.

La gestión de acceso digital aprovecha las credenciales móviles, la automatización inteligente y el análisis para brindar una experiencia fluida y segura. Los empleados y visitantes pueden usar sus teléfonos inteligentes para acceder a las instalaciones, lo que reduce la dependencia de las credenciales físicas y minimiza los riesgos de seguridad asociados con la pérdida o el robo de credenciales. Además, los equipos de seguridad pueden gestionar permisos de forma remota y supervisar los intentos de acceso en tiempo real, lo que garantiza una respuesta rápida ante posibles amenazas.

Otra ventaja de la gestión de acceso digital es su capacidad de integración con soluciones de gestión de identidad, como Symmetry **CONNECT de AMAG. AI** vincular el control de acceso con los sistemas de RR. HH. y TI, las organizaciones pueden aplicar políticas de seguridad automáticamente, garantizando que solo el personal autorizado pueda acceder a áreas específicas.

Las organizaciones deben adoptar un enfoque proactivo para la protección en el lugar de trabajo. La gestión de acceso digital ofrece la agilidad, la inteligencia y la eficiencia necesarias para proteger los lugares de trabajo de las amenazas en constante evolución. AI adoptar estas tecnologías avanzadas, las empresas pueden mejorar la seguridad y la eficiencia operativa, garantizando un entorno de trabajo más seguro y resiliente para el futuro.



VERINT

Perspectivas de los socios

Prevención del Fraude: Lecciones de la Banca para Otros Sectores

En el panorama actual, en constante evolución, la seguridad es un pilar fundamental para la integridad operativa y la confianza del cliente.

Al gestionar grandes cantidades de datos sensibles, los bancos necesitan un enfoque de seguridad integral para hacer frente a las amenazas tanto cibernéticas como físicas. La convergencia de los equipos de TI y seguridad física es vital para sobrevivir en este mercado competitivo.

Los bancos han aprendido que las estrategias de seguridad tradicionales, en las que los equipos de TI y seguridad física operan por separado, ya no son eficaces. Tecnologías modernas como el control de acceso biométrico y la videovigilancia con IA requieren una supervisión integrada. Las soluciones basadas en la nube difuminan aún más los límites entre la seguridad física y digital, lo que subraya la necesidad de colaboración.

Los equipos coordinados pueden abordar mejores amenazas complejas como el robo de identidad en cajeros automáticos y el robo de cuentas digitales. Las estrategias integradas que combinan tecnologías anti-robo de identidad con una vigilancia mejorada y el intercambio de datos en tiempo real ayudan a prevenir el fraude antes de que ocurra.

Una prevención eficaz del fraude también depende de la concienciación humana. Las amenazas internas son significativas, y los bancos implementan programas y formación para garantizar que los empleados puedan identificar y responder a los riesgos internos.

El liderazgo desempeña un papel fundamental en el fomento de un enfoque unificado, promoviendo medidas que combinen la tecnología con estrategias adaptables. Estas estrategias deben ser flexibles para abordar requisitos operativos y regulatorios únicos. La capacitación regular debe abarcar las nuevas tecnologías y los desafíos específicos que enfrenta la organización.

También debe considerarse la situación interna. La experiencia interna es muy valiosa y el establecimiento de centros de seguridad puede ayudar a adaptar las estrategias a las necesidades específicas. No se deben pasar por alto las amenazas internas. Los programas de seguridad deben equilibrar la protección con la privacidad de los empleados, fomentando así la confianza dentro de la organización.

La integración de los equipos de TI y seguridad física es esencial para el éxito de la seguridad bancaria y ofrece lecciones para otros sectores: eliminar los silos, promover la colaboración y enfatizar la capacitación continua. Los bancos que han unificado con éxito sus operaciones de seguridad ofrecen información valiosa para las organizaciones que buscan proteger sus activos, mantener la confianza de los clientes y mantenerse resilientes ante la evolución de los riesgos.


Securitas
Technology
Securitas
Technology

Estrategias para preparar a las organizaciones y a las personas

Además de implementar tecnologías de vanguardia, las organizaciones invierten cada vez más en estrategias avanzadas de anticipación de amenazas. Al aprovechar la inteligencia anticipada y realizar análisis exhaustivos posteriores a incidentes, los profesionales de seguridad buscan estar mejor preparados y protegidos ante futuros eventos de seguridad.

Seguridad basada en inteligencia

En el mundo interconectado actual, la volatilidad, la incertidumbre, la complejidad y la ambigüedad (VUCA) son desafíos omnipresentes. Por ello, observamos un mercado creciente para los servicios de inteligencia de riesgos comerciales que permiten a las organizaciones anticiparse a los riesgos.

En nuestra encuesta, se observó un gran interés en la inteligencia de riesgos, **con un 20 % (empatado en el primer puesto) que afirma tener previsto integrar dichos servicios en su programa de seguridad[1].**

Los servicios de inteligencia de riesgos ayudan a los profesionales de seguridad a decidir dónde centrar su inversión en seguridad, aprovechando la información para determinar cuáles de sus ubicaciones presentan un mayor riesgo. Ayudan a adoptar un enfoque proactivo ante el riesgo mediante funciones como:

- **Informes de pronóstico de riesgos:** Ofrecen a las organizaciones actualizaciones cruciales sobre el conocimiento de la situación, con una frecuencia diaria, semanal y mensual. Estos informes están diseñados para brindar información a nivel local,
- **Informes de Índice de Delincuencia:** Ofrecen análisis delictivos de vanguardia, desde las tendencias globales y nacionales hasta el nivel local. Este servicio tecnológico ayuda a las organizaciones a ver, comparar, estudiar y pronosticar datos de delincuencia en sus áreas de actividad mediante mapas interactivos, estadísticas detalladas y análisis basados en IA.

La preparación es clave para una mayor seguridad

Desde desastres naturales hasta incendios y violencia laboral, las organizaciones se enfrentan a numerosos riesgos potenciales de seguridad que pueden escalar rápidamente a una emergencia. La preparación es vital para generar respuestas serenas, conformes y seguras ante situaciones de crisis.

El interés en los servicios de preparación para emergencias está aumentando, ya que cada vez más organizaciones reconocen la importancia de la planificación proactiva para proteger la seguridad de las personas y del lugar de trabajo.

Según nuestro estudio de mercado, **el 88 % de las organizaciones han implementado un plan formal de respuesta a situaciones de emergencia**, lo que demuestra que esta es un área de enfoque para los profesionales de la seguridad[1].

Sin embargo, **el 18% también afirma tener poca o ninguna confianza en su preparación,** por lo que esto debe seguir siendo una prioridad para las organizaciones[1].

Estos servicios ofrecen apoyo a las organizaciones de diversas maneras, desde la planificación y el cumplimiento normativo hasta la capacitación de los empleados:

- **Planificación de emergencias:** Creación de Planes de Acción de Emergencia (PAE) y Planes de Prevención de Incendios (PPI) personalizados para documentar cómo responde una organización a situaciones de emergencia y las medidas para prevenir incidentes.
- **Servicios de cumplimiento normativo:** Garantizar que los procedimientos de planificación de emergencias de una organización estén documentados, actualizados y cumplan con los requisitos de los organismos reguladores pertinentes.
- **Servicios de capacitación:** Formación para empleados sobre cómo abordar diversas situaciones de seguridad y emergencia mediante capacitación presencial y virtual. Los temas incluyen seguridad contra incendios, respuesta ante tiradores activos, capacitación en primeros auxilios, antiterrorismo y más.

Planificación y procedimientos de seguridad asistidos por IA

La IA está transformando la seguridad organizacional al permitir la extracción de información crítica de los sistemas de seguridad mediante simples comandos de texto o voz. La IA conversacional, que utiliza el procesamiento del lenguaje natural (PLN) y la comprensión del lenguaje natural (NLU), tiene el potencial de agilizar las investigaciones posteriores a incidentes, realizar comprobaciones de seguridad rutinarias e incluso preparar los sistemas para eventos de alta prioridad.

Por ejemplo, los sistemas pueden preconfigurarse con protocolos específicos para prepararse ante un evento de alta prioridad conocido. Imagine que un cliente importante visita la oficina central y requiere mayor seguridad. El sistema de seguridad pertinente podría recibir la simple orden de “elevar el nivel de seguridad” sin necesidad de ninguna acción adicional por parte del equipo de seguridad. Este enfoque proactivo no solo mejora la seguridad, sino que también fomenta la confianza de las partes interesadas al demostrar un compromiso con la seguridad y la preparación.

88%

De las organizaciones cuentan con un plan de respuesta ante emergencias[1]

Confianza en su plan:

Muy seguro **9%**
Seguro **39%**
Moderadamente seguro **35%**
Ligeramente seguro **16%**
Nada seguro **2%**

1 Encuesta ciega de terceros a 575 profesionales de seguridad con autoridad para la toma de decisiones en tecnología de seguridad en Australia, Francia, Alemania, Suecia, Reino Unido y Estados Unidos. Realizada en febrero y marzo de 2025.

Perspectivas de los socios

El poder del almacenamiento en la nube

La necesidad de almacenamiento adicional aumenta a lo largo de la vida útil de su VMS. Sus políticas de retención de video evolucionan y es posible que deba implementar un archivado redundante y otros mecanismos para proteger sus datos. En muchos casos, agregar almacenamiento local conlleva costos significativos de hardware e instalación. Como alternativa, puede optar por almacenamiento híbrido o en la nube completa. Obtendrá la posibilidad de cambiar su capacidad de almacenamiento sin comprar hardware adicional y agregar capas de retención y redundancia. Esto le ayuda a cumplir con las políticas y regulaciones, a la vez que protege sus datos contra desastres y ciberataques con copias por triplicado guardadas en la nube.

Con una solución moderna de software como servicio (SaaS), las capacidades de almacenamiento en la nube están integradas. Puede conectar dispositivos directamente a la nube, lo que facilita la escalabilidad de sus operaciones con requisitos mínimos o nulos para la infraestructura local.

> [Almacenamiento en la nube] le ayuda a cumplir con las políticas y regulaciones, a la vez que protege sus datos contra desastres y ciberataques.

Genetec™ Security Center SaaS ofrece capacidades nativas de la nube, con compatibilidad con cámaras directamente en la nube, grabación y reproducción continuas en la nube y operaciones de video completamente alojadas. Con capacidades híbridas, también existen opciones para llevar la grabación y el procesamiento al borde, conectarse a la infraestructura local y muchas más opciones de implementación que se adaptan a sus necesidades específicas.

Trabaje con su socio de canal para encontrar las mejores soluciones de gestión de video, arquitectura y opciones de implementación. Existen muchas maneras de almacenar video y metadatos localmente y en la nube. Un enfoque híbrido puede maximizar la flexibilidad en cada sitio. Su integrador puede ayudarle a optimizar su sistema y sus operaciones para aprovechar al máximo su inversión en seguridad física.

Perspectivas de los socios

VIAKOO

Protección de los CPS contra los riesgos de ciberseguridad

La proliferación de potentes sistemas de IoT (también conocidos como sistemas ciberfísicos o CPS), desde sensores inteligentes hasta cámaras con IA, ofrece eficiencia, pero amplía significativamente la superficie de exposición a ciberataques.

La gestión eficaz de la exposición es la única manera de abordar las ciberamenazas nuevas (y antiguas). Un hardware de seguridad física mejorado con procesadores neuronales, redes avanzadas y memoria personalizada crea un "campo de juego para los hackers". Los procesadores neuronales permiten ataques locales sofisticados y la participación en botnets. Una red más rápida facilita la exfiltración de datos y la propagación de malware con mayor rapidez. La memoria personalizada almacena datos confidenciales localmente, convirtiéndose en un objetivo prioritario.

Las implicaciones en el mundo real incluyen el aumento de ataques DDoS, filtraciones de datos que exponen información crítica, vulnerabilidades en la cadena de suministro, manipulación de sistemas de seguridad física y espionaje.

Las implicaciones en el mundo real incluyen el aumento de ataques DDoS, filtraciones de datos que exponen información crítica, vulnerabilidades en la cadena de suministro, manipulación de sistemas de seguridad física y espionaje.

Proteger a las empresas requiere una sólida ciberseguridad y automatización. La escala y la naturaleza heterogénea de las implementaciones de seguridad física implican la necesidad de utilizar métodos automatizados. Las prácticas clave incluyen la actualización automática de firmware, la segmentación de la red para aislar los dispositivos CPS, el fortalecimiento de los dispositivos mediante la desactivación de servicios innecesarios, el cambio frecuente de contraseñas seguras, la implementación de una arquitectura de confianza cero, evaluaciones exhaustivas de la seguridad de la cadena de suministro y la formación de los empleados en seguridad CPS.

El auge de los potentes dispositivos CPS presenta tanto oportunidades como riesgos. Comprender estos riesgos e implementar medidas de seguridad robustas es crucial para que las empresas aprovechen el potencial de los CPS y minimicen la exposición a ciberataques.

La preparación ya no es opcional; es esencial. Viakoo ayuda a las empresas a descubrir y remediar las vulnerabilidades de los CPS y se enorgullece de trabajar con Securitas Technology para liderar la lucha contra el desafío de las ciberamenazas a la seguridad física que se acercan a la velocidad de la IA.

Perspectivas de los socios

INTELLICENE
UNIFYING SECURITY, ENABLING ACTION

Seguridad escalable

A medida que las empresas escalan y se expanden a nuevas ubicaciones, aprovechan la oportunidad de crecimiento, pero también se enfrentan a un conjunto cada vez mayor de desafíos de seguridad.
Gestionar la seguridad en una red más amplia puede convertirse rápidamente en una tarea compleja y abrumadora, donde la disparidad de sistemas, los datos aislados y la falta de supervisión centralizada pueden exponer vulnerabilidades críticas.

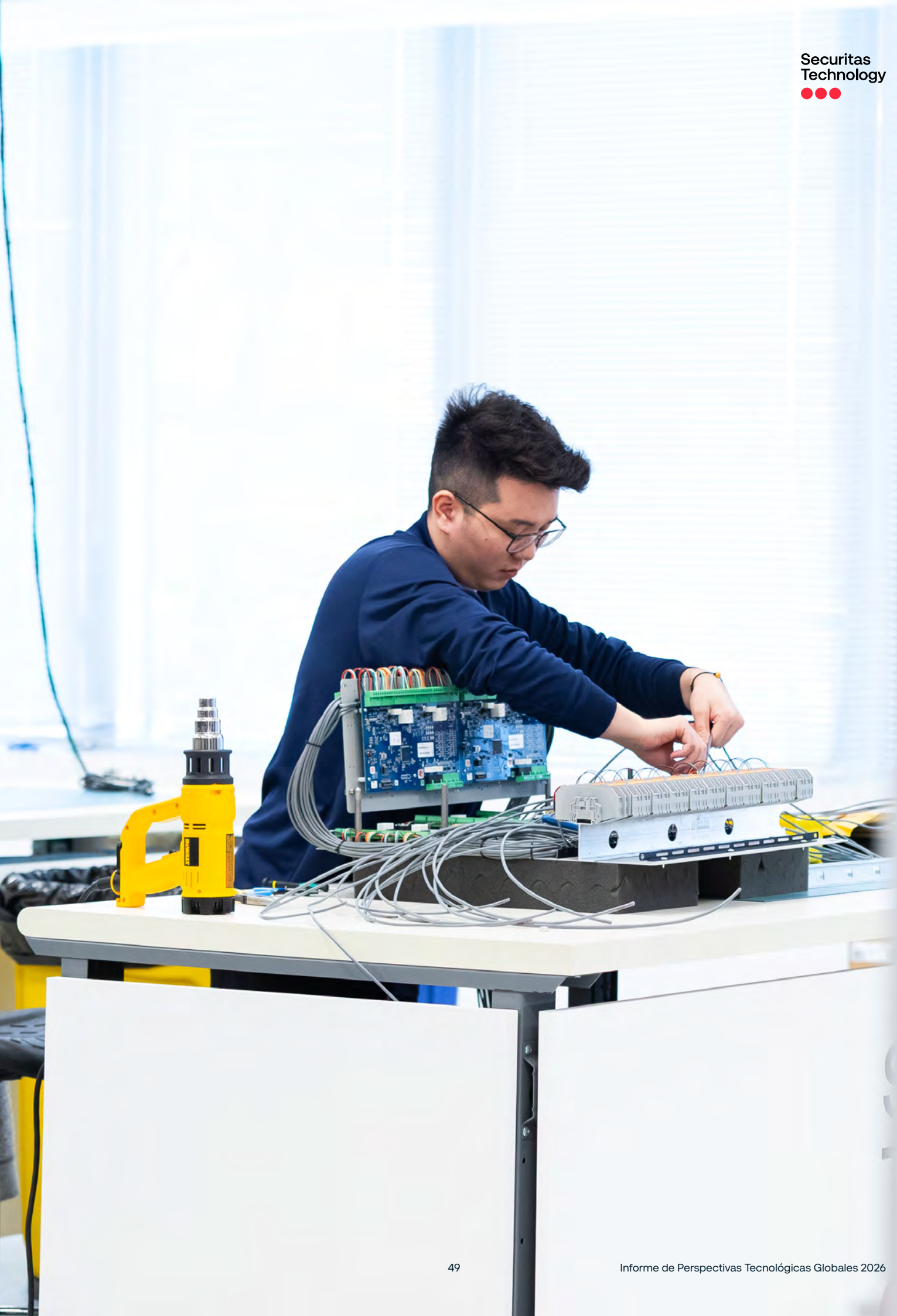
Contar con un sistema de seguridad escalable es clave. En lugar de que las nuevas ubicaciones gestionen su portafolio de seguridad por separado, las plataformas de gestión de seguridad centralizadas permiten a los equipos de seguridad obtener una visión completa de la postura de seguridad de cada sitio con flujos de datos centralizados y correlacionados, y un potencial ilimitado de integraciones.

> Las empresas pueden convertir datos de seguridad correlacionados en información útil para mejorar las operaciones.

Al unificar sistemas de seguridad dispares en una plataforma centralizada, el personal de seguridad puede acceder a la visibilidad integral que necesita para identificar, evaluar y evitar que las amenazas emergentes se conviertan en incidentes graves. Más allá de la seguridad, las empresas pueden convertir datos de seguridad correlacionados en información práctica para mejorar sus operaciones mediante el seguimiento de los patrones de actividad de los clientes y la productividad de los empleados, lo que permite determinar dónde se invierten mejor los recursos y maximizar la eficiencia.

Las empresas necesitan un portafolio de seguridad capaz de adaptarse a la evolución y el crecimiento. La escalabilidad y la flexibilidad no son opcionales; son esenciales para maximizar las inversiones en seguridad y garantizar el éxito a largo plazo.

¿Su estrategia de seguridad está diseñada para crecer con su negocio?



El futuro de la inteligencia sobre riesgos delictivos

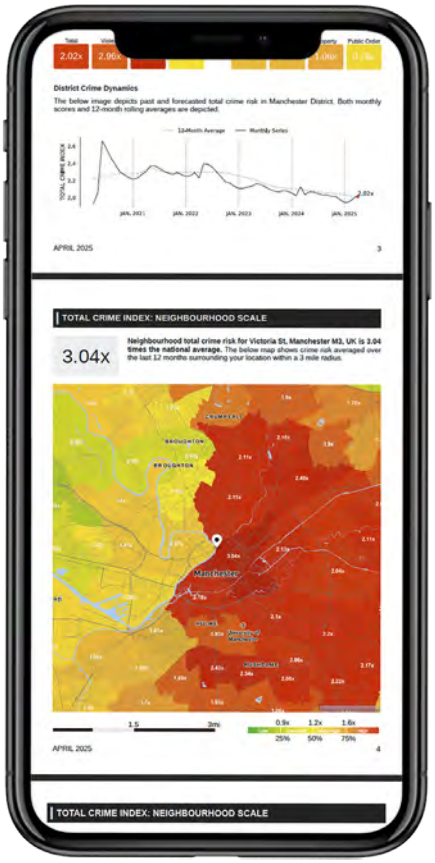
Enfoques innovadores para la protección de personas y lugares

Comprender el flujo y reflujo de la delincuencia es crucial para que las organizaciones protejan a sus grupos de interés, especialmente en regiones donde la violencia y las tendencias delictivas pueden..

La importancia de las puntuaciones de riesgo delictivo

Las puntuaciones de riesgo delictivo, como las del Índice de Delincuencia Pinkerton (PCI), proporcionan una medida precisa, oportuna y cuantificable del riesgo delictivo. Los puntajes de riesgo eliminan la incertidumbre a la hora de evaluar las tendencias delictivas, lo que ayuda a las organizaciones a tomar decisiones basadas en datos para la planificación estratégica de la seguridad, la ubicación de las instalaciones, la asignación de recursos, los seguros y la responsabilidad, la seguridad de las partes interesadas y la gestión de la reputación.

El Índice de Delincuencia Pinkerton se sitúa a la vanguardia del análisis del riesgo delictivo, empleando herramientas estadísticas de última generación y métodos innovadores para captar los matices de los datos sobre delincuencia.



El PCI se sitúa a la vanguardia del análisis del riesgo delictivo, empleando herramientas estadísticas de última generación y métodos innovadores para captar los matices de los datos sobre delincuencia. El proceso comienza con la recopilación meticulosa de datos sobre delincuencia de fuentes clave, como las fuerzas del orden nacionales, regionales y locales, y su cruce de datos para establecer una visión más realista de la delincuencia.

Los datos se depuran para corregir inconsistencias y el subregistro. Por ejemplo, para obtener tasas de delincuencia precisas, se requieren recuentos correctos/delitos totales (numerador) y cifras realistas de población/delincuencia per cápita (denominador), que reflejen la "población flotante" o el número real de personas en una zona —como el turismo y los hábitos de desplazamiento—, no solo la población residente.

Las tasas de delincuencia precisas también tienen una gravedad ponderada que refleja su impacto, medido por factores como las penas de prisión y el coste para las víctimas, lo que garantiza que los delitos más graves tengan una mayor influencia en la puntuación de riesgo general.

En el paso final, los algoritmos de pronóstico se someten a una rigurosa competencia para perfeccionar su precisión predictiva.

Retos únicos y soluciones especializadas

Lo que diferencia a PCI de otras soluciones de pronóstico de delincuencia reside en la forma en que abordamos los datos: adaptamos los retos únicos que cada país enfrenta en la recopilación de datos sobre delincuencia. PCI está disponible actualmente para EE. UU., Canadá, México, Brasil, Reino Unido, Suecia y Australia.

Por ejemplo, en México, el subregistro es significativo. Los datos australianos sobre delincuencia varían enormemente en cuanto a fechas de publicación y clasificación, lo que genera inconsistencias, mientras que los informes brasileños muestran lagunas anuales y variaciones entre las cifras locales y nacionales.

Si bien muchos productos sobre delincuencia y riesgo se basan en informes oficiales de referencia, PCI va más allá: evalúa datos adicionales para subsanar las deficiencias que faltan en los informes oficiales, como encuestas de victimización, certificados de defunción y expertos locales.

Superación

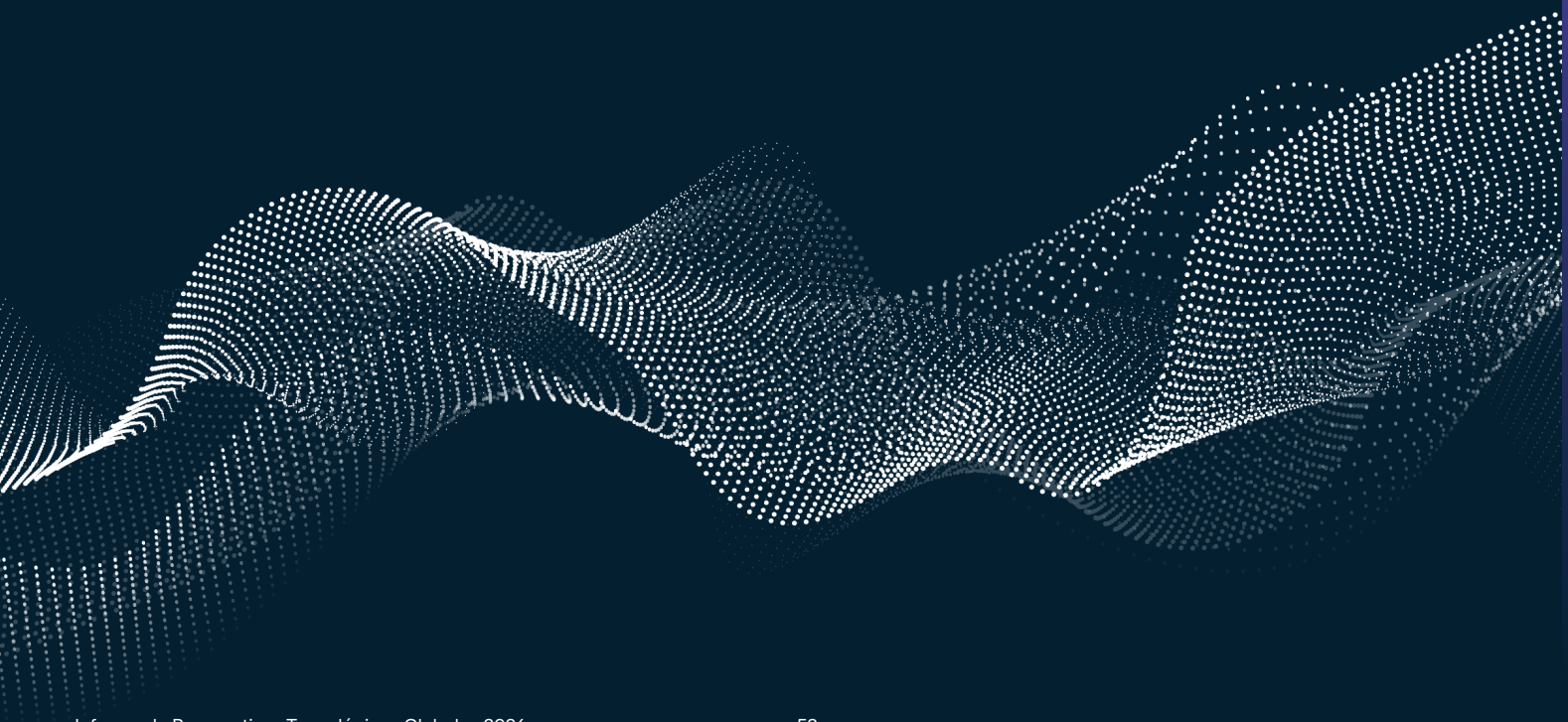
Actualizado mensualmente, PCI no es solo una herramienta, sino un testimonio de la convergencia de la ciencia de datos innovadora y la gestión de riesgos experimentada, lo que lo convierte en una herramienta fiable y con visión de futuro para la gestión del riesgo delictivo.

Más información en pinkerton.com

Plan de Acción para Profesionales de la Seguridad

> En el volátil entorno actual, la mejora de la seguridad en todos los entornos, desde comercios minoristas hasta campus e instalaciones corporativas, se puede lograr mediante tecnologías avanzadas como el análisis basado en IA, los sistemas de comunicación de emergencia y las estrategias proactivas de gestión de incidentes.

Serdar Ince | Vicepresidente Global de Innovación Tecnológica de Securitas Technology



1 Revisar las tecnologías utilizadas para la mitigación de riesgos

Evaluar los enfoques existentes de mitigación y gestión de riesgos para identificar áreas de mejora. Considerar nuevas tecnologías de seguridad, oportunidades de capacitación y estrategias de respuesta a incidentes que puedan ayudar a mejorar la seguridad de los empleados, los clientes y el entorno laboral en general.

2 Evaluar cómo anticiparse al riesgo

Revisar los procesos y tecnologías actuales para la monitorización de riesgos, así como las opciones para aumentar la precisión y la velocidad. Esto podría incluir la inversión en servicios de inteligencia para identificar proactivamente amenazas potenciales, de modo que la organización se mantenga informada y preparada ante la aparición de nuevos riesgos.

3 Actualizar las estrategias de preparación para emergencias y recuperación ante desastres

Revisar y mejorar continuamente los planes de continuidad del negocio y preparación para emergencias. Centrarse en la integración de tecnologías y estrategias de comunicación para mejorar los procedimientos de respuesta, mantener las operaciones, proteger los datos y garantizar la seguridad de los empleados durante las crisis.

4

Seguridad en tiempo real y gestión proactiva

Se está produciendo una importante transformación en la forma en que las organizaciones responden a los eventos, ya sea a través de su propio equipo de seguridad o de un proveedor profesional de monitorización de seguridad.

Estamos dejando atrás la era de la verificación para adentrarnos en una era donde el análisis basado en IA de múltiples fuentes de datos acelera la respuesta a incidentes y facilita la toma de decisiones en tiempo real: una infraestructura de seguridad en constante aprendizaje y mejora.

De cara al futuro, estos datos se combinarán con otras fuentes para impulsar la inteligencia empresarial relacionada con la seguridad, las operaciones y la experiencia del cliente y del empleado.

Mejorando el Agente con IA

En el vertiginoso mundo de la seguridad, la clave para una respuesta eficaz a incidentes reside en comprender rápidamente lo que realmente importa. A medida que evolucionan las amenazas, también deben evolucionar los métodos para abordarlas.

Las tecnologías basadas en IA están revolucionando la forma en que operan los agentes humanos, proporcionándoles información precisa, lo que les permite centrarse en tareas complejas de resolución de problemas. Las fortalezas de la IA residen en su consistencia y enfoque. A diferencia de los agentes humanos, la IA nunca se cansa ni se distrae, lo que la convierte en un aliado virtual ideal en la división del trabajo. Esta colaboración permite a los agentes humanos concentrarse en lo que mejor saben hacer: abordar problemas complejos que requieren una comprensión y una toma de decisiones con matices.

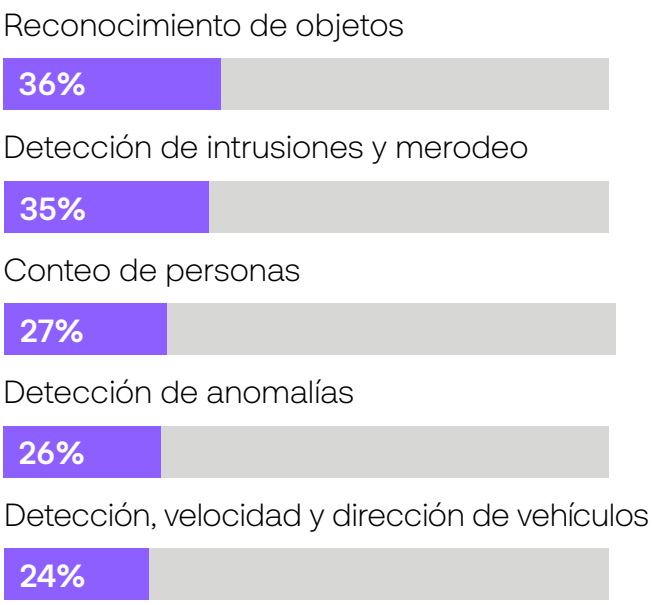
La sinergia entre IA y humanos ofrece ventajas

Uno de los avances más significativos en esta área es el análisis dual de imágenes de video. Equipadas con análisis de borde, las cámaras ahora pueden identificar actividades que podrían requerir una respuesta. Este análisis inicial se revisa posteriormente en el Centro de Operaciones de Seguridad (SOC), lo que garantiza la identificación precisa de posibles amenazas. Cada vez que un agente humano detecta un error, el agente virtual de IA aprende y mejora, volviéndose más hábil para distinguir entre actividades benignas y sospechosas.

Los agentes virtuales también están transformando la respuesta a las alarmas al gestionar las interacciones con los usuarios durante la etapa de verificación. Esta capacidad no solo aumenta la eficacia de la respuesta a las alarmas, sino que también mejora la productividad de los agentes. Al automatizar las tareas rutinarias, la IA permite a los agentes humanos centrarse en aspectos más críticos de la gestión de la seguridad.

IA ya en uso para la detección automatizada[1]

Porcentaje de organizaciones que utilizan:



Respuesta a incidentes cada vez más inteligente

De cara al futuro, se prevé un aumento en la sofisticación de la IA en la respuesta a incidentes. La IA pronto podrá interpretar situaciones complejas con mayor precisión. Indicaciones sencillas en lenguaje natural, como “Generar una alarma si alguien lleva un paquete grande”, pueden generar respuestas detalladas y precisas de los agentes virtuales. Esta capacidad para comprender y actuar ante amenazas específicas será invaluable en entornos como almacenes, donde las necesidades de seguridad son únicas y variadas.

Sin embargo, a medida que las organizaciones adoptan la IA, deben mantenerse atentas a las leyes y regulaciones relativas a la privacidad y el uso ético de la IA. Estas consideraciones son cruciales para garantizar que las aplicaciones de IA sean eficaces y responsables.

En definitiva, complementar a los agentes humanos con IA no se trata solo de mejorar la eficiencia; Se trata de crear una relación donde tanto el ser humano como la máquina destaquen en sus respectivos roles. A medida que la IA continúa evolucionando, promete redefinir la respuesta a incidentes, haciéndola más precisa, proactiva y potente. Al aprovechar las fortalezas de la IA, los equipos de seguridad pueden asegurarse de estar siempre un paso por delante en la protección de sus entornos.

[1]Encuesta ciega de terceros a 575 profesionales de seguridad con autoridad para la toma de decisiones en tecnología de seguridad en Australia, Francia, Alemania, Suecia, Reino Unido y Estados Unidos. Realizada en febrero y marzo de 2025.

Perspectivas de los socios

EAGLE EYE NETWORKS

Cómo la IA transforma la seguridad de reactiva a proactiva

La mayoría de las grabaciones que capturan las cámaras de seguridad nunca se visualizan; simplemente no hay tiempo suficiente. Para que todo este video sea útil, la IA siempre activa puede analizar el video a medida que se captura para generar metadatos, marcar eventos y automatizar las respuestas. La IA reduce los tiempos de respuesta, para que las personas puedan concentrarse en los incidentes que importan.

La IA ofrece estrategias prácticas para la seguridad proactiva:

Alertas basadas en activadores designados

¿Acaba de llegar un vehículo al muelle de carga? ¿Hay movimiento en un pasillo fuera del horario laboral?

Eliminación de costosos falsos positivos

La IA puede eliminar prácticamente las falsas alarmas causadas por el clima o animales, evitando multas costosas y aumentando la fiabilidad de las alarmas.

> La IA que convierte el video en información útil puede activar alertas de incidentes, destacando los eventos para una reacción inmediata.

Enfocando la búsqueda con IA

El reconocimiento y etiquetado de objetos con IA simplifica las investigaciones con términos de búsqueda en lenguaje natural como “persona con mochila” o “camioneta roja”.

Acercamiento a vehículos y armas

La identificación de vehículos es fundamental para la investigación de incidentes de seguridad. El reconocimiento de matrículas de Eagle Eye puede activar alertas cuando un vehículo sospechoso aparece en la cámara. Y la nueva tecnología de detección de armas puede detectar un arma antes de que se dispare.

Quizás lo más importante es que la IA que convierte el video en información útil también puede activar alertas de incidentes, destacando los eventos para una reacción inmediata. Eagle Eye Cloud VMS pone en práctica el análisis y la clasificación continuos, y proporciona un marco para ampliar su inteligencia a través de una API abierta, ya utilizada por una amplia gama de socios tecnológicos para ofrecer software especializado.

Eagle Eye Cloud VMS pone en práctica el análisis y la clasificación continuos, y proporciona un marco para ampliar su inteligencia a través de una API abierta, ya utilizada por una amplia gama de socios tecnológicos para ofrecer software especializado.

Perspectivas de los socios

SONITROL

Estrategias eficaces de verificación de alarmas

La monitorización tradicional de alarmas sigue un modelo de “Detección y Notificación”: cuando un sensor, como un sensor de movimiento, activa una alarma, se notifica a una central de monitoreo. Sin embargo, estas alarmas no confirman una amenaza real, lo que resulta en una tasa de falsas alarmas del 98%.

En respuesta, muchos municipios han implementado multas por falsas alarmas o exigen la verificación de alarmas antes de la intervención policial. Algunos exigen la verificación de alarmas y priorizan la respuesta policial a las alarmas verificadas que indican un delito en curso.

Para abordar las falsas alarmas, técnicas de verificación como la Detección Multi-Viaje y la Verificación Mejorada de Llamadas reducen la incertidumbre, pero no confirman un delito en curso. Las soluciones de verificación más eficaces son la verificación de alarmas por audio y video, que permite a los operadores de la central de monitoreo ver o escuchar un incidente en tiempo real, mejorando los tiempos de respuesta y la precisión.

Algunos municipios requieren verificación de alarmas y brindan respuesta policial prioritaria a las alarmas verificadas que indican un delito en curso.

Verificación de Audio

- Detecta sonidos amenazantes cuando el sistema está armado.
- Los operadores pueden escuchar en tiempo real para evaluar las amenazas.
- Cubre todo el espacio, de piso a techo y de pared a pared, lo que permite la detección temprana de alarmas.

Verificación de video

- Se activa mediante un sensor de alarma o la detección de movimiento de una cámara.
- Los operadores reciben secuencias de video previas y posteriores a la alarma o transmisiones de video en vivo.
- Proporciona confirmación visual de un delito en curso.

La integración de la verificación de audio y video mejora la monitorización de alarmas al reducir las falsas alarmas y optimizar la respuesta policial. El audio proporciona cobertura total y detección temprana, mientras que el video ofrece confirmación visual dentro del campo de visión de la cámara. Juntos, maximizan la seguridad y mejoran los tiempos de respuesta y la eficacia policial, lo que los convierte en el estándar de oro para la monitorización de alarmas actual. making them the gold standard for alarm monitoring today.

Perspectivas de los socios

BOSCH
Invented for life

Potenciando respuestas proactivas y decisiones automatizadas

La IA está transformando el rol de la videoseguridad con inteligencia visual, ayudando a los usuarios a encontrar información significativa en las grabaciones de video, reconocer patrones y comprender qué podría suceder a continuación. Las detecciones tempranas y precisas facilitan la identificación y la respuesta a riesgos potenciales antes de que se conviertan en un problema. Las soluciones basadas en IA detectan de forma rápida y fiable brechas perimetrales, armas de fuego, equipos de protección personal faltantes y más.

Mediante la extracción, las soluciones y servicios de IA también pueden agregar y visualizar datos de múltiples cámaras para recopilar información sobre seguridad y operaciones. El aprovechamiento de estos datos proporciona información para el análisis de tendencias: al comprender los patrones en torno a situaciones que afectan la seguridad, los usuarios pueden tomar decisiones informadas que minimicen la ocurrencia o el impacto de estos eventos.

Reconocer e identificar patrones permite generar alertas cuando las situaciones requieren atención, lo que permite a los usuarios ser proactivos en lugar de reaccionar después de un incidente.

Las capacidades de IA pronto se expandirán más allá de la detección de objetos para una comprensión más profunda de la escena, interpretando entornos complejos y proporcionando información sobre lo que está sucediendo. Analizará imágenes de situaciones sin estar entrenada para objetos o comportamientos específicos. Al integrarse en los procesos organizacionales, puede sugerir acciones para mitigar el riesgo y alertar al personal, lo que aporta mayor valor a los usuarios.

Las capacidades de IA pronto se expandirán más allá de la detección de objetos para una comprensión más profunda de la escena.

Extracción de datos para la mejora continua

En el ámbito de las operaciones de seguridad, la capacidad de monitorear una amplia gama de fuentes de datos está transformando el panorama, ofreciendo nuevos servicios que mejoran tanto la seguridad como la inteligencia empresarial.

Nuevas herramientas que ayudan a los SOC a trabajar de forma más inteligente para sus clientes

Los Centros de Operaciones de Seguridad (SOC) están ampliando sus capacidades más allá de la monitorización de sistemas, allanando el camino para enfoques más sofisticados de seguridad y gestión de operaciones.

Ya se han implementado muchos servicios adicionales, como el seguimiento de activos, que permite la monitorización en tiempo real de los vehículos y activos de alto valor de una organización.

Con acceso en tiempo real a la ubicación de un vehículo, el SOC puede supervisar su recorrido y alertar al responsable de logística sobre cualquier retraso inesperado o incidente de seguridad, garantizando así la fluidez de las operaciones y una mayor seguridad. Este tipo de integración de datos ejemplifica el potencial de los sistemas de seguridad modernos para respaldar eficientemente los procesos empresariales.

La IA también está revolucionando las operaciones de los centros de monitorización, impulsando la eficiencia y la eficacia. Agentes virtuales pueden realizar recorridos de múltiples cámaras, identificando cámaras desalineadas o desenfocadas comparando su estado de instalación con el estado actual. Este enfoque proactivo garantiza el funcionamiento óptimo de los sistemas de vigilancia. Además, la IA facilita el mantenimiento remoto automático, la comprobación del estado de la batería, el estado de los detectores y los contactos de las puertas, y la correcta conservación de las imágenes. Estas capacidades reducen el tiempo de inactividad y mejoran la fiabilidad de los sistemas de seguridad.

La transición a plataformas predictivas ya está en marcha

Quizás aún más impactante sea la capacidad de la IA para analizar datos de eventos y discernir patrones, lo que permite a las organizaciones prepararse mejor para situaciones similares en el futuro. Muchos SOC (incluidos los de Securitas Technology) mantienen un conjunto completo de datos de eventos de alarma, que pueden analizarse en busca de patrones, como la hora del día, el día de la semana o las tendencias estacionales. Las organizaciones también pueden conectar esta información con otras fuentes de datos para obtener información adicional y obtener una visión más completa del entorno de riesgo total: datos operativos y financieros, datos de sistemas de automatización de edificios, monitoreo de ciberamenazas, etc.

Las plataformas predictivas basadas en estos datos están comenzando a surgir, y en pocos años, es probable que el análisis predictivo se convierta en una realidad. Prevemos el desarrollo de nuevos tipos de inteligencia, como la correlación de eventos, que permitirán a las organizaciones comprender los factores que provocan incidentes y anticipar cuándo podrían repetirse condiciones similares. Este conocimiento previo permitirá a las empresas tomar medidas proactivas, reduciendo los riesgos y mejorando la seguridad general.

En conclusión, la extracción de datos para la mejora continua no se trata solo de reaccionar ante incidentes, sino de avanzar hacia un modelo predictivo que ofrezca previsión y ventaja estratégica. A medida que la IA y el análisis de datos siguen evolucionando, prometen redefinir las operaciones de seguridad, haciéndolas más inteligentes, receptivas y eficaces. Al aprovechar el poder de los datos, las organizaciones pueden asegurarse de estar preparadas para cualquier desafío futuro.

> “Las capacidades de IA no solo mejoran los resultados de seguridad; también reducen el coste total de propiedad al reducir la carga de trabajo manual y permitir a las organizaciones utilizar mejor los recursos existentes. Desde el análisis predictivo de amenazas hasta las respuestas automatizadas, la IA influye en todos los aspectos de nuestras soluciones de seguridad, ayudando a los clientes a anticiparse a los riesgos en constante evolución y a optimizar sus operacionest.”
>
> Software House

Perspectivas de los socios

MOTOROLA SOLUTIONS

Desbloqueando el potencial de la seguridad conectada

La evolución de la seguridad exige un cambio de paradigma: de numerosos sistemas dispares a un ecosistema verdaderamente conectado.

Para los usuarios, no se trata solo de la integración de dispositivos; Se trata de diseñar un marco de seguridad inteligente y adaptable que anticipe y mitigue las amenazas en tiempo real.

Una piedra angular de esta visión son las plataformas abiertas e interoperables. Al promover estándares como ONVIF, trascendemos los silos de proveedores, fomentando un ecosistema dinámico donde convergen las mejores tecnologías. Esto permite a las organizaciones adaptar las soluciones de seguridad a sus necesidades únicas, impulsando la innovación y la resiliencia.

Además, la inteligencia basada en datos es fundamental. Debemos aprovechar el poder del análisis centralizado y la IA para transformar los datos sin procesar en información práctica. Esto permite la detección proactiva de amenazas, las respuestas automatizadas y el modelado predictivo de seguridad, elevando la seguridad de una postura reactiva a una preventiva.

En un mundo interconectado, la ciberseguridad se convierte en un imperativo estratégico. Debemos integrar protocolos de seguridad robustos en cada capa, desde la autenticación de dispositivos hasta la segmentación de la red.

Las plataformas basadas en la nube facilitan la administración remota, la colaboración en tiempo real y el intercambio fluido de datos, lo que permite a las organizaciones responder con rapidez a las amenazas emergentes y optimizar la eficiencia operativa.

Un enfoque proactivo y estratificado es esencial para protegerse de las ciberamenazas en constante evolución y mantener la integridad del ecosistema.

La implementación estratégica de tecnologías en la nube permite una escalabilidad y accesibilidad sin precedentes. Las plataformas basadas en la nube facilitan la gestión remota, la colaboración en tiempo real y el intercambio fluido de datos, lo que permite a las organizaciones responder con rapidez a las amenazas emergentes y optimizar la eficiencia operativa.

En definitiva, un ecosistema de seguridad verdaderamente conectado debe estar centrado en el usuario. Debemos diseñar interfaces intuitivas y ofrecer formación integral para que los profesionales de la seguridad puedan aprovechar al máximo el potencial de estas tecnologías. Esta fusión de experiencia humana e innovación tecnológica es la clave para iniciar una nueva era de excelencia en seguridad.

Al adoptar estos imperativos estratégicos, podemos construir un ecosistema de seguridad conectado que no solo proteja los activos, sino que también impulse la eficiencia operativa y fomente una cultura de seguridad proactiva.

Perspectivas de los socios

MARCH networks
A Delta Group Company

Gestión de vídeo empresarial para ubicaciones multisitio

Gestionar la videovigilancia en múltiples ubicaciones es un reto. Las empresas actuales necesitan un sistema que centralice la gestión de vídeo, garantice el estado del sistema y proporcione información práctica para mejorar la seguridad y las operaciones.

Las soluciones de gestión de vídeo empresarial de March Networks, líderes en la industria, están diseñadas para simplificar la gestión y ofrecer soluciones escalables para implementaciones complejas en múltiples ubicaciones.

Un robusto sistema de gestión de vídeo (VMS) permite a las empresas supervisar todas las ubicaciones desde una única interfaz, simplificando la administración diaria al ofrecer un control centralizado a través de escritorio, web o móvil. Con Command Enterprise Software (CES) de March Networks, las organizaciones pueden supervisar y gestionar miles de cámaras, grabadoras y canales de vídeo, con monitorización del estado del sistema en tiempo real, seguimiento de la actividad del usuario y vistas personalizables para mantener a los equipos de seguridad proactivos y receptivos. Administrar y actualizar dispositivos en múltiples ubicaciones es sencillo, con actualizaciones masivas de firmware, gestión de contraseñas y cambios de configuración en todas las ubicaciones. Las funciones de ciberseguridad integradas, como transmisiones de vídeo cifradas y autenticación segura de dispositivos, ayudan a proteger a las empresas de las ciberamenazas en constante evolución. Command Enterprise Cloud proporciona almacenamiento de vídeo centralizado, acceso remoto seguro y escalabilidad fluida sin la carga de una infraestructura local.

Los análisis basados en IA añaden una capa adicional de inteligencia al integrar el vídeo con datos de transacciones y dispositivos IoT, lo que ayuda a las empresas a encontrar el vídeo que necesitan un 90% más rápido.

Los análisis basados en IA añaden una capa adicional de inteligencia al integrar el video con datos de transacciones y dispositivos IoT, lo que ayuda a las empresas a encontrar el video que necesitan un 90% más rápido. Searchlight Cloud de March Networks ayuda a las empresas a detectar fraudes, robos, riesgos de responsabilidad civil e ineficiencias operativas con alertas en tiempo real y paneles visuales para obtener información a nivel empresarial y específico de cada sitio, todo ello vinculado al video.

Al aprovechar un VMS empresarial completo, flexible y escalable, las empresas pueden proteger activos, optimizar las operaciones y tomar decisiones más inteligentes en todas las ubicaciones. Por eso, más de 1500 instituciones financieras, incluidos algunos de los bancos más grandes y complejos del mundo, confían en March Networks para la gestión de su video empresarial.

Perspectivas de los socios

IDIS One Solution. One Company.

Desbloqueando el video de alta velocidad y alta calidad: Cómo la IA y la tecnología en la nube revolucionan la vigilancia

A medida que las organizaciones adoptan cada vez más soluciones basadas en la nube, la videovigilancia de alta velocidad y alta calidad es más crucial que nunca. La nube ofrece escalabilidad, acceso remoto y gestión centralizada, pero mantener un rendimiento de video superior sin comprometer la calidad presenta un desafío único.

En IDIS, combinamos estrategias y tecnología avanzadas para ofrecer streaming de alta velocidad y una calidad de video excepcional en la nube. Una innovación clave de nuestras soluciones es el Códec Inteligente IDIS, que reduce los requisitos de ancho de banda y almacenamiento sin sacrificar la claridad del video.

A diferencia de los métodos de compresión tradicionales, el Códec Inteligente IDIS ofrece hasta un 50% más de eficiencia, lo que permite a las empresas transmitir video de alta definición con mayor rapidez y almacenar más material en la nube sin costosas actualizaciones de infraestructura. Esto permite un acceso fluido a material en vivo y grabado desde cualquier lugar, incluso en condiciones de red variables.

La IA también desempeña un papel fundamental en la mejora del procesamiento de video y audio. La IA mejora la calidad de la imagen al refinar el color, la resolución y la claridad, incluso con datos mínimos. En el análisis de video, la IA mejora la precisión de detección al incorporar fotogramas de meta procesamiento. En audio, la IA aísla la voz humana y amplifica el sonido de fondo, lo que habilita funciones como la cancelación de ruido inversa. Estas mejoras impulsadas por IA hacen que los sistemas de seguridad sean más receptivos y precisos.

En IDIS, nos aseguramos de que nuestras soluciones basadas en la nube aprovechen la IA y las tecnologías de compresión de video, ayudando a las organizaciones a lograr una videovigilancia eficiente, escalable y de alta calidad en todos los sectores.


Securitas
Technology

Securitas

Reforzando al Guardia

Cómo la capacitación y la tecnología están transformando el rol

Cámaras de vigilancia, lectores de acceso, etiquetas de monitoreo de temperatura, dispositivos IoT: los entornos empresariales actuales están repletos de sensores de seguridad conectados que procesan continuamente datos operativos y de seguridad.

Pero hay otro sensor poderoso en la empresa: el oficial de seguridad.

En miles de ubicaciones en todo el mundo, los oficiales desempeñan un papel fundamental en las operaciones comerciales diarias: observan cambios sutiles en el entorno, toman decisiones en tiempo real y previenen, responden y resuelven activamente problemas de seguridad.

A pesar de los avances tecnológicos y la automatización, el valor del oficial de seguridad no deja de crecer, y su rol se vuelve cada vez más esencial para la seguridad empresarial. Por eso, la inversión continua en oficiales y la evolución de su rol dentro de las organizaciones es más crucial que nunca.

Aquí hay tres ejemplos de cómo se ve esto hoy en Securitas:

Convirtiendo la vigilancia en protección basada en inteligencia

A medida que más empresas adoptan plataformas para la inteligencia de riesgos en tiempo real, muchas aún tienen dificultades para aplicar la lógica a su organización, incluyendo la conversión de alertas en acciones. Los agentes, con la capacitación adecuada, pueden superar esa brecha.

Hemos desarrollado un programa piloto para capacitar a los agentes en los fundamentos de la inteligencia, dotándolos de las habilidades y los conocimientos esenciales de un operador de inteligencia. El programa desarrolla competencias básicas, como comprender los requisitos de inteligencia para determinar qué es importante para una organización, utilizar diferentes fuentes de recopilación (incluida la colaboración con los servicios de emergencia locales) y cómo utilizar el análisis de inteligencia para mantenerse a la vanguardia en el cambiante panorama de amenazas actual.

Y lo más importante, los agentes aprenden a integrar la inteligencia en la toma de decisiones diaria in situ, lo que ayuda a las organizaciones a responder con mayor rapidez y a evitar cuellos de botella a nivel local.

Más información en securitas.com

Desarrollo de experiencia especializada en seguridad de centros de datos
Otro programa de capacitación especializada está preparando a más de 10,000 agentes para satisfacer las complejas demandas de una de las industrias más críticas y de mayor crecimiento del mundo: los centros de datos.

Iniciado en 2024 y acreditado por el Instituto Holístico de Profesionales en Seguridad de la Información (HISPI), el programa capacita a los agentes para convertirse en Profesionales Certificados en Seguridad de Centros de Datos. Está diseñado para abordar los riesgos y requisitos específicos de este sector, reconociendo que el enfoque tradicional de protección universal ya no es suficiente para entornos de alta seguridad y alto riesgo como los centros de datos.

Este tipo de conocimiento avanzado y especialización convierte a los agentes en recursos cada vez más vitales que mejoran aún más la seguridad de un centro de datos y refuerzan su resiliencia.

Optimización de rutas y dotación de personal
Si bien la capacitación avanzada prepara a los agentes para roles más estratégicos, la tecnología desempeña un papel igualmente importante a la hora de optimizar su impacto e impulsar una eficiencia significativa para las organizaciones.

En varios países europeos, hemos implementado modelos de IA que mejoran la forma en que desplegamos a los agentes al tener en cuenta los tiempos de desplazamiento, la alineación de habilidades y las previsiones de personal a largo plazo. Solo en el área metropolitana de Berlín, la optimización de rutas tiene el potencial de reducir las distancias diarias de desplazamiento en un 44%.

La IA también nos ayuda a optimizar la ubicación de las oficinas de vigilancia, lo que ya ha generado una reducción promedio del 10% en el tiempo de conducción en Alemania, generando ahorros indirectos en costos para las organizaciones a las que prestamos servicios.

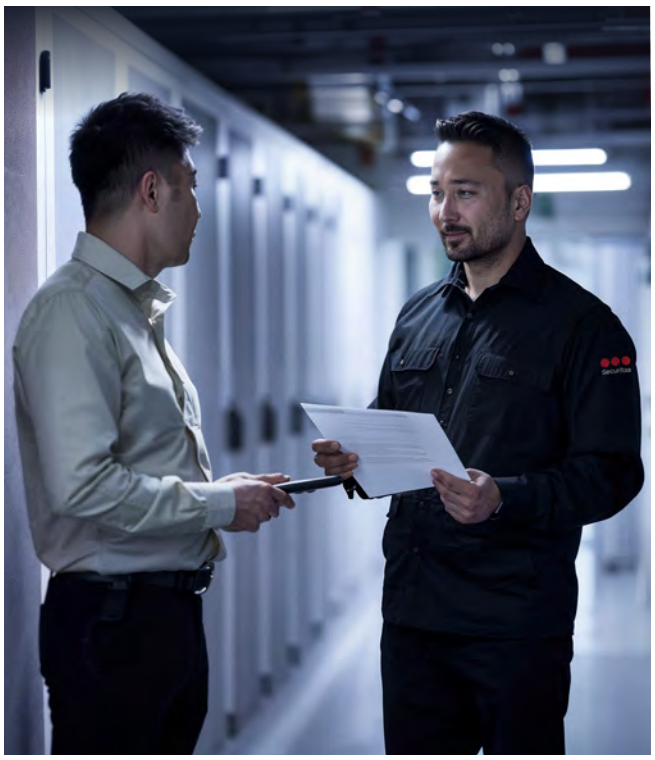
Todo esto amplifica el impacto de los agentes, lo que se traduce en una mayor eficiencia, un soporte más rápido y, en última instancia, clientes más satisfechos.

Reimaginando el rol del agente

Cada uno de estos ejemplos apunta a un cambio más amplio en nuestra forma de pensar sobre la seguridad y sobre las personas.

Las estrategias de seguridad más efectivas no se basan únicamente en la tecnología. Están impulsados por personas capacitadas, confiables y conectadas, que pueden integrarse al ecosistema de seguridad de una organización y garantizar su correcto funcionamiento.

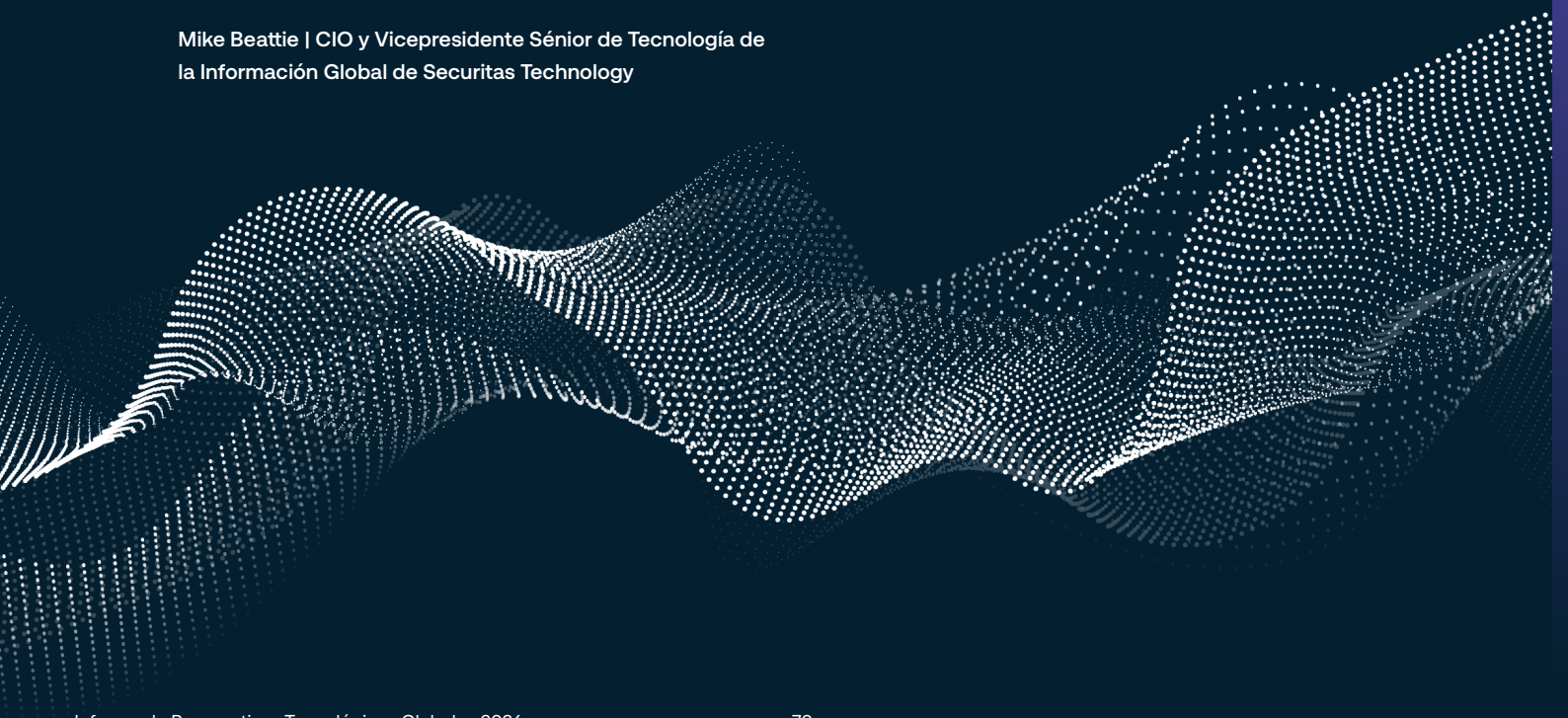
Y a medida que la industria continúa evolucionando, nuestro compromiso con estas personas sigue siendo la base de todo lo que hacemos. Con capacitación avanzada, experiencia especializada e inteligencia artificial, capacitamos a los oficiales con las herramientas necesarias para afrontar el futuro, a la vez que fortalecemos la resiliencia de las organizaciones que ayudan a proteger.



Plan de Acción para Profesionales de Seguridad

"El futuro de la seguridad está cambiando hacia una gestión proactiva en tiempo real, impulsada por la IA, la integración de datos y otras tecnologías de red. Al complementar los agentes humanos con IA, las organizaciones pueden optimizar la respuesta a incidentes, aumentar la eficiencia y anticipar las amenazas con mayor precisión. A medida que las organizaciones adoptan estas potentes tecnologías, es fundamental garantizar también la seguridad de la red, la protección de la privacidad y el cumplimiento de las regulaciones y estándares para el uso responsable de la IA."

Mike Beattie | CIO y Vicepresidente Sénior de Tecnología de la Información Global de Securitas Technology



1

Revisar los Protocolos de Respuesta a Incidentes

Realizar una evaluación exhaustiva de cómo se supervisan y gestionan los eventos en toda la organización, desde los procesos de respuesta a alarmas hasta las tareas rutinarias de seguridad. Comprender la hoja de ruta de capacidades del proveedor de servicios de seguridad de la organización y examinar las oportunidades para crear un ecosistema de información para automatizaciones, soporte de agentes y análisis.

2

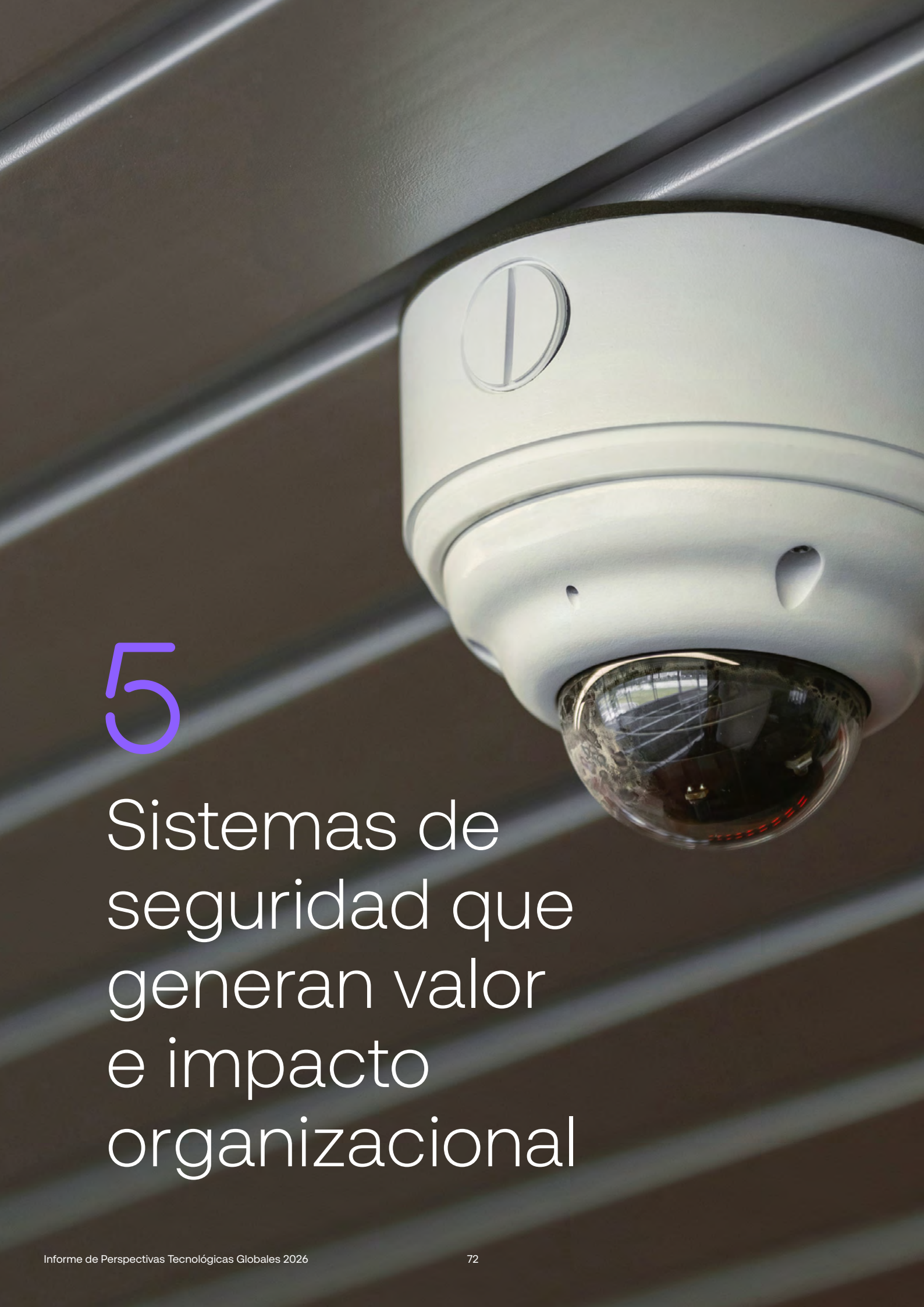
Priorizar la Inversión en Tecnologías Proactivas

Asignar recursos del presupuesto de seguridad para implementar tecnologías de vanguardia e integraciones de datos que permitan la detección proactiva de amenazas, la respuesta a incidentes y el análisis. Considere la automatización basada en IA y los servicios remotos para transformar las operaciones de seguridad en un sistema innovador y con capacidad de respuesta.

3

Integrar la IA en los protocolos de respuesta a incidentes

Colaborar con las partes interesadas internas para crear un plan estratégico para integrar la IA en los protocolos de respuesta a incidentes. Enfóquese en optimizar los procesos existentes con soluciones de IA, garantizando al mismo tiempo el cumplimiento de las normas regulatorias, legales y éticas.



5

Sistemas de seguridad que generan valor e impacto organizacional

La importancia fundamental de la seguridad siempre ha sido bien comprendida. Es una necesidad humana fundamental que ayuda a garantizar la seguridad y el bienestar tanto de las personas como de las organizaciones.

Los sistemas de seguridad han aportado valor de forma constante porque ayudan a las organizaciones a proteger a su personal y sus activos, y a prevenir desastres que cambian la vida. Los profesionales de la seguridad y la prevención de pérdidas participan en una actividad esencial para el progreso humano, brindando tranquilidad y estabilidad en un mundo en constante cambio.

Ahora, existe el potencial de hacer aún más. Los sistemas de seguridad generan una gran cantidad de información que las organizaciones pueden utilizar para generar diferentes tipos de valor, abriendo nuevas posibilidades para mejorar la eficiencia operativa, optimizar la toma de decisiones e impulsar la innovación. Se trata de una nueva perspectiva sobre el retorno de la inversión que las empresas pueden obtener mediante la tecnología de seguridad, transformándola de una medida de protección a un activo estratégico que contribuye al éxito general.

Datos de seguridad que contribuyen a la optimización empresarial

Vivimos en un mundo impulsado por los datos. Las organizaciones ven la necesidad de análisis en todas sus actividades, y la seguridad no es la excepción. Trabajamos con clientes para integrar datos de múltiples sistemas de seguridad con el fin de analizar mejor los patrones en la actividad de seguridad y descubrir información que respalde iniciativas más amplias de mejora empresarial.

Mejorar la experiencia del cliente y del empleado es un

principales 5

Impulsor de la tecnología de seguridad[1]

Integración de datos que impulsa la información

Existe un creciente interés entre las organizaciones por combinar datos de distintos sistemas de seguridad para obtener una comprensión más completa y holística de cómo interactúan sus sistemas de seguridad. Este objetivo se centra en identificar tendencias en los datos que puedan ayudar a comprender cuándo y por qué ocurren los incidentes de seguridad.

Por ejemplo, los responsables de seguridad podrían aprovechar los datos integrados de los registros de control de acceso y los sistemas de videovigilancia para obtener información crucial sobre la seguridad del personal. El análisis de estos datos, aún más sencillo gracias a la IA, permite identificar ubicaciones y momentos específicos donde el personal es más susceptible a incidentes de violencia.

Las organizaciones también están empezando a integrar sus datos de seguridad con datos de plataformas internas (operativas, financieras, etc.) y fuentes externas, como la inteligencia sobre ciberamenazas y riesgos, para crear una visión más integral de los riesgos y el rendimiento organizacional. El análisis mediante IA de la correlación de eventos entre estas diversas fuentes de datos abre la posibilidad de nuevos tipos de alertas sobre amenazas a la seguridad, así como sobre otras actividades empresariales.



[1]Encuesta ciega realizada por terceros a 575 profesionales de seguridad con autoridad para la toma de decisiones en tecnología de seguridad en Australia, Francia, Alemania, Suecia, Reino Unido y Estados Unidos. Realizado en febrero y marzo de 2025.

El cambiante panorama regulatorio de la IA y la ciberseguridad

Dos tendencias regulatorias requieren la atención de los profesionales de la seguridad y sus colegas de TI, Legal y Compliance. La Ley de IA de la UE, promulgada en agosto de 2024, proporciona un marco para el uso responsable de la IA, cuyo cumplimiento entrará en vigor en febrero de 2025 para algunas aplicaciones. Las organizaciones deben determinar cómo se clasifica su uso de la IA según la Ley y cumplir con sus requisitos. En EE. UU., la Ley de IA de Colorado es la primera legislación general sobre IA, mientras que estados como Nueva York, Florida y Utah cuentan con leyes más específicas. A nivel mundial, Australia, Canadá y el Reino Unido, entre otros, también están desarrollando legislación.

Las regulaciones de ciberseguridad también están evolucionando, con la Directiva de Seguridad de las Redes y de la Información 2 (NIS2) de la UE, vigente desde octubre de 2024. Esta directiva exige estándares de ciberseguridad mejorados para sectores críticos, incluidos los sistemas de seguridad física. En EE. UU., las leyes de ciberseguridad varían. Existen regulaciones federales dirigidas a sectores como la banca y las infraestructuras críticas, y leyes estatales de privacidad que afectan las medidas de seguridad, como la protección de grabaciones de video.

Mejorando la Experiencia del Cliente

Al comprender las interacciones y preferencias de los clientes a través de sus datos de seguridad, las empresas pueden adaptar sus servicios y entornos para mejorar su experiencia.

Esto es especialmente importante en el sector minorista, donde la información sobre el comportamiento del cliente puede ayudar a identificar las zonas más concurridas de la tienda y optimizar la ubicación de los productos, una acción que puede contribuir directamente a aumentar las ventas.

En el sector hotelero, un hotel puede programar sistemas de control de acceso con preferencias predefinidas de los huéspedes, como la temperatura de la habitación y la iluminación, y ajustarlas automáticamente al momento del check-in para crear una estancia personalizada y cómoda.

Realizar este tipo de ajustes basados en información basada en datos es una forma eficaz de impulsar el éxito, a la vez que fomenta la satisfacción y la fidelización del cliente.

Optimizando el Lugar de Trabajo

Los sistemas de seguridad empresarial capturan continuamente datos valiosos, ofreciendo información sobre el uso del edificio con cada interacción, como la apertura de puertas con control de acceso o la desactivación de sistemas de alarma. En las oficinas corporativas, los datos de control de acceso y vigilancia pueden revelar patrones en el movimiento de los empleados y la utilización del espacio, lo que permite a las organizaciones optimizar las reservas de salas de reuniones, ajustar los horarios de iluminación y calefacción, y rediseñar la distribución de las oficinas para mejorar la eficiencia y la satisfacción de los empleados.

El reto reside en analizar estos datos, una tarea que requiere tiempo y concentración, algo que los responsables de seguridad e instalaciones a menudo carecen debido a otras prioridades. Tecnologías como la IA pueden ayudar procesando eficientemente grandes conjuntos de datos y proporcionando rápidamente información práctica, simplificando el proceso.

Además, la integración de sensores ambientales en los sistemas de seguridad empresarial permite a las organizaciones supervisar aspectos adicionales del lugar de trabajo. Por ejemplo, en las escuelas, los sensores inteligentes pueden detectar cambios en la calidad del aire y alertar a los equipos de seguridad sobre el vapeo no autorizado o la presencia de sustancias químicas como el THC, el ingrediente activo del cannabis.

Perspectivas de los socios

IA responsable en la industria de la seguridad moderna

A medida que la IA continúa moldeando la industria de la seguridad, es esencial que las empresas comprendan sus riesgos y ventajas. Los proveedores de seguridad tienen una ventaja a la hora de abordar los desafíos relacionados con la IA gracias a su larga trayectoria con soluciones de IA.

Sin embargo, la responsabilidad de usar IA va más allá de la legalidad: requiere transparencia y consideraciones éticas. El marco de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) para la IA centrada en el ser humano destaca la importancia de garantizar que los clientes comprendan cómo funciona la IA y sus limitaciones, fomentando así la confianza con socios y clientes.

La IA en seguridad tiene como objetivo principal automatizar tareas y proporcionar información práctica. Si bien la automatización impulsada por IA mejora la eficiencia, es crucial evaluar los riesgos potenciales, como las consecuencias de un error de IA. La transparencia sobre las capacidades de IA permite a las empresas tomar decisiones informadas y gestionar los riesgos de forma eficaz, especialmente en sectores críticos como la fabricación y las infraestructuras críticas.

> La implementación responsable de IA requiere un diseño ético y un uso responsable.

Además, los sistemas de IA deben evaluarse para detectar sesgos y limitaciones, especialmente al analizar datos en condiciones variables. A medida que surgen nuevas tecnologías de IA, como la IA generativa, es necesario realizar pruebas rigurosas en escenarios reales para comprender plenamente su impacto.

En definitiva, la implementación responsable de IA requiere un diseño ético y un uso responsable. Los proveedores de seguridad deben garantizar que la IA no se utilice indebidamente y establecer relaciones sólidas y transparentes con sus socios. De esta manera, pueden generar confianza y mantenerse competitivos a medida que la IA evoluciona.

Perspectivas de los socios

Aprovechando los Datos de Seguridad para la Inteligencia de Negocios

Los datos de videovigilancia, control de acceso, sensores y otros sistemas de seguridad tienen un gran valor comercial, no solo para mejorar la seguridad, sino también para comprender el rendimiento del negocio.

En el comercio minorista, la hostelería y sectores relacionados, por ejemplo, el fraude y las pérdidas son problemas de larga data: en tiendas de conveniencia y restaurantes, el fraude de empleados genera entre un 25% y un 45% de las pérdidas. Pero ¿cuáles son los factores específicos que impulsan estas pérdidas y qué medidas específicas pueden tomar las organizaciones para reducirlas?

Una nueva generación de herramientas de inteligencia de negocios diseñadas para datos de seguridad ahora permite un análisis sofisticado de tendencias y un mejor conocimiento de la situación. Soluciones como VIGIL **TRENDS de 3xLOGIC** utilizan análisis basado en reglas e inferencia para ayudar a identificar patrones de robo interno, optimizar el rendimiento de los empleados y mejorar la eficiencia general de los procesos.

Un cliente observó una reducción en el fraude promedio por empleado identificado de $800 a $500.

Los datos no tienen por qué limitarse a los sistemas de seguridad. La integración de información de ventas, el clima y otras fuentes permite un análisis aún más completo, que incluye comparaciones entre tiendas, conversiones de ventas, datos de tiempo de permanencia y conteos de tráfico.

Esta información puede generar beneficios financieros directos. Un cliente de 3xLOGIC observó una reducción en el fraude promedio por empleado identificado de $800 a $500 en tres años. Para una cadena con mil sucursales, esto podría significar decenas de miles de dólares en prevención de pérdidas al año.

En definitiva, una inteligencia empresarial eficaz basada en la seguridad permite a las organizaciones anticiparse al riesgo, proteger sus resultados y construir una cultura de integridad.

Perspectivas de los socios

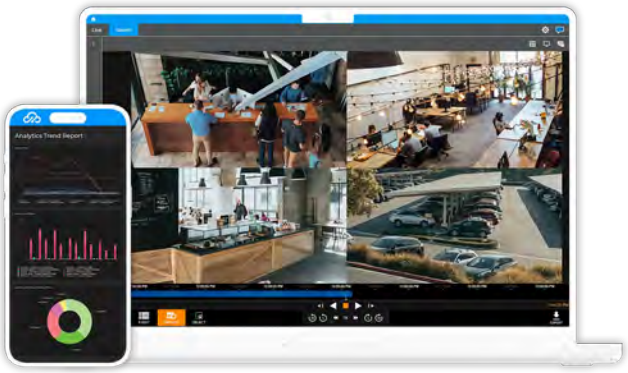
OpenEye

Desbloqueando información empresarial con una plataforma de video abierta

Elegir una plataforma abierta para video en la nube le permite aprovechar diferentes puntos de datos en sus operaciones y combinarlos con video para obtener una visión más completa de su negocio. Estas soluciones unificadas ayudan a impulsar una toma de decisiones más informada, generar eficiencia operativa y mejorar sus resultados.

Una plataforma abierta permite una integración fluida de los sistemas empresariales, como el control de acceso, los sensores ambientales, el punto de venta, la inteligencia empresarial y más, para mejorar la seguridad y las operaciones empresariales.

Estas integraciones ofrecen información práctica que va más allá de los casos de uso históricos del video. En la producción comercial, los gerentes pueden monitorear los niveles de inventario y la actividad de los empleados, garantizando así la eficiencia. Las operaciones de servicio se benefician de la información sobre los patrones de comportamiento de los clientes, junto con los datos de transacciones, lo que permite ajustes estratégicos para mejorar el rendimiento y los ingresos. Los equipos de marketing



y ventas obtienen una comprensión más profunda de las interacciones y preferencias de los clientes, lo que les permite adaptar sus esfuerzos para lograr el máximo impacto.

Al conectar y analizar los datos de los sistemas más importantes para su negocio, una plataforma abierta ofrece una solución de seguridad integral más completa. La seguridad conectada aporta valor a toda la organización al proporcionar los detalles necesarios para obtener información valiosa y, a su vez, tomar mejores decisiones. Al obtener una visión más completa de su negocio, usted ofrece una solución unificada que fortalece la seguridad, mejora sus resultados e impulsa su negocio hacia adelante.

> La seguridad conectada aporta valor a toda la organización.


Securitas
Technology

Promoción de la sostenibilidad y la optimización de las operaciones

La sostenibilidad se ha convertido en un compromiso central y un parámetro operativo para muchas organizaciones. Las empresas están estableciendo objetivos específicos de sostenibilidad con el objetivo de medir y reducir su impacto ambiental. El sector de la tecnología de seguridad está respondiendo a este cambio con un enfoque creciente en la eficiencia, la escalabilidad y la flexibilidad, lo que significa que las organizaciones pueden obtener beneficios concretos al tiempo que cumplen con sus compromisos de sostenibilidad.

> “Muchas organizaciones ahora priorizan la sostenibilidad como un objetivo empresarial fundamental. Al colaborar con nuestros clientes y socios, nos centramos en aprovechar la tecnología de seguridad para ayudarles a alcanzar estos objetivos.”

Kristi Keating | Vicepresidenta Global de Sostenibilidad de Securitas Technology

Descubriendo los beneficios de los servicios remotos

Una tendencia significativa en el sector es el enfoque remoto para el servicio y el mantenimiento. Al priorizar soluciones y servicios con sólidas capacidades remotas, las empresas pueden reducir la necesidad de desplazamientos físicos e inspecciones de sistemas, lo que ayuda a reducir las emisiones de carbono innecesarias.

La mejora de las capacidades remotas es una de las principales ventajas que ofrecen los sistemas de seguridad basados en la nube, que se están convirtiendo progresivamente en la opción preferida por muchas organizaciones. La capacidad de gestionar las operaciones de seguridad de forma remota, especialmente para empresas con múltiples ubicaciones y numerosos sistemas, permite a los responsables de seguridad supervisar todas las actividades de seguridad desde una única interfaz digital. Esto proporciona mayor claridad y control sobre las operaciones, además de ayudar a reducir los costes asociados a la presencia física.

Además, la monitorización y el mantenimiento remotos permiten tiempos de respuesta más rápidos y menos tiempo de inactividad, lo que impulsa la eficiencia operativa y apoya las iniciativas de sostenibilidad. Este enfoque beneficia tanto a clientes como a proveedores de servicios: mejora la prestación de servicios, operaciones más eficientes y una menor huella ambiental.

En búsqueda activa de soluciones más ecológicas

Las innovaciones en tecnología de seguridad también desempeñan un papel crucial en la promoción de la sostenibilidad. Por ejemplo, el desarrollo de cámaras de bajo consumo y el uso de LED en equipos responden directamente a la necesidad de soluciones más ecológicas. Estas tecnologías consumen menos energía, lo que reduce la demanda energética general y ayuda a las organizaciones a reducir su huella de carbono. Al integrar estas tecnologías sostenibles, las empresas pueden alcanzar sus objetivos de seguridad y, al mismo tiempo, contribuir a sus objetivos medioambientales.

Seguimiento eficiente de datos de sostenibilidad

Las organizaciones que participan en marcos como la iniciativa Science Based Targets (SBTi) deben comprender y documentar exhaustivamente su impacto ambiental. Esto incluye el consumo de energía de los sistemas de seguridad, que suele incluirse en las emisiones indirectas que una organización genera a través del uso de electricidad. Calcular estas emisiones requiere conocer el consumo de energía de cada dispositivo y cómo se genera la electricidad utilizada para su funcionamiento.



La industria de la seguridad está comenzando a facilitar este tipo de análisis. En colaboración con sus socios estratégicos, Securitas Technology lidera la iniciativa para incluir información sobre el consumo de energía de todos los equipos en las cotizaciones de los clientes (comenzando en Norteamérica), junto con una estimación de las emisiones en CO2 equivalente basada en la combinación típica de generación de electricidad en cada país o región.

Las mismas técnicas se pueden utilizar para documentar las emisiones de los equipos existentes, con acceso a los datos a través de una herramienta de gestión del ciclo de vida de la tecnología que almacena el historial completo de instalación, servicio y mantenimiento de cada dispositivo.

A medida que las empresas continúan estableciendo y persiguiendo sus objetivos de sostenibilidad, la industria de la seguridad puede apoyar estos esfuerzos, garantizando que tanto la seguridad como la sostenibilidad vayan de la mano.

Sostenibilidad como Prioridad de Seguridad[1]

33% de los profesionales de seguridad participan en actividades de sostenibilidad.

48% Considera que la sostenibilidad es importante o muy importante en la selección de tecnología.

El impulso hacia la sostenibilidad está transformando la industria de la seguridad, impulsando innovaciones que ofrecen beneficios tanto operativos como ambientales. Al adoptar estrategias de teletrabajo e integrar tecnologías de bajo consumo, las organizaciones pueden optimizar sus operaciones y, al mismo tiempo, contribuir a un futuro más sostenible.

[1]Encuesta ciega de terceros a 575 profesionales de seguridad con autoridad para la toma de decisiones en tecnología de seguridad en Australia, Francia, Alemania, Suecia, Reino Unido y Estados Unidos. Realizada en febrero y marzo de 2025.

Perspectivas de los socios

Flujos de Trabajo Eficientes con Acceso Simple y Seguro a los Sistemas

En los entornos de trabajo modernos de alto ritmo, las personas requieren un acceso rápido y sin fricciones a los sistemas físicos y digitales que las rodean sin comprometer la seguridad.

Algunos sectores, como el sanitario, lo perciben con mucha intensidad. Los profesionales sanitarios necesitan un acceso rápido y seguro a la información y los sistemas de los pacientes, mientras que los administradores requieren herramientas para gestionar las credenciales y optimizar los procesos eficazmente.

Los métodos tradicionales de control de acceso, como las contraseñas y los PIN, son vulnerables al robo, la pérdida y el uso indebido. Además, no ofrecen el nivel de seguridad necesario en entornos sanitarios donde los errores o el fraude pueden tener consecuencias graves.

Una nueva generación de tecnología de control de acceso permite a las organizaciones sanitarias y de otro tipo equilibrar eficazmente la facilidad de acceso con la seguridad y el control. Una plataforma unificada para la autenticación de identidad, como HID OMNIKEY, permite un inicio de sesión rápido y seguro en las estaciones de trabajo, ahorrando tiempo y mejorando la protección de datos.

Estos sistemas son compatibles con diversas tecnologías de tarjetas y se integran a la perfección con la infraestructura de TI existente, garantizando un acceso fluido a la información del paciente y cumpliendo con la normativa de protección de datos sanitarios.

La autenticación biométrica avanzada a través de una plataforma como **HID DigitalPersona®** para el sector sanitario es otra solución que aborda eficazmente los retos de acceso específicos de la atención sanitaria. El inicio de sesión único mediante factores biométricos, como huellas dactilares o reconocimiento facial, optimiza el acceso a múltiples aplicaciones, sistemas y espacios físicos del sector sanitario. Esto mejora la seguridad al eliminar contraseñas compartidas o débiles, mejora la experiencia del usuario y la productividad del personal sanitario, y cumple con los requisitos de seguridad de datos y privacidad. Además, ofrece un ahorro significativo de costes al reducir la sobrecarga de la gestión de contraseñas.

Al optimizar los flujos de trabajo y mejorar la seguridad, un control de acceso eficaz permite a los profesionales sanitarios dedicar menos tiempo a iniciar sesión en los sistemas y más a brindar atención y mejorar la experiencia del paciente.

Perspectivas de los socios

ASSA ABLOY
Opening Solutions

Cómo se integra la tecnología de seguridad en los edificios sostenibles

Ingenieros y arquitectos evalúan la huella de sostenibilidad de un edificio examinando toda la estructura para identificar áreas de consumo o pérdida de energía. Tradicionalmente, estas evaluaciones se han centrado en los sistemas de climatización (HVAC) y el aislamiento. Sin embargo, a medida que surgen nuevos productos, la atención se está centrando en otras áreas de alto consumo energético, como los entornos con gran cantidad de puertas y el consumo energético de las cerraduras y los dispositivos de control de acceso.

La mayoría de los edificios ya cuentan con infraestructura de red. Al aprovechar estas redes de TI existentes para aplicaciones de seguridad, como el control de acceso, podemos optimizar el consumo de energía, reducir los costes de cableado y mano de obra, y maximizar el valor de las inversiones iniciales en infraestructura. Las cerraduras con tecnología IP Power over Ethernet (PoE) y Wi-Fi facilitan este proceso. El uso de la infraestructura de TI existente permite a las instalaciones ampliar los sistemas de control de acceso de forma sencilla y rentable. La integración de la tecnología de seguridad en las prácticas de construcción sostenible mejora tanto la eficiencia como la sostenibilidad.

Los propietarios de edificios están estableciendo objetivos de sostenibilidad para reducir su huella de carbono. Buscan activamente productos que se ajusten a estos objetivos y desean asociarse con fabricantes con objetivos ambientales similares. Los clientes exigen cada vez más transparencia sobre dónde se fabrican los productos, los materiales utilizados y la energía empleada a lo largo de su ciclo de vida.

Ofrecemos este nivel de transparencia a nuestros clientes utilizando nuestra Brújula de Sostenibilidad para cada nuevo producto que desarrollamos, con el objetivo de lograr un menor impacto ambiental que los productos anteriores. Emitimos documentación de sostenibilidad verificada por terceros para educar a nuestros consumidores y ayudarles a obtener certificaciones ecológicas que les permitan alcanzar sus objetivos. Facilitamos a los clientes la incorporación de la sostenibilidad en cada proyecto de construcción, introduciendo productos más responsables en el mercado.

Perspectivas de los socios

Explorando el ROI de la Seguridad

Los sistemas de seguridad actuales van más allá del control de acceso y la vigilancia tradicionales, optimizando las operaciones comerciales e impactando positivamente en el Retorno de la Inversión (ROI). Es crucial que los usuarios e integradores de seguridad midan y comuniquen estos beneficios a las partes interesadas, transformando la seguridad de un centro de costos reactivo a un socio estratégico proactivo y aumentando la aceptación de futuras inversiones.

Cómo la videovigilancia y el control de acceso pueden generar ROI

Con IA y análisis, que a menudo operan en la nube, se pueden automatizar tareas repetitivas y que consumen mucho tiempo. Se pueden generar alertas sobre comportamientos inusuales, lo que permite a los operadores dedicarse a otras tareas. Esto mejora la eficiencia del equipo y el conocimiento de la situación.

La gestión de la respuesta también se ve mejorada, ya que los equipos de tierra pueden dirigirse en función de datos atribuibles, como el color de los vehículos o la ropa captados por las cámaras, o los repetidos intentos de acceso a zonas protegidas por parte de personas no autorizadas. Las cámaras pueden rastrear objetos en movimiento y transferir la supervisión de situaciones y objetos entre diferentes dispositivos. Esto facilita la respuesta ante intrusiones y el control perimetral.

A largo plazo, la información sobre el uso del sitio generada por los sistemas de control de acceso puede influir en la eficiencia del uso de un edificio, influyendo en la señalización y la planificación de rutas, e incluso ayudando a ajustar los programas de mantenimiento y limpieza en zonas de alto tráfico.

Primeros pasos

Colaborar con las partes interesadas de otros departamentos permite a los responsables de seguridad identificar áreas donde el control de acceso y el vídeo aportan valor añadido. También facilita la generación de métricas más amplias que los equipos de seguridad podrían desconocer, como tiempos de caja o de espera más cortos, la optimización de la programación, el ahorro, las mejoras en salud y seguridad y la gestión del consumo energético.

Por lo tanto, la consolidación de las soluciones de seguridad en una única plataforma de gestión facilita la obtención de información de valor añadido. Al estar todo en un solo lugar, los datos de los sistemas de video, control de acceso, detección y control perimetral se pueden utilizar para identificar mejoras y eficiencias.

También facilita mantener informados a todos los interesados, de modo que el retorno de la inversión (ROI) sea claro y comprensible.


Securitas
Technology

> “Cuando el personal se siente protegido, es más probable que permanezca en sus puestos, lo que reduce la rotación de personal y garantiza una mejor atención.”

Bill McCarthy, President of Securitas Healthcare

Securitas Healthcare

Construyendo una Cultura de Seguridad Laboral

Lecciones desde la primera línea del sector sanitario

La violencia en entornos sanitarios es un problema global y bien documentado, identificado por organismos que van desde la Organización Mundial de la Salud1 hasta la Unión Europea2 y los Centros para el Control y la Prevención de Enfermedades de EE. UU3. En EE. UU., el sector sanitario es el entorno laboral más peligroso para la violencia no mortal, representando un asombroso 73 %4 de todos los casos.

Por ello, el sector sanitario ha desarrollado un enfoque sólido para mitigar el riesgo de violencia laboral del que otros sectores pueden aprender.

“Proteger al personal sanitario requiere un enfoque multifacético que evoluciona junto con las amenazas emergentes. Al integrar tecnología de seguridad avanzada con la capacitación del personal, podemos crear entornos más seguros tanto para los cuidadores como para los pacientes”, observa Ara Kouchakdjian, vicepresidente de Inteligencia de Datos e Innovación en Salud de Securitas Healthcare.

Más información en securitashealthcare.com

1. “Violencia y acoso”. Organización Mundial de la Salud, 2025. https://www.who.int/tools/occupational-hazards-in-health-sector/violence-harassment
2. “Violencia en el lugar de trabajo”. Eurofound, 27 de febrero de 2023. https://www.eurofound.europa.eu/en/blog/2023/ violence-workplace-women-and-frontline-workers-face-higher-risks
3. “Priorizar a nuestro personal sanitario”. Centros para el Control y la Prevención de Enfermedades, 29 de mayo de 2024. https://blogs.cdc.gov/niosh-science-blog/2024/05/29/hcw_violence_mh/
4 “Violencia en el trabajo en el sector sanitario”. 2018. Oficina de Estadísticas Laborales, abril de 2020. https://www.bls.gov/iif/factsheets/workplace-violence-healthcare-2018.htm

Un enfoque multicapa para la seguridad

Garantizar un entorno de atención médica seguro requiere seguridad perimetral, acceso controlado, monitoreo en tiempo real y coordinación de respuesta rápida. Securitas Healthcare observa que cada vez más centros están desarrollando comités directivos contra la violencia en el lugar de trabajo que involucran a los departamentos legales, de gestión de riesgos, de seguridad y médicos para desarrollar una estrategia de seguridad integral y multicapa.

1

Fortalecimiento de la seguridad perimetral y el control de acceso inteligente

La seguridad hospitalaria comienza en su perímetro. La videovigilancia y el análisis de video monitorean áreas de alto riesgo como estacionamientos y puntos de acceso. La detección de movimiento y el reconocimiento facial permiten detectar amenazas en tiempo real, lo que permite a los equipos de seguridad intervenir antes de que los incidentes se agraven.

Los sistemas de detección de armas en cualquier entrada pueden prevenir situaciones peligrosas antes de que entren en las instalaciones. La autenticación con credenciales garantiza que solo el personal autorizado acceda a áreas sensibles.

Para optimizar la gestión de visitantes, los hospitales también implementan sistemas de seguimiento y notificación en tiempo real que brindan al personal visibilidad sobre quién entra y sale de las instalaciones.

2

Protección del personal: clave para la seguridad y la retención

Incluso con sólidas defensas perimetrales, los trabajadores de la salud siguen siendo vulnerables. La violencia es impredecible; la seguridad no siempre puede estar presente en todas partes.

Por esta razón, los hospitales invierten con frecuencia en soluciones de protección para el personal, como credenciales portátiles con botones de pánico integrados, como las que ofrece la solución de protección del personal de Securitas Healthcare. Estas permiten a los empleados solicitar ayuda discretamente durante incidentes de presión.

3

Invertir en capacitación para la desescalada y la preparación para emergencias

La tecnología por sí sola no es suficiente: el personal necesita habilidades para gestionar situaciones agresivas. La capacitación para la desescalada ayuda a los empleados a reconocer las señales de alerta temprana y a calmar las interacciones tensas.

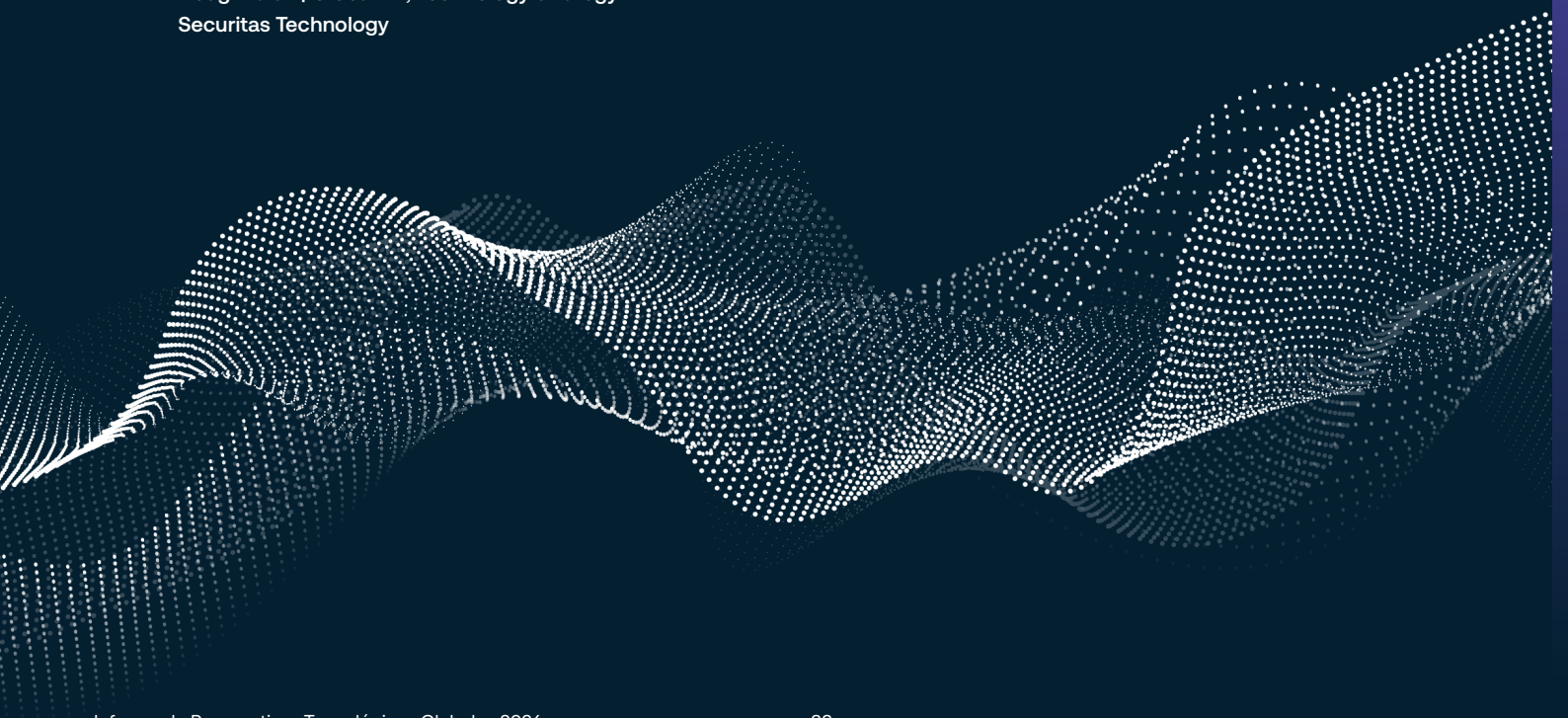
Los hospitales también realizan simulacros de preparación para emergencias de forma rutinaria. La capacitación para escenarios de agresores activos, incidentes con múltiples víctimas y violencia laboral garantiza que el personal comprenda su papel en una crisis.

“Cuando el personal se siente protegido, es más probable que permanezca en sus puestos, lo que reduce la rotación y garantiza una mejor atención al paciente”, afirma Bill McCarthy, presidente de Securitas Healthcare. “Al invertir en medidas de seguridad proactivas y desarrollar una estrategia de seguridad integral, los hospitales crean un entorno donde el personal se siente valorado, protegido y capacitado para brindar la mejor atención posible”.

Plan de Acción para Profesionales de Seguridad

> La tecnología de seguridad es ahora un motor de valor empresarial, además de cumplir con su misión principal de proteger a las personas y los bienes. Las inversiones estratégicas en soluciones y análisis basados en IA, servicios remotos y tecnología sostenible pueden ayudar a las organizaciones a mejorar la eficiencia operativa y alcanzar sus objetivos de seguridad, comerciales y ambientales.

Doug Walsh | Global VP, Technology Strategy
Securitas Technology



1 Desarrollar Casos de Uso para Datos de Seguridad basados en el ROI

En colaboración con las áreas operativas, financieras y otras áreas funcionales, analice cómo los datos de los sistemas de seguridad pueden contribuir a objetivos organizacionales específicos (por ejemplo, reducir las pérdidas, reducir los tiempos de espera, identificar riesgos de seguridad, etc.). Defina estos casos de uso y cree la infraestructura de datos y análisis, probablemente aprovechando la IA, para obtener información valiosa, mejorar la eficiencia empresarial y demostrar el valor añadido de las inversiones en seguridad.

2 Aprovechar los Servicios Remotos a través de la Nube

Infórmese sobre la creciente gama de servicios remotos disponibles para respaldar los sistemas de seguridad, desde la administración remota hasta el mantenimiento preventivo, e inclúyalos en la hoja de ruta de migración a la nube. Considere cómo un enfoque remoto puede contribuir a una mayor eficiencia y sostenibilidad.

3 Comprenda cómo la seguridad puede contribuir a los objetivos de sostenibilidad

Colabore con los líderes internos de sostenibilidad para definir la información necesaria para la función de seguridad. Esto puede implicar documentar el consumo de energía de los dispositivos de seguridad, que constituye una parte importante de la huella ambiental de la tecnología de seguridad. Trabaje con integradores y proveedores de tecnología de seguridad para establecer un proceso de generación eficiente de informes sobre estos datos, de modo que las operaciones de seguridad se mantengan alineadas con los objetivos de sostenibilidad.

Acerca de Securitas Technology

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

Con más de 13 000 empleados en 40 países, nuestra misión es hacer del mundo un lugar más seguro mediante tecnología de seguridad de vanguardia y un compromiso inquebrantable con el éxito del cliente.

Securitas Technology

Descubre un mundo diferente

3800 Tabs Drive
Uniontown, OH 44685

securitastechnology.com