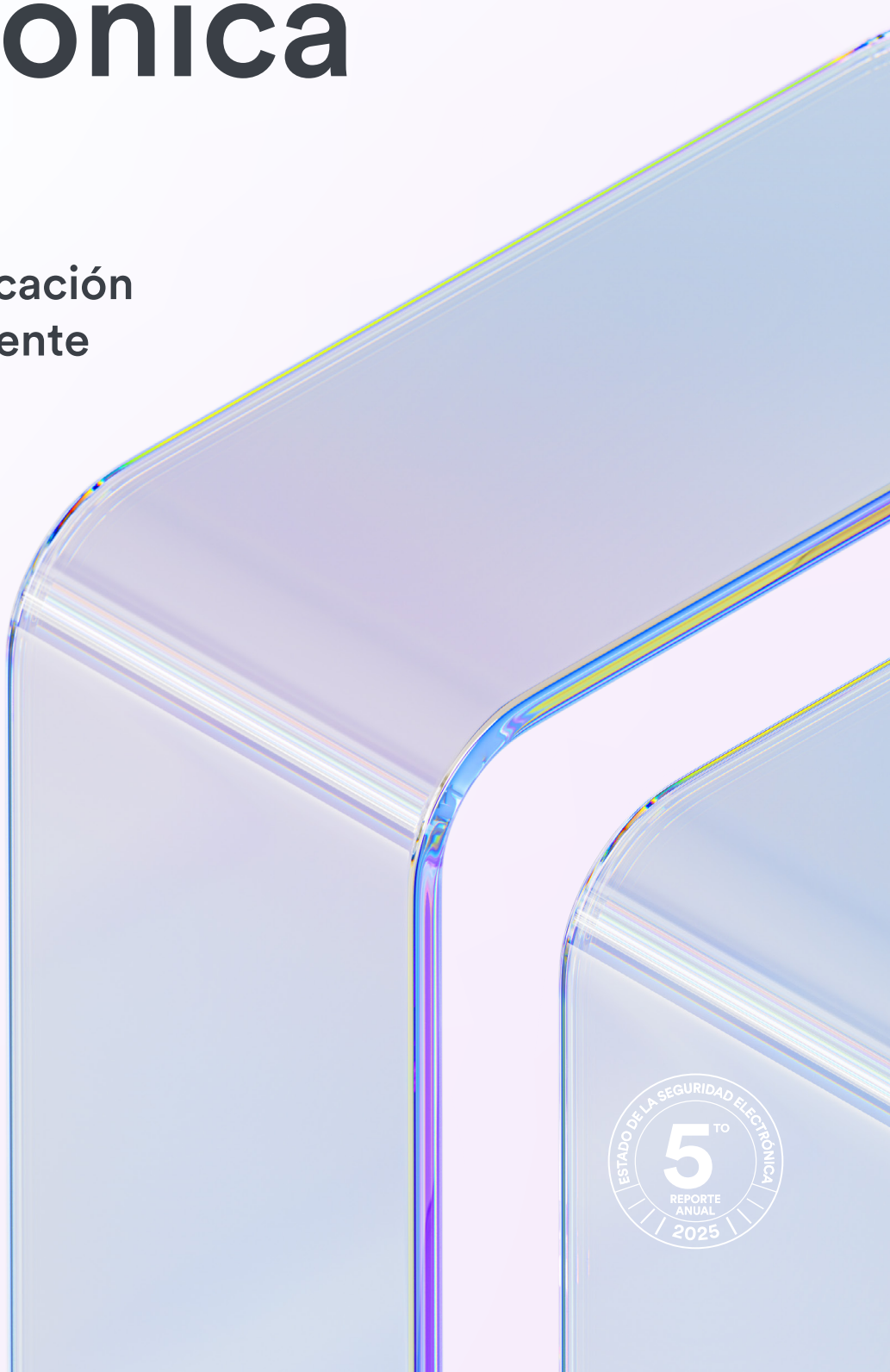
Estado de la Seguridad Electrónica 2025

Estrategia, planificación e inversión inteligente



Genetec™

Índice

Acerca de la investigación

Genetec Inc. encuestó a profesionales de la seguridad electrónica de todo el mundo del 12 de agosto al 15 de septiembre de 2024. Después de revisar los resultados y filtrar los datos, se incluyeron 5.696 encuestados en la muestra para su análisis.

El objetivo de la investigación fue:

- Conocer las operaciones y entornos de seguridad electrónica en 2024
- Identificar las perspectivas de los proyectos de seguridad electrónica para 2025
- Comprender los desafíos futuros

Resumen de la metodología de la investigación

La población objetivo de la encuesta se enfocó en tres grupos principales:

Usuarios finales

Individuos que trabajan para organizaciones que realizan actividades de adquisición, gestión o uso de tecnología de seguridad electrónica.

Integradores

Personas que asesoran, instalan, dan servicio o producen soluciones de seguridad.

Consultores

Personas que asesoran en el diseño, la instalación, el mantenimiento y el funcionamiento de soluciones de seguridad electrónica.

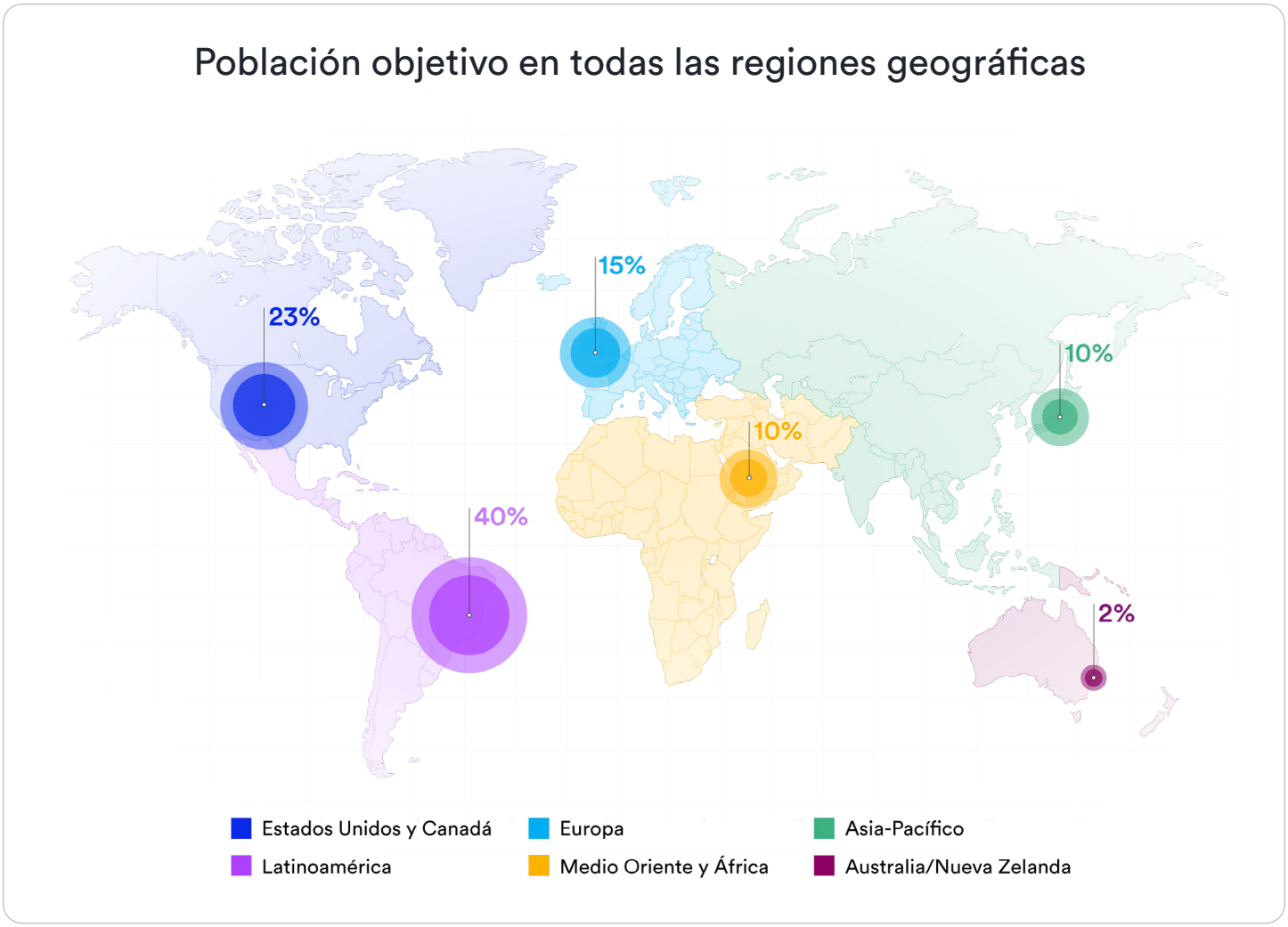


FIGURA A: DISTRIBUCIÓN DE LOS ENCUESTADOS POR REGIÓN.

- Se llegó a la población objetivo a través de eventos presenciales y mediante las listas de correo electrónico opt-in de terceros, listas de correo electrónico opt-in de Genetec y promociones digitales.
- Un conjunto de preguntas se dirigió a los usuarios finales, y otro a los integradores y consultores.
- Este reporte señala si las respuestas proceden de usuarios finales, integradores, consultores o todos los encuestados.
- En el análisis final sólo se incluyeron las encuestas completadas y enviadas por personas dentro de la población objetivo.
- En la mayoría de la encuesta, apenas hubo diferencias significativas entre las respuestas recibidas de las distintas regiones geográficas. Para más detalles sobre estas diferencias, mira el “Resumen de diferencias en todo el mundo.”

Para obtener más detalles sobre la metodología de la encuesta y la información demográfica de los encuestados, consulta los apéndices 1 y 2.

Resumen ejecutivo

El reporte de este año documenta interesantes cambios en el sector de la seguridad electrónica. A partir de los datos recopilados, observamos algunos cambios sorprendentes en las prioridades y un renovado interés por la excelencia operativa. En 2024:

El 57% de los usuarios finales afirmaron que los principales desafíos eran una infraestructura de seguridad electrónica y/o de tecnología de la información (TI) obsoleta.

El 65% de los integradores afirmaron que sus clientes quieren beneficiarse de las nuevas tecnologías y capacidades.

El 66% de los usuarios finales clasificaron el control de acceso (50%) y/o la videovigilancia (39%) como procesos clave o sistemas principales para este año. Esto coincide con que el 81% del trabajo de los integradores se centra en cualquiera de estos sistemas principales.

El 49% de los usuarios finales informaron que en 2024 tenían el 100% de sus sistemas de seguridad electrónica en sitio (no en la nube).

El 77% de los usuarios finales afirmaron que los departamentos de seguridad electrónica y tecnologías de la información (TI) trabajan en estrecha colaboración.

Principales hallazgos a nivel global

La economía influye en el cronograma de los proyectos

El 49% de los usuarios finales retrasaron sus proyectos en 2024 y el 45% en 2023. Sin embargo, las razones fueron muy distintas. En 2023, los problemas de la cadena de suministro fueron el principal motivo, pero en 2024 la causa fue la incertidumbre económica.

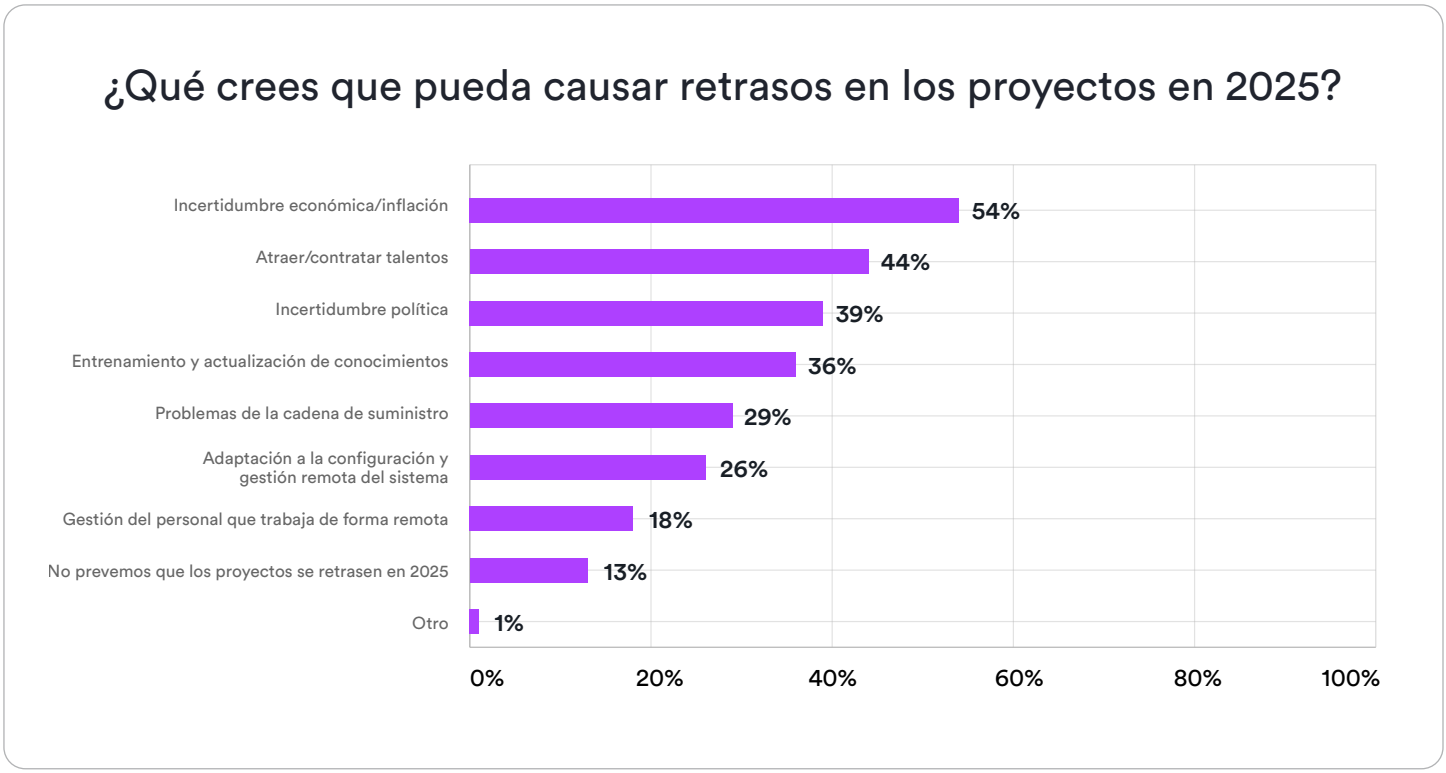


FIGURA B: PRINCIPALES CAUSAS PREVISTAS DE RETRASOS DE PROYECTOS EN 2025.

Perspectivas

Los cambios políticos también podrían haber influido. La revista Time se refirió a 2024 como “el año de las elecciones”, ya que al menos 64 países, entre ellos Estados Unidos, India, Taiwán, Corea del Sur y el Reino Unido, celebrarán elecciones nacionales decisivas en 2024.[1]

[1] Elecciones en todo el mundo en 2024 | TIME

Los problemas de contratación persisten

Desde 2021, tanto los usuarios finales como los integradores han informado constantemente sobre problemas de personal. Las perspectivas para 2025 muestran preocupaciones constantes. El 72% de los integradores esperan seguir teniendo problemas de contratación, mientras que sólo el 6% cree que mejorará.

Los integradores también preven que esta escasez de talento afectará sus proyectos, ya que el 44% afirma que atraer y contratar trabajadores provocará retrasos en los proyectos en 2025.

76%

de los integradores afirmaron que el rol del técnico en instalaciones es el más difícil de encontrar

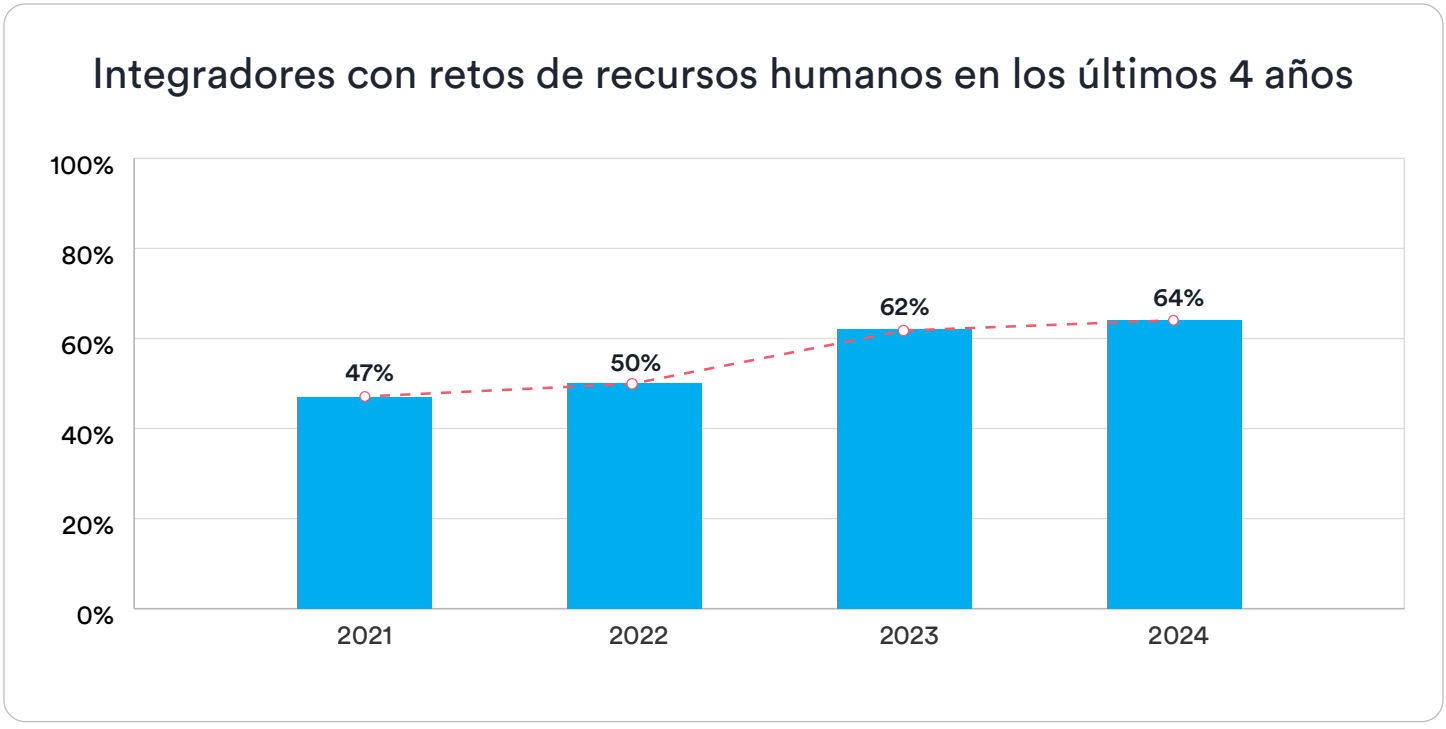


FIGURA C: PORCENTAJE DE INTEGRADORES QUE EXPERIMENTARON RETOS DE RECURSOS HUMANOS (2021-2024).

“Para tener éxito, los usuarios finales del sector de la seguridad electrónica necesitan soporte, entrenamiento y servicios que les ayuden a sacar el máximo provecho de sus inversiones en tecnología. Asociarse con expertos en seguridad reconocidos a lo largo de la implementación y el ciclo de vida de su solución seleccionada, garantiza que puedan maximizar su inversión y crear una postura de seguridad electrónica efectiva, confiable y escalable para su organización.”

Nadia Boujenoui
Vicepresidente de Experiencia del Cliente y Operaciones
Genetec Inc.

Ajuste de los presupuestos

Los presupuestos de gastos operativos (OpEx) en 2024 no coincidieron con las predicciones para 2023, donde más del 50% de los encuestados esperaban que los presupuestos de OpEx se mantuvieran estables o aumentaran. Por el contrario, el 44% informó de un aumento o una estabilización del presupuesto de OpEx. Los presupuestos de inversión (CapEx) también se mantuvieron estables, y sólo el 17% de los usuarios finales registraron un descenso. En medio de las incertidumbres económicas y políticas, estos ligeros ajustes resaltan el pragmatismo de la industria de la seguridad electrónica y el papel esencial que estos sistemas desempeñan en las organizaciones de todo el mundo.

48%

de los encuestados afirmaron que su presupuesto de CapEx aumentaría o se mantendría estable en 2024. De este grupo, el 48% indicó que aumentó entre un 11-25%

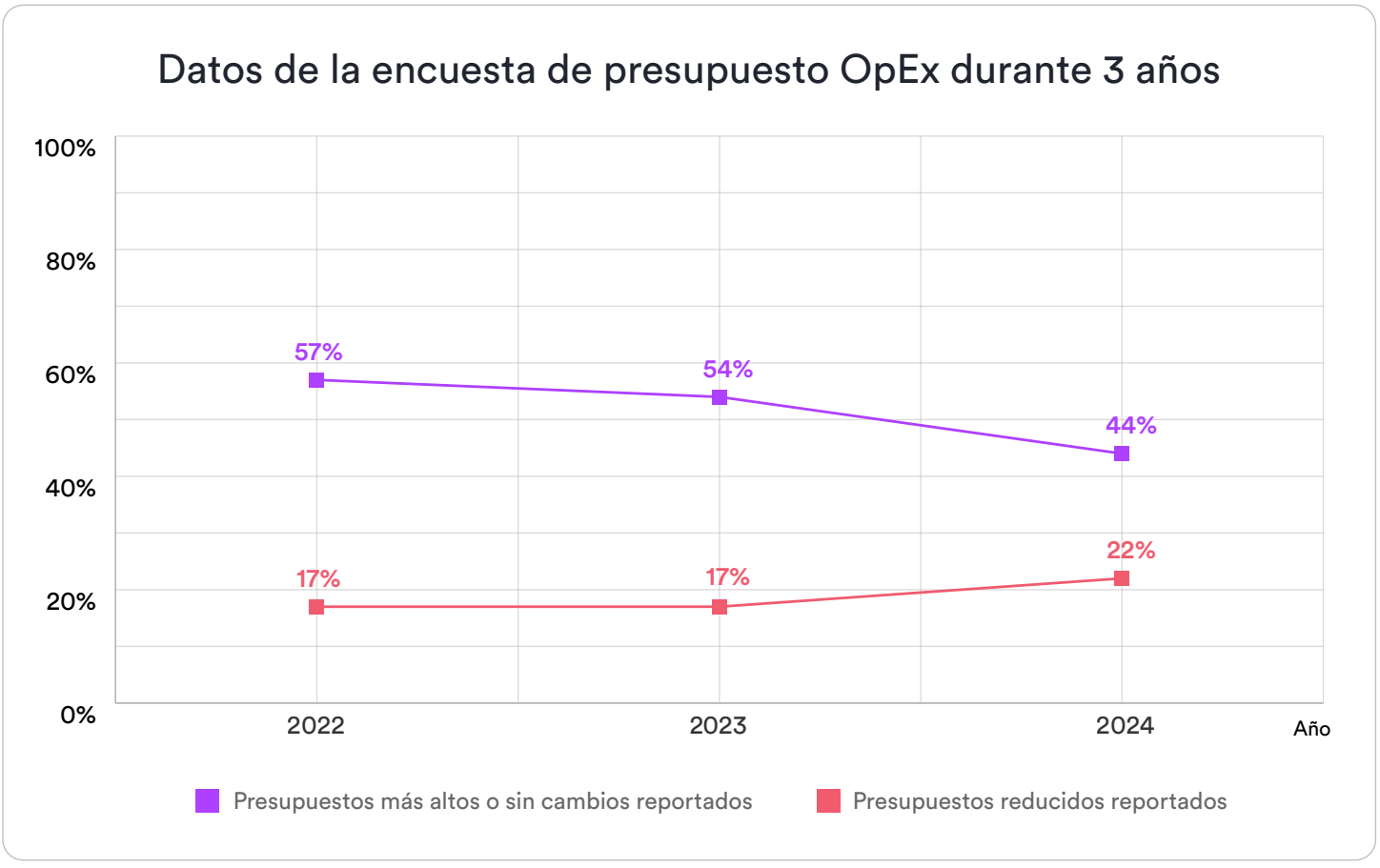


FIGURA D: PROPORCIÓN DE ENCUESTADOS QUE INFORMAN QUE LOS PRESUPUESTOS PARA GASTOS OPERATIVOS AUMENTARON, SE MANTUVIERON ESTABLES O DISMINUYERON (2022-2024).

La ciberresiliencia sigue siendo una prioridad

A medida que aumentan las ciberamenazas, más usuarios finales toman medidas para reforzar su ciberseguridad. Las organizaciones se guían por las normativas de la industria y los socios de ciberseguridad que cuentan con la experiencia necesaria para crear planes y ponerlos en marcha.

38%

de los consultores indicaron que planean ampliar su cobertura en ciberseguridad

Principales prácticas de ciberseguridad implementadas

	2023	2024
Educar a los usuarios en las mejores prácticas de ciberseguridad	61%	71%
Ajustar los permisos y privilegios de los usuarios	42%	51%
Protección del almacenamiento de datos	41%	47%
Endurecimiento de la infraestructura de seguridad	47%	44%
Protección del sistema contra accesos no autorizados	42%	44%

FIGURA E: PROPORCIÓN DE LOS ENCUESTADOS QUE IMPLEMENTARON PRÁCTICAS DE CIBERSEGURIDAD (2023-2024).

La normativa de la industria también está impulsando mejoras en la protección de datos y la ciberresiliencia. En 2024, el 67% de los usuarios finales afirmaron que su organización se vio afectada por estas normativas, un gran salto comparado con 2023, donde solo el 13% afirmó esto. Se mencionaron repetidamente ejemplos como el cumplimiento de la NIS2, el RGPD y otras normas específicas de la industria.

"A medida que la sociedad va ganando conciencia de los daños que una ciberseguridad inmadura puede causar en la vida cotidiana, los gobiernos de todo el mundo van implementando más directivas y normativas. Como era de esperar, esto ha llegado a la industria de la seguridad electrónica, aumentando la atención que prestamos a nuestra postura general de seguridad."

Mathieu Chevalier
Gerente y Arquitecto de Seguridad Principal
Genetec Inc.

“Una empresa que no cumple las leyes de privacidad y protección de datos, y que no adopta las medidas necesarias para proteger los datos personales que maneja y almacena, es una empresa que acabará perdiendo la confianza de sus clientes, sus empleados, sus socios y sus accionistas. A largo plazo, esto provocará pérdidas económicas.”

–Consultor encuestado

La adopción de la nube se enfrenta a las realidades de la seguridad electrónica

La adopción de la nube en la industria de la seguridad electrónica creció rápidamente entre 2022 y 2023, mientras que los resultados de la encuesta más reciente de 2024 revelaron una desaceleración. En 2024, el 38% de los usuarios finales informaron que más del 25% de su entorno de seguridad electrónica era nube o nube híbrida, un 6% menos que en 2023.

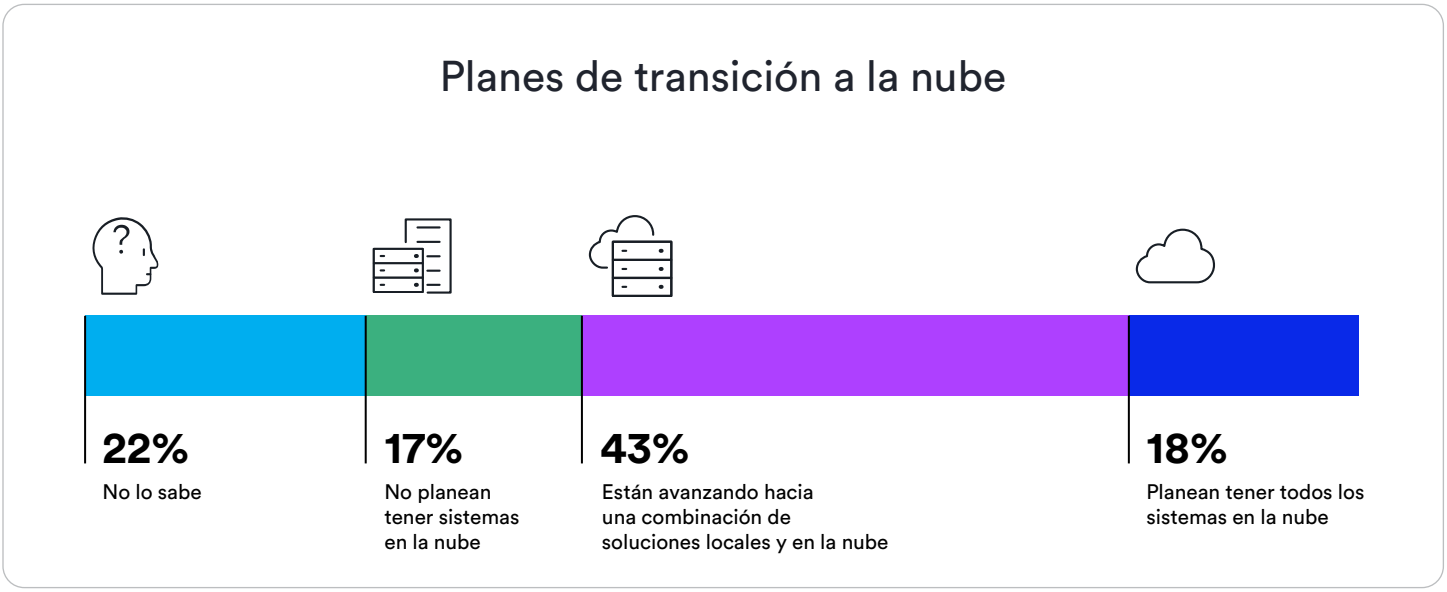


FIGURA G: PROPORCIÓN DE LOS ENCUESTADOS QUE PIENSA INCORPORAR LA NUBE.

Cuando se les preguntó a los usuarios finales qué había influido en la adopción de soluciones en la nube por parte de sus organizaciones, mencionaron razones en presupuestos relacionadas con “los costos de almacenamiento en la nube, retención de datos y ancho de banda.” “El temor a la pérdida de datos y el control general” fue la segunda razón, lo que demuestra que los profesionales de la seguridad electrónica desean trasladar las cargas de trabajo a la nube de forma gradual, a un ritmo adecuado para su empresa.

Equilibrio entre la adopción de la nube y sus costos

Las organizaciones con sistemas de seguridad electrónica más pequeños son más propensas a utilizar la nube para el almacenamiento, mientras que las que tienen sistemas más grandes no la adoptan tan rápidamente. De hecho, el 41% de los encuestados afirma haber ralentizado la adopción de la nube debido a los costos del almacenamiento, retención de datos y ancho de banda.

FIGURA H: DISTRIBUCIÓN DE CÁMARAS ALMACENADAS LOCALMENTE, EN SITIO O EN LA NUBE.

Los indicadores apuntan a que las organizaciones más pequeñas con menos problemas de almacenamiento y ancho de banda se beneficiarán más rápidamente de la comodidad y accesibilidad de la videovigilancia como servicio (VSaaS). A la hora de implementar sistemas más grandes y complejos en la nube, no es de extrañar que las organizaciones revisen sus inversiones antes de empezar a trabajar, o a medida que llegan los datos de las primeras implementaciones. La necesidad de encontrar un retorno de la inversión óptimo en la nube se ha convertido en una cuestión urgente.

Está claro que la gestión de los gastos en la nube es un reto emergente en el ámbito de la seguridad electrónica y que las organizaciones están empezando a estudiar con detenimiento el problema del desperdicio de la nube.

Perspectivas

La mayoría de las organizaciones carecen de estrategias proactivas de ahorro de costos en la nube.

Un estudio de Gartner muestra que las empresas desperdician un promedio del 35% de su gasto en la nube, con niveles de desperdicio que oscilan entre el 15% en entornos bien optimizados y el 55% en los no optimizados.

Las perspectivas de la nube son prometedoras para las implementaciones híbridas

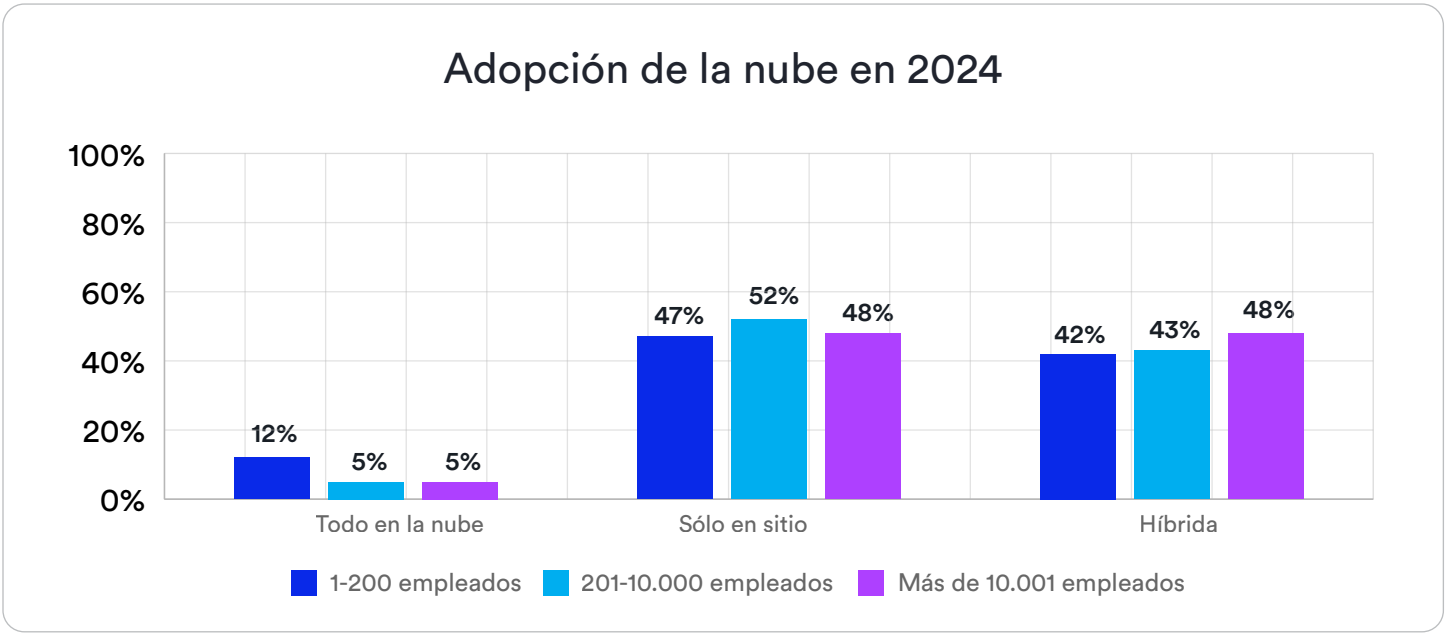


FIGURA I: ADOPCIÓN DE LA NUBE PARA IMPLEMENTACIONES DE SEGURIDAD ELECTRÓNICA.

En cuanto al futuro de la adopción de la nube, los resultados de la encuesta de 2024 dejan claro que la mayoría de las organizaciones consideran que la mejor forma de aprovechar la nube con éxito es a través de implementaciones híbridas. Las organizaciones más pequeñas, con probablemente menos problemas de hardware, retención y datos, están previsiblemente más interesadas y abiertas a las implementaciones completas en la nube.

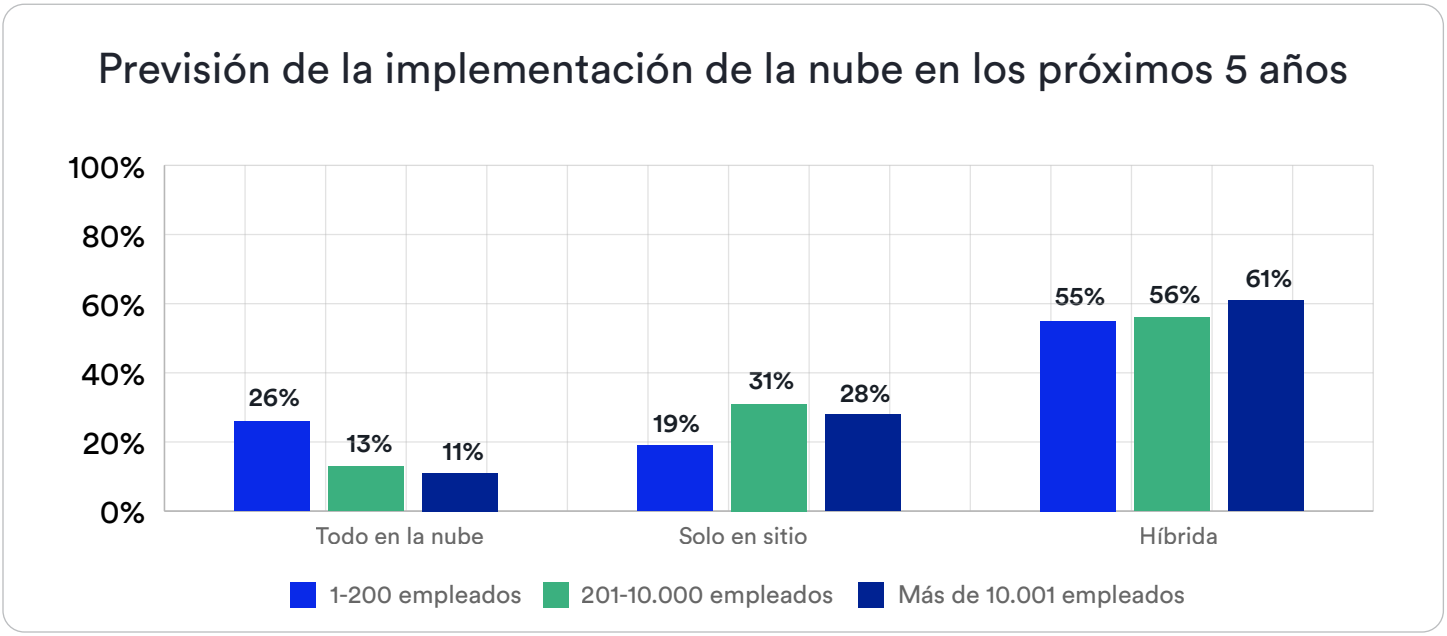


FIGURA J: PREVISIÓN DEL TIPO DE IMPLEMENTACIÓN DE LA NUBE POR TAMAÑO DE LA ORGANIZACIÓN.

Integradores

Los integradores también valoran positivamente los sistemas de seguridad electrónica basados en la nube:

78%

creen que habrá un aumento de nuevos sistemas en nube en 2025, frente al 73% del año pasado

2%

esperan una disminución, frente al 5% del año pasado

Consultores

Los consultores de seguridad electrónica también predicen que las implementaciones en la nube seguirán creciendo:

58%

estiman que el plazo típico para que sus clientes trasladen algunas cargas de trabajo a la nube sería dentro de los próximos 12 meses

66%

dicen que especificarían implementaciones de seguridad de nube híbrida en los próximos 5 años

25%

esperan especificar implementaciones completamente en la nube

Continúan las mejoras de los sistemas principales

En 2024, el 58% de los integradores vieron un aumento en los usuarios finales "añadiendo nuevas tecnologías a los sistemas existentes, incluyendo soluciones en la nube." Sin embargo, si miramos hacia 2025, el 51% de los usuarios finales respondieron que se centrarán en aprovechar las tecnologías existentes, como las herramientas de ciberseguridad, las analíticas de datos y la mejora de la colaboración entre departamentos. Esto demuestra que los usuarios finales buscan obtener valor de sus sistemas actuales y de sus inversiones en nuevas tecnologías.

Cuando se les pidió que dieran prioridad a los proyectos para 2025, todos los encuestados situaron el control de acceso y la videovigilancia entre los primeros de la lista.

FIGURA J: PRINCIPALES PROYECTOS QUE LOS CONSULTORES, INTEGRADORES Y USUARIOS FINALES ESTÁN PRIORIZANDO EN 2025.

Perspectivas
55% de los consultores indicaron que sus clientes planean aprovechar las tecnologías actuales para abordar nuevos retos y evaluar nuevos sistemas para casos de uso específicos.

“Año tras año, los encuestados siguen dando prioridad a la inversión en sistemas de gestión de video y control de acceso, ya que son fundamentales para su éxito. Ellos necesitan soluciones específicas que aporten valor a largo plazo con una confiabilidad, ciberseguridad y transparencia en la que pueden confiar. A medida que planifican el futuro, los usuarios finales buscan sistemas diseñados para crecer con ellos, que respalden sus objetivos actuales y futuros. Esto incluye soluciones flexibles de nube híbrida que equilibran los beneficios de la escalabilidad de la nube con el control de la infraestructura local, garantizando un retorno de la inversión óptimo y adaptabilidad a medida que evolucionan sus necesidades.”

Christian Morin
Vicepresidente de Ingeniería de Productos
Genetec Inc.

Inversiones en control de acceso

Cuando se trata de control de acceso, los usuarios finales quieren hacer más con su tecnología. Tradicionalmente centrados en restringir el acceso no autorizado, los usuarios finales están buscando construir funcionalidades adicionales que creen eficiencias y ofrezcan un enfoque más moderno para el acceso. La gestión de visitantes (41%), la biometría (39%) y la gestión de identidades (37%) encabezan la lista de nuevas inversiones en control de acceso en 2025.

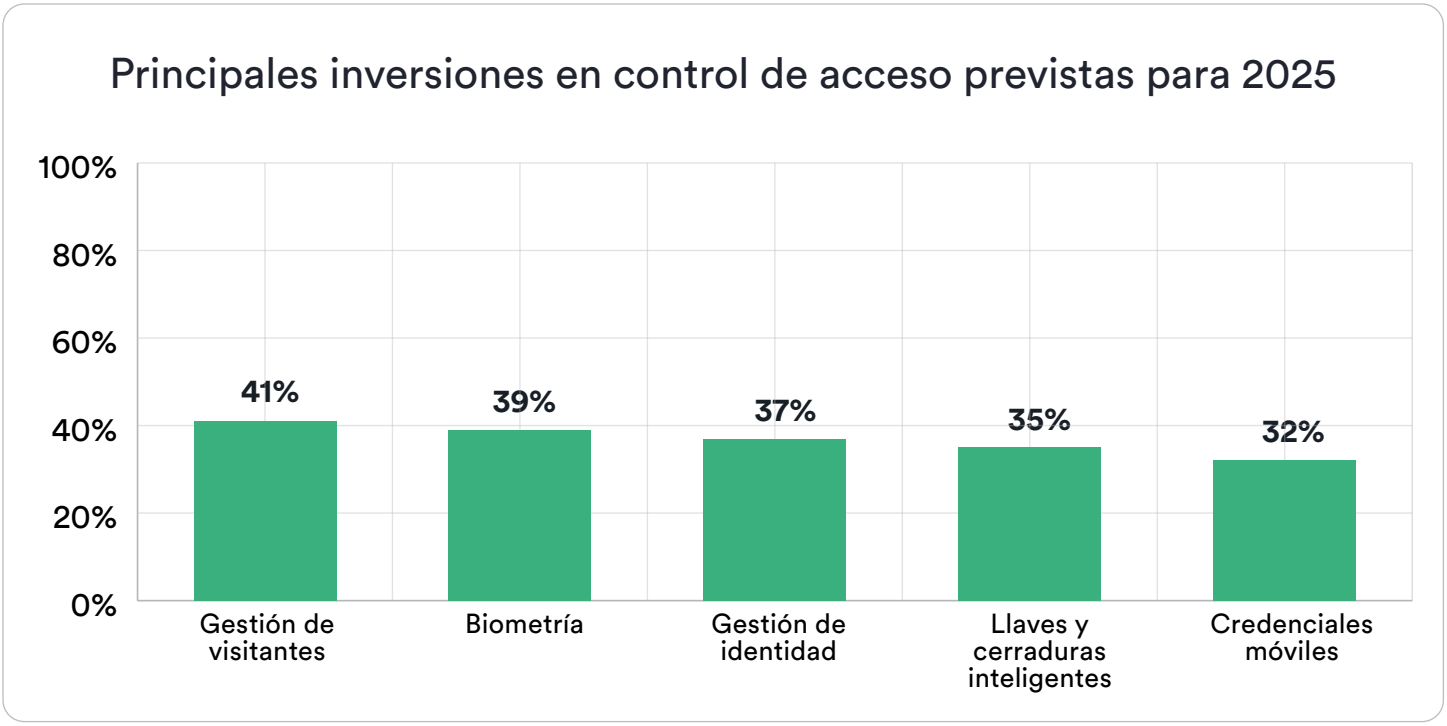


FIGURA K: DISTRIBUCIÓN DEL INTERÉS EN VARIAS TECNOLOGÍAS DE CONTROL DE ACCESO PARA 2025.

Actualizaciones de videovigilancia

En cuanto a la videovigilancia, los integradores dijeron que los usuarios finales se centran en las cámaras y los sistemas de gestión de video (VMS) como áreas clave dentro de los sistemas de seguridad electrónica antiguos a reemplazar o actualizar en 2025. También informaron de que sus clientes quieren sustituir los sistemas antiguos para integrar nuevas tecnologías y acceder a nuevas funciones, como:

- Mayor calidad de video
- Interfaz VMS simplificada
- Funcionalidades inteligentes en las analíticas de video impulsadas por el Deep Learning

Los usuarios finales sacan el máximo provecho de los datos de seguridad

La tendencia a recopilar, utilizar y compartir datos de seguridad para mejorar la seguridad electrónica y/o las operaciones empresariales ha continuado en las respuestas a la encuesta de este año. Tanto los usuarios finales como los consultores coincidieron en el creciente interés y uso de esta información en los principales departamentos.

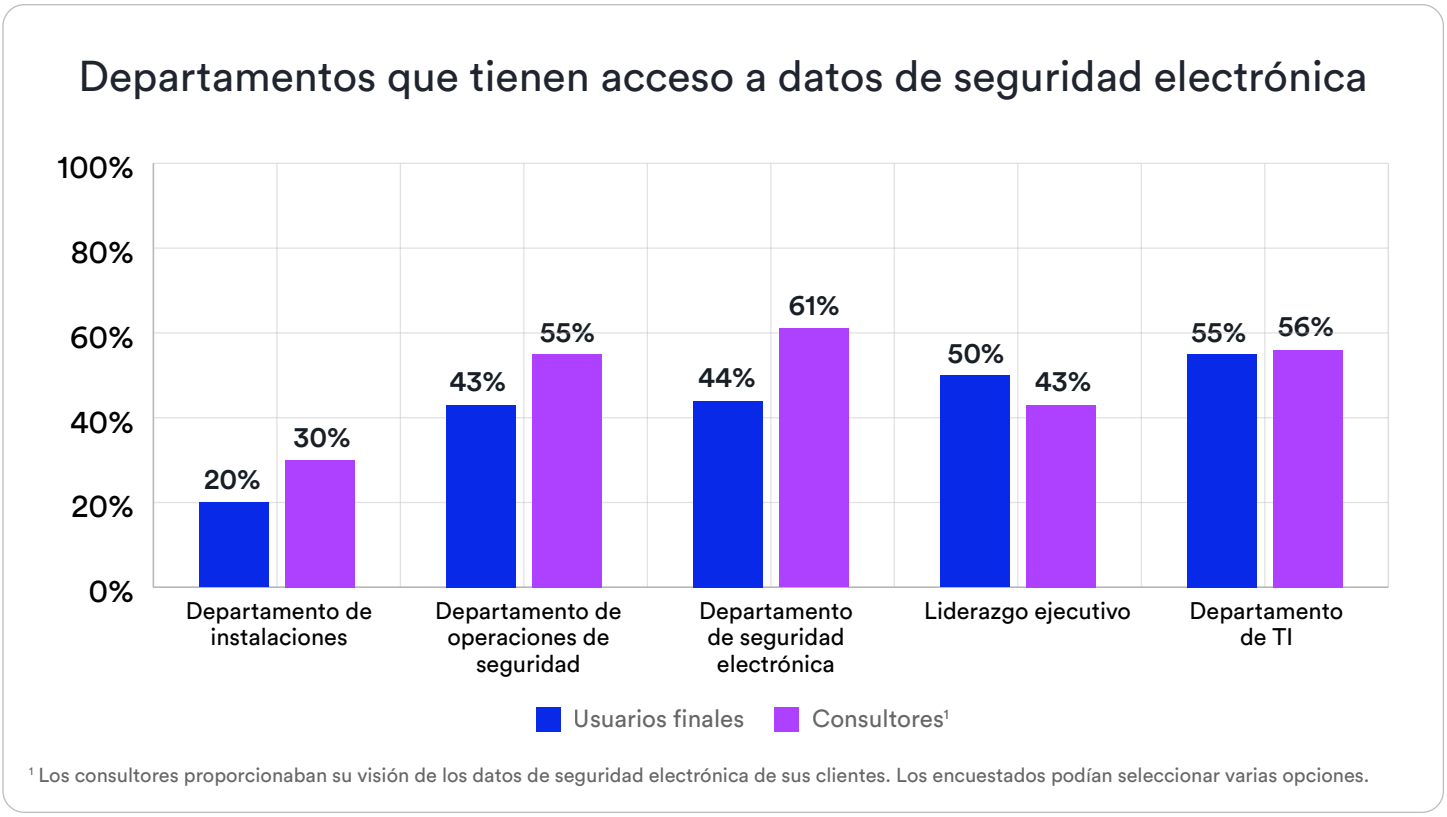


FIGURA L: DISTRIBUCIÓN DE LOS DEPARTAMENTOS DE USUARIOS FINALES Y CONSULTORES QUE TIENEN ACCESO A DATOS DE SEGURIDAD.

Los datos de seguridad electrónica son esenciales para configurar la estrategia y alinear la seguridad con los objetivos empresariales. Las respuestas a la encuesta revelan que los líderes ejecutivos consideran que estos datos son cruciales para alcanzar objetivos empresariales más amplios. El aprovechamiento de los datos disponibles en sus sistemas permite a los departamentos de seguridad electrónica desempeñar un papel fundamental en el empoderamiento del éxito general de su organización, así como de su protección y seguridad.

El uso estratégico de los datos de seguridad es cada vez mayor, ya que los usuarios finales desean mejorar el trabajo entre departamentos y la disponibilidad de los datos:

23%
Quieren herramientas de análisis y visualización de datos

22%
Quieren colaborar con otros departamentos para obtener otros resultados empresariales

22%
Quieren la democratización de los datos de seguridad en toda la organización y mejores reportes

En sus Centros de Operaciones de Seguridad (SOC, por sus siglas en inglés), los usuarios finales también están mirando más allá de los datos y tareas tradicionales, continuando con la integración de otros datos para observar, medir y reaccionar mejor ante incidentes, eventos y requisitos operativos.

Datos más comunes recopilados de otros sistemas para utilizarlos en los SOCs

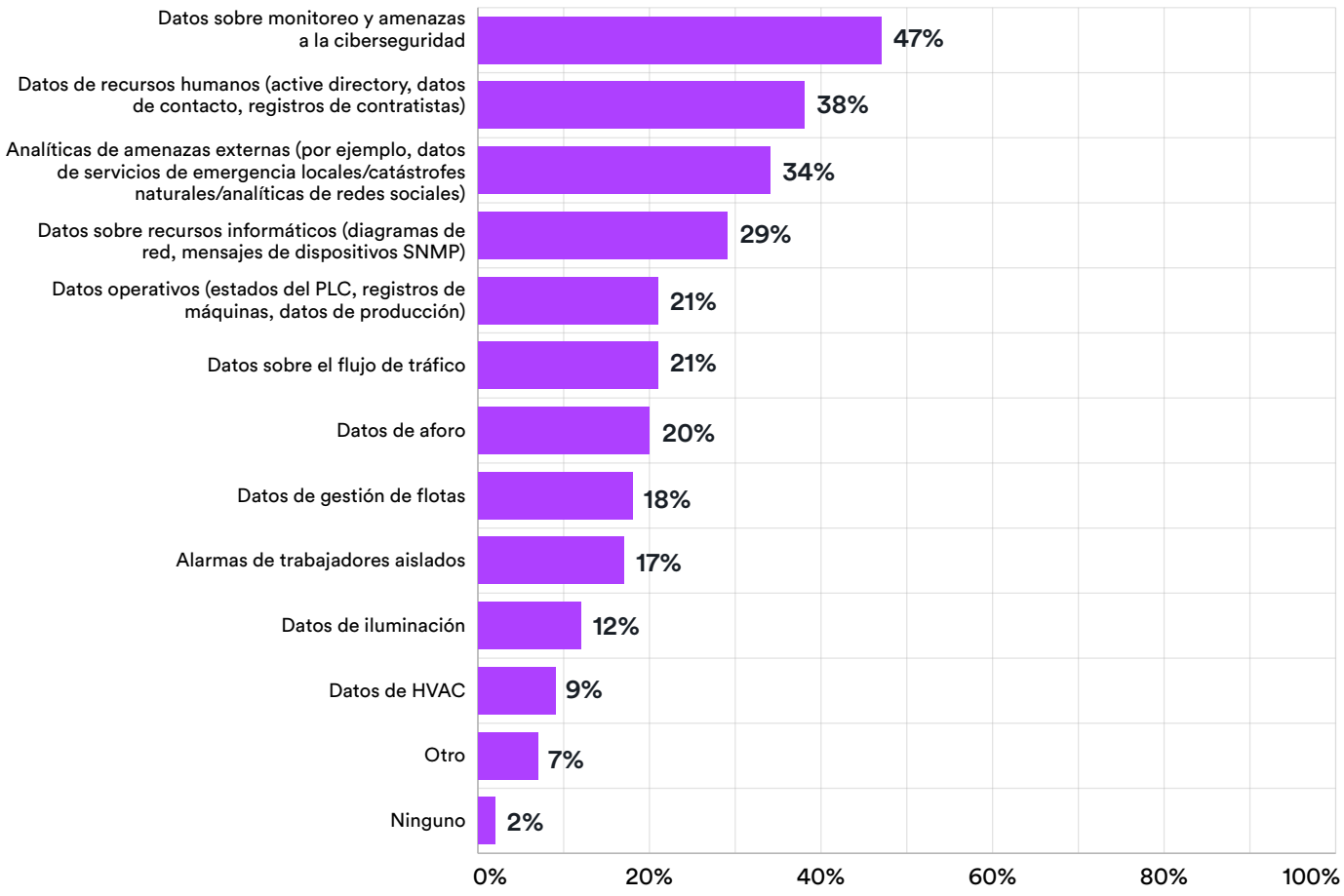


FIGURA M: DISTRIBUCIÓN DE LOS DIFERENTES TIPOS DE DATOS GESTIONADOS EN UN CENTRO DE OPERACIONES DE SEGURIDAD EN 2024.

“La seguridad electrónica es el guardián involuntario de datos increíblemente valiosos sobre los flujos de personas, bienes y vehículos. Esta información puede orientar decisiones críticas, pero históricamente el desafío ha sido transformar rápidamente los incidentes en datos de valor agregado. La verdadera oportunidad para la seguridad electrónica es proporcionar visibilidad de estos datos a un nivel superior y ayudar a los directivos a tomar medidas basadas en ellos.”

Pervez Siddiqui
Vicepresidente, Ofertas y Transformación
Genetec Inc.

Comprendiendo el valor de la IA

La integración de la inteligencia artificial (IA) en los sistemas de seguridad electrónica es un desarrollo prometedor y que los usuarios finales están ansiosos por explorar (el 10% lo hizo en 2024 y el 37% planea hacerlo en 2025).

El 27% de los usuarios finales responden que no están seguros de cómo implementar la IA de forma que añada valor. Además, más del 40% de los integradores afirman que los usuarios finales necesitan entrenamiento para comprender mejor las tecnologías.

La mayoría de los usuarios finales que se han comprometido activamente con la tecnología creen que el valor de la IA será el resultado de ayudarles a racionalizar y automatizar diferentes aspectos de sus operaciones de seguridad.

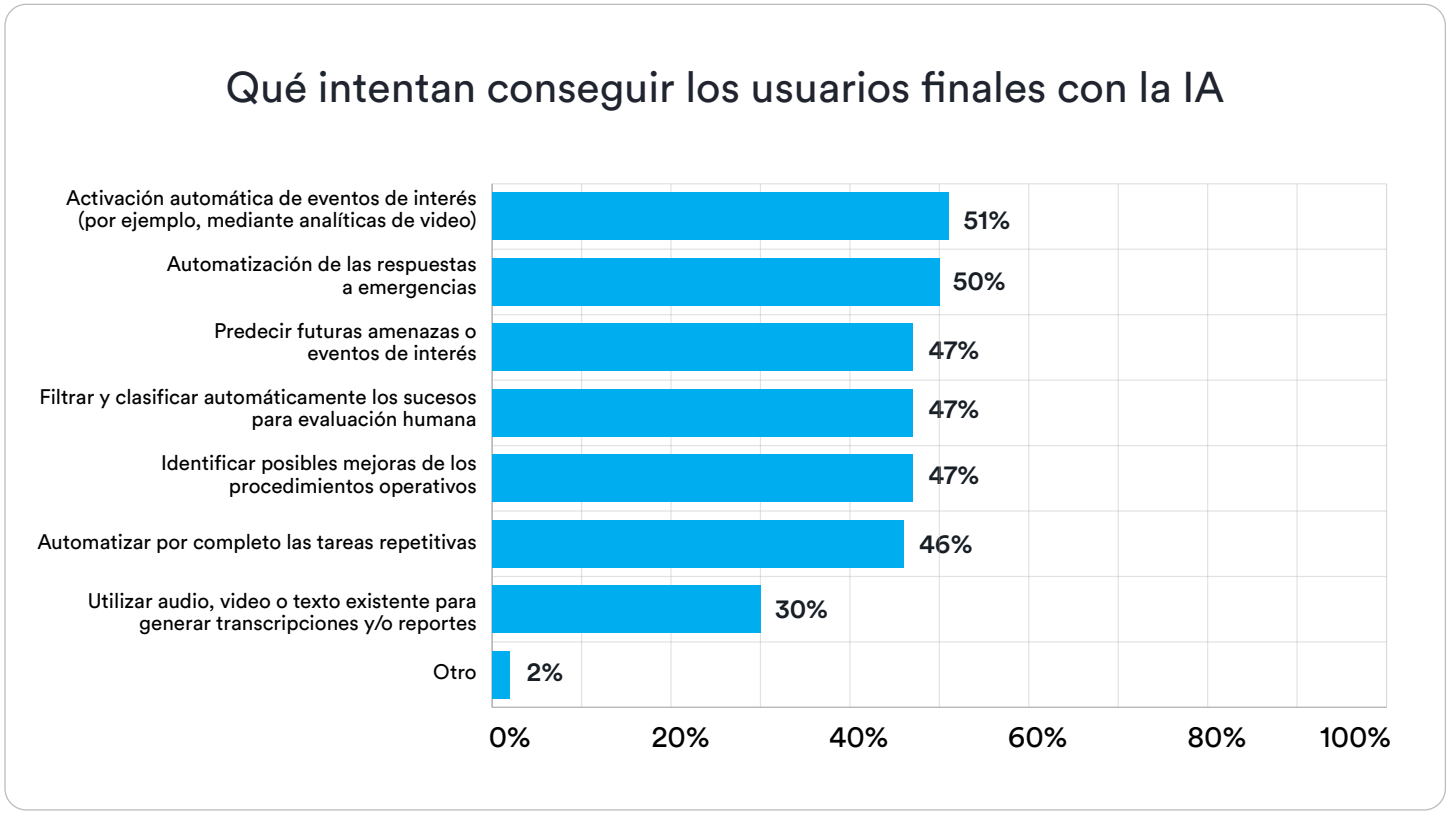


FIGURA N: DISTRIBUCIÓN DE OBJETIVOS PARA EL USO DE APLICACIONES DE INTELIGENCIA ARTIFICIAL EN 2024.

“Las técnicas de analíticas de IA continuarán marcando el comienzo de nuevas posibilidades, permitiendo a las empresas capitalizar los datos de seguridad electrónica existentes, la infraestructura y los sensores para automatizar tareas cotidianas e impulsar mayores niveles de eficiencia operativa en toda la empresa.”

Florian Matusek, PhD, MSc
Director de Estrategia de IA
Genetec Inc.

Al mismo tiempo, el 75% de los usuarios finales expresaron su preocupación por la forma en que se diseña y aplica la IA. Es importante que los fabricantes y los integradores aborden estos desafíos para ayudar a estimular la adopción y la utilización de la IA en los próximos años.

75%

de los usuarios finales tienen dudas sobre el diseño y la aplicación de la IA, sobre todo en lo que respecta a la responsabilidad y las directrices éticas

48%

de los integradores afirman que a los usuarios finales les preocupan los proveedores que no siguen las directrices de la IA responsable

“La IA seguirá dependiendo de la supervisión y el juicio humano durante las próximas décadas. El ser humano proporciona la creatividad y la intuición, y la máquina hace el trabajo pesado.”

Pierre Racz
CEO
Genetec Inc.

Las equipos de TI influyen en las decisiones de seguridad electrónica

Las tecnologías de la información (TI) siguen desempeñando un papel cada vez más importante en la gestión y en la toma de decisiones de los sistemas de seguridad electrónica. Cuando se les preguntó a los encuestados qué departamentos participaban más en las decisiones de compra, los departamentos de TI se situaron claramente por encima de los de seguridad electrónica.

Teniendo en cuenta que son muchos los departamentos implicados en el proceso de compra de seguridad electrónica, los encuestados también destacaron la importancia del liderazgo ejecutivo en estas decisiones de compra, a menudo cruciales para la misión, sobre todo planteadas por los usuarios finales.

Los 3 principales departamentos implicados en las decisiones de compra para 2024 [1]

	Usuarios finales	Integradores	Consultores
Departamento de TI	51%	51%	51%
Departamento de seguridad electrónica	44%	44%	47%
Liderazgo ejecutivo	55%	36%	41%

[1] La tabla representa un subconjunto de departamentos

FIGURA O: DISTRIBUCIÓN DE LOS PRINCIPALES DEPARTAMENTOS IMPLICADOS EN LAS DECISIONES DE COMPRA POR TIPO DE ENCUESTADO.

“A medida que evolucionan las exigencias en materia de seguridad electrónica, es importante poder ayudar tanto a los equipos informáticos como a los de seguridad electrónica en la adopción de los productos existentes y la implementación de nuevas tecnologías. Con la ciberseguridad, y las cuestiones de seguridad y protección en juego, la selección de proveedores que comprendan y satisfagan las necesidades de capacidad y cumplimiento de ambos grupos es fundamental para el éxito.”

Michel Chalouhi
Vicepresidente de Ventas Globales
Genetec Inc.

Como era de esperar, los encuestados que trabajaban en departamentos de TI y de seguridad electrónica tienen prioridades diferentes en relación con la implementación de la tecnología. En 2024, el 47% de los profesionales de TI se centraron en la implementación de herramientas de ciberseguridad, en comparación con el 27% de los profesionales de seguridad y protección. De forma similar, el 37% de los encuestados de TI señalaron las soluciones basadas en la nube como una prioridad, en comparación con el 27% de los encuestados de seguridad electrónica.

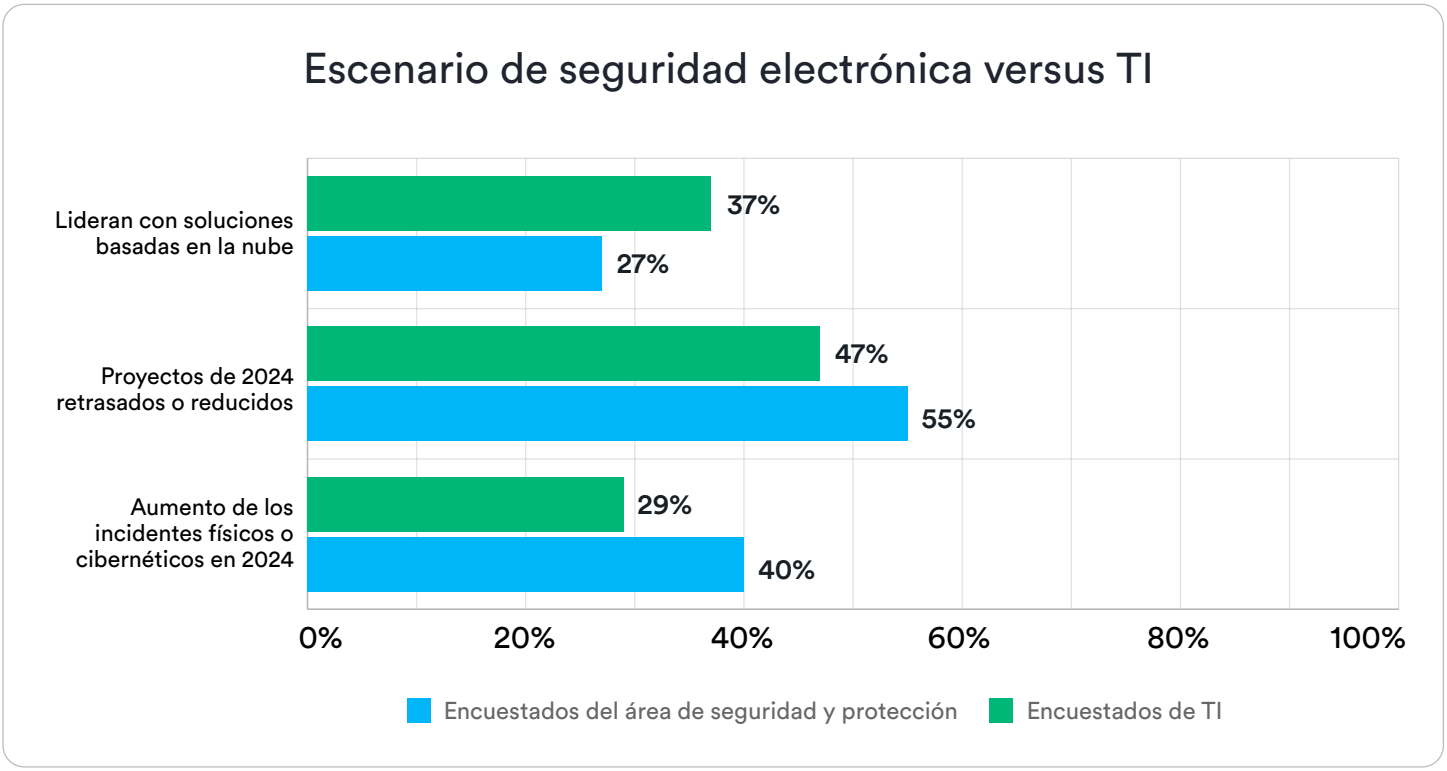


FIGURA P: DISTRIBUCIÓN DE LOS PRINCIPALES ESCENARIOS DE LOS EQUIPOS DE SEGURIDAD ELECTRÓNICA VERSUS TI.

Conclusiones principales

Conclusión 1
Practicidad frente a tendencias pasajeras

Saliendo de las incertidumbres del mercado de 2024, los usuarios finales están haciendo planes prácticos para 2025. Buscan soluciones confiables y rentables que mejoren la seguridad sin introducir complejidades ni costos innecesarios. La industria se centra cada vez más en tecnologías que respondan a las necesidades cotidianas, al tiempo que siguen de cerca las innovaciones tecnológicas para determinar cuándo les conviene implementarlas.

Continúa el deseo de innovar, de adoptar nuevas tecnologías e implementar la seguridad electrónica de nuevas formas; sin embargo, los usuarios finales buscan soluciones reales que puedan mejorar de forma confiable su trabajo y eficiencia sin salirse de su presupuesto. La migración a la nube y la adopción de herramientas de IA siguen siendo prioritarias, pero se basan en realidades empresariales que dan prioridad a las implementaciones de nube híbrida y a un enfoque mesurado para encontrar casos de uso adecuados para las nuevas tecnologías.

En el centro de las prioridades y el presupuesto, está la necesidad permanente de construir sistemas confiables de control de acceso y videovigilancia. Éstas siguen siendo las principales preocupaciones de los departamentos de seguridad electrónica. Las organizaciones se están centrando en formas de adoptar nuevas tecnologías en su infraestructura existente para ayudarles a mejorar las operaciones, aumentar la resistencia cibernética y ofrecer seguridad electrónica de una manera más rentable.

Control de acceso #1

El control de acceso es la máxima prioridad por quinto año consecutivo. Los proyectos centrados en la videovigilancia ocupan el segundo lugar.

Conclusión 2
El equipo de TI influye en la toma de decisiones

El rol de TI es proteger las redes digitales y mantener los datos seguros. La seguridad electrónica protege a las personas, los edificios y otros bienes. Sin embargo, hoy estos roles están más interconectados que nunca. Los resultados de la encuesta muestran que esta asociación ha dado lugar a una mayor colaboración con TI en las decisiones de compra.

Al combinar sus conocimientos, estos equipos trabajan juntos en beneficio de la organización para sortear las complejidades de la evaluación tecnológica y apoyar a las numerosas partes implicadas en el proceso de compra. Conjuntamente, los equipos de TI y de seguridad electrónica pueden aportar un enfoque de seguridad más completo combinando la experiencia en evaluación de amenazas y respuesta de los profesionales de seguridad electrónica con los conocimientos especializados de TI en diseño de redes, analíticas de datos y ciberseguridad. Esta colaboración fortalece tanto la seguridad de la organización como la seguridad de la red y la eficiencia operativa, creando una postura de seguridad más resistente y unificada.

Más del 50%

de todos los encuestados afirman que los departamentos de TI participan en las decisiones de compra.

Conclusión 3
De un centro de costos a una inversión rentable

En la actualidad, los datos de seguridad electrónica suelen compartirse con los departamentos de TI, pero más allá de esto, el conocimiento de su contenido puede ser limitado en una organización. Debido a que el equipo de TI tiene en sus manos las claves de la seguridad electrónica y, a menudo, las solicitudes de integración de sistemas, es posible que los responsables de los departamentos de seguridad electrónica no comprendan ni controlen plenamente el valor organizacional adicional que puede derivarse de sus propios sistemas.

Las integraciones entre sistemas de seguridad, otros dispositivos del IoT y tecnologías operativas pueden aportar un valor fundamental a las operaciones empresariales. Es necesario invertir para identificar problemas y explorar integraciones y fuentes de datos beneficiosas de los sistemas existentes. Cuando se adopta este concepto, se puede convertir un centro de costos tradicional como la seguridad electrónica en un retorno de la inversión cuando sus datos se utilizan para tomar decisiones empresariales. Este hecho permite al equipo de seguridad electrónica ayudar e influir en la estrategia y la toma de decisiones de la organización en general.

22%

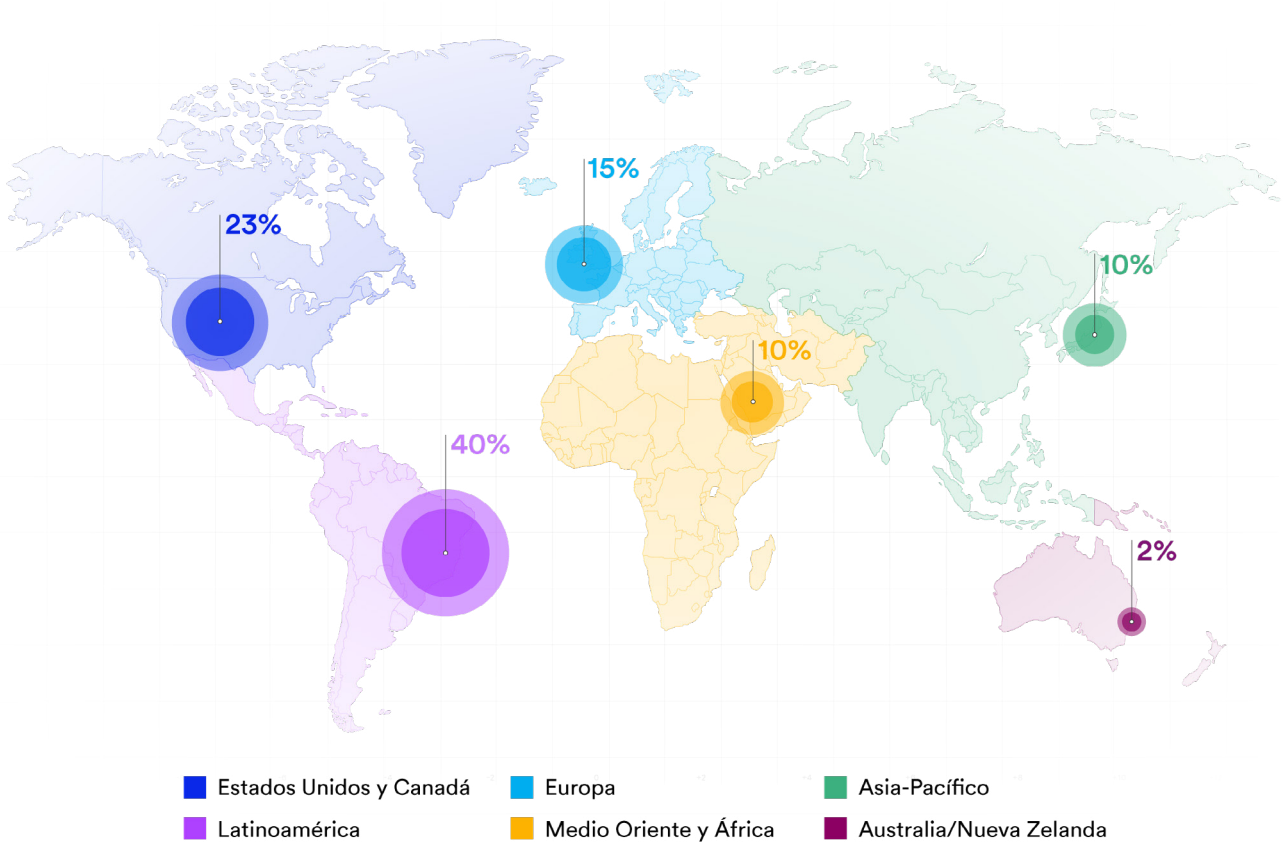
de los usuarios finales tienen previsto centrarse en la seguridad del acceso a los datos y en la mejora de los reportes en 2025.

Resumen de las diferencias en todo el mundo

El análisis de la encuesta se centró en las seis grandes regiones geográficas siguientes:

- Asia-Pacífico
- Australia, Nueva Zelanda y el resto de Oceanía
- Europa
- Latinoamérica
- Medio Oriente, Turquía y África
- Estados Unidos y Canadá

Esta sección documenta algunos ejemplos interesantes en los que las respuestas a la encuesta de una región determinada variaron con respecto al promedio global.



Asia-Pacífico

Interrupción mínima de los proyectos en 2024, fuerte adopción de la nube y la nube híbrida en entornos de seguridad electrónica.

Alto uso de la nube híbrida en entornos de seguridad electrónica: Los usuarios finales de Asia-Pacífico informaron de un mayor uso de la nube híbrida en general entre todas las regiones. Sólo el 40% de los usuarios finales describe su entorno de seguridad electrónica como totalmente local.

Control de acceso en la nube: Los usuarios finales de Asia-Pacífico tenían la mayor proporción de ACaaS – utilización de todo el control de acceso en la nube y, en consecuencia, el menor uso de sistemas de control de acceso en sitio.

La historia más positiva en cuanto a implementaciones de proyectos en 2024: Los usuarios finales de Asia-Pacífico fueron los que reportaron la mayor proporción de proyectos que no se vieron afectados por retrasos. El porcentaje de usuarios finales que declararon retrasos fue inferior al de las demás regiones. Los usuarios finales de Asia-Pacífico también reportaron el mayor porcentaje de proyectos que habían sido ampliados (más del 20%, frente al promedio global del 14%).

Australia, Nueva Zelanda y el resto de Oceanía

El uso de la nube es menor debido a la preocupación por alojar los datos dentro del país.

El mayor porcentaje de seguridad electrónica permanece en sitio: Más del 62% de los usuarios finales afirmaron no utilizar actualmente ninguna nube en el entorno de seguridad electrónica.

Es muy probable que la falta de infraestructura de centros de datos en Australia y Nueva Zelandia, ralentice la adopción de la nube: el 21% de los usuarios finales mencionaron "la falta de infraestructura de centros de datos en mi región" como motivo para ralentizar su adopción de la nube. Esto se compara con el promedio global de 6% y no más del 8% en las otras regiones.

Europa

Los mercados maduros se centraron en la modernización de sistemas antiguos y la detección de intrusos.

Ciclo de actualizaciones en 2025: Los usuarios finales europeos eligieron la migración y la renovación de los sistemas antiguos como primer objetivo para 2025. Esta opción fue la 4ª más popular en el promedio global.

Escaso almacenamiento de video en la nube: El 55% de los usuarios finales europeos afirma que no almacenará ningún tipo de video en la nube en 2025. Esta cifra es muy superior al promedio global del 33%.

Los sistemas de detección de intrusión son más populares en los entornos de seguridad: Un mayor porcentaje de los encuestados europeos tiene implementada la detección de intrusión en su entorno de seguridad electrónica: 55% frente al 33% de promedio global.

Latinoamérica

Preocupación por la falta de personal en la región, pero son los más optimistas sobre la futura migración a la nube e implementaciones de IA.

Retos de personal en 2025: Los integradores de Latinoamérica son los más preocupados por los retos de personal que se avecinan, ya que el 88% afirma que aumentarán un poco o significativamente en 2025. Aunque esta cifra fue alta en todas las regiones, ninguna superó el 71%.

Los más optimistas sobre el uso futuro de la nube: Más del 45% de los usuarios finales en Latinoamérica prevén una implementación de nube híbrida en sus sistemas de seguridad dentro de los siguientes 5 años. Además, el 84% de los integradores esperan ver un aumento en la instalación de nuevos sistemas de seguridad que permitan la conectividad a la nube, en comparación con un promedio global del 78%.

Adoptando con cautela la IA: Latinoamérica es una de las primeras regiones que planea implementar el aprendizaje automático y/o aplicaciones de grandes modelos del lenguaje (LLM) en su entorno de seguridad física para 2025 (44% frente al 37% a nivel global). El 56% de las organizaciones que planean integrar IA tienen como objetivo automatizar el envío de respuestas de emergencia. Sin embargo, están procediendo con cautela, expresando preocupaciones significativas sobre cómo se utilizarán los datos y cómo funciona la IA.

Medio Oriente, Turquía y África

Grandes presupuestos, fuertes implementaciones de IA, pero dificultades con el personal calificado.

Los presupuestos más altos: Los usuarios finales de esta región fueron los que más afirmaron haber tenido un aumento del presupuesto OpEx para 2024, con un 37% comparado con el promedio global del 23%. Los usuarios finales de esta región también fueron los que más aumentaron su presupuesto, entre un 76% y un 100%.

El entrenamiento del personal es el principal reto: Los usuarios finales de esta región seleccionaron "el entrenamiento y la capacitación del personal" como su reto #1 en 2024, ninguna otra región seleccionó este reto como #1.

Implementaciones de IA: Un mayor porcentaje de usuarios finales de Medio Oriente que cualquier otra región declaró que ya había implementado la IA en su entorno de seguridad electrónica en 2024 o tenía previsto hacerlo en 2025. Un total del 60% de los usuarios finales frente al promedio global del 47%. Esto refleja la naturaleza avanzada de algunos de los proyectos empresariales y gubernamentales en la región de Medio Oriente.

Estados Unidos y Canadá

Más implicación de las TI y, por tanto, mayor atención a la ciberseguridad, pero más cautela en el uso de la IA.

Menos planes inmediatos para la integración de la IA: En Estados Unidos y Canadá, la mayoría de los usuarios finales (57%) afirmaron no tener planes de integrar el Machine Learning, la IA o los LLMs en sus entornos de seguridad electrónica. El promedio global fue del 42%. En comparación con otras regiones, también son las menos propensas a declarar que tienen planes para hacerlo en 2025.

Inversión en cibereducación: El 77% de los usuarios finales de Estados Unidos y Canadá educaron a los empleados de su organización en las mejores prácticas de ciberseguridad. En otras regiones fue del 66-69%.

Mayor participación de TI: El 61% de los integradores en EE.UU. y Canadá consideraron que los departamentos de TI participaban más en la decisión de compra de nuevos sistemas de seguridad, frente al 51% del promedio global.

Apéndice

Apéndice 1: Metodología de la encuesta

Genetec Inc. encuestó a profesionales de la seguridad electrónica del 12 de agosto al 15 de septiembre de 2024.

El objetivo de la investigación fue:

- Obtener una visión de las operaciones y los entornos de seguridad electrónica
- Comprender la respuesta de las organizaciones a los desafíos externos, como las ciberamenazas y las dificultades de recursos humanos
- Comprender el enfoque global de 2024

Detalles sobre la encuesta y el análisis

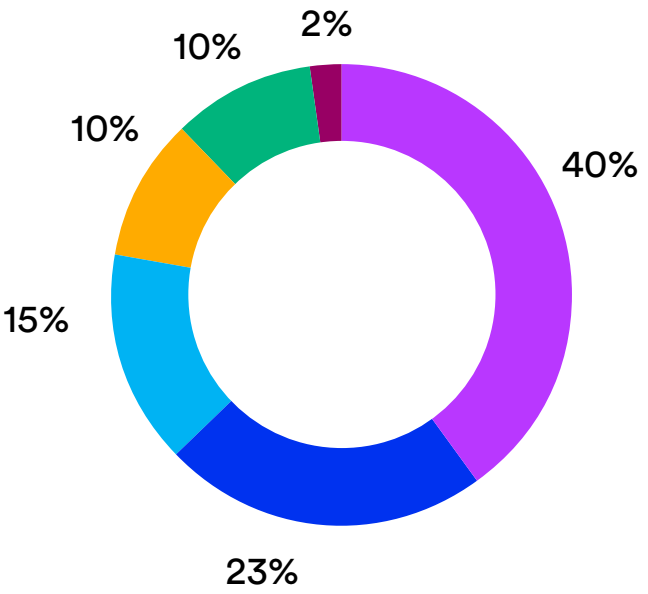
- Después de revisar los resultados y filtrar los datos, se incluyeron 5.696 encuestados en la muestra para su análisis
- El público objetivo de la encuesta se centró en personas que trabajan para organizaciones que participan en la adquisición, gestión, servicio, y/o uso de tecnología de seguridad electrónica. El público objetivo incluyó a los usuarios finales de Genetec y otros contactados a través de anuncios digitales o directamente por terceros a través de sus listas de correo electrónico opt-in
- Las invitaciones para realizar la encuesta en línea fueron enviadas a los posibles participantes sólo por correo electrónico en inglés, francés, alemán, italiano, español, portugués, japonés y coreano
- El formulario de encuesta en línea estuvo disponible en inglés, francés, alemán, italiano, español, portugués, japonés y coreano
- En el análisis final sólo se incluyeron las encuestas completadas y enviadas por personas de la población objetivo
- Las encuestas se tomaron en todas las regiones: EE.UU. y Canadá, México, Centroamérica, El Caribe, Sudamérica, Europa, Reino Unido, Medio Oriente, África, Asia Oriental, Asia del Sur, Asia Sudoriental, Asia Central, Asia Occidental, y Australia - Nueva Zelanda
- Las tasas de respuesta y de finalización de la encuesta variaron según la región y el tamaño de la organización, introduciendo posibles errores de muestreo en los conjuntos de submuestras
- Se recopilaron respuestas de tres poblaciones objetivo principales: usuarios finales de seguridad electrónica, integradores y consultores. Se realizó una limpieza de datos para validar la clasificación de los encuestados en una de estas tres poblaciones y limitar posibles errores. Cualquier error que no sea de muestreo son asumidos como resultado de la recopilación de datos por fuera de la población objetivo (por ejemplo, personas que se identifican incorrectamente como usuarios finales cuando en realidad son empleados como integradores)

Un nota sobre los cálculos de la encuesta

Debido al redondeo y al diseño de la encuesta (incluidas la escala de calificación, selecciona todas las opciones que aplican y de opción múltiple), no todos los porcentajes totales en este reporte serán iguales al 100%. En el caso de las preguntas "todas las que apliquen" (en las que los encuestados pueden elegir varias respuestas), los porcentajes se refieren a la proporción de encuestados que seleccionaron la respuesta individual.

Apéndice 2: Información demográfica de la encuesta

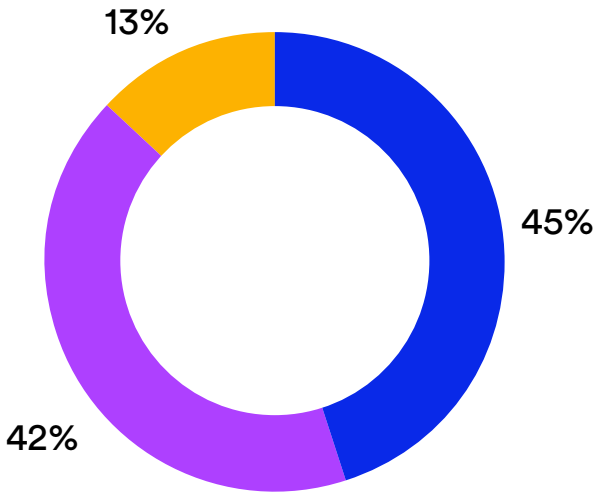
Regiones geográficas



Latinoamérica	40%
Estados Unidos y Canadá	23%
Europa	15%
Medio Oriente y África	10%
Asia-Pacífico	10%
Australia/Nueva Zelanda	2%

FIGURA 1: ENCUESTADOS POR REGIÓN GEOGRÁFICA.

Tipo de encuestado



Usuarios finales	45%
Consultores	42%
Integradores	13%

FIGURA 2: ENCUESTADOS POR TIPO DE ORGANIZACIÓN.

Apéndice 3 – Información demográfica del usuario final

Cargo

Seguridad y protección	15%
Tecnología de la Información (TI)	14%
Ventas	13%
Ingeniería, I+D, diseño de sistemas y control de calidad	11%
Administrador/Administrador de Oficina	11%
Servicio al cliente o soporte (Soporte técnico)	7%
Dirección de operaciones	6%
Dirección de instalaciones/operaciones	5%
Dirección de proyectos/Gestión del cumplimiento normativo o riesgo	5%
Contabilidad/Finanzas	5%
Marketing	4%
Compras y contratación	2%
Documentación Legal	2%

FIGURA 3: USUARIOS FINALES ENCUESTADOS POR FUNCIÓN LABORAL.

Industrias

Industrial y manufactura	17%
Educación	14%
Energía, servicios públicos y telecomunicaciones	12%
Transporte	8%
Gobierno estatal/local	8%
Asociaciones y servicios profesionales	7%
Retail	6%
Centros de salud	6%
Gobierno federal/nacional	6%
Banca y finanzas	6%
Deportes, salas de juegos y casinos, y hostelería	5%
Servicios de sistemas de seguridad	2%
Otro	2%
Tráfico y estacionamientos	2%
Cannabis	0%

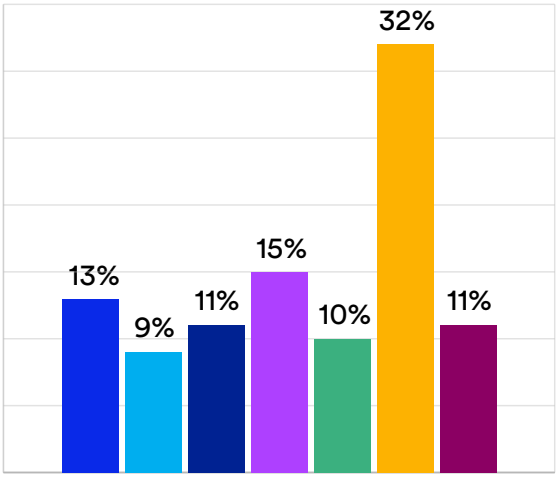
FIGURA 5: USUARIOS FINALES ENCUESTADOS POR SECTOR.

Cantidad de empleados

1-20 empleados	27%
21-200 empleados	24%
201-1.000 empleados	21%
1.001-10.000 empleados	19%
10.001-100.000 empleados	8%
Más de 100.001 empleados	3%

FIGURA 4: USUARIOS FINALES ENCUESTADOS SEGÚN EL NÚMERO TOTAL DE EMPLEADOS DE SU ORGANIZACIÓN.

Portadores de credenciales de control de acceso



	20 tarjetahabientes	13%
	21-50 tarjetahabientes	9%
	51-100 tarjetahabientes	11%
	101-500 tarjetahabientes	15%
	501-1.000 tarjetahabientes	10%
	Más de 1.001 tarjetahabientes	32%
	Ninguna de las anteriores/no aplica	11%

FIGURA 6: USUARIOS FINALES ENCUESTADOS POR NÚMERO TOTAL DE PORTADORES DE CREDENCIALES DE CONTROL DE ACCESO.

Implementación de videovigilancia

(cantidad de cámaras)

1-9	20%
10-100	27%
101-500	21%
501-1.000	11%
1.001-5.000	13%
>5.000	8%

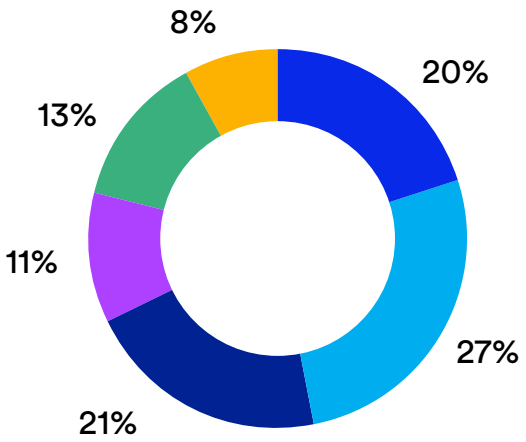


FIGURA 7: USUARIOS FINALES ENCUESTADOS POR NÚMERO TOTAL DE CÁMARAS DE VIDEOVIGILANCIA INSTALADAS.

Ingresos anuales (USD)

USD$500.000-USD$4,9M	17%
USD$5MM-USD$24,9MM	8%
USD$25MM-USD$99,9MM	7%
USD$200MM-USD$499,9MM	5%
USD$500MM-USD$999,9MM	4%
USD$1.000MM-USD$10.000MM	6%
Más de USD$10.000MM	4%
No puedo revelarlo	48%

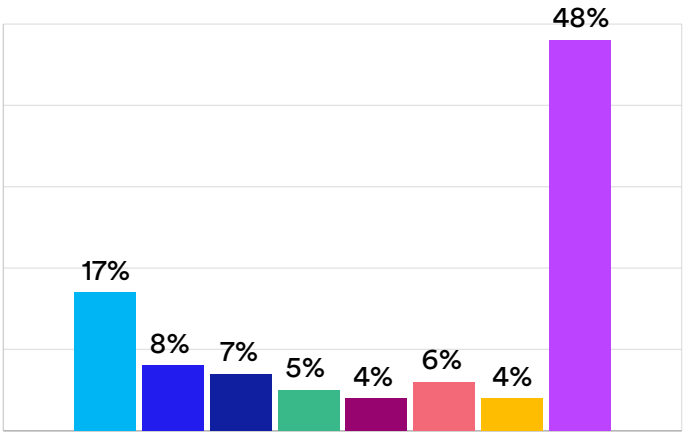


FIGURA 8: USUARIOS FINALES ENCUESTADOS SEGÚN LOS INGRESOS ANUALES TOTALES DE SU ORGANIZACIÓN (USD).

Cantidad de empleados (departamento de seguridad electrónica de la organización)

1-20 empleados	61%
21-200 empleados	25%
201-1.000 empleados	9%
Más de 1.001 empleados	4%

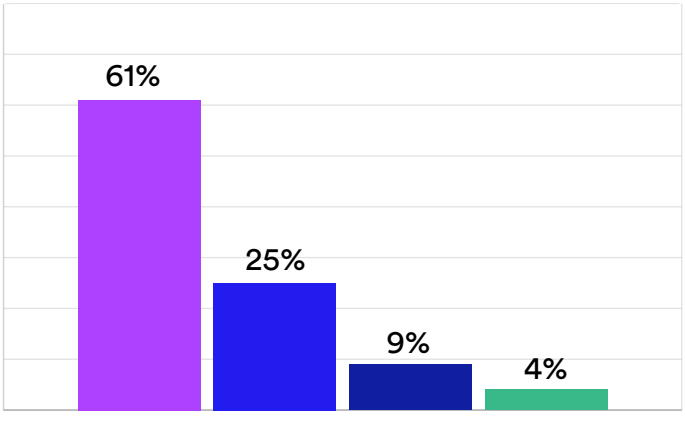


FIGURA 9: USUARIOS FINALES ENCUESTADOS POR LOS EMPLEADOS DEL DEPARTAMENTO DE SEGURIDAD ELECTRÓNICA DE SU ORGANIZACIÓN.

Apéndice 4: Comentarios generales

Los participantes de la encuesta pudieron proporcionar comentarios adicionales asociados a algunas preguntas de la encuesta. Las siguientes son respuestas seleccionadas que son representativas de los sentimientos generales:

Usuarios finales: ¿Qué tecnología adicional tienes instalada en el entorno de seguridad electrónica en tu organización?

- Sistema de asesoramiento para la industria del retail
- Biometría
- Identificación de cliente
- Recopilación de datos
- Detección de drones
- Notificación masiva de emergencias
- Escolta, guardaespaldas, seguridad reforzada, agentes armados
- Detección de disparos (audio), robots
- Sistema de información sobre la salud
- Sistema de iluminación inteligente
- Gestión de facturas
- Gestión de llaves
- Logística
- Analíticas del tráfico vial
- Detección de humo de cigarrillos, cigarrillos electrónicos, fuego
- Videovigilancia en flotas de camiones de suministro, GPS y mecanismos electrónicos de seguridad
- Sistema de coacción inalámbrico

Usuarios finales y consultores: ¿Integras otras funcionalidades (intrusión, detección perimetral, analíticas, etc.) en esta aplicación?

- IA
- Controles de alcoholemia para conductores
- Gestión de llaves
- Ascensor Kone, jornada laboral
- Analíticas de video de cruce de línea, personas, vehículos y merodeo
- LPR, gestión de eventos, etc
- LPR, analíticas de juegos de mesa
- Mapas de edificios
- PSIM
- Radar
- Robots, detección de disparos, analíticas de video
- Scada, analíticas de video, IoT
- Geolocalización de trabajadores

Integradores: ¿Cuál es la principal motivación de los clientes para reemplazar los sistemas antiguos?

- Antigüedad
- Mal servicio y sistema deficiente
- Violación de la privacidad
- Cambiarlo porque ya no funciona
- Cumplimiento de la política de estandarización de la organización
- Cumplir las nuevas normas
- Costo
- Eliminación de sistemas antiguos u obsoletos
- Fin de la vida útil/soporte/incidente
- Política de la ESG
- Bloqueo del integrador/vendedor
- Proveedor de Internet

- Obsolescencia
- Ciclo de vida del producto
- Reducir el tiempo de inactividad
- Aumento de la velocidad o la capacidad
- Vulnerabilidades de los dispositivos/tecnologías existentes

Integradores: Cuando vendes nuevas soluciones de seguridad electrónica a los clientes, ¿qué departamentos intervienen habitualmente en la decisión de compra?

- Soporte de ingeniería
- Gestión de portafolios tecnológicos
- Esto se decide en el área de ventas y en el diseño incluiremos a operaciones hasta cierto punto

Integradores: ¿Qué esperas que pueda causar retrasos en los proyectos en 2025?

- El sector de la construcción se estanca y los clientes recortan sus presupuestos
- T.I.R. del Gobierno Permisos de construcción y remodelaciones
- ¡Contratación de talentos interesantes!
- Desconfianza de los clientes
- Escasez de personal en el lado del cliente
- Recesión
- Guerra
- Voluntad y capacidad de las empresas para adoptar nuevas tecnologías

Integradores: ¿Cómo ha influido en tu negocio la creciente tendencia del Machine Learning, la inteligencia artificial (IA) y/o grandes modelos del lenguaje (LLM)?

- Los clientes necesitan mucho más entrenamiento
- De hecho, sólo ahora estamos viendo ejemplos concretos del uso de la IA con retorno de la inversión (ROI)
- Está confundiendo al mercado
- La mayoría solicita analíticas con IA/ML
- Se habla mucho de IA, pero en seguridad la única evolución que se está produciendo es la creciente implementación de algoritmos de analíticas de video en los dispositivos de videovigilancia
- Se requiere entrenamiento para poder ofrecer lo que el cliente requiere
- No cabe duda de que estamos observando un mayor interés por el entrenamiento y la utilización de analíticas basadas en la inteligencia artificial en general. Especialmente en aplicaciones de videovigilancia

Usuarios finales: ¿Cuáles son las razones principales por las que tu organización eligió una implementación de nube híbrida?

- Accesibilidad a otros datos de interés
- Ancho de banda
- Cumplimiento
- La conectividad también es un problema en la vigilancia y control de estacionamientos ya que no está totalmente cableada
- Driven by infosec
- Almacenamiento a largo plazo y compartir información de casos
- Restricciones de red

Usuarios finales: ¿Cuáles fueron los principales retos a los que se enfrentó tu organización en 2024?

- Aceptación de riesgos por parte de los ejecutivos sin procesos de gestión de riesgos empresariales (no creo que eso ocurra, así que no gastamos dinero en mitigarlo) sin transparencia hacia la empresa ni la junta directiva
- Acceso al repositorio de datos
- Alerta de cansancio
- Auditorías, redacción de reportes generados por el sistema, gestión de incidentes y elaboración de reportes
- Broadcom adquiere vmware y los precios aumentan inesperadamente
- Presupuestos

- Campaña electoral y referéndum
- Actualizaciones constantes de la TI (seguridad de la información) que afectan constantemente a los sistemas SOC
- COVID-19
- Disminución de las ventas
- Hacer más con menos presupuesto que era muy poco
- Reducción de activos/sedes corporativas.
- Aumento del presupuesto para acomodar la nueva infraestructura y los nuevos 30 empleados, de sólo 6 empleados
- Inflación
- Inestabilidad del país para las inversiones
- Gestión de la percepción de seguridad
- Cumplimiento de los plazos y presupuestos de los proyectos
- Cortes de electricidad
- El bajo precio del combustible
- Vulnerabilidades de seguridad en sistemas antiguos
- El plazo de entrega de los dispositivos adquiridos, la mayoría de las veces los dispositivos Genetec tardan entre 60 y 90 días en entregarse
- Proveedor que no responde
- Conocimiento del proveedor

Usuarios finales y consultores: ¿A qué nuevos procesos o capacidades has dado prioridad en 2024?

- Técnico de seguridad propio para complementar el contrato existente con el integrador
- Reconocimiento facial
- Gestión de la obsolescencia
- Sistemas unificados
- Uso de drones en la gestión de la seguridad
- Detección de armas

Usuarios finales y consultores: ¿Cuál es la causa de los retrasos del proyecto?

- Retrasos en la construcción
- Problemas de toma de decisiones
- Documentación
- Certificación/calificación del equipo
- Los directivos de las instalaciones no están dispuestos a gastar el presupuesto en la reducción de riesgos recomendada, sin procesos de gestión de riesgos empresariales ni transparencia ante la empresa ni la junta directiva
- Encontrar el producto adecuado
- Catástrofe natural: inundaciones
- Retrasos en procedimientos
- Lanzamientos de productos
- Cronograma del proyecto
- Programación de proveedores
- Descenso interanual de los ingresos

Usuarios finales: ¿En qué tipo de proyectos estará enfocado tu departamento en 2025?

- Actualización de hardware obsoleto que se encuentra al final de su vida útil
- Detección de vapores

Usuarios finales: ¿Qué capacidades planeas agregar a tu sistema de control de acceso en 2025?

- Agregar alarma acústica a las alarmas de cámara y puerta
- Control del riesgo de incendio
- Mejorar las analíticas de video y la IA
- Integrar CCTV con control de acceso
- Integración con el sistema de recursos humanos
- Plan de gestión de viajes (JMP)
- Sistemas LPR para la gestión de la capacidad del estacionamiento

- Reloj de control
- Actualización al protocolo OSDP y actualización de credenciales de proximidad
- Analíticas de video integradas con el control de acceso para localizar seguimientos de cerca de personas y vehículos, armas, etc.

Usuarios finales: En materia de ciberseguridad, ¿qué medidas o enfoques concretos ha adoptado tu organización?

- Revisión anual de autocumplimiento de ciberseguridad basada en ISO 27001
- Sólo sistema cerrado
- Realización de ataques de simulación de phishing
- Autenticación de dos factores
- Red de confianza cero

Usuario finales: ¿Tuvo tu organización un aumento en los incidentes de seguridad electrónica y/o ciberseguridad en 2024?

- Amenazas de muerte
- Ataques de deepfake
- Amenazas en las redes sociales
- Evolución del panorama de amenazas, transformación digital e inestabilidad global
- Cortes prolongados de Internet
- Correos electrónicos falsos
- Hacking
- Cámaras desinstaladas
- Daños por agua en los equipos

Usuarios finales: ¿Tu organización está aprovechando las herramientas de IA fuera de las aplicaciones de seguridad electrónica?

- Alexa
- Desarrollo de contenidos audiovisuales
- Chat automático
- Generación de reportes de BI
- BMS gestión inteligente (medidas de eficiencia energética)
- Facturación, pagos y saldos de los clientes
- Recursos humanos, publicidad
- HVAC
- Mensajería instantánea
- Chat interno, gestión de llamadas y analíticas de datos
- Búsqueda en Intranet, chatgpt específico de la empresa
- Servicio de soporte informático
- Comunicaciones y mercadeo
- Materiales de marketing
- O365
- Automatización de oficinas
- Operaciones
- Nuestra empresa creó un sistema interno de gpt
- Control de calidad, Inteligencia comercial, Recursos humanos
- Empieza a utilizar copilot para aplicaciones ofimáticas
- Watsonx

Consultores: Cuando se trata de tus clientes, ¿qué departamentos intervienen en las decisiones de compra de productos relacionados con la seguridad?

- Gerente de proyecto de construcción
- Departamento de salud y seguridad
- Departamento comercial

Consultores: ¿Cuáles fueron los principales retos a los que se enfrentaron la mayoría de tus clientes en 2024?

- Compras
- Iniciativas de reducción de personal y costos
- Políticas gubernamentales y falta de conocimiento

Usuarios finales y consultores: ¿Qué nuevos procesos o capacidades priorizaste en 2024?

- Monitoreo centralizado del control de acceso a instalaciones multinacionales
- Gestión de visitas guiadas
- Solución de una sola tarjeta
- Evaluación de riesgos y amenazas
- ¿Qué tipo de proyectos fueron afectados?
- Nuevas instalaciones
- Proyectos debido a un cambio en la amenaza o a una decisión política. Se convierten en máxima prioridad y retrasan al mismo tiempo otros proyectos
- Integraciones de sistemas

Consultores: ¿Qué tipo de proyectos crees que tus clientes quieren priorizar para 2025?

- Encriptación y cambio de tarjetas
- Algo en el ámbito de la sostenibilidad

Consultores: ¿Qué aumento(s) de incidentes de seguridad electrónica y/o ciberseguridad experimentaron en 2024?

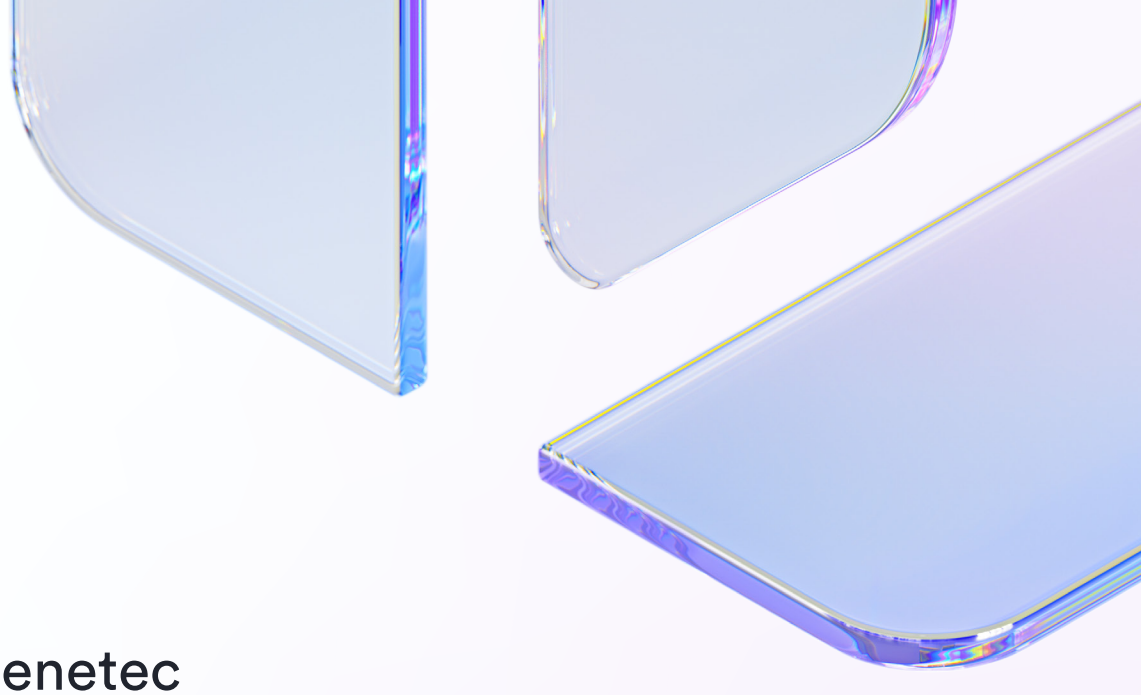
- Incendios intencionales
- Interrupciones en la nube
- Peleas en la escuela
- Fraude
- Sondeo general, comprobación de vulnerabilidades
- Suplantaciones
- Pérdida de confidencialidad de determinados datos personales
- Protestas

Consultores: ¿Qué tipo de datos crees que tus clientes deberían recopilar en su Centro de Operaciones de Seguridad (SOC) procedentes de otros sistemas?

- Documentación
- Información sobre amenazas internas
- Sistemas de vigilancia de intrusos y activos
- Sistemas de emergencia exteriores, meteorología, tiradores activos, etc.

Integradores y consultores: ¿Cómo ha influido en tu negocio la creciente tendencia del Machine Learning, la inteligencia artificial (IA) y/o los grandes modelos del lenguaje (LLM)?

- Ha sido tremendamente útil con las tareas repetitivas del día a día
- Evitando que la gente crea que esto lo arregla todo
- Creando la necesidad de ayudar a los clientes a evaluar los riesgos relacionados con las capacidades de los productos y plataformas de seguridad nuevas y existentes basadas en la inteligencia artificial
- Automatizando equipos/sensores para operaciones comerciales y protegiendo el diseño universal
- La venta abusiva ha provocado falsas expectativas que intentamos reducir
- Reduciendo el ruido, permitido usar analíticas de video, automatización de tareas, predicción de eventos



Acerca de Genetec

Genetec Inc. es una empresa global de tecnología que ha estado transformando la industria de la seguridad electrónica durante más de 25 años. El portafolio de soluciones de la compañía permite a empresas, gobiernos y comunidades de todo el mundo proteger a las personas y los activos, al tiempo que mejora la eficiencia operativa respetando la privacidad individual.

Basada en una arquitectura abierta y construida con la ciberseguridad en su núcleo, Genetec ofrece productos líderes en el mundo para la gestión de video, control de acceso y LPR. Otras soluciones ofrecidas por la empresa incluyen productos para la detección de intrusión, intercomunicación y gestión de evidencias digitales.

Con sede principal en Montreal, Canadá, Genetec atiende a sus más de 42.500 clientes en todo el mundo a través de una extensa red de distribuidores, integradores, integradores acreditados y consultores en más de 159 países.

Para conocer más sobre nosotros, visita **genetec.com/es**

Si deseas más información sobre este reporte, escríbenos a **Genetec-research@genetec.com**

Genetec Inc.
genetec.com/oficinas
info@genetec.com
@genetec