Resumen Ejecutivo del
Estado de la Seguridad Electrónica 2026

1. Metodología de la Investigación y Alcance Global

Para esta sexta edición, se recopilaron datos entre el **18 de agosto y el 15 de septiembre de 2025**, analizando un total de **7,368 encuestas válidas** de profesionales en seis regiones: Estados Unidos y Canadá (29%), Latinoamérica y el Caribe (26%), Europa (21%), Asia-Pacífico (15%), Medio Oriente y África (7%), y Australia y Nueva Zelanda (2%).

La muestra incluyó cuatro perfiles clave:

- **Sócios de negócio (42%):** Integradores e instaladores.
- **Usuarios finales (37%):** Operadores y gestores directos de los sistemas.
- **Consultores (11%):** Asesores técnicos y estratégicos.
- **Fabricantes (9%):** Desarrolladores de hardware y software.

2. La Seguridad Electrónica como Función Estratégica

La industria ha entrado en una fase donde los sistemas ya no solo protegen activos, sino que **aportan valor de negocio** a través de la inteligencia operativa.

El Valor de la Unificación y la Integración

- **Sistemas Interconectados:** Más del **70% de los encuestados** ya operan bajo arquitecturas unificadas o integradas.
- **Motivación para el cambio:** La principal razón para reemplazar tecnologías antiguas (citada por el **60%**) es la necesidad de **integrar sistemas con nuevas tecnologías**.
- **Visión de negocio:** El 91% de los socios de negocio reportaron que la demanda para añadir nuevas capacidades a sistemas existentes se mantuvo o creció en 2025, buscando obtener información accionable para la continuidad del negocio.

3. La Revolución Digital y el Rol de la Tecnología de la Información (TI)

La sofisticación de las operaciones ha convertido al departamento de TI en un actor central en las decisiones de compra de seguridad electrónica.

Colaboración Interdepartamental

- **Influencia de Compra:** Los usuarios finales identifican a la alta dirección, finanzas y TI como los grupos más influyentes en el proceso de adquisición.
- **Prioridades de TI:** Para 2025, los equipos de TI priorizan las herramientas de ciberseguridad (**47%**) y las soluciones basadas en la nube (**47%**) de forma mucho más agresiva que los departamentos de seguridad tradicionales.
- **Derribando Silos:** La unificación de defensas físicas y cibernéticas permite una adopción más ágil de infraestructura de red compartida y analíticas avanzadas.

4. La Nube como Fuerza Habilitadora de la Modernización

La adopción de la nube ha dejado de ser una tendencia para convertirse en un requisito de agilidad y escalabilidad.

El Auge de los Modelos Híbridos

- **Flexibilidad:** Los usuarios prefieren modelos híbridos que equilibran la escalabilidad de la nube con la redundancia de las instalaciones locales para asegurar la continuidad durante interrupciones.
- **Adopción por Escala:** Mientras que las organizaciones pequeñas (1-10 cámaras) son más propensas a alojarse 100% en la nube, las grandes corporaciones (>5,001 cámaras) dependen de modelos híbridos por razones de **redundancia y rendimiento**.
- **ACaaS (Control de Acceso como Servicio):** Este segmento está ganando terreno debido a su facilidad de implementación; el **27% de los usuarios finales** ya operan sistemas de control de acceso híbridos.

5. Inteligencia Artificial (IA) y Analíticas Avanzadas

El interés por la IA se ha duplicado entre los usuarios finales, posicionándose como una de las tres prioridades principales para 2026 junto a la videovigilancia y el control de acceso.

Aplicaciones y Expectativas

- **Objetivos de Integración:** Las organizaciones buscan la IA para **automatizar tareas repetitivas (48%)**, buscar e investigar incidentes (55%) y filtrar eventos automáticamente (46%).
- **Liderazgo de Grandes Empresas:** Las organizaciones con más de 100,000 empleados lideran la adopción de IA (**34%**) y herramientas de visualización de datos (**35%**).
- **Desafíos de Confianza:** El 70% de los usuarios finales tiene preocupaciones sobre la implementación de la IA, citando la **falta de comprensión (37%)**, el uso de datos (36%) y el riesgo de uso malicioso (32%).

6. Convergencia entre Seguridad Física y Riesgo Cibernético

A medida que los sistemas se conectan a la red, la protección de dispositivos IoT se vuelve una prioridad operativa fundamental.

Panorama de Amenazas en 2025

- **Incidentes en Aumento:** El 31% de los encuestados reportó un incremento en incidentes de ciberseguridad, cifra que sube al **41% en organizaciones grandes** (>10,000 empleados).
- **Tipos de Ataques:** Los ataques más comunes incluyen **phishing/smishing (50%)**, software malicioso (41%) y hackeo de dispositivos para acceder a la red (40%).
- **Medidas de Mitigación:** El 70% de las organizaciones se enfoca en **educar y entrenar empleados**, mientras que el 48% ajusta permisos y privilegios de usuario para endurecer la infraestructura.

7. Dinámicas de Mercado y Desafíos de Personal

El entorno económico y social plantea obstáculos que podrían retrasar la innovación en 2026.

Obstáculos para 2026

- **Presiones Económicas:** La incertidumbre económica y la **inflación (55%)**, junto con problemas en la cadena de suministro, son las mayores preocupaciones para el próximo año.
- **Escasez de Talento:** Atraer personal calificado es un reto crítico, especialmente técnicos de instalación (**52%**) e ingenieros de sistemas (**36%**) con experiencia en nube e IA.
- **Estrategias de Retención:** Los socios de negocio están invirtiendo en **entrenamiento transversal**, automatización de flujos de trabajo y políticas de bienestar para mejorar la retención.

8. Conclusiones y Visión a Largo Plazo

El reporte concluye que la seguridad electrónica ha superado su fase reactiva para convertirse en un motor de resiliencia organizacional.

Pilares del Futuro

1. **Tecnología como Catalizador:** La innovación no es opcional; es esencial para proteger personas y bienes en una fase digital.
2. **Colaboración como Motor:** El éxito depende de la alianza entre TI y seguridad para resolver problemas de formas novedosas.

3. **Asociaciones Estratégicas:** Los clientes ya no buscan proveedores, sino **socios de confianza** que ofrezcan estabilidad, arquitectura abierta y un costo total de propiedad optimizado a largo plazo.

Bibliografía y Referencias

- **Genetec Inc.** (2025). *Estado de la Seguridad Electrónica 2026: Transformación colaborativa*. Sexta edición. Montreal, Canadá.

Resumen compilado por:

Cámara de Experiencias Rurales
Jorge Fallas Cascante
Presidente Ejecutivo
+ 506 87513076
info@experienciasruralescr.com
https://experienciasruralescr.com