Diciembre de 2022

Estado de la Seguridad Electrónica 2022:

Navegando efectivamente en un ambiente cambiante

Perspectivas y conclusiones de más de 3.700 profesionales de la seguridad electrónica

Genetec™

Contenido

Sobre la investigación 2

Resumen ejecutivo 4

Resumen de las diferencias en todo el mundo 5

Resultados principales 7

Los presupuestos OPEX crecen 8
TI con mayor presencia en la seguridad electrónica 8
Compitiendo por los componentes 9
RR.HH. enfrentan muchos desafíos 11
Observaciones sobre la adopción de la nube 13
La seguridad electrónica y los datos relacionados son de misión crítica 18
La ciberseguridad sigue siendo la máxima prioridad 20
La seguridad electrónica se unifica 22
Cambios en la tecnología: el año pasado 23
Cambios en la tecnología: el año que viene 23

Conclusiones principales 25

Apéndice 27

Apéndice 1: Metodología de la encuesta 27
Apéndice 2: Información demográfica de la encuesta 28
Apéndice 3: Comentarios abiertos 30

Sobre la investigación

Genetec Inc. encuestó a profesionales de la seguridad electrónica entre el 24 de agosto y el 21 de septiembre de 2022. Después de una revisión de las respuestas y la limpieza de los datos, se incluyeron 3.711 respuestas en la muestra para su análisis.

Algunos detalles sobre la metodología de la encuesta

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

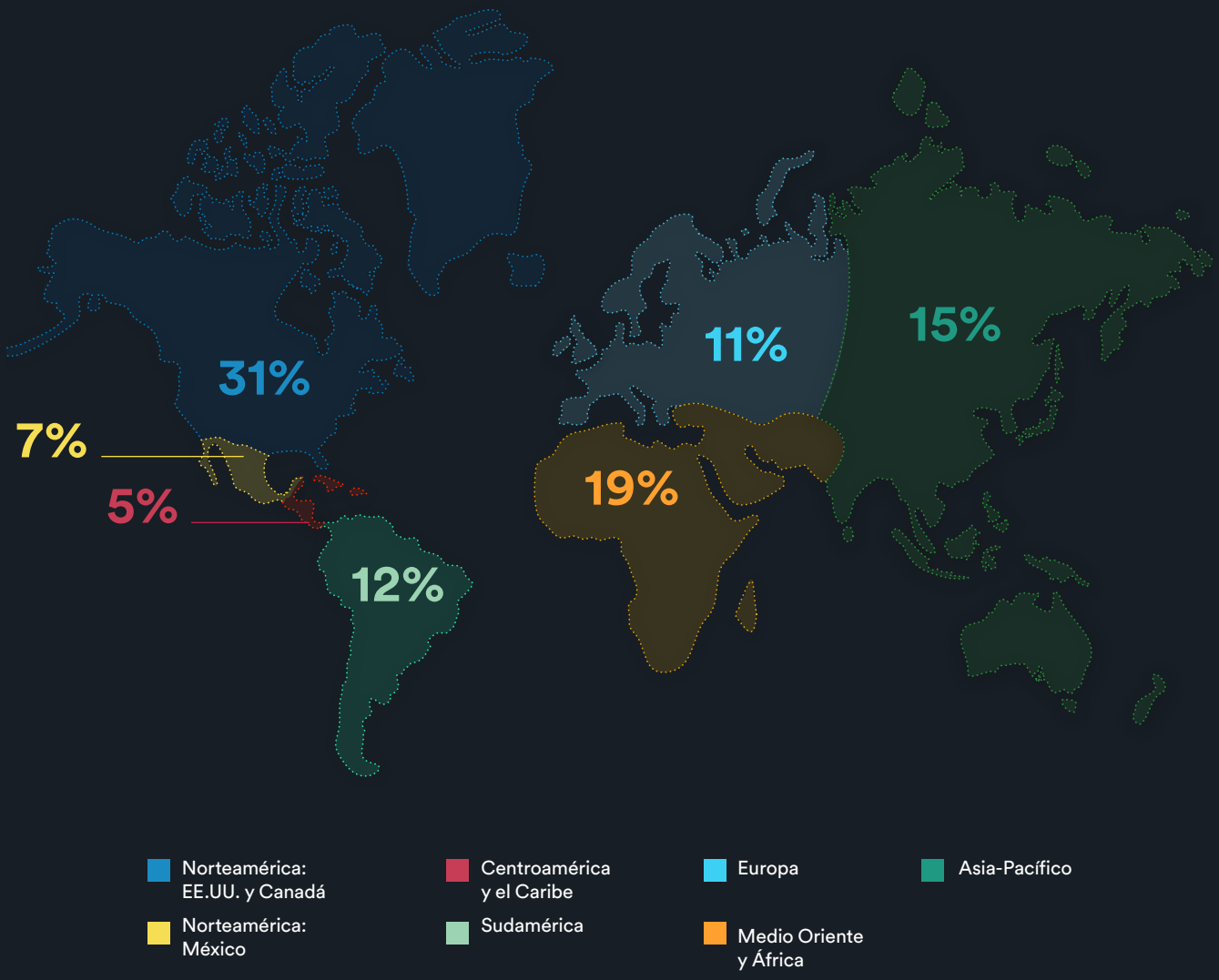
- **Usuarios finales** (individuos que trabajan para organizaciones que participan en la adquisición, gestión y/o uso de tecnología de seguridad electrónica) e
- **Integradores, proveedores e instaladores de sistemas** (individuos que dan asesoría, integran, instalan, venden o proporcionan servicios de soluciones de seguridad)

La población objetivo fue alcanzada a través de terceros mediante sus listas de correo electrónico opt-in, listas de correo electrónico opt-in de Genetec y promociones digitales. Los resultados de este reporte están basados en las respuestas tanto de los usuarios finales como de los integradores de sistemas/instaladores/proveedores. Sin embargo, algunas preguntas solo se hicieron a los usuarios finales y otras solo a los integradores/instaladores/proveedores de sistemas. Este reporte señala si las respuestas son de todos los encuestados, usuarios finales encuestados o integradores/instaladores/proveedores de sistemas encuestados.

Incluso para las preguntas hechas a ambos grupos (usuarios finales e integradores/instaladores/proveedores de sistemas), cada resultado fue analizado por las respuestas de 'solo usuarios finales' y 'solo integradores/instaladores/proveedores de sistemas', así como por ambos grupos combinados. En la mayoría de los casos, hubo poca diferencia en los resultados. Las respuestas de 'solo usuarios finales' coincidieron en términos generales con las respuestas de 'solo integradores/instaladores/proveedores de sistemas'. El reporte muestra las instancias donde este no fue el caso. También destaca los casos en los que el porcentaje de respuestas difiere significativamente según la región geográfica, la industria del usuario final o el tamaño de la organización, medido por la cantidad de empleados a nivel global.

VOLVER AL ÍNDICE

La población objetivo fue muestreada en todas las regiones geográficas.



En el análisis final solo se incluyeron las encuestas completadas y enviadas por personas dentro de la población objetivo.
Para obtener más detalles sobre la metodología de la encuesta y la información demográfica de los participantes, consulta el apéndice 1 y 2.

VOLVER AL ÍNDICE

Resumen ejecutivo

Las organizaciones están haciendo un balance y adaptándose a una nueva forma de trabajar después de un período de incertidumbre y cambio ocasionado por la pandemia de COVID-19. Muchos de los resultados de la encuesta de 2022 fueron similares a las respuestas de la encuesta de 2021. Sin embargo, algunos también descubrieron nuevos desafíos que la industria enfrenta, como la escasez de productos y problemas de recursos humanos.

Lo que está claro es que las organizaciones están listas, son capaces de adaptarse y miran hacia el futuro en lo que respecta a la aplicación de tecnologías de seguridad electrónica.

El futuro de la nube es híbrido: Muchas organizaciones imaginan una combinación de soluciones locales y basadas en la nube para sus implementaciones de seguridad electrónica a la vez que buscan optimizar sus inversiones en infraestructura y aprovechar las opciones híbridas para ahorrar costos y aumentar la eficiencia.

La influencia de la ciberseguridad y la TI: Las preocupaciones cibernéticas van en aumento y están inspirando nuevos métodos para implementar y mantener una estrategia sólida de ciberseguridad.

El uso de la seguridad electrónica para las operaciones del negocio: La pandemia empujó a más organizaciones a aprovechar múltiples sistemas y fuentes de datos para gestionar mejor sus instalaciones y el flujo de personas. La tendencia de considerar las soluciones de seguridad electrónica como algo más que un simple costo asociado con la protección de personas y activos continuará, y los nuevos enfoques sobre cómo se utilizan los datos de seguridad electrónica ayudarán en la toma de decisiones organizacionales y operativas.

Superar la escasez de suministros: La industria se ha adaptado a los problemas de la cadena de suministro ampliando el valor de su hardware existente o retrasando proyectos. Dado que los presupuestos para 2023 se mantienen saludables, los departamentos de seguridad y TI planean completar implementaciones o comenzar nuevos proyectos dependiendo de la disponibilidad de los componentes.

Resumen de las diferencias en todo el mundo

La mayoría de las preguntas de nuestra encuesta mostraron ligeras diferencias entre los encuestados a nivel regional. Es decir, el porcentaje de respuestas para cada pregunta y cada región fue similar. Esto sugiere una visión global consistente de cómo se ha desarrollado la seguridad electrónica durante el último año.

A continuación se muestran los casos en los que las respuestas de una región específica defirieron significativamente del promedio global.

Asia-Pacífico: Cadena de suministro y nube

Los integradores de sistemas en Asia-Pacífico son más pesimistas sobre el impacto de los problemas de la cadena de suministro en el próximo año. El 57,5% respondió que los problemas de la cadena de suministro "aumentarían mucho" o "aumentarían algo". Esto está por encima del promedio global del 49%.

Se pidió a los encuestados que aplicaran una clasificación a las diferentes razones para la lenta adopción de la nube. En general, la clasificación promedio más alta estuvo en los "riesgos de ciberseguridad percibidos". Sin embargo, en Asia-Pacífico, el más alto es el "miedo a la pérdida de datos", seguido de cerca por la "falta de comprensión de la nube".

La región de Asia-Pacífico está a la cabeza en el uso de la nube privada. La mayoría de los encuestados a nivel mundial aún almacenan su video en dispositivos de almacenamiento locales (NVRs, servidores, NAS, SAN). En Asia-Pacífico, el 4,55% seleccionó que almacenan sus datos de video “principalmente en una nube privada”, este fue el nivel más alto entre todas las regiones.

Centroamérica y el Caribe: Unificación y nube

Los sistemas de seguridad unificados son menos comunes en Centroamérica y el Caribe. "Los sistemas de control de acceso y videovigilancia de mi organización no están conectados (son sistemas separados)", fue la segunda respuesta seleccionada más común en esta región. Por el contrario, ésta fue la respuesta menos común en las demás regiones.

Los encuestados de Centroamérica y el Caribe también indicaron que utilizan el almacenamiento en la nube pública con más frecuencia que en otras regiones. El 6,9% de los encuestados en esta región seleccionó “Almacenado principalmente con servicios de almacenamiento en la nube pública”, en comparación con el 2,6% a nivel global.

VOLVER AL ÍNDICE

Europa, Medio Oriente, Turquía y África (EMEA): nube, amenaza de credenciales y cadena de suministro

EMEA es la región más conservadora en lo que respecta a la adopción de la nube dentro de la seguridad electrónica. El 69% de los encuestados afirmó que no ha trasladado ninguna parte de su infraestructura a la nube, en comparación con un promedio del 58% a nivel global.

Los encuestados de EMEA confirmaron que el "robo de credenciales" es la mayor amenaza para sus organizaciones: el 50,2% seleccionó esta opción frente al 39,6% a nivel global.

Europa experimentó la mayor cantidad de desafíos con la entrega de proyectos en los últimos 12 meses con el 82% de los encuestados afirmando que se vieron afectados, en comparación con el 71% a nivel global. Esto puede deberse a reducciones en los presupuestos y problemas de la cadena de suministro. A pesar de estos desafíos, los encuestados afirmaron que la mayoría de los proyectos no se cancelaron sino que se aplazaron hasta 2023.

México: Nube

Solo el 17,4% de los encuestados de México sugirió que el COVID-19 aceleró un poco su estrategia de nube cuando ya se estaba implementando, en comparación con el 30,9% a nivel global. Asimismo, tuvieron la porción más baja de encuestados (29,4%) que indicaron que se aceleró "algo" o "mucho", en comparación con el 46,7% a nivel global y el 47,9% en EE. UU. y Canadá combinados.

Sin embargo, para proyectos sin implementación de la nube, en México se indicó que el COVID-19 había "activado" su estrategia de nube con más frecuencia que en cualquier otra región (9,8%). Un contraste marcado en comparación con EE. UU. y Canadá, donde solo el 0,35% de los encuestados seleccionaron esto (por mucho, el nivel más bajo entre todas las regiones).

Sudamérica: Trabajo remoto y ciberseguridad

El 50,4% de los encuestados de Sudamérica dijeron que sus organizaciones no tienen personal de seguridad electrónica configurado para trabajar de forma remota, en comparación al 33,7% de promedio global.

También fueron los menos propensos en identificar una "mejor estrategia de ciberseguridad" como uno de los nuevos procesos que priorizaron este año. Solo el 38% de los encuestados seleccionó esto en comparación con el 49,2% a nivel global y el 52,9% en EE. UU. y Canadá.

EE.UU. y Canadá: Menos despidos, lectura de temperatura y unificación

El 41% de los encuestados de EE. UU. y Canadá indicaron que "ninguno" de sus empleados de seguridad había sido despedido en 2021. Esto en comparación con el 29% a nivel global.

La tecnología de lectura de temperatura fue seleccionada con menos frecuencia por los encuestados de EE. UU. y Canadá que por todas las demás regiones: 14% frente al 24% a nivel global.

La unificación de los sistemas de video y control de acceso fue la segunda más común en los EE. UU. y Canadá, donde el 80% de los encuestados indicó que sus sistemas estaban unificados en comparación con el 77% a nivel global.

VOLVER AL ÍNDICE

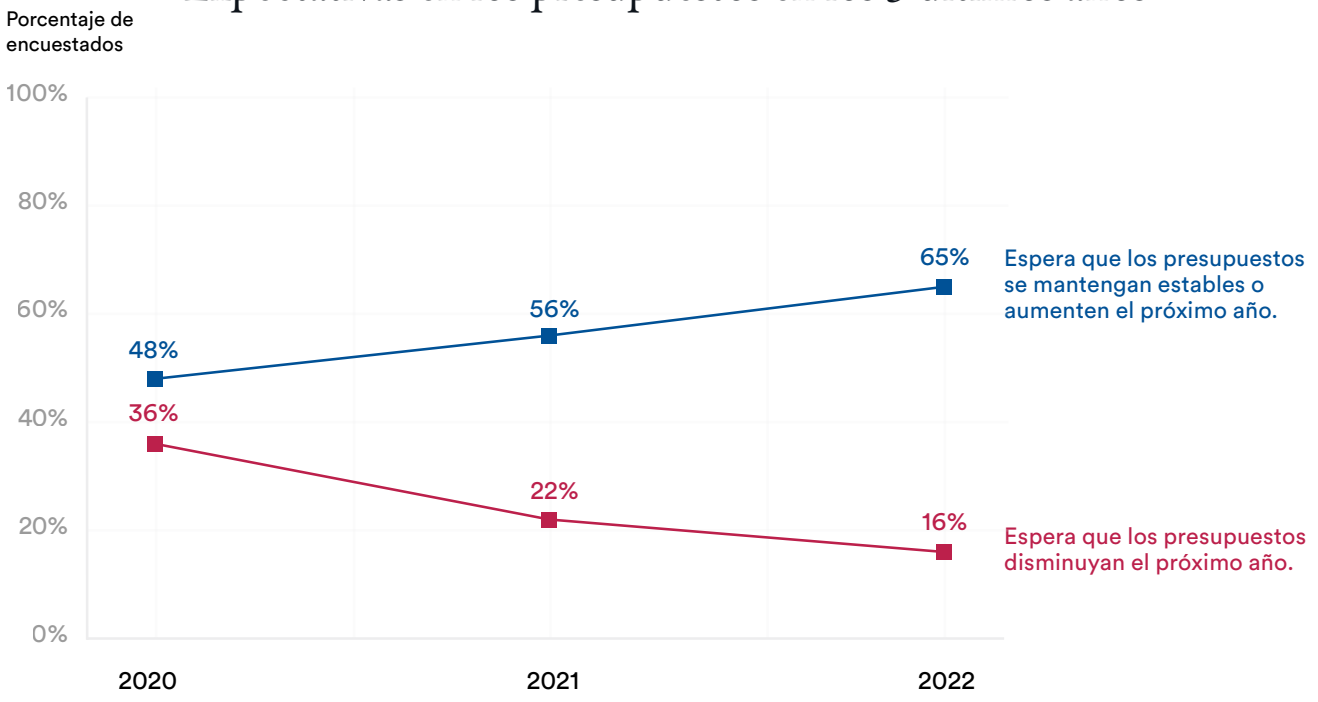
Resultados principales

Los presupuestos OPEX crecen

Con una perspectiva económica desafiante para 2023 que predice una recesión en muchos países, es importante tener en cuenta que en períodos anteriores de recesión y desaceleraciones, el mercado de la seguridad electrónica siguió creciendo. Esta resiliencia parece reflejarse en los resultados de la encuesta, ya que la perspectiva general de los presupuestos OPEX sigue siendo positiva para 2023 y continúa recuperándose de los resultados de la pandemia:

PRESUPUESTOS OPEX

Expectativas en los presupuestos en los 3 últimos años



Dadas las diferentes condiciones económicas en todo el mundo, las respuestas a esta pregunta no variaron significativamente por región. Esto refleja una visión general optimista en toda la industria de la seguridad electrónica.

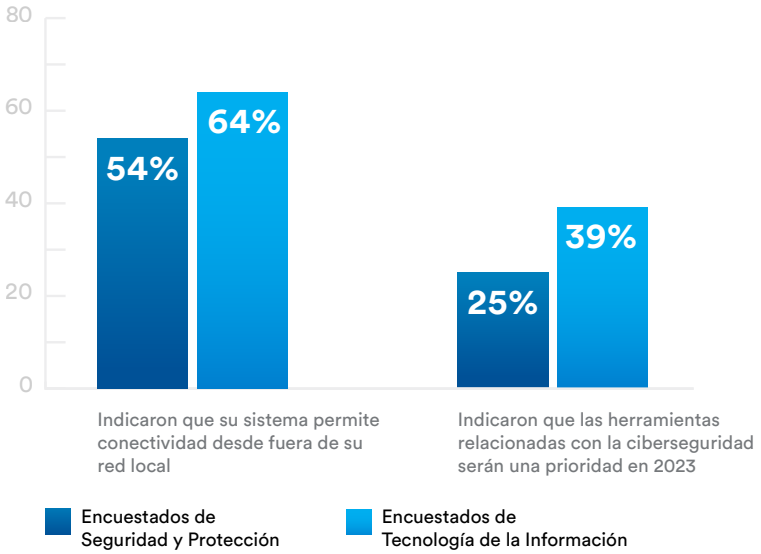
VOLVER AL ÍNDICE

TI juega un papel más importante en la seguridad electrónica

Hace una década, la mayoría de los sistemas de seguridad electrónica en las organizaciones más grandes eran gestionados por personal de departamentos de seguridad especializados. Sin embargo, la transición a los sistemas de seguridad electrónica en la red ha significado que los departamentos de tecnología de la información (TI) asuman una mayor responsabilidad en la gestión de los sistemas de seguridad electrónica como parte de la gobernanza de la red y la tecnología. No resulta sorprendente que en nuestra encuesta de 2022, los encuestados que identificaron su función laboral como "Tecnología de la Información" tuvieran un punto de vista diferente al de sus contrapartes que seleccionaron "Seguridad y protección". Los problemas de red y ciberseguridad se priorizaron en las respuestas de los encuestados de "Tecnología de la Información" relacionados con la gestión e implementación de estos sistemas de seguridad electrónica.

TI VERSUS SEGURIDAD

Priorizando las herramientas de ciberseguridad



Los encuestados de TI ven los ataques de ransomware, ingeniería/ phishing y ejecución remota como una amenaza mayor para su organización que los encuestados de Seguridad y Protección.

VOLVER AL ÍNDICE

Compitiendo por componentes

En 2021, hubo reglas y restricciones a causa de la pandemia, además de desafíos en las fábricas de Taiwán, bloqueos en el Canal de Suez y dificultades en los puertos de entrada. Adicionalmente, el aumento masivo en la demanda de componentes en todas las industrias (como los fabricantes de teléfonos inteligentes y automóviles) y las nuevas necesidades "en el hogar" de los consumidores, provocó una escasez sin precedentes de hardware de seguridad electrónica y y retrasos en los proyectos.

Los resultados de la encuesta demuestran los efectos generalizados de los problemas en la cadena de suministro y cómo los profesionales de la seguridad electrónica trabajaron pragmáticamente para gestionarlos.

El 60 % de los usuarios finales indicaron que los proyectos de seguridad electrónica se habían retrasado debido a problemas en la cadena de suministro. Muchos de los retrasos fueron por largos períodos.

- El 46% de los usuarios finales enfrentaron más de 3 meses de retrasos.
- El 28% de los usuarios finales enfrentaron más de 6 meses de retrasos.

Se retrasaron una variedad de proyectos. Para los usuarios finales encuestados que enfrentaron demoras, el reemplazo de tecnología o equipos fue lo más difícil (66%), seguido de la expansión de las instalaciones actuales (51%) y las actualizaciones (51%).

Para los proveedores de hardware de videovigilancia, los retrasos tuvieron graves consecuencias, ya que el 45% de los usuarios finales buscaron alternativas y cambiaron de marca para implementar los equipos disponibles.

Los integradores de sistemas también destacaron la necesidad de probar diferentes estrategias para hacer frente a la escasez de hardware, incluido el uso de "equipos de segunda mano" y "un centro de reparación para volver a poner en producción algunos componentes electrónicos fáciles de reparar".

VOLVER AL ÍNDICE

Punto de vista

La crisis del COVID-19 y el impacto posterior en la disponibilidad de hardware y componentes electrónicos han destacado el papel fundamental que desempeñan la cadena de suministro y la logística en la mayoría de las industrias.

Si bien la pandemia ya casi pasó por completo, la nueva situación socioeconómica y la incertidumbre provocada por los conflictos geopolíticos actuales continúan ejerciendo presión sobre la cadena de suministro global.

Para la industria de la seguridad, eso se traduce en integradores de sistemas que necesitan:

- Seguir haciendo pedidos de hardware con mucha anticipación a los proyectos para asegurar su material cuando sea necesario.
- Desarrollar relaciones más estrechas con socios que puedan proporcionar alternativas potenciales a los productos pedidos en espera.
- Asociarse con proveedores que sean resilientes y adaptables, y que puedan rediseñar rápidamente sus productos en función de la disponibilidad de materias primas y componentes.

En una nota positiva, los primeros indicadores apuntan a que los cuellos de botella de la cadena de suministro se aliviarán en 2023, lo que debería proporcionar el alivio tan necesitado por los integradores de sistemas que buscan implementar nuevos proyectos de manera oportuna.

Nadia Boujenoui
Vicepresidente de Experiencia del Cliente
Genetec Inc.

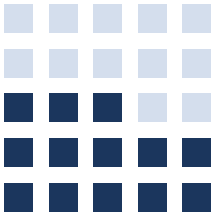
VOLVER AL ÍNDICE

Los recursos humanos enfrentan muchos desafíos

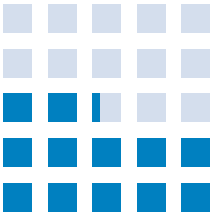
En los últimos años y en todas las industrias, las organizaciones se vieron desafiadas por la escasez de talento, los planes de regreso a la oficina y las expectativas de los empleados sobre nuevas formas de trabajo. Los resultados de la encuesta demostraron que la industria de la seguridad electrónica no es diferente.

El 50% de todos los encuestados de 2022 indicaron que en el último año su organización de seguridad electrónica había experimentado desafíos de recursos humanos. Los encuestados comentaron que los desafíos plantearon la necesidad de cambiar y reasignar al personal, y que el tiempo y el presupuesto para la capacitación eran limitados.

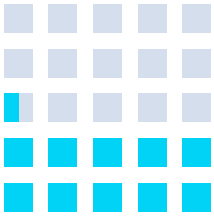
Para los encuestados que enfrentaron tales desafíos:



52%
Enfrentó escasez de personal



49%
Enfrentó dificultades de contratación



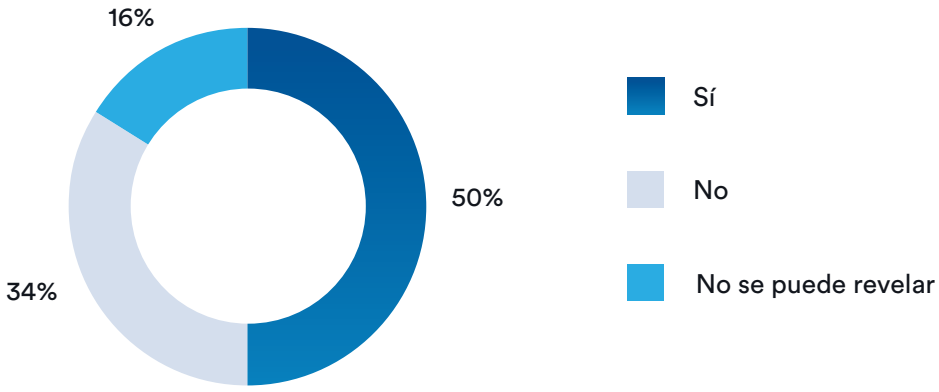
42%
Enfrentó problemas de moral de los empleados

La encuesta reveló que del 48% que priorizó lo anterior, el 83% son del sector del cannabis y el 73% son del sector de salas de juego y casinos

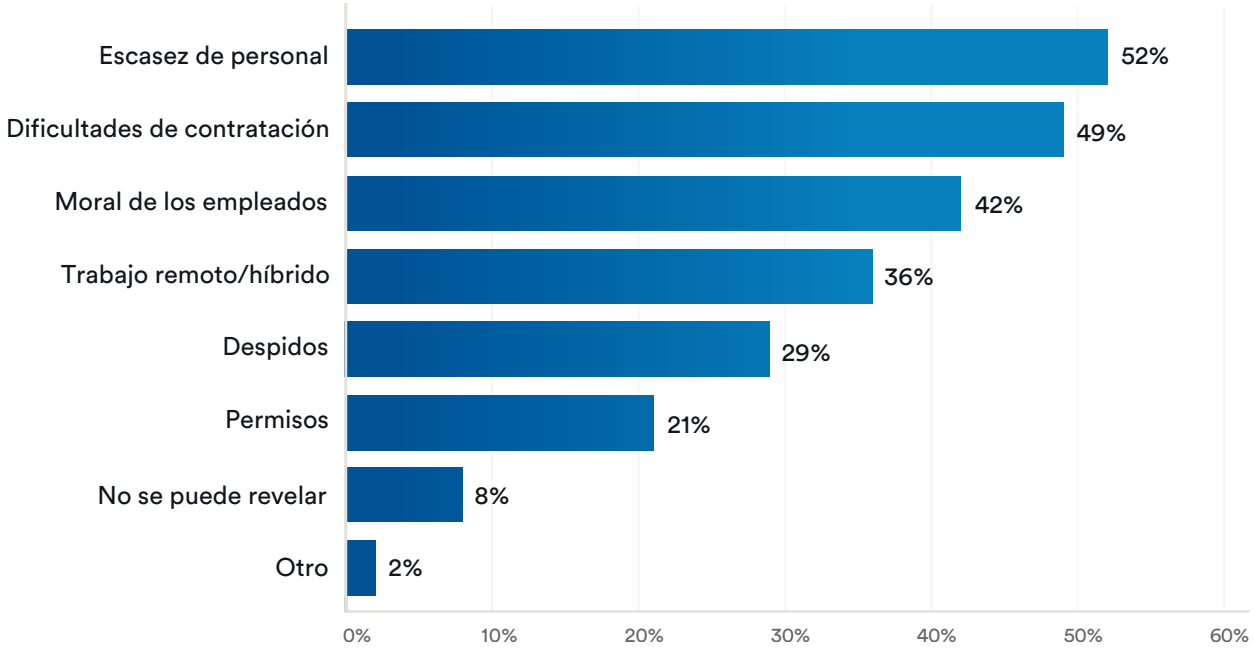
VOLVER AL ÍNDICE

LOS RECURSOS HUMANOS ENFRENTAN MUCHOS DESAFÍOS

¿Tu organización de seguridad electrónica ha experimentado desafíos de recursos humanos en el último año?



¿Qué tipo de desafíos de recursos humanos afectaron a tu departamento de seguridad electrónica en el último año?



VOLVER AL ÍNDICE

Observaciones sobre la adopción de la nube

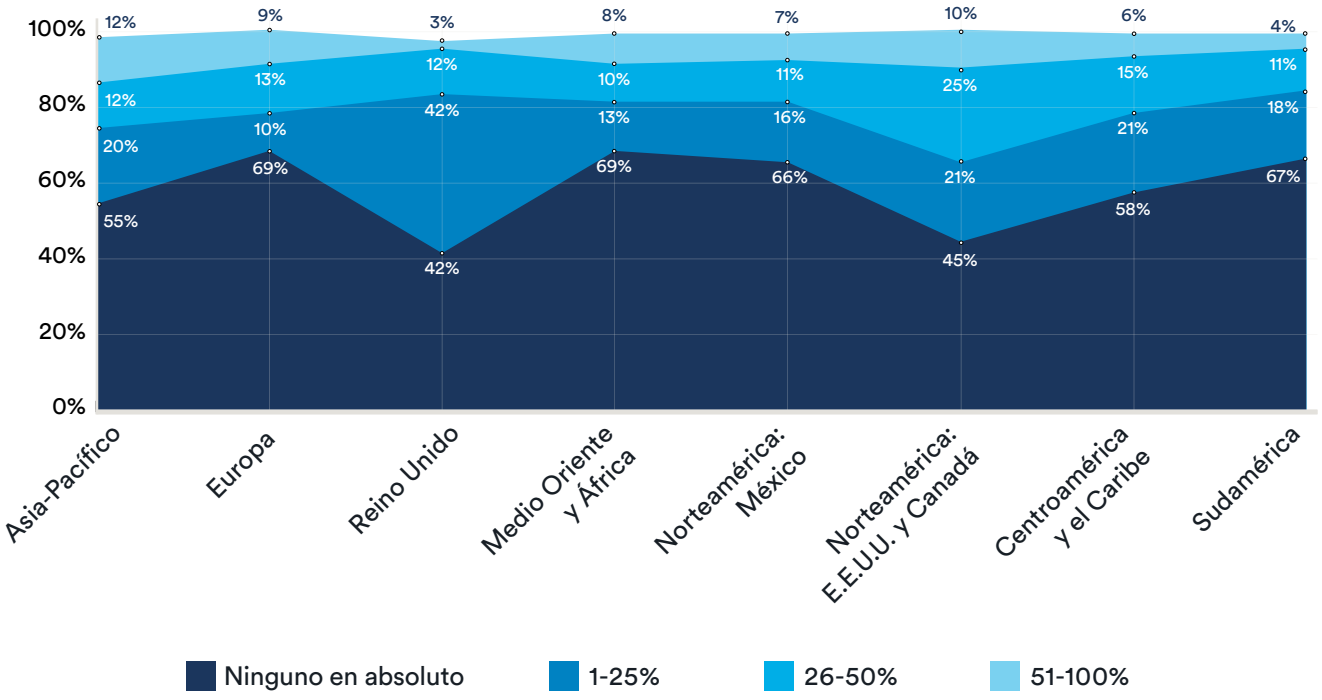
Aceptación de la nube por región

La mayoría de los usuarios finales encuestados (82%) indicaron que principalmente almacenan su video en dispositivos de almacenamiento locales (NVRs, servidores, NAS, SAN). Solo el 6% indicó que utiliza la nube pública o privada para este propósito. El principal impulsor es aprovechar el trabajo remoto, lo que tiene sentido ya que menos personas van a la oficina regularmente.

El porcentaje fue más alto en el sector de usuarios finales del retail, donde el 81% de los encuestados indicaron que cambiarían a la nube. Además, un porcentaje menor de encuestados en Europa y Medio Oriente pensó que su organización pasaría a gestionar o almacenar sus datos de seguridad electrónica en la nube que en otras regiones.

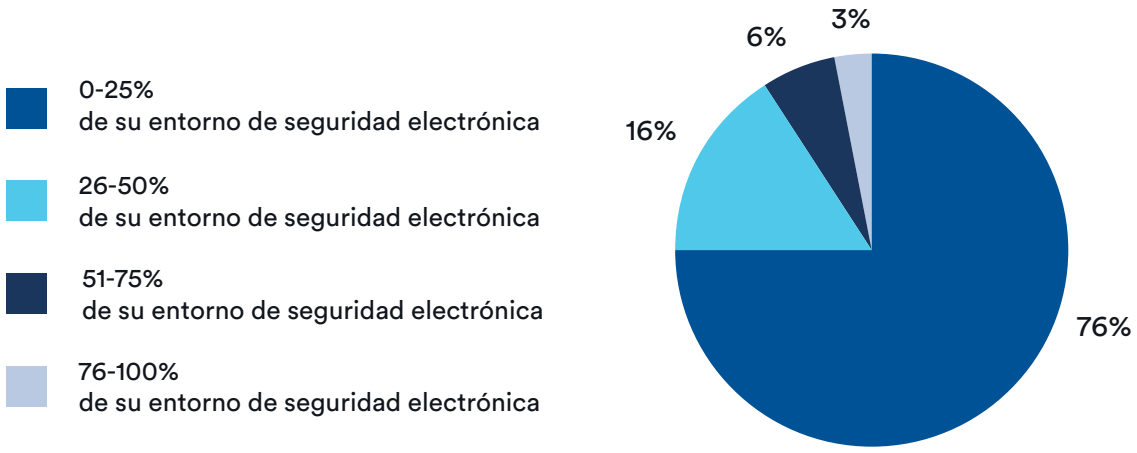
Casi 2/3
de los encuestados indicó que durante los próximos dos años, su organización pasará a gestionar o almacenar más datos de seguridad electrónica en la nube.

Adopción de nube o nube híbrida por región



VOLVER AL ÍNDICE

¿Qué parte de tu entorno de seguridad electrónica está en la nube o en una nube híbrida? (Selecciona una opción)

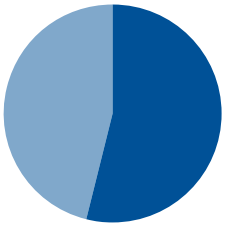


Este movimiento a la nube es consistente con las previsiones de los analistas de la industria. Novaira Insights informó que en las Américas, el porcentaje de ingresos del software de gestión de video que proviene del software de gestión de video en la nube crecerá del 19% en 2021 al 45% en 2026.

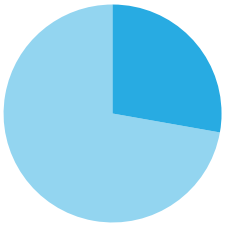
VOLVER AL ÍNDICE

OBSERVACIONES SOBRE LA ADOPCIÓN DE LA NUBE

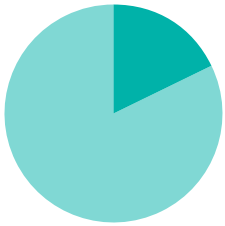
El futuro se pinta híbrido



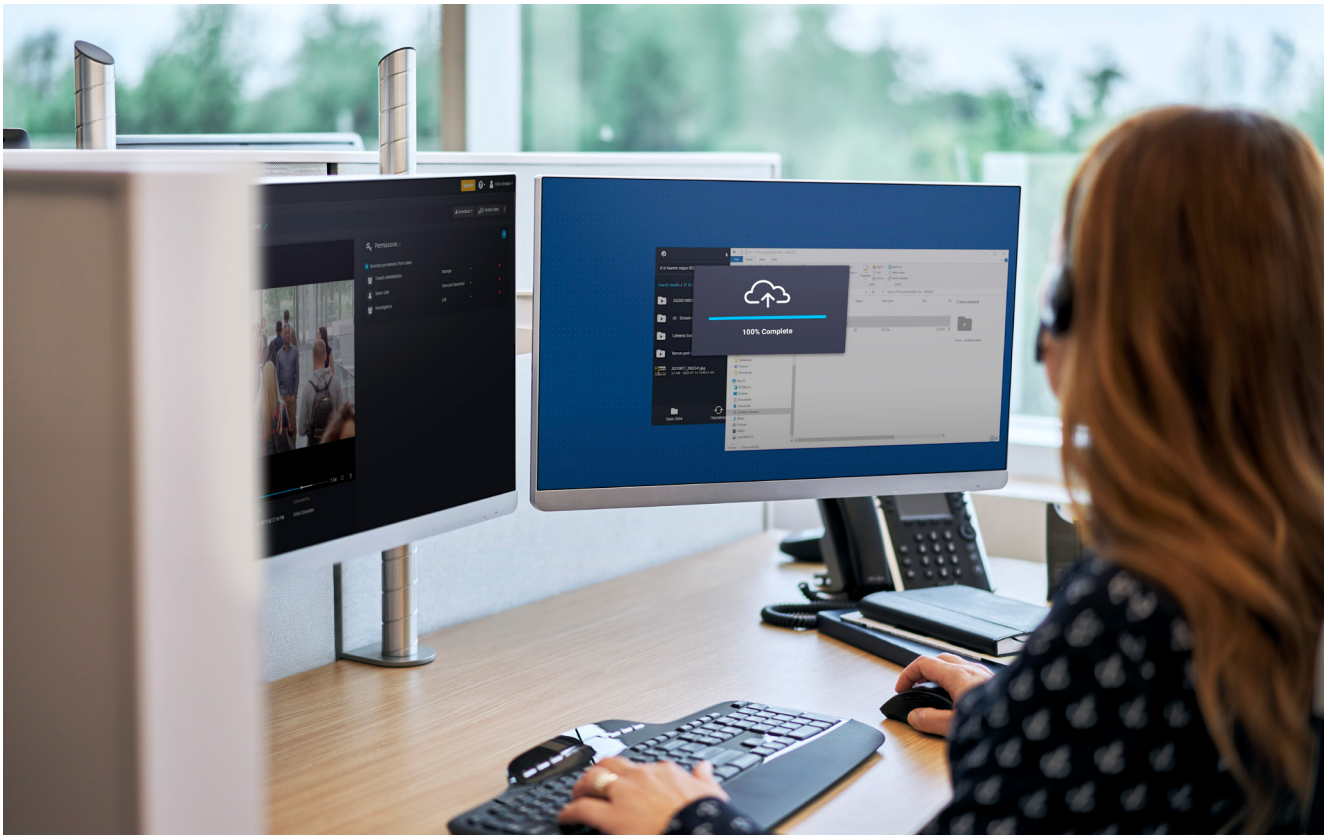
54%
de los usuarios finales indicaron moverse hacia una combinación de soluciones locales y basadas en la nube



28%
de los usuarios finales indicaron que tienen todas las soluciones basadas en la nube

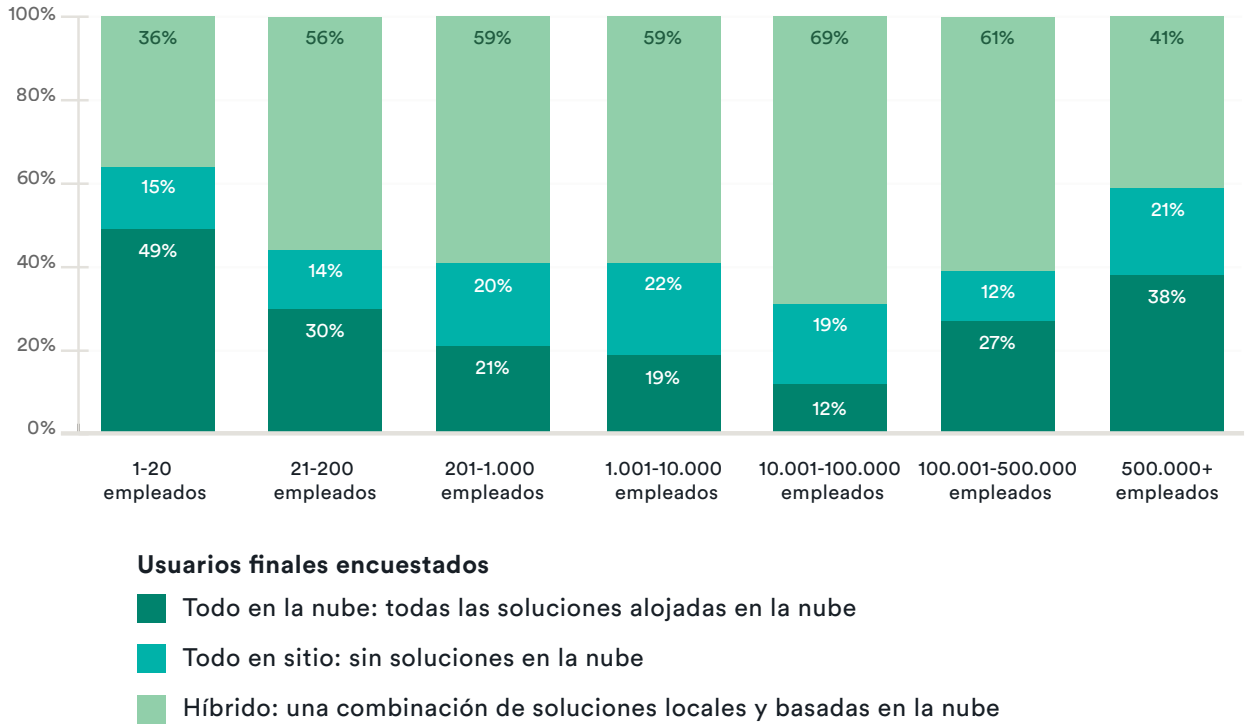


18%
de los usuarios finales indicaron que no tienen soluciones basadas en la nube



VOLVER AL ÍNDICE

En los próximos 5 años, ¿cuál es la visión de tu empresa sobre la implementación de seguridad en la nube?



La ciberseguridad es una barrera

La industria de la seguridad electrónica todavía está rezagada con respecto a otras industrias en su adopción de la nube. La percepción de la tecnología entre los profesionales de la seguridad sigue siendo conservadora. Los riesgos percibidos de ciberseguridad en la nube se clasificaron como la razón más destacada para desacelerar la adopción de la nube. Esto podría verse como una barrera algo autocumplida y basada en la falta de comprensión de la ciberseguridad inherente a las soluciones basadas en la nube.

En el sector de la salud, el 26% de los usuarios finales encuestados indicaron que ninguna solución estaría alojada en la nube, y en el sector del gobierno estatal/local esto fue del 24%. Si bien estos sectores pueden estar preparándose para colocar sus herramientas de productividad de oficina en la nube, parece haber una resistencia residual para trasladar allí sus cargas de trabajo de seguridad electrónica.

> "Falta de cultura para el uso de tecnología [en la nube] [en seguridad electrónica]"
>
> **– Usuario final encuestado**

VOLVER AL ÍNDICE

Punto de vista

La ciberseguridad no tiene por qué ser una barrera para la adopción de la nube. Hay que tener los controles, socios, procedimientos y mecanismos para gestionar el riesgo. Se trata de un modelo de responsabilidad compartida que puede ser muy seguro si se toman las decisiones correctas y se coopera con los socios adecuados.

Mathieu Chevalier
Gerente y Arquitecto de Seguridad Principal
Genetec Inc.

La seguridad electrónica y los datos relacionados son de misión crítica

Durante las restricciones de la pandemia, la seguridad electrónica a menudo se utilizó para proteger los movimientos de las personas alrededor de los edificios. Podía ayudar a mantener el distanciamiento social, contar personas y verificar que los ocupantes usaran mascarillas. Sin embargo, ahora que las restricciones por la pandemia han terminado en gran medida, la seguridad electrónica todavía se considera más que una herramienta para responder al crimen o un gasto necesario para proteger activos y personas. Hoy tiene un rol más significativo como elemento central en la transformación digital de los procesos organizacionales.

63%

de los usuarios finales encuestados indicaron que la seguridad electrónica y los datos relacionados eran de misión crítica. Esto fue similar a la encuesta de 2021 (68%).

En particular, la videovigilancia ofrece una rica fuente de datos. Es posible que las organizaciones ya tengan suficientes sistemas de videovigilancia instalados, pero pueden utilizar los datos existentes para cambiar fundamentalmente los procesos operativos a través de la creación de nuevos resultados y/o valor adicional. Por ejemplo, en las organizaciones de retail, se puede monitorear el largo de las filas de clientes y, en las ciudades, se puede disminuir los niveles de congestión de tráfico mediante la medición de tiempo de las señales de los semáforos.

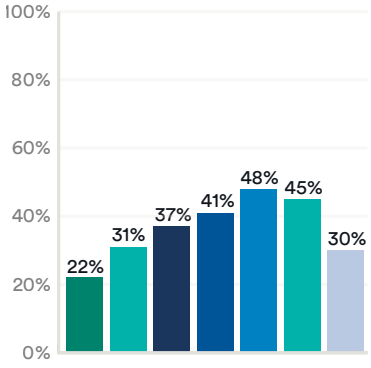
También parece que a medida que crecen las organizaciones, cambian sus puntos de vista sobre el valor y/o el uso de los datos de seguridad electrónica. Un mayor porcentaje de los usuarios finales encuestados en organizaciones con más de 100.000 empleados indicaron que la seguridad electrónica y los datos relacionados eran de misión crítica, que en organizaciones con menos empleados. Esto puede deberse a que están más avanzados en sus iniciativas de transformación digital que las empresas más pequeñas. Tener suficiente gestión y estructura de datos es fundamental para desbloquear el valor adicional de los datos recopilados en los sistemas de seguridad electrónica.

Desde la perspectiva del sector de usuarios finales, un valor atípico notable con el porcentaje más alto de encuestados que indicaron que la seguridad electrónica y los datos relacionados que eran de misión crítica fue el sector de usuarios finales de transporte (71%). Aquí, la seguridad electrónica no solo tiene un rol fundamental en la seguridad del personal y los pasajeros, sino que también ayuda a cumplir con los estrictos estándares de puntualidad en el transporte público.

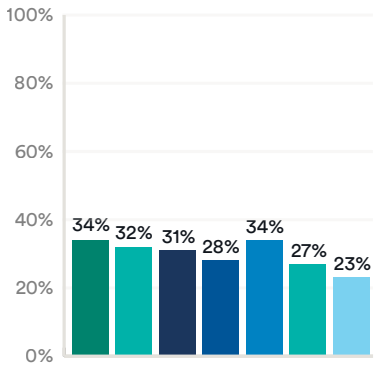
VOLVER AL ÍNDICE

EL ROL DE MISIÓN CRÍTICA DE LA SEGURIDAD ELECTRÓNICA

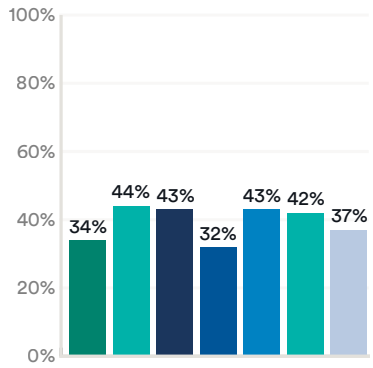
Cómo las organizaciones ven la seguridad electrónica y los datos relacionados según el tamaño de la organización



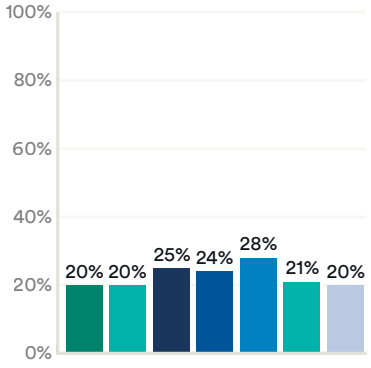
Una forma de garantizar el cumplimiento de las pautas reglamentarias



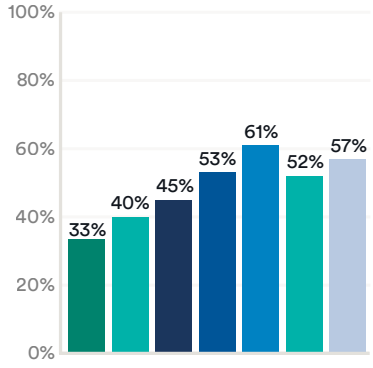
Una forma de ayudar a mejorar la satisfacción del cliente a través de una mejor eficiencia y conocimiento



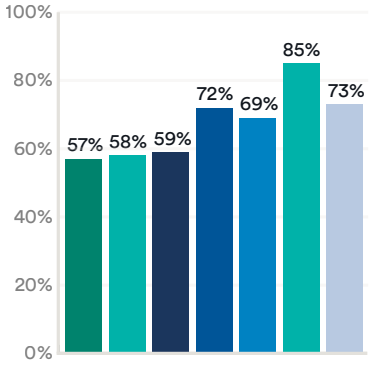
Una forma de ayudar a mejorar la productividad general del negocio, la eficiencia y la optimización de activos



Una forma de ayudar a reducir los costos operativos



Una forma de asegurar las instalaciones/oficinas



Misión crítica para el negocio para respaldar la seguridad del personal, los ciudadanos, los clientes, la seguridad de los activos y la propiedad intelectual

- 1-20 Empleados
- 21-200 Empleados
- 201-1.000 Empleados
- 1.001-10.000 Empleados
- 10.000-100.000 Empleados
- 100.001-500.000 Empleados
- 500.000+ Empleados

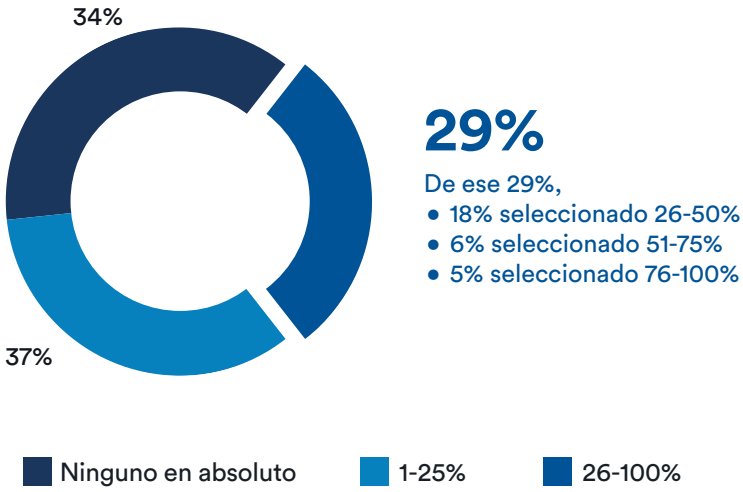
VOLVER AL ÍNDICE

La ciberseguridad sigue siendo la principal prioridad

En la encuesta de 2021, el 54% de los encuestados tenía más del 25% de su personal de operaciones de seguridad electrónica organizado para trabajar de forma remota. En la encuesta de 2022, esta cifra se redujo al 29%.

LA CIBERSEGURIDAD SIGUE SIENDO LA PRINCIPAL PRIORIDAD

¿Qué porcentaje de tu personal de operaciones de seguridad electrónica trabaja en forma remota?



Curiosamente, el 46% de los encuestados en Europa y el 48% en Latinoamérica indicaron que ninguno de sus empleados de operaciones de seguridad electrónica estaba organizado para trabajar de forma remota. Esto se compara con el 21% en los EE. UU. y Canadá y solo el 15% en el Reino Unido.

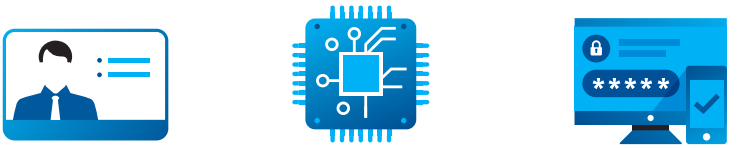
A medida que las restricciones de la pandemia disminuyeron, el trabajo remoto hizo lo propio. A pesar de esto, al igual que en la encuesta de 2021, el principal desafío al que se enfrentaron todos los encuestados al gestionar la seguridad de los empleados y visitantes siguió siendo la ciberseguridad. No sorprende que el 49% de todos los encuestados indicaran que su organización había activado una estrategia de ciberseguridad mejorada este año.

Un porcentaje mayor de todos los encuestados en organizaciones con más de 100.000 empleados indicó que el principal desafío al que se enfrentaron para gestionar la seguridad de los empleados y visitantes fue la ciberseguridad, que en las organizaciones con menos empleados. Esto podría deberse a la mayor complejidad de los sistemas de TI en organizaciones más grandes (incluida la cantidad de dispositivos para proteger y gestionar) y la percepción de que esto puede aumentar la vulnerabilidad de la ciberseguridad. También podría deberse a la percepción de que las organizaciones más grandes son objetivos más atractivos para los ciberdelincuentes.

VOLVER AL ÍNDICE

LA CIBERSEGURIDAD SIGUE SIENDO LA PRINCIPAL PRIORIDAD

Dónde se centran los esfuerzos de ciberseguridad

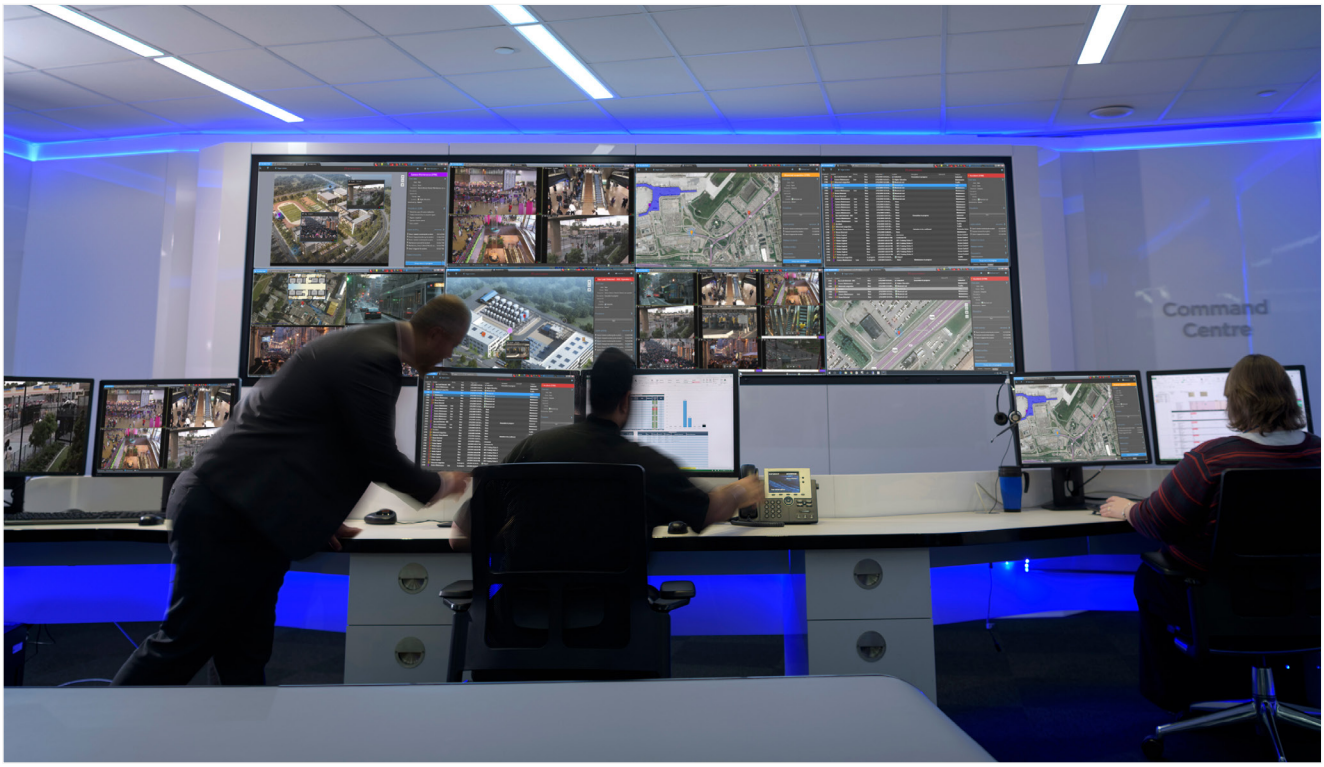


40% control de acceso

39% endurecimiento cibernético del hardware de seguridad

37% políticas de contraseña seguras

La nube percibida como un riesgo de ciberseguridad sigue siendo una barrera importante para una mayor adopción de la nube en soluciones de seguridad electrónica. Los encuestados calificaron los riesgos percibidos como el factor más importante para desacelerar la adopción de soluciones basadas en la nube para aplicaciones de seguridad electrónica. De manera similar, los usuarios finales calificaron los riesgos percibidos como el factor más importante para disuadir a su organización de implementar sistemas de seguridad en la nube. Sin embargo, como se mostró anteriormente en este reporte, la transición gradual a la nube continúa en la seguridad electrónica.



VOLVER AL ÍNDICE

La seguridad electrónica se unifica

Para algunos, las restricciones de la pandemia actuaron como un catalizador adicional para unificar sus sistemas de videovigilancia y control de acceso, ya que algunos usuarios finales necesitaban dar este paso para gestionar de manera efectiva el movimiento seguro de los ocupantes alrededor de sus instalaciones. El aumento de la demanda de este enfoque puede haber provocado que algunos integradores de sistemas ganaran mayor experiencia y conocimiento de los beneficios de la unificación, lo que generó más recomendaciones para que los usuarios finales consideren este enfoque.

Según las respuestas de la encuesta, a nivel regional, los usuarios finales de EE. UU. y Canadá tenían más probabilidades de haber implementado un sistema de control de acceso y video unificado (donde el software de control de acceso y video se unifican como un sistema de un solo fabricante).

El 44,4% de los encuestados de EE. UU. y Canadá seleccionaron que habían implementado un sistema de control de acceso y video unificado, un porcentaje mayor al de todas las demás regiones.

poseen tanto la videovigilancia como el control de acceso en sus implementaciones de seguridad electrónica.

De ese 64%, más del 75% tiene alguno:

- Integración entre sistemas de videovigilancia y control de acceso de diferentes marcas, o
- Soluciones unificadas de videovigilancia y control de acceso de una sola marca

Cambios en la tecnología: el año pasado

En la fase inicial de la pandemia, creció rápidamente el interés por una variedad de soluciones de seguridad que podrían ayudar con la gestión de visitantes, la implementación de regulaciones gubernamentales y a mejorar las capacidades remotas. El interés en algunas de estas soluciones disminuyó en 2021 y la última encuesta sugiere que ha disminuido aún más en 2022.

Un porcentaje menor de todos los encuestados en 2022 indicó que las capacidades asociadas con la pandemia eran una prioridad. La encuesta de 2022 también indicó que las capacidades "tradicionales relacionadas con la seguridad" fueron el foco.

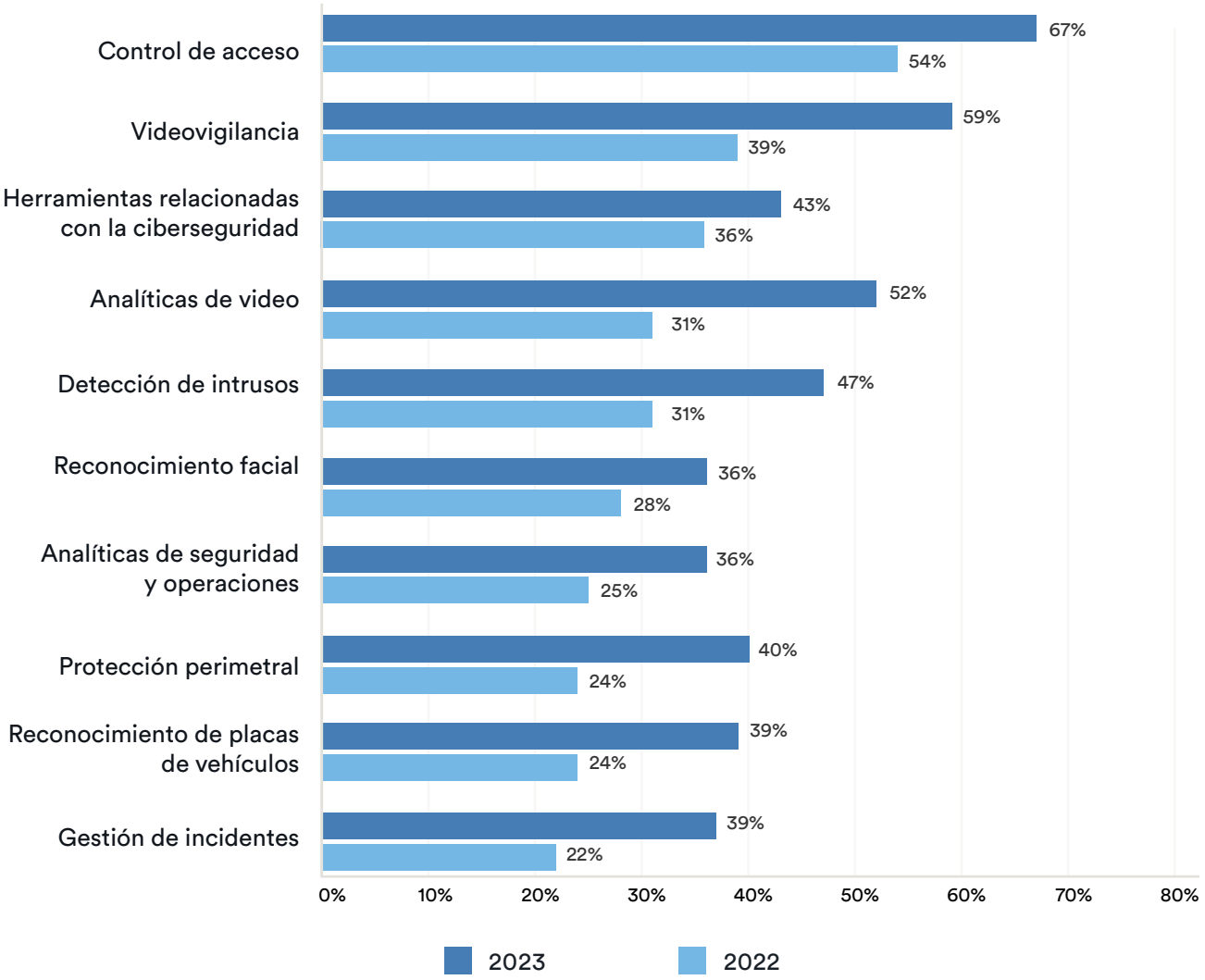
Cambios en la tecnología: el año que empieza

Como se mencionó anteriormente en este reporte, la importancia de la unificación entre el control de acceso y la videovigilancia ha ganado terreno en muchas organizaciones. Se ha vuelto a dar prioridad al trabajo en los sistemas principales de seguridad que se había dejado de lado durante la pandemia. El control de acceso y la videovigilancia son los dos sistemas principales de seguridad, entre otros, en el que se enfocará el trabajo en 2023.

VOLVER AL ÍNDICE

CAMBIOS EN LA TECNOLOGÍA: EL AÑO PASADO VERSUS EL AÑO QUE EMPIEZA

Las 10 principales tecnologías en las que las organizaciones planean invertir



VOLVER AL ÍNDICE

Conclusiones principales

1 La economía y la cadena de suministro son desafíos que se pueden superar

Las restricciones de la pandemia comenzaron a levantarse gradualmente en la mayoría de los países en 2021 y 2022, pero dejaron secuelas reales. Estos efectos económicos están afectando a la industria de la seguridad electrónica en forma de escasez de productos y dificultades de recursos humanos. Estos factores también estuvieron presentes en 2022, y las previsiones para 2023 son inciertas, lo que hace que esta sea una preocupación constante para los negocios. A pesar de los efectos de los problemas actuales con el cambio de suministro, la economía y las predicciones de una recesión, la encuesta apunta a señales alentadoras de una perspectiva general positiva para los presupuestos OPEX de 2023.

2 Priorizando la seguridad de los sistemas de seguridad electrónica

Aunque la industria de la seguridad electrónica está atrasada en su enfoque de ciberseguridad en comparación con otras industrias, es evidente que se ha producido un cambio y que se ha producido la necesidad de priorizar estas iniciativas como parte de la gestión del sistema de seguridad electrónica. El principal desafío al que se enfrentó en la gestión de la seguridad de los empleados y visitantes en 2022 siguió siendo la ciberseguridad. Esta también es una prioridad principal para 2023.

3 La migración a la nube continúa

Aunque la industria de la seguridad electrónica todavía está rezagada con respecto a otras industrias en cuanto a la adopción de la nube, hay señales claras de que el movimiento continuará en esta dirección. Todo apunta a que las implementaciones de nube híbrida son el camino que las empresas deben seguir para racionalizar sus costos, preocupaciones y empezar una migración a la nube.

El 31%
de todos los encuestados informaron que esperaban que los presupuestos en 2023 aumenten

El 34%
de todos los encuestados informaron que esperaban que los presupuestos en 2023 se mantengan

EL 16%
de todos los encuestados informaron que esperaban que los presupuestos en 2023 aumenten

El 36%
de los encuestados están buscando invertir en herramientas relacionadas con la ciberseguridad para mejorar su entorno de seguridad en los próximos 12 meses

El 66%
de los encuestados indicó que durante los próximos dos años, su organización pasará a gestionar o almacenar más datos de seguridad electrónica en la nube

VOLVER AL ÍNDICE

Punto de vista

Los proveedores de servicios compartidos dentro de los usuarios finales están descubriendo que necesitan perfeccionar nuevas habilidades para superar los siguientes retos:

- El aumento de la participación de otras partes interesadas del negocio que tienen interés en los datos de seguridad relacionados.
- La superación de las preocupaciones en torno a la ciberseguridad y el uso responsable de la red.
- El equilibrio entre el interés en aprovechar los avances tecnológicos con limitaciones internas, como la financiación y la escasez de talento.

Pervez R. Siddiqui
Vicepresidente, Ofertas y Transformación
Genetec Inc.

Apéndice

Apéndice 1: Metodología de la encuesta

Genetec Inc. encuestó a profesionales de la seguridad electrónica entre el 24 de agosto y el 21 de septiembre de 2022.

El objetivo de la investigación fue:

- Obtener una vista de las operaciones y los entornos de seguridad electrónica
- Comprender la respuesta de las organizaciones a los desafíos externos, como la escasez de productos y las dificultades de recursos humanos
- Comprender el enfoque global para 2023

Después de revisar las respuestas y de hacer una limpieza de los datos, se incluyeron 3.711 encuestados en la muestra para su análisis.

Detalles sobre la encuesta y el 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 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 solo por correo electrónico en inglés, francés, alemán, japonés, coreano y español.
- El formulario de encuesta en línea estaba disponible en francés, inglés, alemán, español, coreano y japonés.
- En el análisis final solo se incluyeron las encuestas completadas y enviadas por personas de la población objetivo.
- Las encuestas se tomaron en todas las regiones: EE.EE y Canadá, México, Centroamérica, El Caribe, Suramérica, Europa, Medio Oriente, África, Asia Oriental, Asia del Sur, Asia Sudoriental, Asia Central, Asia Occidental, y Australia y Nueva Zelanda.
- Las tasas de respuesta y de finalización de la encuesta variaron según la región y el tamaño de la organización, introduciendo potencialmente errores de muestreo en los conjuntos de submuestras.
- Se recopilaron respuestas de tres poblaciones objetivo principales; usuarios finales de seguridad electrónica e integradores de sistemas. Se realizó una limpieza de datos para validar la clasificación de los encuestados en una de estas dos poblaciones y limitar posibles errores. Cualquier error que no sea de muestreo es asumido 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 de empresas integradoras de sistemas).

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%. Para todas las preguntas de selecciona todas las opciones que aplican (donde los encuestados pueden elegir múltiples respuestas), los porcentajes se refieren a la proporción de encuestados que seleccionaron la respuesta individual.

Apéndice 2: Información demográfica de la encuesta

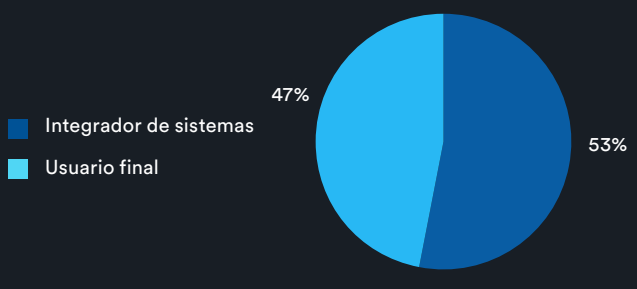
INDUSTRIAS

Servicios de Sistemas de Seguridad	55%
Otros	8%
Educación	6%
Transporte	5%
Banca y Finanzas	3%
Energía y Servicios Públicos	3%
Seguridad Nacional	2%
Ingeniería y Construcción	2%
Manufactura y Ventas Mayoristas	2%
Tecnología y Medios de Prensa	2%
Centros de Salud	2%
Retail	2%
Administración Pública	2%
Alimentos, Cosméticos, Productos Químicos y Farmacéuticos	2%
Transporte y Logística	1%
Gestión de Propiedades	1%
Asociaciones y Servicios profesionales	1%
Salas de Juegos y Casinos	1%

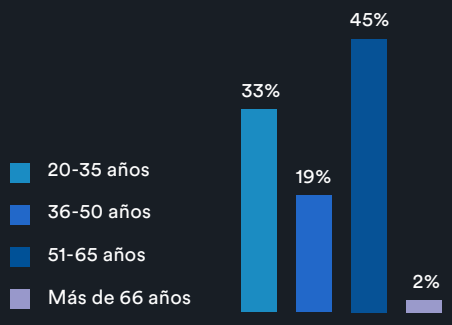
CARGO

Ingeniería, I+D, Diseño de Sistemas y Control de Calidad	23%
Gestión de Instalaciones/Operaciones	14%
Ventas	11%
Tecnología de la Información (TI)	10%
Servicio al Cliente o Soporte (incluido Soporte Técnico)	8%
Gestión de Proyectos/Riesgo o Gestión del Cumplimiento	8%
Gestión/Gestión de Oficina	6%
Seguridad y Protección	5%
Contabilidad/Finanzas	3%
Gestión, Documentación Legal	3%
Perito	2%
Marketing	2%
Documentación Legal	1%
Compras y Contratación	1%
Gestión de la Calidad	1%

TIPO DE ENCUESTADO

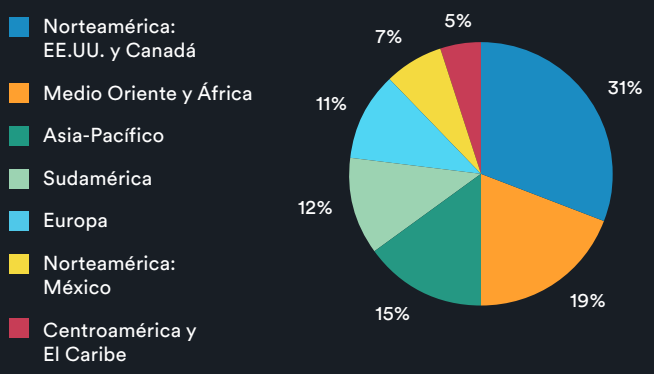


EDAD DEL ENCUESTADO



VOLVER AL ÍNDICE

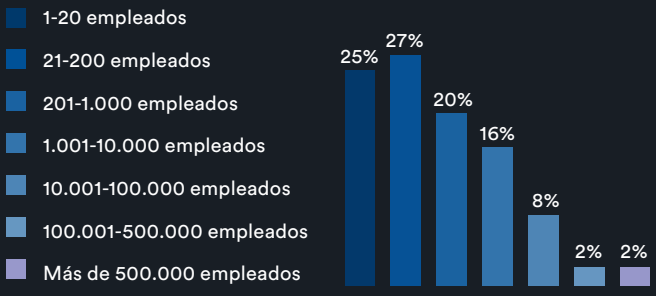
REGIONES GEOGRÁFICAS



INGRESOS DE LA ORGANIZACIÓN (USD$)

USD$5M - USD$24,9M	31%
USD$25M - USD$199,9M	16%
USD$200M - USD$499,9M	11%
USD$500M - USD$999,9M	6%
USD$1.000M - USD$10.000M	4%
Más de USD$10.000M	2%
No se puede revelar	30%

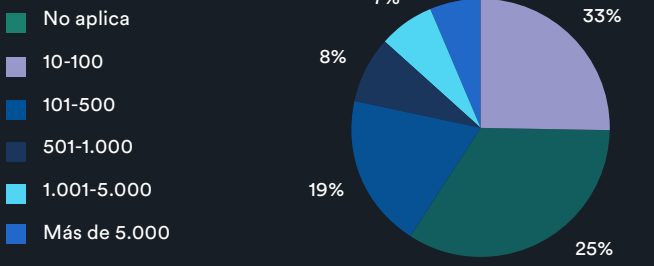
NÚMERO DE EMPLEADOS DE LA ORGANIZACIÓN A NIVEL GLOBAL



DEPARTAMENTO DE SEGURIDAD ELECTRÓNICA NÚMERO DE EMPLEADOS

1-20 empleados	54%
21-200 empleados	29%
201-1.000 empleados	11%
1.001-10.000 empleados	5%
Más de 10.000 empleados	2%

IMPLEMENTACIÓN DE VIDEOVIGILANCIA (CANTIDAD DE CÁMARAS)



IMPLEMENTACIÓN DE CONTROL DE ACCESO (CANTIDAD DE CREDENCIALES O LECTORES DE ACCESO SIN CONTACTO)

No aplica	36%
1 - 20	13%
21 - 200	13%
201 - 1.000	14%
1.001 - 5.000	10%
Más de 5.001	14%

VOLVER AL ÍNDICE

Apéndice 3: Comentarios abiertos

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

¿Tu organización está implementando otros tipos de infraestructura de seguridad electrónica?

- Alarmas
- Audio
- Barreras automatizadas
- Control de estacionamiento automatizado
- Biometría
- Barreras de bolardos
- Barreras de contención
- Sistemas de gestión de edificios
- Drones
- Rejas eléctricas
- Sistema de alertas de emergencias (EAS, por sus siglas en inglés)
- Detectores de explosivos
- Reconocimiento de huellas dactilares
- Sistemas de detección y represión de incendios
- Proyectores
- Lidar
- Escáneres de equipaje
- Detectores de metal
- Radios móviles
- Radares
- Sistema de localización en tiempo real
- Monitoreo de activos RFID
- Torniquetes
- Sistemas de rayos X

¿Existieron otras razones que llevaron a tu organización a empezar a utilizar la nube para aplicaciones de seguridad electrónica?

- Capacidad para unificar productos y compartir datos del sistema con socios de Infraestructura crítica/ fuerzas del orden público
- El almacenamiento en la nube es más seguro y conveniente
- Cumplimiento de regulaciones gubernamentales
- Seguridad de datos
- Obtener la certificación de seguridad según las pautas de seguridad nacional
- Facilidad de uso
- Miedo al robo de NVRs
- Evitar la pérdida de datos grabados si se roba el hardware
- Grabación de redundancia/copias de seguridad
- Reducción del personal de TI/salarios de TI
- Normativa sectorial
- Escasez de personal de TI
- Se requiere un pequeño gasto de capital
- Rapidez de acceso a los archivos

¿Existe algo adicional que haya frenado la adopción de soluciones en la nube para aplicaciones de seguridad electrónica en tu organización?

- Acceso a suficiente ancho de banda
- Los datos almacenados en la nube ya no te pertenecen, necesitas un administrador de datos para usarlos
- Problemas de conectividad
- RGPD
- Falta de cultura para el uso de la tecnología
- Cortes de energía

¿Hay alguna otra razón que desmotive a tu organización a implementar soluciones de seguridad en la nube?

- RGPD
- Falta de espacio suficiente en nuestro centro de datos
- Prohibido para infraestructura crítica

¿En qué tipo de proyectos estará enfocado tu departamento el próximo año?

- Drones
- Vigilancia electrónica de artículos
- Detección y supresión de incendios
- Gestión y rastreo de activos de IoT
- Control de inventario logístico
- Botón de pánico
- Integraciones de terceros que ofrecen menos consumo de energía
- Infracciones de tránsito

VOLVER AL ÍNDICE

Selecciona los 3 principales desafíos a los que se enfrentó tu organización en 2022

- Limitaciones de presupuesto
- Cambios en las políticas gubernamentales
- Largos tiempos de entrega
- Escasez de materiales
- Consumo de energía
- Regulaciones
- Costos en aumento

¿Qué tipo de desafíos de recursos humanos afectaron a tu departamento de seguridad electrónica el año pasado?

- Movimiento constante/reasignación de personal
- Altas tasas de inflación y salarios en aumento
- Falta de presupuesto para impartir formación

¿Qué nuevos procesos o prioridades fueron activados por tu organización este año?

- Desarrollo de aplicaciones
- Cambio CRM/ERP
- Sistema de seguridad contra incendios
- Reducción de emisiones hasta 2025
- Trabajo remoto

¿Qué funcionalidades se priorizaron en el último año?

- Control de acceso
- Ciberseguridad
- Reconocimiento facial
- Detección y supresión de incendios
- PSIM
- Analíticas de Video
- Monitoreo GPS de vida silvestre

¿Qué tipo de proyectos se han visto afectados? (por retrasos causados por problemas en la cadena de suministro)

- Nuevas instalaciones/proyectos
- Mudanzas de oficinas

¿Cómo respondieron a los retrasos causados por problemas en la cadena de suministro?

- Equipos alquilados a subcontratistas
- Mayor inventario
- Comprado con antelación

¿Qué capacidades de ciberseguridad y protección de datos han implementado en el último año?

- Auditorías de sistemas de información
- Certificación ISO 27k
- VLAN aislada para dispositivos de seguridad IOT
- Planes contingentes operativos
- Solo comunicaciones salientes
- VPN
- Lista blanca de direcciones IP y puertos de comunicación específicos

¿Existen otras capacidades remotas que tus clientes solicitan frecuentemente?

- Monitoreo de control de acceso
- Acceso a mapas basados en SIG
- Activar y desactivar
- Alertas a plataformas de mensajería como Telegram, Signal o Whatsapp
- Gestión de casos
- Privacidad de datos
- Diagnóstico y estado del sistema
- Sistemas de protección de activos electrónicos (EAS, por sus siglas en inglés)
- Geolocalización
- Sistema de monitoreo de recorridos de guardia
- Control de integración HVAC al sistema de seguridad
- Integración con sistemas de alarma contra incendios
- Intercomunicadores
- Intercambio de videos en vivo con terceros
- Control de rutas logísticas
- Sistemas de llamado de enfermeras
- Botón de pánico
- Mantenimiento predictivo
- Comunicación remota de audio
- Mantenimiento remoto
- Gestión de sistemas de terceros
- Control remoto de drones
- Virtualización

VOLVER AL ÍNDICE

¿En qué soluciones tus clientes pretenden invertir para avanzar o mejorar su entorno de seguridad electrónica en los próximos 12 meses?

- Sistema de alertas de emergencias (EAS, por sus siglas en inglés)
- Sistemas de detección y represión de incendios
- Botón de pánico
- Conteo de personas
- Tecnología de detección de objetos que utiliza ondas de radio para determinar el intervalo, la altitud, la dirección y la velocidad de dichos objetos
- Detección térmica
- Monitoreo GPS de vida silvestre

¿Qué acciones han tomado para mitigar los problemas de compra de hardware e inventario, relacionados con los desafíos actuales de la cadena de suministro?

- Permitir que los clientes realicen pedidos por adelantado antes de lanzar las licitaciones
- Ciertos proyectos simplemente se retrasan si no hay sustitutos
- Dirigir los esfuerzos a los servicios profesionales y soporte técnico
- Plazos de entrega prolongados
- Se abrió un centro de reparación para volver a poner en producción algunos componentes electrónicos fáciles de reparar
- Rediseño de sistemas
- Utilizar equipos de segunda mano

¿Se verán afectadas otras operaciones por el trabajo en el volumen de pedidos pendientes para implementación?

- Acceso a financiamiento
- Todas las operaciones se verán afectadas
- Flujo de caja, facturación, generación de ingresos
- Cuidado de la ciberseguridad para el trabajo remoto
- Electricidad y otros servicios públicos
- Protección del medio ambiente
- Todo está conectado
- RR.HH.
- Logística
- Contratos de mantenimiento
- Fábricas
- Operaciones
- Disponibilidad de personal calificado
- Se ha retrasado el entrenamiento sobre las nuevas marcas que incorporamos al portfolio de soluciones

VOLVER AL ÍNDICE

Acerca de Genetec

Genetec Inc. es una empresa de tecnología innovadora con un amplio portafolio de soluciones que abarca seguridad, inteligencia y operaciones. El producto emblemático de la empresa, Security Center, es una plataforma de arquitectura abierta que unifica la videovigilancia, el control de acceso, el reconocimiento de placas vehiculares (LPR, por sus siglas en inglés), las comunicaciones y las videoanalíticas, todas basadas en redes ip. Genetec también desarrolla soluciones y servicios basados en la nube diseñados para mejorar la seguridad y aportar nuevos niveles de inteligencia operativa para gobiernos, empresas, transporte y las comunidades en las que vivimos. Fundada en 1997 y con sede en Montreal, Canadá, Genetec atiende a sus clientes en todo el mundo a través de una extensa red de distribuidores, integradores, socios de negocios certificados y consultores en más de 159 países.

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

Para obtener más información sobre este reporte, por favor escríbenos a **Genetec-research@genetec.com**

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