CON SEGURIDAD

Magazine Latam

C4 Y C5

TECNOLOGÍA PARA PROTECCIÓN

Noviembre - Diciembre 2025 / Edición 3°

www.conseguridad.com

Noviembre - Diciembre 2025 / No. 3° / Año 1
Precio $60.00 MXN / $3.00 USD

GRUPO EDITORIAL • GRUPO EDITORIAL • GRUPO EDITORIAL • GRUPO EDITORIAL
MS GLOBAL

HIKVISION® | Guanlan

To understand the nature and movement of water, one must observe its waves.

Protección perimetral
Impulsado por Hik

De 1 m a 100 km con protección precisa en cualquier entorno.

Nuestras soluciones perimetrales combinan **inteligencia artificial con tecnología avanzada** para proteger de forma precisa cualquier tipo de espacio: fábricas, puertos, granjas, residencias, fronteras y más.

Incluso bajo lluvia intensa, niebla o viento fuerte, la seguridad no se detiene.

- **IA con 99.9%** de precisión.
- **Estabilidad** en condiciones climáticas adversas.
- **Cobertura** desde 1 m hasta 100 km.
- **Alertas inmediatas** y verificación en tiempo real.

@HikvisionMx
www.hikvision.com/mx

Hikvision México
sales.mexico@hikvision.com

C5 espacio gubernamental para la seguridad ciudadana

Actualmente, la seguridad pública se encuentra en un punto de inflexión en el que los Centros de Comando, Control, Comunicaciones, Cómputo y Contacto Ciudadano (C5), junto a los Centros de Comando y Control (C4), son ya infraestructuras críticas para responder a emergencias, coordinar a fuerzas policiales, y prevenir delitos. Y es en este terreno en el que la tecnología dejó de ser un apoyo accesorio: hoy es el centro de la operación.

En un "C5" como espacio gubernamental es el que monitorea con cámaras de videovigilancia urbana, coordina servicios de emergencias como seguridad ciudadana, atención médica, protección civil y medio ambiente. Opera el número de emergencias 911, gestiona la alerta sísmica y utiliza aplicaciones para recibir reportes y enviar unidades de respuesta; pero para hacer posible esto, la tecnología juega un papel preponderante para hacer posible toda esta convergencia.

Hoy, empresas internacionales y grandes fabricantes, así como mayoristas e integradores son parte del engranaje de estos sitios que han salvado en el mundo miles de vidas humanas. A nivel internacional ya no es raro ubicar C2, C4, C5 y C5i de niveles municipales y estatales que mantienen comunicación estrecha y directa con sus gobiernos nacionales, y América Latina no es ajeno a esta tendencia.

Destacadas marcas de seguridad electrónica, telecomunicaciones, radiocomunicación y telemetría; entre otros, procedentes de Estados Unidos, Asia o Europa mantienen en México y América Latina un importante core de negocios con los C5 y C5i a través de una amplia o profesional red de mayoristas, integradores e instaladores con modernos e imponentes desarrollos, que incluso éstos han sido premiados a nivel internacional en ferias de seguridad electrónica, cómputo o comunicaciones.

En el caso de México, desde hace dos décadas fue creada la asociación civil para representar oficialmente a la National Emergency Number Association (NENA 9-1-1) y se ha destacado como un organismo especializado en la gestión de los Centros de Atención de Emergencias Latinoamérica. Su actividad se centra en la oferta de cursos y capacitación, así como la certificación del personal e instituciones.

Desde hace más de 2 lustros en México, NENA 911 reúne a líderes de cada entidad de nuestro país y Latinoamérica que dirigen, administran, coordinan y operan Centros de Atención de Llamadas de Emergencia. Dicha organización tiene presencia en varios países de Latinoamérica con más de 100 instructores certificados bajo los estándares de NENA 9-1-1 Internacional

Sin duda, la tecnología hoy es el eslabón más fuerte en todos los Centros de Atención de Llamadas de Emergencia, ya sea a través de videovigilancia urbana, botones de pánico, líneas telefónicas convencionales o celulares, el posicionamiento GPS, la telemetría o la radiocomunicación, sin olvidar el talento humano que está detrás de cada línea o monitor dando seguimiento a un incidente con avanzada tecnología.

CON SEGURIDAD
Magazine Latam

DIRECCIÓN GENERAL

HUMBERTO MEJÍA, DSE, CPSI, CIEIE
NORTEAMÉRICA / ESPAÑA
hmejia@conseguridad.com

ALFREDO YUNCOZA, CSSM, CPOI, CPO
CENTRO / SUDAMÉRICA
ayuncoza@conseguridad.com

DIRECCIÓN COMERCIAL

MARÍA ANTONIETA JUÁREZ CARREÑO
DIRECCIÓN COMERCIAL Y RELACIONES PÚBLICAS
marieclaire@conseguridad.com

COORDINACIÓN EDITORIAL

BEATRIZ CANALES HERNÁNDEZ
COORDINACIÓN EDITORIAL
edicion@conseguridad.com

COORDINACIÓN DISEÑO

SERGIO GIOVANI REYES POZO
COORDINACIÓN DISEÑO
diseno@conseguridad.com

MARKETING LATAM

SARA MEJÍA CASTRO
DESARROLLO DE NEGOCIOS LATAM
negocios@conseguridad.com

CORRESPONSAL

CARMEN CHAMORRO
CORRESPONSAL ESPAÑA
corresponsal@conseguridad.com

ADMINISTRACIÓN Y CONTABILIDAD

OSCAR TENORIO COLÓN
ADMINISTRACIÓN Y CONTABILIDAD
contabilidad@conseguridad.com

CONTACTO

Tel: +52 55 1607 1398 (México)
WhatsApp: +58 424 1390 359 (Venezuela)
WhatsApp: +52 55 1894 7067 (México)
asistencia@conseguridad.com

Con Seguridad Año 1, No 3, Noviembre/Diciembre 2025, Publicación Bimestral de **Grupo Editorial MS Global S. de R.L. de C.V.**, con domicilio en Av. Primero de Mayo No 15, Piso 11, Ofic. 1108, Col. San Andrés Atoto, Naucalpan, Estado de México, C.P. 53500, Tel: +52 5518447067 . **Editor responsable: Humberto Mejía Hernández.** Certificado de Reserva 04-2022-050614181900-102 otorgado por el Instituto Nacional del Derecho de Autor. Certificado de Licitud de contenido No. 11483 y Certificado de Licitud de Título No. 13910, otorgados por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. Autorización del Registro Postal: PP15-5134 otorgado por Sepomex. Se autoriza la reproducción citando al medio y autor del texto, previo acuerdo por escrito con el editor. Impresa en: **Grupo Mejía Impresores**, calle La Poza No. 72, Col. San Lorenzo Totolinga, Naucalpan de Juárez, Estado de México, Tel: +52 5518947067.

CONTENIDO


ReputationUP
ReputationUP, expertos en defender el activo más frágil: la reputación.
REPUTATIONUP.COM

El Profesional

Licenciado en Derecho. Técnico Profesional en Administración de Recursos Humanos. Profesional de Protección Certificado (CPP), Investigador Profesional Certificado (PCI®) y Profesional de Seguridad Física (PSP®), todas estas certificaciones por ASIS International.

Miembro fundador de ASIS International, Capítulo México. Director de SIPROSI Corporativo S.A. de C.V.

Ampliamente reconocido como consultor, posee una larga y exitosa trayectoria en la preparación de profesionales en el área de la seguridad. Invitado frecuente en eventos de la industria de la seguridad de América y Europa.

Rubén Fajardo Correa

Humberto Mejía Hernández, DSE.

¿Prepara EE.UU. operación militar en México vs cárteles?

En los pasillos de varias dependencias de gobierno federal, redes sociales de algunos periodistas y ciertos partidos políticos de oposición, se menciona con preocupación y hasta miedo, que mientras el gobierno mexicano ofrece condolencias por el reciente asesinato del alcalde de Uruapan, Michoacán, Carlos Manzo (el cual se presume fue obra del crimen organizado), y promete que "no habrá impunidad", la administración del Presidente Donal Trump, evalúa operaciones militares contra cárteles de drogas en territorio mexicano. El plan incluye envío de tropas del Comando de Operaciones Especiales, agentes de la CIA, y uso de drones para atacar laboratorios e instalaciones del narco. El entrenamiento ya comenzó, aunque no hay fecha confirmada, según lo publicó la cadena noticiosa NBC News.

Las fuerzas estadounidenses operarían bajo el Título 50 (operaciones encubiertas de inteligencia fuera del marco militar tradicional) utilizando drones de largo alcance para desmantelar laboratorios y ejecutar ataques dirigidos contra líderes de cárteles. Algunos equipos requieren operadores en tierra, lo que implica presencia física de personal militar estadounidense en México. La misión sería tratada con máximo secretismo, similar a los recientes ataques contra embarcaciones en el Caribe (Venezuela) que han dejado, hasta el cierre de edición de **Con Seguridad**, 64 muertos.

Cabe resaltar que, en febrero de este año, el Presidente Donal Trump, a través del Departamento de Estado, designó a los cárteles mexicanos de Sinaloa, Jalisco Nueva Generación, del Noreste, del Golfo, Cárteles Unidos y la nueva Familia Michoacana, como organizaciones terroristas extranjeras, junto con el grupo salvadoreño MS-13 y la banda venezolana Tren de Aragua. Esta medida otorga a las agencias estadounidenses mayores facultades legales para realizar operaciones encubiertas, lo cual es tema que debería ser de mayor preocupación para la administración federal mexicana.

En abril pasado, Trump propuso a la Presidenta Claudia Sheinbaum Pardo, permitir tropas estadounidenses en México. Ella rechazó categóricamente. Ahora NBC revela que Washington planea actuar "con o sin coordinación mexicana". Los altos mandos y la Casa Blanca discuten el alcance de la misión. Sin embargo, la pregunta no es si atacarán, sino cuándo y con qué intensidad. Asunto de mayor preocupación para nuestra nación.

La misión estadounidense no buscaría "socavar al gobierno de Sheinbaum", aclaran funcionarios de EE. UU., pero el mensaje es claro: si México no puede o no quiere proteger a su gente del narco, Estados Unidos actuará unilateralmente en su territorio. Es la consecuencia inevitable de un gobierno que ignora a alcaldes como Manzo, que abandona a líderes como Bernardo Bravo, que deja solos a 112 políticos ejecutados en seis meses. Cuando el Estado mexicano falla, otros ocupan el vacío. Y Trump ya tomó la decisión de llenar ese vacío con fuerzas especiales, drones y operaciones encubiertas. Sin duda, México perdió su soberanía en seguridad el día que decidió no ejercerla.

De ser aprobada esta medida del gobierno de Trump, esta sería la primera vez que EE. UU. ejecuta operaciones militares directas dentro de México, según el informe. A diferencia de misiones anteriores, más centradas en inteligencia o apoyo a fuerzas locales, esta implicaría acciones ofensivas secretas contra objetivos de los cárteles, pues el gobierno de Trump está comprometido a usar "todo el aparato del Estado" para combatir la amenaza que representan los cárteles para los ciudadanos estadounidenses. Ni la CIA ni el Pentágono hasta hoy han ofrecido comentarios sobre el informe. Mientras tanto en la República Mexicana, la atención de los medios y la sociedad se centra en el acoso del que fue objeto la Presidenta…

¡Gracias y nos leemos pronto, pero Fuera de Grabación!

Presentó recientes lanzamientos para la protección contra intrusiones, videovigilancia, protección contra incendios, confort y automatización

• Ajax Systems, fabricante de soluciones inteligentes de seguridad y automatización, presentó en la Feria ESS+ 2025 sus últimos lanzamientos e innovaciones, dirigidas al mercado residencial y empresarial de América Latina.

Bogotá, Colombia.- Ajax, fabricante europeo de sistemas inteligentes y profesionales de seguridad, presentó sus soluciones en intrusión, protección contra incendios, comunicación y videovigilancia para los mercados residencial y de negocios para América Latina.

"En el marco de la Feria Internacional de Seguridad ESS+ 2025, en entrevista para **Con Seguridad**, Felipe Hoyos, Director Técnico de Ajax para Latinoamérica, destacó que la compañía cuenta con un departamento específico que cada trimestre se encarga de lanzar novedades y actualizaciones de sus productos y soluciones que están en el mercado.

"Nuestro objetivo es garantizar la privacidad de los usuarios. Es el usuario final quien decide qué empresa, instalador o persona autorizada puede acceder a las imágenes, grabaciones o al control de las cámaras PTZ, y bajo qué condiciones. Además, define cómo actuar ante una confirmación de alarma. De esta forma, Ajax no solo ofrece soluciones en intrusión, automatización, confort e incendios, sino también un completo portafolio en videovigilancia que respalda la seguridad integral del cliente", afirmó Felipe Hoyos.

En intrusión, la empresa exhibió un nuevo panel de alarma diseñado para instalaciones que están desatendidas como por ejemplo un rancho, una finca o una infraestructura en donde no hay conectividad a nivel de Ethernet y demanda de autonomía con las baterías de Ajax y la posibilidad de extender la cobertura con antenas externas.

También presentó un nuevo sensor de cortina para exterior, con doble infrarrojo pasivo, microondas, banda K y antimasking y que cuenta con una detección antisabotaje por acelerómetro.

Además, exhibió su portafolio de sensores de incendios que pueden ser desde subida repentina de temperatura, detección de humo o monóxido de carbono, para cualquier tipo de instalación a nivel profesional y también con estaciones manuales. En protección contra incendios estos dispositivos están interconectados a los hubs de Ajax, que son un "cerebro" con diferentes posibilidades tanto manuales, a nivel de aplicación o botones y de forma automatizada.

"Cada panel que tiene Ajax o hub permite escenarios de automatización, temperatura, programación horaria, confirmación de alarma o el cambio del modo de seguridad del panel", aseguró Felipe Hoyos.

Ajax dio a conocer apagadores o interruptores, que se controlan vía inalámbrica desde cualquier parte y que poseen múltiples características para aprovechar de mejor manera el sistema de alarma. Así como las electroválvulas Water Stop, 100% inalámbricas para control de riesgos que permiten cerrar de forma remota el suministro de agua en la estancia protegida por el sistema de seguridad Ajax.

En sistemas de comunicación e intrusión, dio a conocer el SpeakerPhone Jeweller, que permite una comunicación bidireccional con la instalación, protección anti sabotaje avanzada y se puede conectar el panel de alarma con un conmutador que permite hacer audio verificación en el lugar donde está sucediendo el evento.

Finalmente, en el área de videovigilancia presentó dos innovaciones para ampliar su portafolio de CCTV. La primera es un doorbell inteligente, disponible en cuatro colores, que integra dos funciones en un solo dispositivo: por un lado, una cámara de 4 megapíxeles con ángulo de visión de 110° y batería con autonomía de hasta dos horas; y por otro, la capacidad de convertirse en un sensor de movimiento, que se conecta al panel de alarma incluso cuando se pierde la señal de Wi-Fi.

El otro lanzamiento es la Ajax IndoorCam, una cámara de seguridad Wi-Fi para interiores con sensor de movimiento PIR e IA integrada, con conexión inalámbrica y con una resolución de 4 megapixeles para aquellas instalaciones en donde se requiere una instalación más práctica sin cableado.

Felipe Hoyos, Director Técnico de Ajax para Latinoamérica

Altronix exhibe novedades para LatAm en ESS+ 2025

- La empresa tiene más de 40 años, cuenta con un departamento de más de 3 mil productos de alta calidad, con garantía de por vida.
- Exhibió los novedosos productos EBC48, NetWay5PQ, NetWaySP2BT y Pace1STR.

Bogotá, Colombia.- Altronix —fabricante de soluciones de transmisión de energía y datos— estuvo presente en la Feria Internacional de Seguridad 2025 ESS+ con la demostración de su línea de productos, que incluyen cargadores de baterías, convertidores de medio, transmisores de video, adaptadores y soluciones de comunicación en red para sistemas de seguridad, control de acceso, videovigilancia y detección de incendios.

Ronnie Pennington, Director de Ventas para las Américas en Altronix, indicó a **Con Seguridad** que la compañía, con sede en Estados Unidos, tiene más de 40 años y cuenta con un departamento de más de 3 mil productos de alta calidad, lo cual le permite ofrecer garantía de por vida, y ese valor es su principal diferenciador en el mercado.

"Somos hechos en Estados Unidos, usamos componentes de buena calidad por eso podemos ofrecer garantía de por vida, no somos el más barato ni el más costoso, somos competitivos. El mercado confía en Altronix como empresa con equipos de buena calidad y nuestros clientes son atendidos directamente por personas, respondemos correos y contamos con un chat en la página web para hablar sobre nuestro portafolio de productos", explicó Pennington.

En la Feria Internacional de Seguridad ESS+ 2025, Altronix presentó desarrollos nuevos como: el EBC48, un cargador de batería rápido externo que permite una carga de 16 horas y es ideal para aplicaciones en donde no se dispone de alimentación constante; el NetWay5PQ, un conmutador PoE+ compacto, reforzado y gestionado por red, que conecta directamente al puerto de gestión y cuenta con cuatro salidas de puertos.

También el NetWaySP2BT, un convertidor de medios de fibra a Ethernet que proporciona hasta 180W de potencia a dos dispositivos mediante puertos 802.3bt (4PPoE), y adaptadores como el Pace1STR, un kit adaptador Ethernet de largo alcance diseñado para extender la transmisión de datos y la alimentación a dispositivos IP.

Además, la compañía exhibió nuevas versiones de soluciones existentes como: el PACE1KRT, un kit adaptador Ethernet de largo alcance que transmite datos y alimentación mediante par trenzado en formato compatible con PoE (+); la Serie Trove, una solución de integración de alimentación y control de acceso en un cajón de rack; y la Serie NetWay Spectrum, el gabinete más grande con el que cuenta la empresa y es una solución para desplegar dispositivos de red usando fibra y energía PoE, además recientemente se le agregó otra tarjeta para cuente con el respaldo de baterías de largo alcance.

Ronnie Pennington aseguró que todas las soluciones de Altronix son compatibles con las principales marcas de control de accesos, videovigilancia, control de incendios y alarmas, incluidas las de origen chino o japonés, países a donde también surte producto.

Todas las soluciones ya están disponibles a nivel mundial y para América Latina a través de distribuidores, desde México hasta Argentina. Específicamente en Colombia, Altronix vende a través de empresas como: SYSCOM, ISTC, Full Protection, Sac Seguridad, Anixter, Silmar, entre otras.

Para Altronix, las verticales que son el core de su negocio son control de accesos y videovigilancia. Por volumen, México es la región más importante y la más grande de todas, le siguen República Dominicana, Panamá, Costa Rica, Colombia, Perú y el Caribe con Trinidad y Tobago, Puerto Rico. Chile y Argentina están creciendo constantemente.

El objetivo de Altronix es que sus distribuidores mantengan un stock importante en el país de venta a fin de que puedan despachar un producto en un lapso de entre cinco a 10 días, dependiendo de la cantidad y el tipo de producto. Cabe destacar, que en el mercado de control de accesos, la empresa trabaja con más de 65 socios.

Ronnie Pennington concluyó que Altronix actualmente trabaja en un nuevo proyecto que va a modificar la forma en cómo se hace la instalación de un control de acceso, y afirmó: "Siempre estamos enfocados a los diferentes mercados y aplicaciones. No hay una empresa como Altronix en el mundo, nos enfocamos en fuente de poder para control de accesos, videovigilancia, incendios, alarmas y seguridad".

Ronnie Pennington, Director de Ventas para las Américas en Altronix

IDIS® presentó portafolio de soluciones

- El fabricante surcoreano exhibió cámaras de seguridad 360, nueva línea de cámaras AI, servidores con funcionalidad de AI y BI, NVR muy competitivos de 8, 16 y 64 canales y su línea de servidores.

Bogotá, Colombia.- IDIS, fabricante surcoreano de sistemas de videovigilancia y seguridad, presentó en la Feria Internacional de Seguridad (ESS+) 2025 su línea IDIS AI, que abarca diferentes soluciones de protección integral desde cámaras con Inteligencia Artificial (IA) embebida, equipos de reconocimiento facial, servidores y dispositivos de videovigilancia NVR (Network Video Recorder).

En entrevista para **Con Seguridad**, Víctor Merino, Director Regional en Latinoamérica, indicó que IDIS tiene casi 30 años en el mercado y originalmente habían estado enfocados en ser fabricantes OEM y SDM, pero hasta hace algunos años decidieron lanzar su marca de forma directa, por lo que, dijo, los productos son nuevos, basados en tecnologías recientes como la Inteligencia Artificial, NDAA Compliance y muy amigables en el entorno de Ciberseguridad.

"Hay mucha tecnología en el ámbito de la ciberseguridad, ese es el gran factor diferenciador de nuestra marca, la oferta es muy grande, tenemos cámaras de distintos tamaños, modelos y formas, y eso nos permite ser muy flexibles en distintos casos de usos", explicó Víctor Merino.

En el stand de BTCO —su distribuidor autorizado para la región de Sudamérica— IDIS dio a conocer sus cámaras de seguridad 360 con IA, con protocolos muy seguros y en las que se pueden "correr" aproximadamente 40 algoritmos diferentes de inteligencia artificial; así como servidores para aplicaciones más robustas; y NVR muy competitivos de 8, 16 y 64 canales.

"Otro diferenciador de nuestros productos es la parte técnica, lo robusto que somos en el ambiente de ciberseguridad, cada NVR tiene su propio firewall, eso no es muy común en la industria, y nos da un posicionamiento muy fuerte en instalaciones grandes. Hoy todo corre en la red, de alguna forma estas cajas son muy robustas", señaló.

Víctor Merino, aseguró que la línea ADIS se ha posicionado fuertemente en el sector bancario en América Latina, aunque precisó que las soluciones tecnológicas se adecúan a muchas verticales.

Reconoció que, a diferencia de otros países de Latinoamérica, el mercado mexicano tiene diferentes requerimientos en materia de seguridad bancaria con los cuales cumplen, pero que todavía no han atacado de forma efectiva.

"Estamos en esa estrategia, cumplimos 100% con Seproban (Seguridad y Protección Bancaria), y estamos en conversaciones con un banco transnacional muy grande, donde estamos próximos para lograr el sponsor venderla (la tecnología) abiertamente en el mercado como Seproban lo exige. México también es a través de distribución, estamos en conversaciones con algunos distribuidores para tener un mejor posicionamiento de la marca", concluyó Víctor Merino.

Víctor Merino, Director regional para IDIS en Latinoamérica

Poderoso sistema **Autonomous Management Framework** (AMF) Plus de Allied Telesis

- **La empresa es desarrolladora y propietaria de su tecnología, tanto en hardware como en software, y el 18% del revenue del negocio lo destina al departamento de investigación y desarrollo.**

Bogotá, Colombia.- En la Feria Internacional de Seguridad ESS+ 2025, Allied Telesis —fabricante japonés con presencia en más de 100 países— presentó su sistema de administración, virtualización y automatización de datos denominado Autonomous Management Framework (AMF) Plus, el cual también se puede aplicar a la vertical de videovigilancia.

Henry Hernández, Director Regional de Allied Telesis para el Norte de Sudamérica, indicó a **Con Seguridad**, que la compañía se caracteriza porque acompaña a los integradores y a su canal de distribución a desarrollar productos y proyectos con el objetivo de hacerles más fácil el desarrollo, implementación, así como el mantenimiento preventivo y correctivo.

"Somos una compañía que está trabajando de la mano con sus integradores y distribuidores, estamos generando demanda en el usuario final, el mejor marketing que tenemos en estos momentos es el usuario final, y es lo que nos está haciendo crecer y cerrar cada vez más negocios", afirmó Henry Hernández.

Además, aseguró que cada año la firma presenta nuevos lanzamientos de productos y es propietaria de la tecnología, "no dependemos de terceros, ni en hardware ni en software, el 18% del revenue que tiene la empresa está dedicado al departamento de investigación y desarrollo", desglosó.

El sistema Autonomous Management Framework (AMF) Plus automatiza las tareas de administración de la red como respaldos, recuperación y aprovisionamiento. La empresa desarrolló este producto en 2017, ya está disponible en el mercado de América Latina y no es exclusivo para videovigilancia, ya que también se puede aplicar en voz y datos, y redes corporativas.

Henry Hernández señaló que el AMF está desarrollado para la gestión, monitoreo y visualización con otros productos de otras marcas, pero aclaró que sólo se va a poder automatizar o virtualizar con equipos de sus propias marcas.

El objetivo de Allied Telesis es diseñar cada vez más producto, pero más que a nivel de hardware, busca que sea todo lo intangible. Recientemente, la empresa lanzó la familia IGS950, una serie de switches de red con capacidad de Power over Ethernet (PoE+).

"Entregamos en las manos del usuario final una herramienta que le haga la vida más fácil en el mantenimiento preventivo y correctivo, que ahorre tiempo y dinero y que pueda dedicar más tiempo a otras labores de su empresa", concluyó Henry Hernández

Henry Hernández, Director Regional de Allied Telesis para el Norte de Sudamérica

Presenta LiDar RLS-50100 Pro™ y sistema DAS "EchoPoint™

- La empresa lanzó el sensor LiDar, un dispositivo láser sofisticado que cubre una zona de hasta 100 metros, y el sistema de fibra óptica EchoPoint, sensores acústicos distribuidos (DAS).

Bogotá, Colombia.- Optex —fabricante especialista en soluciones de detección de seguridad mediante tecnología de detección láser, pasiva e infrarroja activa— dio a conocer en la Feria de Seguridad ESS+ 2025, el sensor LiDar, uno de los más nuevos de su portafolio de productos para detección de intrusiones, y el sistema de fibra óptica EchoPoint.

En entrevista con Hans Klein, presidente en Latinoamérica de Optex, destacó que todos los productos presentados y son fabricados en Japón y EE.UU.

"Hasta hace pocos meses nuestro hub fue Estados Unidos, pero debido a las tarifas que este país impuso, ahora ofrecemos soluciones directo a cliente, quien puede importar directamente desde Japón, con lo cual se evita tarifas más altas del mercado estadounidense", explicó Hans Klein.

A parte de los sensores reconocidos con tecnología PIR, Dual y AIR, se lanzó recientemente el sensor LiDar RLS-50100V, es un dispositivo láser sofisticado que cubre una zona de hasta 100 metros, cuenta con una cámara Onvif integrada y posee la tecnología de detección más precisa y confiable del mercado.

Optex ofrece diferentes modelos de estos sensores LiDar, desde 20mts, 60mts y hasta 100, así como otros productos reconocidos, fotoeléctricos, infrarrojos pasivos y modelos inalámbricos o cableados.

Otras de las novedades que presentó en la exposición es el sistema de fibra óptica EchoPoint, sensor acústico distribuidos (DAS, distributed acoustic sensing), que tiene la capacidad de cubrir hasta 100 kilómetros desde un punto o un controlador de alarma. Este sistema se encuentra instalado y operando desde hace casi tres años para la protección perimetral en el Aeropuerto Internacional Felipe Ángeles (AIFA), ubicado en el Estado de México.

Sobre EchoPoint, Hans Klein indicó que lo más destacado de este sistema de fibra óptica es que mantiene una precisión de 6 metros para localizar la intrusión y puede instalarse en infraestructuras como oleoductos, para detectar tomas clandestinas o para la protección de perímetros largos.

Otro producto que exhibió Optex son los sistemas de detección de intrusos por fibra óptica de la serie Fiber Defender para la protección de perímetros de hasta aprox. 10km. Fiber Defender es la serie más exitosa de Fiber SenSys Inc. (Grupo Optex), de los cuales actualmente están instalados en más de 100 sitios petroleros solamente en Colombia.

Hans Klei, Presidente en Latinoamérica de Optex

CURSOS ALAS

¡Aún estás a tiempo!

Certifícate antes de fin de año y abre nuevas oportunidades

OCT	NOV	DIC
28 - 31	25 - 28	9 - 12
Gerencia de Proyectos	Video Vigilancia	Operadores de Cuartos de Control

Si eres **Socio ASIS,** obtendrás **puntos CPEs** en esta actividad

CRISTIAN MOLINA
Coordinador de Cursos
Whatsapp:
+57 321 6153367

ALAS ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

HID lanza HID Amico, lector de reconocimiento facial biométrico

- Esta terminal cuenta con cinco factores de autenticación, y se integra con la mayoría de las plataformas de control de acceso más reconocidas del mercado.

Bogotá, Colombia.- Durante la Feria Internacional de Seguridad (ESS+) 2025, el fabricante HID introdujo al mercado de América Latina el lector de reconocimiento facial biométrico HID Amico, una terminal que se caracteriza porque es compatible con su solución de credencialización virtual Origo.

Entrevistado por **Con Seguridad**, Jorge Bejarano, gerente Senior de Ventas para la Solución de Credencialización Virtual de HID, destacó que este producto es el primer biométrico dentro del portafolio de la marca y es un desarrollo completamente nuevo para el mercado de biometría facial.

Describió que HID Amico es una terminal capaz de arrancar con 10 mil usuarios, pero puede expandirse hasta 100 mil usuarios en memoria, y además se integra con la mayoría de las plataformas de control de acceso más reconocidas del mercado.

Este equipo cuenta con cinco factores de autenticación, el principal es el de biometría facial, cuyo algoritmo es de Paravisión, certificado por el NIST (Instituto Nacional de Estándares y Tecnología). También es compatible con su solución de credencialización virtual Origo y puede soportar cualquier tarjeta de proximidad en 125 kHz en 13.56 MHz de HID o de terceros, códigos de QR dinámicos o estáticos para aplicaciones de visitantes y una opción de PIN.

Jorge Bejarano afirmó que HID está presente en mercados de segmentos medios y altos, pero especificó que HID Amico se puede aplicar en cualquier vertical en donde hay ingresos masivos y no se puede carnetizar a los usuarios, se requiere un alto nivel de seguridad y se necesita mezclar diferentes tipos de autenticación. Funciona a través de tarjetas virtuales y físicas, así como con biometría facial con altos estándares de ciberseguridad y de privacidad.

"En el mercado existen algunos equipos en la línea alta con un costo más alto, pero uno que combine las cinco soluciones y que tenga la de credencialización virtual de HID no lo hay. Muchos usuarios que han trabajado con la plataforma de credencialización virtual estaban esperando soluciones de biometría facial, pero no se decidían porque tenían que comprar terminales de otros fabricantes que no eran compatibles con las soluciones de credenciales virtuales. Ya tenemos la solución in house, compatible con diversas tarjetas y formatos", aseguró Jorge Bejarano.

Jorge Bejarano, Gerente Senior de Ventas para la Solución de Credencialización Virtual de HID

Agregó que este producto es muy competitivo, enfocado para un segmento con una clasificación alta, pero con un precio que está por debajo de otras marcas y con integraciones con una plataforma grande de control de acceso, con toda la calidad y el respaldo de HID.

HID Amico fue presentado oficialmente al mercado global durante la feria ISC West 2025, celebrada del 31 de marzo al 4 de abril en Estados Unidos. Actualmente, la solución ya está disponible en varios países de Latinoamérica. En Brasil, Colombia, Costa Rica y México, se han iniciado procesos de adopción y adecuación conforme a las normativas locales, como parte de su despliegue regional.

AFÍLIATE

ASIS CAPÍTULO MÉXICO 217	ASIS INTERNACIONAL
$ 5, 650 MXN	$ 125 USD

> COMUNÍCATE A: SOCIOS@ASIS.ORG.MX
55 1321-1289

FORMA PARTE DE LOS PROFESIONALES DE LA SEGURIDAD

¿Cómo ser sponsor?

Escanea el código QR.

SUMA TU MARCA AL MEJOR CAPÍTULO

¡CONOCE MÁS!

ESCANEA NUESTRO LINKTREE

REUNIONES MENSUALES 2025

RM

LIVE STREAMING

ASIS CAPÍTULO MÉXICO 217

7 OCTUBRE

11 NOVIEMBRE

2 DICIEMBRE

Elevando la calidad del servicio y atención al cliente en el sector de la seguridad

Hanoys González
Ingeniero Mecánico. Magíster en Sistemas de la Calidad. Presidenta de Servicios VISEG AMC 2019, C.A. Miembro de la junta directiva de IFPO Comunidad Venezuela.
Articulista invitada

Caracas, Venezuela.- En un mundo tan globalizado, competitivo y en constante transformación, se hace imperioso que cada día las organizaciones cuenten con estrategias que garanticen la calidad de sus productos y servicios, tal es el caso del sector de la seguridad, donde se ha visto en la necesidad de brindar un servicio holístico no sólo para prevenir o mitigar riesgos, sino para construir relaciones duraderas con sus clientes, basadas en fidelización y satisfacción.

La seguridad es una necesidad para la población, sentirse protegido protegido genera más confianza y desarrollo para los países; es por ello que los proveedores de este servicio no se pueden limitar en solo desarrollar soluciones específicas que garanticen la protección y el resguardo de las personas, bienes tangibles e intangibles, sino que deben darse la tarea de comprender las necesidades y expectativas actuales y futuras de los clientes.

Una organización de seguridad que busque posicionarse en el mercado y sobre todo mantener un alto rendimiento durante extensos períodos de tiempo, debe buscar apoyo en los siete principios de la gestión de la calidad y no es casualidad que en estas premisas se inicie con el "*Enfoque al Cliente*", donde se devela que cada organización debe abocarse por la satisfacción de estos, a través del cumplimiento de los requisitos, además de tener la capacidad de esforzarse en exceder sus expectativas.

Las necesidades de los clientes no son estáticas, se debe ser consciente que el mundo se encuentra en un constante cambio y que las personas se han vuelto cada día más exigentes, por eso la atención al cliente ha sido una gran debilidad para este sector, donde se ha visto inmerso en diversos factores negativos, como la falta de liderazgo sólido y compromiso por parte de la Alta Dirección.

Hoy se tiene un gran reto y es el de generar más allá de la cultura de seguridad, se debe mejorar la experiencia para los clientes para así generar lealtad hacia nuestros servicios y operaciones. Hay que comprender que en todos los niveles organizativos estratégicos, tácticos y operativos, el cliente es la razón principal por la que existen las organizaciones y que sin ellos no habría camino hacia la sostenibilidad y el éxito. En virtud de la crisis de la calidad y atención, se han planteado algunas recomendaciones, con el objetivo de mitigar riesgos reputacionales, además de generar valor para los clientes:

1. **Comprensión de necesidades:** realizar estudios de mercado, conversar previamente con el cliente sobre sus expectativas, preocupaciones, situaciones y razones por las cuáles requiere el servicio, serán insumos importantes para la satisfacción de sus necesidades.
2. **Conocimiento del entorno:** es esencial ser consciente del contexto siempre cambiante en el que opera la organización. Incluye la comprensión de los factores políticos, económicos, sociales y tecnológicos que podrían afectar al negocio, ya que estos aspectos pueden influir en cómo se pueden atender los requerimientos exigidos por los clientes.
3. **Capacitación:** los líderes deben priorizar y sobre todo argumentar la importancia de entrenar al personal, no sólo considerando los aspectos técnicos, sino también la formación en habilidades blandas para el manejo de situaciones que pueden suscitarse.
4. **Role Playing:** es necesario emplear la empatía como herramienta de trabajo, proponiendo simulaciones que ayuden al personal a manejar diferentes situaciones con los clientes, desde las más simples hasta la generación de crisis.
5. **Aprendizaje:** para tener una ventaja competitiva, es necesario mantenerse informado con las últimas tendencias del sector y tomar las mejores prácticas de organizaciones reconocidas que puedan influir de manera positiva en el éxito del negocio.
6. **Encuestas de satisfacción:** permite que el cliente comente su experiencia y sugerencias con respecto al servicio, considerando aspectos desde la indumentaria de trabajo, profesionalismo y capacidad de resolución de conflictos.
7. **Establecer canales de comunicación:** se deben cerrar las brechas que impidan la constante comunicación con el cliente y proveedor del servicio. La Alta Dirección debe conocer a fondo cómo se siente el cliente con los servicios prestados.
8. **Calidad latente:** aplicar este tipo de calidad es el valor agregado que le brindamos a los clientes, algo que no solicitó, pero se le está otorgando para que su experiencia con el servicio sea formidable y excepcional. "Dales lo que quieren y un poco más".
9. **Apoyo entre profesionales:** la competencia debe ser leal, la unión entre profesionales, es una estrategia que permite fortalecer los lazos para compartir experiencias y estrategias exitosas, fomentando un diálogo constructivo para el impulso y avance del sector.

Santander Academy (2024), refiere lo siguiente: *"Teniendo en cuenta que el 70% de la experiencia de compra se basa en cómo los clientes se sienten tratados, disponer de un buen servicio de atención al cliente es realmente importante"*; en ese sentido, es ineludible cavilar sobre mantener un enfoque centrado en el cliente en todas las operaciones, donde verdaderamente ellos se sientan apoyados, seguros, escuchados y se les garantice una actuación con responsabilidad.

¿En qué momento se jodió la seguridad?

Milagros Céspedes
Consultora internacional en gestión de riesgos, liderazgo y seguridad corporativa. Fundadora de CES Latam, con más de dos décadas formando profesionales en Latinoamérica.
Articulista invitada

Lima, Perú.- En el país solemos preguntar *¿en qué momento se jodió el Perú?* Como una manera de reflexionar del cómo nos desviamos del rumbo como sociedad. No es que un día de pronto todo se fue "al garete", sino que ha sido un proceso silencioso de desgaste, de erosión. Hoy me atrevo a lanzar la misma pregunta, pero enfocada en nuestro rubro: *¿en qué momento perdimos el rumbo en seguridad?*

Esta reflexión me vino a la mente, luego de leer un artículo sobre securitización, donde el autor comentaba que se gritan amenazas por moda sin evaluar si realmente lo son y si tienen impacto. Ese artículo me removió porque coincide con lo que vengo observando y viviendo.

A lo largo de más de tres décadas que llevo en el mundo de la seguridad, he visto la evolución desde sus cimientos. Hubo una época en que algunos se creían dueños de los temas, los proyectaban y defendían su territorio con celo, eran, según ellos, los dueños de la verdad. Luego vino una etapa esperanzadora: la seguridad floreció, la gente se preocupó por aprender, investigar, estudiar, aplicar, certificar. Era un tiempo de crecimiento genuino, de construcción profesional y ética. Pero hoy… algo cambió.

Estamos viviendo una involución preocupante. Muchos buscan el camino corto, lo fácil, lo inmediato. Quieren resultados sin esfuerzo, respuestas sin reflexión, títulos sin mérito. Y eso, lentamente está vaciando de sentido a nuestra profesión.

En algún punto, dejamos de ver la seguridad como una vocación con propósito y la reducimos a un cargo, un sueldo o una rutina. La zona cómoda se volvió refugio: repetir fórmulas viejas, metodologías arcaicas, contentarse con protocolos mínimos, maquillar informes para complacer al jefe.

A eso se suma la ignorancia voluntaria: la información está disponible, los estándares existen, los referentes abundan, pero muchos prefieren justificarse con un "así se hace en mi empresa" o "estoy con sobrecarga de trabajo y no me da el tiempo" antes que asumir la disciplina de actualizarse, investigar y poner en práctica. Esa pereza intelectual normaliza la mediocridad.

Y, por supuesto, la viveza criolla —el famoso "Pepe el vivo"— que se entornilla en cargos sin mérito, busca atajos para mantener poder y confunde astucia con capacidad. Esa viveza es corrosiva: destruye la confianza y desalienta a quienes sí quieren hacer las cosas bien.

¿Ignorancia? ¿Viveza? ¿Conformismo? Probablemente una mezcla de todo. La ignorancia explica errores técnicos; la viveza, los errores intencionales, y el conformismo es quedarse en la zona cómoda. La primera se corrige con formación; la segunda requiere ética, liderazgo y consecuencias. La última es mejor quedarse en casa. Cuando ninguna se enfrenta, la seguridad se convierte en un cascarón vacío, más simbólico que efectivo.

Vivimos tiempos donde todo se "*securitiza*": se etiqueta cualquier tema como riesgo sin entenderlo, sin medir impacto real. Así, la seguridad se transforma en moda o discurso, no en gestión profesional.

La seguridad no se jodió por falta de tecnología ni de normas. Se jodió cuando olvidamos que esta profesión exige rigor, ética y liderazgo. Cuando dejamos de cuestionar, estudiar y actuar con convicción.

La pregunta que queda no es sólo *cuándo* nos perdimos, sino *cómo* vamos a recuperar el rumbo. Porque mientras la política y la salud se llenan de modas "securitizadas", nosotros no podemos caer en la trampa de la superficialidad. Nuestra tarea es devolverle profundidad, sentido estratégico y propósito humano a esta profesión.

Y aunque el panorama parezca desalentador, sí existe una comunidad de profesionales que siguen apostando por el aprendizaje, la ética y la excelencia. Son los que estudian, se certifican, comparten, cuestionan y lideran con ejemplo. Ese porcentaje —pequeño pero firme— debe ser el faro que inspire al resto. Porque es ahí, en ese compromiso silencioso y constante, donde la seguridad puede volver a encontrar su rumbo.

"La seguridad necesita líderes con propósito, no profesionales de ocasión".

Anticipar para proteger: Liderar la seguridad en un mundo posnormal

María Elena Pinto Mota
Certified Foresight Practitioner (TSFX, IFTF), APF Professional Member. Profesora Adjunta y Coordinadora del Acelerador de Pensamiento IESA.
Articulista invitada

Caracas, Venezuela.- Desde finales de los 80s, el mundo entró en una era de cambios sin precedentes. Inicialmente, se pensó que estas disrupciones eran excepcionales y transitorias. Sin embargo, el paso del tiempo evidenció que en realidad lo que estaba ocurriendo era un cambio en los rasgos de los sistemas.

Esto llevó al prospectivista Jamais Cascio a hablar del mundo FANI (BANI en inglés)[1]: frágil, por la vulnerabilidad y debilidad de los sistemas globales, ansioso, dada de la expectativa constante de que puedan ocurrir eventos disruptivos; no lineal, pues los eventos reverberan en formas inusitadas e imprevisibles; e incomprensible, por el caos volátil omnipresente[2]. El *Center for Posnormal Policy and Futures Studies* en Reino Unido, por su parte, habla de que estamos en una era *posnormal*, en la que la naturaleza misma de los cambios está transformándose, dando origen a un mundo complejo, caótico y contradictorio[3].

Es indudable que en un mundo posnormal, en el que las amenazas ya no son lineales ni previsibles, sino que se entrelazan en sistemas dinámicos donde lo físico, digital, social y ambiental confluyen, emergen riesgos que desafían los enfoques tradicionales de protección. Por tal motivo, los profesionales de la seguridad y gestión de riesgos requieren, necesariamente, contar con perspectivas analíticas adecuadas para la evaluación y comprensión de lo que ocurre. Una de esas perspectivas es, sin duda, la prospectiva estratégica.

La prospectiva estratégica brinda los marcos necesarios para dar sentido y significado a lo incierto, disruptivo y emergente. Consta de métodos y herramientas que permiten identificar qué es lo que está cambiando, concretamente cómo está cambiando y cuáles pueden ser las potenciales implicaciones de tales cambios. La red *United Nations Global Pulse*, la define como un "enfoque sistemático y estructurado para integrar la anticipación en los procesos y programas, de tal forma de informar las estrategias y políticas con la finalidad de moldear activamente el futuro"[4].

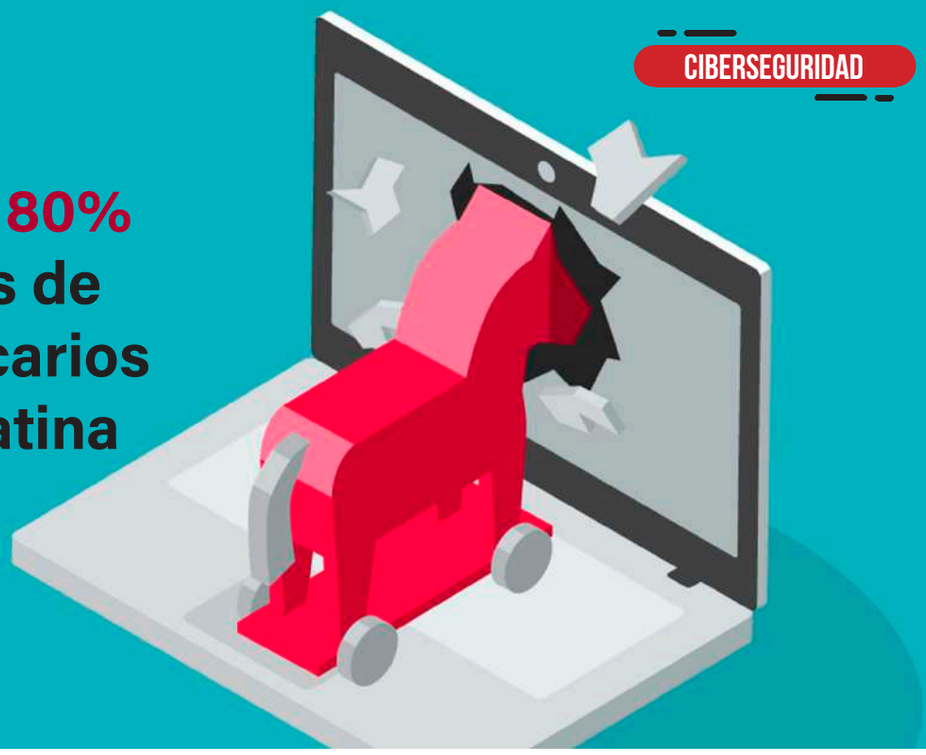
Esta definición integra aspectos que merecen ser comentados. En primer lugar, destaca el carácter sistemático y estructurado de la prospectiva estratégica, denotando así su rigurosidad; en segundo lugar, expresa que nos permite integrar la anticipación al funcionamiento de organizaciones, instituciones y programas con la intención de informar sus estrategias y políticas; finalmente, remarca su propósito último: moldear activamente el futuro. En otras palabras, la prospectiva estratégica apunta a que podamos ser agentes activos de la construcción de futuros, más que actores reactivos ante los cambios que ocurren.

A través de herramientas como la identificación de señales débiles y asuntos emergentes, la evaluación de tendencias en el marco de las grandes fuerzas de cambio presentes en el mundo, la identificación de patrones y la construcción de escenarios alternativos de futuros, el profesional de la seguridad desarrolla aptitudes esenciales para el mundo de hoy, como la sagacidad, innovación, flexibilidad mental, agilidad y proactividad. Al identificar tempranamente los cambios que ya están gestándose, puede anticipar sus potenciales rutas de evolución e implicaciones, lo que le permite diseñar estrategias robustas ante distintos futuros probables y posibles, así como construir una visión del futuro deseable con la conciencia clara de cómo navegar lo disruptivo, emergente y cambiante con la mirada puesta en el logro de esa visión.

El propósito esencial del profesional de seguridad es la salvaguarda de las personas, activos e información frente a las amenazas actuales y las emergentes. Para ello, debe cumplir un conjunto de tareas operativas, como la detección, prevención y respuesta oportuna. Más aún, debe desarrollar *habilidades estratégicas* que le permitan gestionar los riesgos, garantizar la continuidad operativa de sistemas y organizaciones, y asesorar ante decisiones críticas.

Las capacidades anticipatorias y la incorporación del pensamiento prospectivo fortalecen al profesional de seguridad en el logro de su misión, al permitirle pasar de una lógica reactiva a una preventiva y orientada a la resiliencia. La gran promesa de la prospectiva estratégica radica en esto último, pues brinda al especialista en estos temas la posibilidad de ir más allá del rol de operador, para convertirse en un líder y estratega de seguridad.

Brasil tiene el 80% de los ataques de troyanos bancarios de América Latina



Antonio Celso Ribeiro Brasiliano
PhD, Doctor en Filosofía en Ciencias de la Seguridad Internacional, Cambridge International University, Inglaterra. Presidente de Brasiliano INTERISK.
Articulista invitado

São Paulo, Brasil.- El país sigue siendo el principal objetivo y desarrollador de troyanos bancarios en América Latina, una amenaza que roba los datos financieros de los usuarios para acceder a cuentas y realizar transacciones fraudulentas, según *el nuevo Panorama de Amenazas de Kaspersky*.

El estudio informa que el país concentró más del 80% de las detecciones de troyanos bancarios en la región, con 1,5 millones de ataques bloqueados entre agosto de 2024 y junio de 2025, un alarmante promedio de 4.109 intentos por día. Además de ser el epicentro de los ataques, Brasil también destaca en la creación de estas amenazas, originando casi la mitad de las familias más comunes de troyanos bancarios. Los expertos señalan que los grandes objetivos ahora son los dispositivos móviles.

Los números muestran que la dinámica de los ataques de troyanos bancarios se ha transformado. Si antes el enfoque principal eran las computadoras, Kaspersky ahora está observando una migración significativa a dispositivos móviles. El año pasado, por ejemplo, solo había una familia de troyanos bancarios centrados en Android en el ranking de amenazas móviles. Para 2025, ya hay tres familias distintas activas: Trojan-Banker.AndroidOS.Agent, Trojan-Banker.AndroidOS.Mamont y Trojan-Banker.AndroidOS.Creduz.

Esta rápida adaptación demuestra que los ciberdelincuentes están cada vez más enfocados en los teléfonos celulares, dispositivos donde los usuarios realizan gran parte de sus transacciones financieras.

Brasil no solo destaca en el volumen de ataques de troyanos bancarios, sino también en la creación de estas amenazas. La experiencia brasileña en ciberdelincuencia financiera es evidente al observar que de las 22 familias de troyanos bancarios identificadas por Kaspersky en la región, 10 son de origen brasileño. Entre las amenazas de Windows que aún se destacan se encuentran Trojan-Banker.Win32.ChePro, Trojan-Banker.Win32.BestaFera y Trojan-Banker.Win32.Banbra.

La dinámica del cibercrimen está bien ilustrada por el caso del troyano Grandoreiro (Trojan-Banker.Win32.Grandoreiro). En 2023, la intensa actividad de este troyano bancario provocó un aumento significativo de los ataques. Sin embargo, tras la

detención de parte del grupo responsable en una operación internacional coordinada entre INTERPOL, la Policía Federal brasileña y la Policía Nacional española, el número de ataques en Grandoreiro volvió a niveles más bajos.

A pesar de esta "normalización", la amenaza persiste: la resiliencia de los delincuentes es notable, con nuevas variantes emergentes y una alta capacidad de adaptación, lo que demuestra que la lucha contra el cibercrimen es continua. Esta continua adaptación de los delincuentes explica el escenario general en la región: aunque el número total de ataques de troyanos bancarios en América Latina ha disminuido en un 45,5% en el último año (totalizando 1,8 millones de detecciones), el peligro no ha disminuido, solo se ha transformado. La caída refleja la disminución en el uso del acceso a la banca por internet por parte del escritorio, mientras que la amenaza real ahora crece y se vuelve más sofisticada en el entorno móvil.

Para evitar ataques de troyanos bancarios, Kaspersky recomienda:

- Tenga cuidado con los enlaces, documentos adjuntos a correos electrónicos y mensajes: antes de hacer clic en cualquier enlace o abrir archivos adjuntos, verifique si el mensaje proviene de un remitente confiable. Tenga cuidado con direcciones desconocidas, solicitudes urgentes u ofertas sospechosas. En caso de duda, confirme con la empresa a través del canal oficial o persona por otro medio.

- Mantenga todos los programas actualizados, en computadoras y teléfonos celulares. Esto evita que los troyanos bancarios exploten las fallas del sistema para invadir los dispositivos, ya que las actualizaciones corrigen estas vulnerabilidades.

- Use contraseñas seguras y únicas: evite repetir contraseñas en diferentes cuentas y no use combinaciones obvias, como secuencias numéricas ("123456") o nombres de mascotas. Prefiera combinaciones de letras mayúsculas y minúsculas, números y símbolos. Las contraseñas seguras dificultan que los piratas informáticos accedan a sus cuentas, incluso si obtienen información sobre usted.

- Habilite la autenticación de dos factores (2FA) como una capa adicional de seguridad: 2FA agrega una segunda barrera de protección además de la contraseña. Incluso si un troyano o ciberdelincuente se apodera de su contraseña, aún necesitará un código generado o enviado a otro dispositivo confiable para acceder a la cuenta.

Siempre que sea posible, prefiera métodos más seguros, como aplicaciones de autenticación o tokens físicos, en lugar de SMS. Además, considere registrar el dispositivo de una persona de confianza, como un miembro de la familia, como una de las opciones para recibir el código de recuperación.

- Instale una solución de seguridad confiable: Un antivirus eficaz identifica y bloquea amenazas, como troyanos bancarios, antes de que causen daños. Mantener la protección activa en los dispositivos garantiza una capa adicional de seguridad para los datos personales y corporativos.

- Invierte en educación digital continua: las estafas y el malware siempre están evolucionando. Aprender sobre nuevas amenazas, reconocer signos de fraude y adoptar buenas prácticas de seguridad ayuda a reducir el riesgo y proteger su presencia digital.

Tenemos que entender que los ciberdelincuentes siempre están estudiando nuevas formas de actuar, por esta razón la estrategia crucial es siempre identificar el Estado Final Deseado del delincuente. El EFD estudiado identifica el modus operandi, su motivación y capacidad técnica, lo que permite a los gestores realizar escenarios y simulaciones. Con esta estrategia, reduciremos la efectividad de los hackers.

Hacia una seguridad ética en la era de la IA: retos y estrategias para América Latina

Gerardo Gutiérrez Lanz
PhD en Ciencias de la Educación. Abogado.
Presidente de IFPO Comunidad Venezuela.
Certificado CPO por IFPO. Vicepresidente de Seguridad del Banco Venezolano de Crédito.
Articulista invitado

Caracas, Venezuela.- El mundo corporativo cada vez más competitivo y exigente hace que los ejecutivos y/o directivos de manera inadvertida e inconsciente y en ocasiones consciente, pero sin medir las consecuencias en el negocio, divulgan información sensible de las empresas, facilitado por el inmediato acceso a medios de comunicación masivo como las redes sociales o los canales de difusión internos de cada empresa.

Los atacantes también cada vez más sofisticados acuden entre otros a los anuncios de viajes de negocio, visitas a grandes clientes o competidores, fotos, bocetos y videos de nuevos productos o servicios, propuestas de nuevos organigramas con sus responsables, acceso a áreas restringidas, contraseñas visibles en tableros, entre muchas otras formas que inadvertidamente se convierten en vulnerabilidades.

Entre las modalidades más utilizadas por los atacantes están la suplantación de identidad física o digital, la ingeniería social, las contraseñas fáciles de descubrir o inferir, los seguimientos al entorno digital de cada persona objetivo y de la misma empresa, los malware en los sistemas informáticos de equipos de cómputo y móviles, el fácil acceso a las basuras de las áreas sensibles e incontables maneras de lograr los objetivos de los atacantes.

Dado lo anterior, es relevante concientizar periódicamente a todos los empleados, contratistas y en especial a los directivos de la organización en las diferentes formas en que puede divulgarse inadvertidamente la información sensible y, de la misma manera como tomar medidas preventivas y correctivas de manera decidida y consciente.

Considerando lo previamente mencionado, es imperioso realizar un diagnóstico de seguridad que permita identificar las debilidades y exposiciones que pueden presentar la empresa, los directivos y empleados con cargos sensibles y de alta visibilidad en la organización; para ello se hace necesario analizar y evaluar entre otros aspectos los siguiente:

Análisis del contexto externo

- Mapeo de la huella digital, donde se revisa y analiza la información pública con el objeto de identificar información sensible expuesta y vulnerable.

- Las políticas corporativas para el acceso y uso de las redes sociales, buscando identificar claridad, pertinencia legal, cubrimiento, niveles de difusión, acceso y, por ende, restricciones o prohibiciones en el manejo de la información.

- Capacitar a todos los directivos y empleados con cargos sensibles y de alta visibilidad en la organización, ofreciendo formación regular, especializada y actualizada sobre los riesgos y las diferentes modalidades de ataque, y a su vez, dar a conocer e implementar las mejores prácticas para el uso responsable de las redes sociales.

- Monitoreo permanente de las redes sociales a través de herramientas especializadas que identifiquen y alerten sobre actividades que puedan representar una amenaza para la seguridad y la reputación de la organización.

Análisis del contexto interno

- Identificación y clasificación de datos sensibles, a través de un inventario de la información confidencial para la organización, donde se detalle entre otros, la relación de los clientes, propiedad intelectual, nuevos productos, secretos comerciales, organigrama, nómina, procesos internos con información sensible. A su vez la clasificación de la información, donde se detalle entre otros aspectos si la información es pública, interna, privada, restringida, confidencial o muy alta confidencialidad.

- La accesibilidad a la información donde se detalla quién o quiénes tienen acceso a la información sensible, las herramientas y privilegios de acceso a la información para los empleados, sistemas de autenticación robustos como la autenticación de dos factores, restricción de dispositivos de almacenamiento de información o de conexión.

- Auditorías periódicas para identificar y hacer seguimiento al tráfico de la red informática, a patrones sospechosos como los accesos en horario no laboral, a información no autorizada, cambios inusuales en los puertos de conexión, transferencia de datos inusuales o no permitidas, entre otros.

- Alertas y notificaciones con el objeto de detectar en tiempo real actividades sospechosas relacionadas con la información clasificada como sensible, quienes reciben y tramitan las alertas.

- Planes de respuesta a incidentes y recuperación de la información con el apoyo forense para los casos que lo ameriten.

Implementar un programa de lecciones aprendidas, con el objeto conocer de las vulnerabilidades aprovechadas por los atacantes o por los descuidos al interior de la organización.

Tecnología y seguridad convergen en los C4 y C5 de América

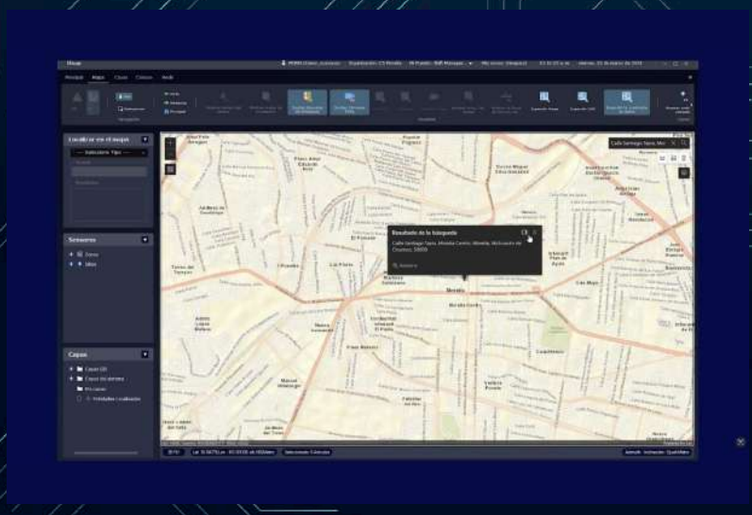
- Integración de sistemas, inteligencia artificial y costos eficientes, la apuesta de Kabat One, Genetec, Hikvision y Uniview.
- Desde México hasta América Latina, los proyectos de videovigilancia y control, buscan salvar vidas y anticipar riesgos.

Beatriz Canales Hernández

La seguridad pública se encuentra en un punto de inflexión en el que los Centros de Comando, Control, Comunicaciones, Cómputo y Contacto Ciudadano (C5), junto a los Centros de Comando y Control (C4), son ya infraestructuras críticas para responder a emergencias, coordinar a fuerzas policiales, y prevenir delitos. Y es en este terreno en el que la tecnología dejó de ser un apoyo accesorio: hoy es el centro de la operación.

Empresas como Kabat One, Genetec, Hikvision y Uniview han construido un portafolio de soluciones que incluyen la integración total de subsistemas, el uso de analíticas avanzadas e Inteligencia Artificial. Cada una con su propio sello, pero con un objetivo convergente: salvar vidas y generar ciudades más seguras.

Kabat One, el "sistema de los subsistemas". Niv Yarimi, fundador y presidente de Grupo Kabat y Kabat One, describe la esencia de su solución estrella con una frase: "Nuestro objetivo es integrar lo que ya existe. No se trata de tener más cámaras, sino de hacer que hablen entre sí".



La plataforma Kabat One se presenta como un ecosistema capaz de integrar telefonía, videovigilancia, bases de datos, GPS, radio, sistemas CAD y video analítico en un solo núcleo.

"El problema que encontramos en los C4 y C5 es que cada sistema funciona aislado. Nosotros los conectamos para que, en segundos, un operador pueda despachar la patrulla más cercana, la ambulancia y hasta los bomberos en caso de un accidente", explicó Yarimi.

Los resultados hablan: En la ciudad de Morelia, Michoacán, México, tras la implementación del sistema, los homicidios pasaron de 2,761 en 2022, a menos de mil en 2024, y "solo se logra con tecnología que analiza la data en tiempo real y que automatiza decisiones", subraya el directivo.

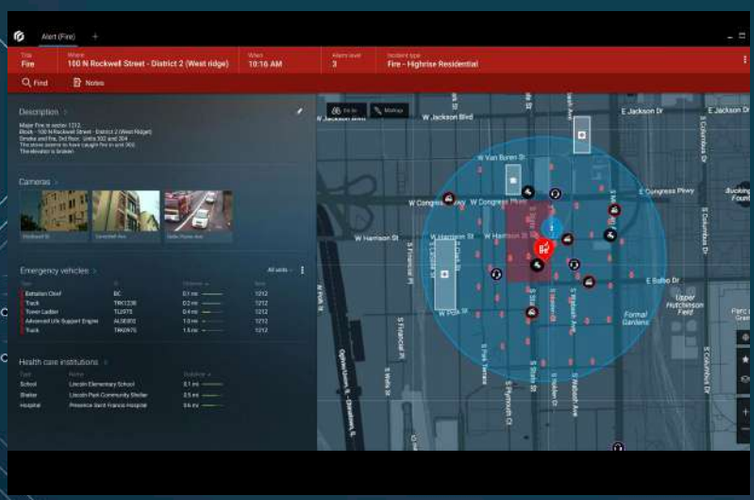
NIV YARIMI, fundador y presidente de Grupo Kabat y Kabat One.

Actualmente, Kabat One opera en Ciudad de México, Michoacán, Tamaulipas, Nayarit, Oaxaca y Chiapas, y comienza a expandirse hacia Perú, Ecuador y Brasil.

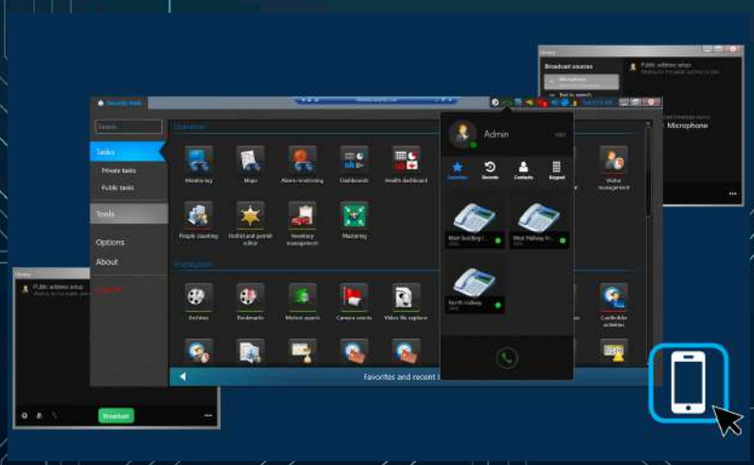
Genetec y la visión unificada. Con más de 25 años de experiencia, la empresa aporta la flexibilidad de integrar múltiples dispositivos en una sola plataforma. Michelle Nieto, Vertical Sales Manager para el sector público e infraestructura crítica en Genetec,

lo explica: “Nuestro enfoque es dar una visión unificada al operador. Por ejemplo, Security Center concentra videovigilancia, control de accesos, comunicaciones, analíticos y hasta sensores IoT en un solo tablero”.

La plataforma Security Center incluye el módulo Citigraph, utilizado por la policía de Chicago, que permite integrar información de patrullas, drones y cámaras corporales en tiempo real.



“La Inteligencia Artificial es fundamental porque las cámaras crecen cada año, pero no así la cantidad de monitoristas. Con IA balanceamos esa ecuación y logramos identificar patrones delictivos, incidentes viales o actividades potencialmente violentas”, explica Nieto.



En México, Genetec está presente en C4 y C5 de 11 estados, especialmente en el centro y norte del país, y mantiene proyectos activos en más de 150 países. Sus soluciones no solo atienden a gobiernos: también se aplican en aeropuertos, puertos, prisiones e incluso centrales nucleares, donde la seguridad no admite margen de error.

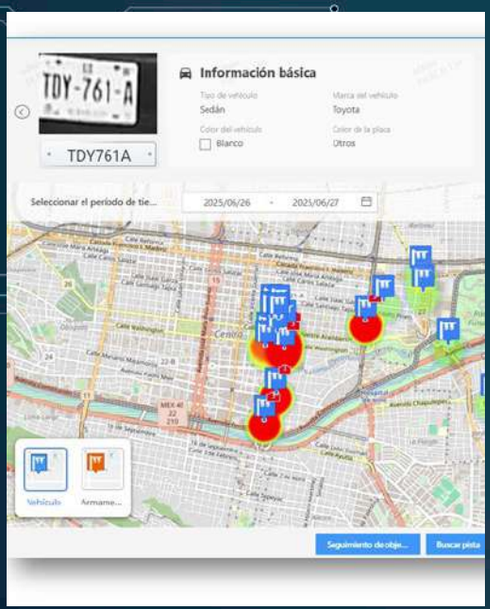
Michelle Nieto, Vertical Sales Manager para el sector público e infraestructura crítica en Genetec Latinoamérica.

Hikvision, inteligencia en tres capas. Para esta empresa, la clave es dotar de inteligencia a cada nivel del ecosistema de seguridad.

Al respecto, Rubén García Soriano, gerente de soluciones de gobierno del Centro de Investigación y Desarrollo de Hikvision, detalla: “Hablamos de inteligencia en el borde, en los servidores y en el software. Cada capa aporta eficiencia y reduce tiempos de respuesta”.

En el borde, las cámaras integran analíticas capaces de detectar peleas, aglomeraciones o vehículos en sentido contrario. En los centros de datos, el sistema Acuseek procesa video plano de cualquier marca y lo convierte en información accionable.

Y en el software, la plataforma Hikcentral Master administra millones de imágenes para generar mapas de calor, listas negras de vehículos o gemelos digitales de las ciudades.



Actualmente, Hikvision opera en Puebla, Durango, Sinaloa, Baja California Sur, Querétaro y la Ciudad de México, además de proyectos internacionales en Brasil, Colombia y Chile.

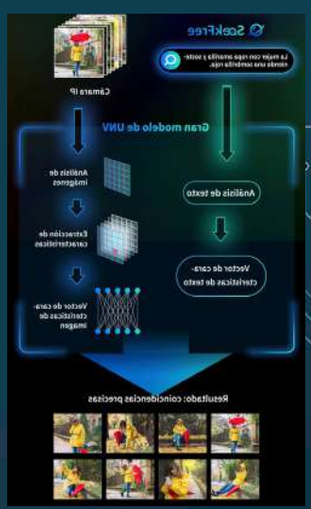
"No se trata solo de prevenir delitos, también de gestionar emergencias como inundaciones o incendios con información en tiempo real", afirma Rubén García.

Rubén García Soriano, gerente de soluciones de gobierno del Centro de Investigación y Desarrollo de Hikvision.

Uniview, costo-beneficio y visión nocturna a color. Con apenas una década en el mercado, esta compañía se ha posicionado como uno de los cuatro líderes globales en videovigilancia.

En México, su presencia se expande gracias a la combinación de innovación y precios competitivos. Roberto Ávila, gerente de ventas y proyectos de ciudades seguras en Uniview México, destaca la tecnología Owlview, que permite ver a color en condiciones de muy baja iluminación.

"Antes, revisar horas de video era un trabajo difícil. Hoy, con nuestras analíticas de IA en los NVRs, se pueden buscar patrones por palabras: persona con camisa negra, audífonos o paraguas rojo, y el sistema localiza las imágenes en segundos", explica.



La marca ha instalado más de 10 mil cámaras en alcaldías de la Ciudad de México y equipos en Guanajuato, Mérida y Baja California. Además, su certificación NDAA le abre puertas en Estados Unidos y Canadá, donde otras marcas chinas no pueden participar.

"Nuestro reto es competir de tú a tú con marcas internacionales, y lo hacemos con innovación constante y mejor precio", asegura Ávila.

Roberto Ávila, gerente de ventas y proyectos de ciudades seguras en Uniview México.

Convergencia hacia ciudades inteligentes

Aunque cada compañía tiene un enfoque particular, todas coinciden en que la seguridad pública no puede limitarse a reaccionar. La tendencia va hacia ciudades inteligentes capaces de anticipar riesgos, integrar sistemas de movilidad, medio ambiente y transporte, así como gestionar información en tiempo real.

Los proyectos de C4 y C5 en México y Latinoamérica muestran que la innovación tecnológica puede reducir homicidios, robos y delitos de alto impacto, siempre y cuando vaya acompañada de una correcta coordinación policial y una visión de largo plazo.

La interoperabilidad dejó de ser aspiración técnica para convertirse en requisito operativo. La "visión unificada" de Genetec, el "sistema de los subsistemas" de Kabat One, las tres capas de IA de Hikvision y la combinación costo-beneficio + analítica embebida de Uniview, convergen en un mismo punto: disminuir segundos críticos entre el evento y la respuesta. Con reglas claras de datos, flujos guiados y tableros que resuelven — no solo muestran—, el C2, C4 o C5 funciona como un cerebro en tiempo real.

Para **Kabat One**, el reto inmediato es profundizar la automatización de eventos entre agencias y escalar su módulo ciudadano Connect sin sacrificar privacidad. Niv Yarimi lo resume con una meta medible: "Queremos que cada despacho tarde menos, que cada investigación sea más sólida y que cualquier cámara útil se sume de forma segura. Si la tecnología no salva vidas, no cumple su propósito".

En **Genetec**, la apuesta pasa por mantener estándares abiertos, gobernanza de datos y ciberseguridad certificada para escalar desde municipios hasta estados completos, sin cambiar de plataforma. Michelle Nieto lo plantea

así: "Seguiremos unificando sensores, video, accesos y comunicaciones bajo marcos de privacidad. Que el operador decida mejor y más rápido es la verdadera innovación".

En **Uniview**, el camino seguirá anclado en el costo-efectivo con IA utilitaria dentro de NVRs, visión nocturna a color (Owlview) y certificaciones como NDAA para abrir mercado en entornos críticos.

Para Roberto Ávila, "buscamos tecnología que cualquiera pueda operar y que rinda en campo. Si la búsqueda por palabras resuelve en segundos lo que antes tomaba horas, estamos haciendo lo correcto".

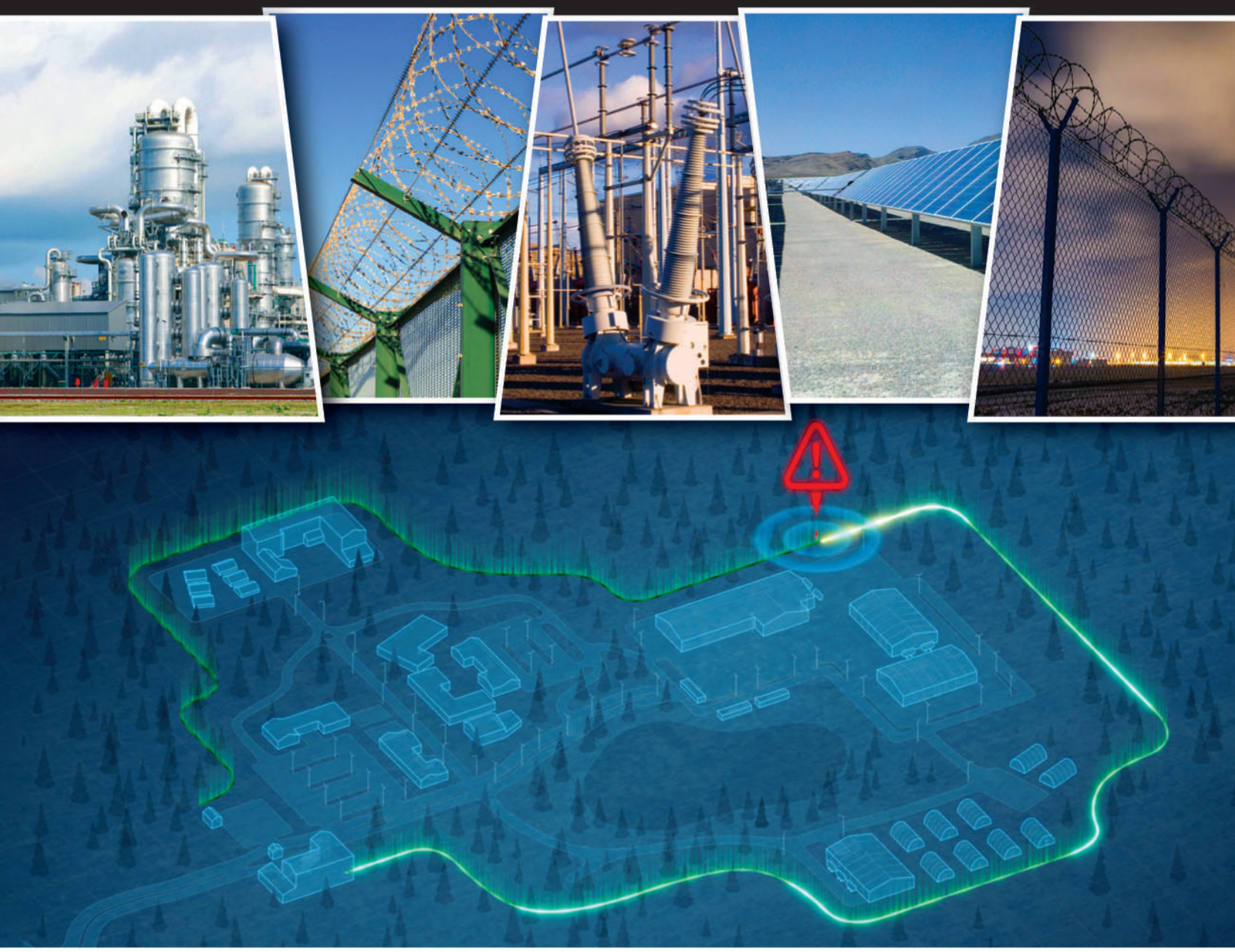
Hikvision llevará su estrategia de inteligencia en el borde, en el centro y en el software hacia tableros ejecutivos con gemelos digitales y mantenimiento predictivo de infraestructura. Rubén García Soriano, cierra con una línea: "Alta disponibilidad 24/7, menos falsas alarmas y análisis a gran escala. La ciudad necesita saber qué pasa ahora y prever qué puede pasar después".

Los cuatro actores coinciden en que 2025–2026 será decisivo por la presión de grandes aforos, movilidad, turismo y eventos deportivos. Más que sumar miles de cámaras, la clave será orquestarlas: analíticas coherentes, flujos de despacho auditables, videowalls que prioricen incidentes y módulos móviles — bodycams, torretas inteligentes, motos lectoras— sincronizados con la red de postes y con los CAD/911.

Como sintetiza Niv Yarimi al hablar del cambio cultural que ya se ve en diversos estados: "De edificios monumentales pasamos a decisiones basadas en datos"; Michelle Nieto cierra: "la seguridad no solo reacciona, también anticipa"; Rubén García de su lado, subraya "información accionable en segundos"; y Roberto Ávila concluye "innovación útil, accesible y lista para operar".

Con esta ecuación, el C4/C5 para de ser sala de pantallas para convertirse en palanca real de seguridad y desarrollo tecnológico en seguridad de alto desempeño.

Sensor Acústico Distribuido por Fibra Óptica de Largo Alcance



Los sensores acústicos distribuidos (DAS) **EchoPoint™** utilizan la última tecnología en algoritmos de detección y clasificación por fibra óptica para proporcionar la solución más avanzada para aplicaciones que requieren sensores de detección de intrusiones confiables y de localización puntual. Estos avances hacen que los sensores **EchoPoint™** sean una parte clave de la solución en sitios grandes donde se necesita la ubicación precisa de una intrusión.

Serie EP9000

- Robusta solución para Cercos, Muros, soterrado, ductos, infraestructura de redes de datos
- Opciones de cobertura desde 5km hasta 100km con +/- 2 – 6m de precisión
- Total inmunidad a tormentas eléctricas, campos EMI y RFI
- Con Interfaz Gráfico de Usuario, requiere de 2U de Rack
- Tolerancia al corte y redundancia de sistema
- Instalaciones Híbridas (sobre Cercos y soterrado)

www.optex.net

Gestión de calidad y sostenibilidad: Herramientas estratégicas para líderes de seguridad corporativa

Carmen Rincón Arrieta
Maestrante en Gerencia Empresarial.
Abogado. Vicepresidente de la Comunidad IFPO Venezuela.
Articulista invitada

Caracas, Venezuela.- En el dinámico entorno de la seguridad corporativa, los ejecutivos enfrentan una creciente presión para integrar calidad de servicio, sostenibilidad y cumplimiento normativo en sus estrategias operativas. La experiencia reciente de empresas como Securitas Argentina —involucrada en un caso de corrupción autodenunciado— evidencia que la falta de gobernanza y transparencia puede derivar en sanciones severas y daño reputacional irreversible. Este tipo de incidentes subraya la necesidad de adoptar marcos técnicos robustos que alineen la seguridad con los principios ESG (ambientales, sociales y de gobernanza).

La calidad de servicio en seguridad no es un concepto abstracto. Es una herramienta de gestión de riesgos que permite anticipar incidentes, fortalecer la confianza del cliente y garantizar la continuidad operativa. Modelos como SERVQUAL, que evalúan dimensiones como tangibilidad, fiabilidad, capacidad de respuesta, seguridad y empatía, ofrecen indicadores clave para tableros de control y auditorías internas. Asimismo, métricas como NPS, CSAT, CES y TTR permiten mejorar la retención de clientes y sostenibilidad financiera, medir la percepción del cliente, identificar fricciones operativas y evaluar la capacidad de respuesta del equipo.

Desde una perspectiva técnica, la norma ISO 18788:2015 establece un marco de gestión empresarial para operaciones de seguridad, promoviendo la rendición de cuentas, el respeto a los derechos humanos y la mejora continua. Su integración con otras normas ISO —como ISO 9001, ISO 31000, ISO 10002 e ISO 10010— permiten fortalecer la cultura organizacional, estructurar la calidad en niveles operativo, táctico y estratégico. Esta sinergia facilita la planificación, la toma de decisiones informadas y la transformación cultural hacia una organización centrada en el cliente.

En paralelo, la sostenibilidad se ha convertido en un requisito operativo. Los informes ESG, aunque aún diversos en formato y alcance, son cada vez más exigidos por reguladores, inversores y clientes. La futura norma ISO/UNDP 53001 busca estandarizar estos criterios, alineándolos con los Objetivos de Desarrollo Sostenible (ODS). Para los líderes de seguridad, esto implica medir el impacto ambiental de sus operaciones, promover la inclusión y garantizar condiciones laborales dignas.

El impulso a la innovación y a la mejora continua debe ser nuestro *leiv motiv* a través de muchas herramientas existentes como por ejemplo Lean Management y TQM que ayudan a optimizar procesos, reducir desperdicios y mejorar la experiencia del cliente. Igualmente la adopción tecnológica —IA, Big Data, IoT— transforma la oferta de servicios, personaliza la atención y mejora la eficiencia. Bajo estas premisas, el diseño centrado en el cliente y la escucha activa se convierten en pilares para generar valor sostenible.

En conclusión, los beneficios para los equipos de seguridad son concretos:

- Menos incidentes críticos: Protocolos claros y personal capacitado reducen fallos operativos.
- Mayor fidelización: Clientes satisfechos renuevan contratos y recomiendan el servicio.
- Compromiso del personal: La calidad genera sentido de propósito y reduce la rotación.
- Cumplimiento normativo: La trazabilidad y orden facilitan auditorías y evitan sanciones.
- Innovación operativa: Escuchar al cliente impulsa mejoras y adaptación tecnológica.

Troya: Cuando la confianza venció a la vigilancia

Pedro Oré
MBA - CPO© - CIO©
Miembro por Perú del Consejo Consultivo Latino de IFPO.
Articulista invitado

Lima, Perú.- Troya no cayó bajo el filo de las espadas ni bajo el fuego de los arietes, cayó en silencio, porque quienes se juraban invencibles confundieron murallas con certezas. No fue vulnerada, inicialmente, en el campo de batalla, los griegos habían chocado contra sus murallas una y otra vez, ninguna catapulta, ningún ejército, ningún héroe había logrado abrir una brecha en la ciudad orgullosa. Troya resistía porque sus muros eran altos, sus puertas fuertes y sus guerreros valientes.

El caballo de madera no era un obsequio, era la prueba de que el enemigo no necesitaba vencer por fuera si podía entrar disfrazado, así la ciudad más vigilada del mundo ardió porque la confianza superó a la sospecha, porque la emoción venció al análisis, porque las decisiones se tomaron mirando la grandeza de las murallas y no la fragilidad del juicio humano.

Los griegos entendieron que no necesitaban derribar los muros si podían derribar la percepción de riesgo, un obsequio, un símbolo de retirada, un objeto que despertaba curiosidad y hasta devoción. Lo que los troyanos vieron como trofeo, era en realidad un agujero en su sistema de seguridad. Claramente, una decisión estratégica equivocada.

Hoy no construimos murallas de piedra, sino sistemas y protocolos, en muchos casos con grandes inversiones, pero la historia se repite, el enemigo rara vez golpea la puerta principal, se disfraza de proveedor confiable, de correo inocente, de colaborador intachable, de "siempre lo hicimos así". Ningún hacker necesita un ariete si un empleado abre un correo sin verificarlo, ningún estafador necesita saltar muros si alguien, confiado, firma sin leer, ningún infiltrado requiere violencia si se le entrega una credencial sin las verificaciones correspondientes.

Troya no cayó por falta de soldados, cayó porque sus líderes dejaron de escuchar la voz de la prudencia, y esa es la lección que atraviesa siglos. En seguridad, lo que te derrota no es solo lo que viene de afuera, sino lo que decides ignorar desde adentro. Cada organización tiene hoy su propio caballo de madera esperando en la puerta, la diferencia estará en si tenemos el coraje de desconfiar de lo fácil, de lo obvio, de lo regalado, o si preferimos abrir las puertas y celebrarlo como un triunfo.

La Inteligencia de Fuentes Abiertas (OSINT) como pilar de la peguridad física y la auditoría corporativa

Diofanor Rodríguez
CPP, PCI, PSP. Máster en ciberseguridad y apasionado por la seguridad corporativa.
Articulista invitado

Bogotá, Colombia.- En un mundo hiperconectado, donde cada interacción digital deja una huella, la Inteligencia de Fuentes Abiertas (OSINT, por sus siglas en inglés) ha emergido como una herramienta estratégica para la seguridad física y la auditoría corporativa. Lejos de ser una técnica reservada para expertos en ciberseguridad, OSINT representa una metodología accesible, rigurosa y profundamente útil para quienes gestionan riesgos en entornos operativos complejos. Su valor radica en la capacidad de transformar información pública en conocimiento accionable, permitiendo anticipar amenazas, validar hechos y fortalecer la toma de decisiones en escenarios críticos.

Definición y alcance de OSINT

OSINT se define como el proceso de recopilación, análisis y explotación de información disponible públicamente, con el objetivo de generar inteligencia útil para diversos fines (Ortega Candel, 2018). Esta información puede provenir de redes sociales, medios de comunicación, registros públicos, foros, blogs, bases de datos académicas, entre otros. Lo esencial no es la fuente en sí, sino la capacidad de extraer valor de ella mediante un enfoque sistemático.

En el ámbito corporativo, OSINT permite validar la veracidad de datos obtenidos por otros medios, detectar inconsistencias en procesos internos, y complementar investigaciones de seguridad física con evidencia contextual. Su aplicación no se limita al entorno digital: también fortalece la trazabilidad en auditorías, la verificación de antecedentes, y la detección de vulnerabilidades en infraestructura crítica.

El ciclo de vida de OSINT: metodología y rigor

La inteligencia OSINT no se genera por accidente. Requiere un proceso metódico conocido como el ciclo de vida de OSINT, compuesto por seis fases esenciales: (1) identificación del objetivo, (2) selección de fuentes abiertas, (3) adquisición de información, (4) análisis y normalización, (5) visualización de dependencias, y (6) calificación de resultados. Cada fase demanda habilidades técnicas, pensamiento crítico y conocimiento del contexto operativo.

Además, existen fases funcionales que complementan este ciclo: requisitos, identificación de fuentes, adquisición, procesamiento, análisis y presentación. Estas etapas permiten estructurar la búsqueda de información de forma coherente, garantizando que los hallazgos sean relevantes, verificables y útiles para la toma de decisiones (Ortega Candel, 2018).

Aplicaciones prácticas en seguridad física

La utilidad de OSINT en seguridad física es amplia y concreta. Permite anticipar riesgos, detectar fugas de información, investigar incidentes, y validar la autenticidad de eventos reportados. Por ejemplo, en proyectos energéticos ubicados en zonas de alto riesgo, OSINT puede identificar patrones de hurto, movimientos sospechosos en redes sociales, o publicaciones que revelen información sensible sobre la operación.

Entre las herramientas más utilizadas se encuentran:

- **Google Dorks:** Búsquedas avanzadas que permiten detectar documentos expuestos públicamente, como planos de instalaciones o manuales operativos.
- **Maltego y SpiderFoot:** Plataformas de visualización que trazan relaciones entre personas, correos, dominios y activos digitales.
- **Shodan:** Motor de búsqueda especializado en dispositivos conectados a internet, útil para identificar cámaras IP o sistemas SCADA expuestos.
- **Búsqueda inversa de imágenes:** Herramientas como TinEye o Google Lens permiten verificar si una imagen es auténtica, reciente o manipulada, apoyando investigaciones de incidentes.

Estas herramientas no solo fortalecen la seguridad física, sino que también aportan evidencia técnica para auditorías internas, investigaciones disciplinarias y procesos judiciales.

OSINT como apoyo a la auditoría corporativa

En el contexto de la auditoría, permite validar la trazabilidad de procesos, identificar inconsistencias en la documentación, y detectar riesgos reputacionales. Por ejemplo, al analizar publicaciones en redes sociales de empleados, se pueden identificar posibles filtraciones de información o comportamientos que comprometan la seguridad institucional. Asimismo, el análisis de registros públicos puede revelar vínculos no declarados entre proveedores, conflictos de interés o antecedentes judiciales relevantes.

La auditoría moderna no puede depender únicamente de documentos internos. OSINT complementa la revisión tradicional con una capa externa de verificación, permitiendo contrastar lo que se declara con lo que realmente ocurre en el entorno digital y físico.

Consideraciones éticas y normativas

El uso de OSINT debe estar alineado con principios éticos y normativos. Aunque la información es pública, su recopilación y análisis deben respetar la privacidad, la legalidad y la finalidad legítima del proceso. En Colombia, por ejemplo, la Ley 1581 de 2012 sobre protección de datos personales establece límites claros sobre el tratamiento de información, incluso si esta es accesible públicamente.

Por ello, es fundamental que los analistas OSINT en seguridad física y auditoría corporativa actúen con responsabilidad, documentando sus hallazgos, justificando sus métodos y garantizando la confidencialidad de los resultados.

Finalmente, la Inteligencia de Fuentes Abiertas ha dejado de ser una técnica marginal para convertirse en un pilar estratégico de la seguridad física y la auditoría corporativa. Su capacidad para transformar datos públicos en inteligencia útil permite anticipar amenazas, validar hechos y fortalecer la toma de decisiones en entornos complejos. En un mundo donde la información fluye sin control, OSINT ofrece orden, contexto y profundidad. Su implementación rigurosa, ética y estratégica es hoy una necesidad para cualquier organización que aspire a proteger sus activos, su reputación y su gente.

México registra gran atraso en materia de Protección Civil

- Se ha avanzado en cuestión de sismos, pero aún tenemos grandes carencias en materia de prevención de incendios.
- En el primer semestre de 2025 llevamos pérdidas por 12 mil millones de pesos, y diariamente se registran en territorio nacional 260 incendios.

Guadalajara, Jalisco.- México tiene un gran atraso en materia de protección civil que se debe corregir de inmediato para evitar muertes y daños económicos. Y es que en el primer semestre de 2025 se llevan ya 12 mil millones de pesos en pérdidas por incendios.

Por ello es necesario que juntos, gobierno, industria y sociedad en general actúen y generen políticas públicas para, como en el caso de los sismos, preparar a la población para saber qué hacer en caso de incendios en casas, escuelas, oficinas, comercios y fábricas, pero sobre todo cómo prevenirlos y evitarlos, aseguró Juan José Camacho Gómez, presidente del Consejo Nacional de Protección contra Incendios (CONAPCI).

.

A su vez, Juan Francisco Guzmán Hernández, presidente de la Asociación Mexicana de Rociadores Automáticos Contra Incendios (AMRACI) informó que en el territorio nacional se registran al año más de 95 mil incendios urbanos y no urbanos, es decir 260 al día, según datos del INEGI.

Ambos especialistas en materia de prevención de incendios participaron en la inauguración de la 8ª Expo Fire & Safety 2025, que se llevó a cabo en octubre pasado en la ciudad tapatía.

El presidente de AMRACI advirtió que el 31% de los desastres en México son ocasionados por los incendios, que son responsables del 26.1% de la totalidad de la mortalidad por humo y gases tóxicos.

Esto, sin duda es muestra del gran impacto que tienen los incendios, que, a diferencia de los sismos y huracanes, no reciben la misma importancia de las autoridades e incluso de la misma sociedad, a pesar de que provocan mayores daños que estos últimos.

Asimismo se dieron a conocer avances del programa "Aprende a Mantenerte Seguro" para niños de preescolar y primaria que se pretende implementar en todo el país y se llevó a cabo en "Rally de Prevención" el cual estuvo conformado por diversas actividades educativas en las que se enseñó a niños pequeños cómo actuar en casos de incendios.

Durante el mismo evento, AMRACI y CONAPCI concretaron la firma de un convenio de colaboración con la Secretaría de Educación Pública del estado de Jalisco, para aplicar en la entidad dicho programa que consiste en capacitar a los niños en qué hacer previo, durante y posteriormente a un incendio, pero, sobre todo, en cómo provenirlo y evitarlo.

Esta firma de convenio es punta de lanza en el país, al poner en marcha de manera conjunta esta prueba piloto del programa de educación en materia de prevención de incendios en niños de tercer año de educación básica, en planteles ubicados en zonas de alta vulnerabilidad.

Por su parte, Bomberos de Madrid, España donaron equipo y capacitaron a sus homólogos del estado de Jalisco sobre nuevas técnicas para la prevención y combate de incendios urbanos; en especial mostraron nuevas formas de enseñanza a niños y jóvenes para que estén alertas y sepan cómo actuar ante siniestros de este tipo, en sus casas y escuelas.

La inauguración del evento a nombre del gobernador del estado Pablo Lemus Navarro, estuvo a cargo de la Coordinadora General Estratégica de Gestión del Territorio, Karina Hermosillo Ramírez. En el acto, ambos organismos otorgaron un donativo por 100 mil pesos a la fundación Michou & Mau que encabeza su presidenta Virgina Sendel, para la atención de niños quemados.

La Expo Fire & Safety contó con la participación de diversos especialistas en materia de prevención de incendios provenientes de varios estados de la República, así como de Costa Rica, República Dominicana, Perú, Brasil, Colombia, Paraguay, Ecuador y Estados Unidos.

A lo largo de 240 stands se presentaron las últimas tendencias de prevención y protección de riesgos por la llegada de tecnologías emergentes, baterías de litio, almacenamiento, manufactura, edificios altos y centros de datos, privilegiando la seguridad humana y la continuidad de operaciones. Participaron los proveedores líderes y las soluciones más avanzadas en protección pasiva, detección, alarma y supresión de conflagraciones, así como personalidades varias del sector de la prevención de incendios.

MEX 2025

FORO INTERNACIONAL DE SEGURIDAD Y FACTORES HUMANOS

CAMBIO DE PARADIGMAS

UNA PERSPECTIVA DIFERENTE SOBRE LAS LESIONES LABORALES

13-14 DE NOVIEMBRE 25

CIUDAD DE MÉXICO
HOTEL HILTON SANTA FE

¡No te lo pierdas!

ORGANIZADO POR

SAFESTART®

APOYO:

Grupo STE Your Safety Partner

Instituto Internacional de Administración de Riesgos, S.A. de C.V.

MÁS SEGURIDAD Magazine

prevencionar.com.mx

tasvalúo

El valor asegurable de los activos

- Por qué un avalúo actualizado protege a las empresas.
- México fue uno de los principales países afectados por siniestros registrados en 2024, los cuales causaron las mayores pérdidas económicas a nivel mundial, tal es caso del huracán Helene se convirtió en el evento más costoso del año y el Huracán Milton .

En un contexto donde los fenómenos naturales y los riesgos operativos son cada vez más impredecibles, proteger el patrimonio empresarial se vuelve prioritario. Las recientes lluvias intensas que han provocado inundaciones en distintas zonas del país y que septiembre, mes históricamente asociado a sismos, son recordatorios claros de que contar con un avalúo actualizado de los activos es una herramienta esencial para prevenir pérdidas materiales y garantizar la cobertura adecuada en caso de siniestros.

Para entender mejor este tema, Diana Muñoz Grande, especialista de consultoría en la empresa, explica cómo el proyecto de consultoría de valuación anual de activos ayuda a las empresas a mantener protegidos sus activos. "El objetivo es que las empresas mantengan el control sobre la evolución del valor de sus inmuebles y bienes, con información confiable tanto para tomar decisiones estratégicas como para asegurar correctamente sus activos".

El valor asegurable: La clave para proteger los activos

El valor asegurable es el monto por el que una póliza respalda un activo en caso de siniestro. Mantenerlo actualizado es crítico para no poner en riesgo la estabilidad financiera de la empresa.

"Imagina que ocurre un incendio en tu planta industrial y la póliza de seguro no refleja las últimas ampliaciones o remodelaciones", explica Diana Muñoz. "El seguro solo cubrirá el monto declarado originalmente. Un avalúo con propósito de aseguramiento permite a las empresas contratar pólizas justas y precisas, alineadas al valor real de sus activos", subraya la especialista.

Decisiones informadas, empresas protegidas

Ante fenómenos naturales como inundaciones o sismos, y riesgos operativos como incendios o robos, tener información precisa sobre el valor de los activos marca la diferencia. Tasvalúo, acompaña a las empresas con consultorías especializadas, peritos certificados y herramientas de análisis que garantizan que cada activo esté protegido.

Finalmente, Diana Muñoz, enfatiza que los riesgos son inevitables, pero las pérdidas no tienen porqué serlo. Contar con un avalúo con propósito de aseguramiento es la mejor manera de proteger los activos.

Jóvenes sicarios en América Latina: caminos de prevención más allá del castigo

Asunción, Paraguay.- En la calurosa tarde de Asunción, el 2 de octubre de 2025, mientras llegaba a sus estudios de Derecho, el teniente coronel de Justicia Militar Guillermo Moral, caía víctima de un mortal disparo encargado y pagado por el crimen organizado al cual él había impedido controlar por medio de sobornos la prisión a su cargo.

El evento llevaba en sí fuertes mensajes simbólicos: ocurrió en una zona opulenta y "segura" de la capital paraguaya, en la sede de la Facultad de Derecho de la Universidad nacional (la cuna de la ley en el país); tuvo por víctima a un militar honesto por cuya negativa al soborno por parte de un narco preso habían sido condenados su superior inmediato, la esposa de éste y un abogado. Y el mensaje más profundo aún: si esto ocurrió con un militar entrenado, ¿quién se atrevería ahora a negar un celular u otro privilegio a un narcotraficante preso?

Sin embargo, el dato más perturbador vendría en las horas siguientes con la individualización de los autores del crimen…dos adolescentes, uno de 16 y otro de 18 años, cuyos rostros aparecieron sin cobertura en cámaras de vigilancia después del atentado, convirtiéndose en material descartable para sus mandates.

El dato de estos sicarios adolescentes se sumaba a otro de 16 años que asesinó a un trabajador de motocicleta repartiendo mercancías, apenas en el mes de junio (aparentemente como prueba de sangre para iniciarse en un grupo criminal), y a otro de 14 que asesinó a domicilio a un oficial de la policía paraguaya y a toda su familia en el interior del país, a mediados del año pasado.

En los últimos años, América Latina ha sido testigo del alarmante fenómeno de la creciente participación de jóvenes, en actos de sicariato. Desde México hasta Paraguay, pasando por Colombia, Ecuador, Brasil o El Salvador, se repite una misma realidad: adolescentes de 13, 14 o 15 años son reclutados para ejecutar asesinatos por encargo, convertidos en piezas desechables de estructuras criminales. Detrás de cada caso hay más que una historia individual de violencia; hay un entramado social, económico y cultural que explica su emergencia y persistencia.

Causas estructurales y culturales

La primera gran causa es la exclusión social. En muchos contextos urbanos de la región, amplios sectores juveniles viven sin acceso sostenido a educación de calidad, empleo digno o servicios básicos. Las desigualdades históricas y la falta de movilidad social alimentan un sentimiento de frustración que las organizaciones criminales aprovechan hábilmente. La promesa de dinero rápido y estatus simbólico en barrios donde las oportunidades son escasas convierte el sicariato en una salida aparente, aunque efímera.

A ello se suma la normalización de la violencia en entornos donde la vida cotidiana está atravesada por conflictos armados, pandillas o ajustes de cuentas. En este contexto, matar por encargo deja de ser un acto excepcional para transformarse en una tarea funcional dentro del ecosistema criminal.

Otra causa determinante es la fragmentación familiar y comunitaria. La desintegración de vínculos afectivos, la ausencia de referentes positivos, mecanismos de freno y la debilidad de redes de apoyo hacen que muchos adolescentes busquen identificación y pertenencia en grupos delincuenciales. Las bandas no sólo ofrecen dinero: ofrecen identidad, reconocimiento y protección.

Por último, hay factores institucionales y culturales que refuerzan el ciclo. La impunidad generalizada, la corrupción policial y judicial, y la falta de confianza en el Estado envían un mensaje peligroso: el delito puede pagar. En paralelo, los medios de comunicación y las redes sociales, al glorificar a los "narco héroes" o figuras del crimen organizado, crean un imaginario aspiracional que seduce a muchos jóvenes vulnerables.

Consecuencias sociales y humanas

El involucramiento de adolescentes en el sicariato tiene consecuencias devastadoras. En el plano individual, implica la pérdida precoz de la infancia y la adolescencia. Muchos jóvenes terminan muertos, encarcelados o con traumas profundos que perpetúan el ciclo de violencia. De hecho, los dos adolescentes identificados en el último caso en Paraguay, están técnicamente "desaparecidos".

El reclutamiento de menores por parte de redes criminales socava la legitimidad del Estado, amplía la brecha entre ciudadanos y autoridades, y convierte la violencia en un mecanismo paralelo de control social.

Prevención más allá del castigo

Las respuestas centradas exclusivamente en el enfoque policial o punitivo —mayor presencia policial, endurecimiento de penas o militarización de territorios— han mostrado su insuficiencia. El problema no se resuelve con más cárceles ni con la criminalización de la pobreza. La prevención debe entenderse en al menos tres ejes: social, situacional y ambiental.

La prevención social apunta a las causas profundas. Supone invertir en educación inclusiva, en programas de empleabilidad juvenil, en servicios de salud mental, en apoyo a familias vulnerables y en la promoción de valores de convivencia. Experiencias como los programas de mediadores comunitarios en Medellín o los centros "Territorios de Paz" en El Salvador han mostrado que ofrecer alternativas reales puede rescatar a muchos jóvenes del circuito del crimen.

La prevención situacional busca reducir las oportunidades delictivas mediante intervenciones concretas en el espacio público. Iluminación, actividades culturales, vigilancia comunitaria y recuperación de espacios urbanos degradados. Un barrio activo y cuidado es menos propicio para el reclutamiento.

Finalmente, la prevención ambiental propone transformar el entorno social y simbólico donde crece la violencia. Esto incluye políticas urbanas que promuevan cohesión social, acceso a cultura y deporte, y participación ciudadana. También implica romper la narrativa cultural que glorifica al "sicario exitoso" o al "narco poderoso".

Un llamado regional

El sicariato adolescente no es sólo un problema de seguridad, sino un síntoma de crisis social. Enfrentarlo requiere voluntad política, empatía social y una mirada integral que combine justicia, educación y desarrollo. América Latina tiene experiencia y creatividad suficientes para construir modelos preventivos que pongan la vida por encima del miedo y la exclusión. Apostar por los jóvenes no es ingenuidad: es la única estrategia sostenible para cortar el ciclo de violencia que amenaza el futuro de toda la región. No hacerlo, implicaría esperar que la represión sane lo que la exclusión provocó… Una receta para el colapso.

José María Amarilla
CPP EIE, Miembro por Paraguay del Consejo Consultivo Latino de IFPO.
Articulista invitado

Seguridad en Latinoamérica: entre la resiliencia y la vulnerabilidad

Juan Luis Parra
MBA, CPP
Articulista invitado

San José, Costa Rica.- La seguridad en América Latina se encuentra en un punto de inflexión. La región combina crecimiento económico desigual, fragilidad institucional, brechas tecnológicas y una criminalidad cada vez más sofisticada.

Desde la óptica de un profesional en seguridad, entender este entorno implica reconocer que el riesgo no solo proviene de amenazas directas —como el crimen organizado o la corrupción—, sino también de vulnerabilidades estructurales: informalidad, debilidad institucional y escasa cultura de prevención.

En este contexto, el profesional en seguridad debe actuar como un gestor estratégico del riesgo, integrando inteligencia, datos y liderazgo organizacional para construir resiliencia.

1. Panorama de amenazas en la región

Latinoamérica concentra el 8% de la población mundial, pero cerca del 30% de los homicidios, según la ONU. Esta desproporción refleja un entorno de riesgo persistente y dinámico.

A los delitos tradicionales se suman fenómenos emergentes:

- Ciberdelincuencia y fraude digital.
- Corrupción corporativa.
- Polarización política y conflictividad social.
- Crimen organizado transnacional.

Frente a ello, las empresas deben pasar de un enfoque reactivo a uno basado en la gestión integral del riesgo (ESRM).

2. Incorporación de modelos estadísticos de riesgo

Para dar fundamento técnico a la gestión de riesgos en seguridad, se recomienda aplicar herramientas estadísticas que permitan cuantificar la probabilidad e impacto de los eventos adversos.

Uno de los modelos más útiles es la Simulación Monte Carlo, ampliamente usada en finanzas y seguridad corporativa. Este modelo permite:

- Estimar la probabilidad de ocurrencia de incidentes mediante miles de iteraciones.
- Cuantificar pérdidas esperadas considerando escenarios optimistas, moderados y críticos.
- Determinar niveles de tolerancia al riesgo visualizados en un histograma de pérdidas.

Por ejemplo, un análisis aplicado en parques industriales demostró que, ante 10 mil simulaciones, el 65% de los incidentes críticos se concentran en el 20% de las áreas con menor supervisión o control tecnológico.

Complementar este enfoque con matrices FMEA o ISO 31000 permite priorizar acciones preventivas y justificar presupuestos con evidencia cuantitativa.

3. De la protección a la resiliencia

El modelo tradicional centrado en guardias y cámaras debe evolucionar hacia una seguridad predictiva y basada en inteligencia.

El profesional en seguridad necesita dominar metodologías como:

- Análisis FMEA para anticipar fallas críticas.
- Modelos ISO 31000 para alinear la gestión del riesgo con la estrategia.
- Planes de Continuidad del Negocio (BCP).
- Analítica de datos e Inteligencia Artificial.

4. Factores humanos y culturales

El principal desafío en América Latina no es tecnológico, sino cultural. En muchas organizaciones, la seguridad se percibe como un gasto y no como una inversión estratégica.

El liderazgo debe promover una cultura de accountability y aprendizaje continuo, donde la prevención forme parte del ADN organizacional.

5. Mirada hacia el futuro

Las tendencias más relevantes para los próximos años son:

- Integración regional de estándares ASIS e ISO.
- Expansión de tecnologías autónomas (IA, drones, sensores inteligentes).
- Profesionalización del sector.
- Gestión del riesgo reputacional.

En conclusión, la seguridad en Latinoamérica se redefine cada día. En un entorno donde la incertidumbre es la norma, el verdadero valor del profesional en seguridad radica en su capacidad para prever, analizar y liderar con datos.

Integrar modelos estadísticos, pensamiento estratégico y liderazgo humano permitirá transformar la vulnerabilidad en resiliencia. Así, la seguridad dejará de ser una reacción ante el riesgo para convertirse en un activo estratégico que impulsa la sostenibilidad y competitividad de la región.

Escolta o especialista en protección: una clarificación necesaria

Jonathan Borges
Ingeniero industrial con 18 años de experiencia en la protección de activos sensibles y riesgos especiales en organizaciones públicas y privadas. Miembro de la junta directiva de IFPO Comunidad Venezuela.
Articulista invitado

Caracas, Venezuela.- En el mundo actual, donde la seguridad personal se ha vuelto una prioridad tanto para figuras públicas como para individuos que enfrentan riesgos específicos, es crucial entender las diferencias entre los términos que a menudo se utilizan de manera intercambiable: "guardaespaldas", "escolta" y "especialista en protección". Esta confusión puede llevar a malentendidos sobre las habilidades y competencias necesarias para desempeñar cada uno de estos roles. Por ello, es fundamental profundizar en el concepto de "especialista en protección" y cómo se distingue de un simple guardaespaldas.

El término "guardaespaldas", conocido internacionalmente como "bodyguard", evoca la imagen de una persona imponente, generalmente de gran tamaño y fuerza física, cuyo principal objetivo es proporcionar una presencia disuasoria. Este estereotipo, aunque tiene algo de verdad, no refleja la realidad del trabajo de protección personal. Muchos guardaespaldas son contratados por figuras del entretenimiento, donde la apariencia física puede ser más importante que las habilidades técnicas. Sin embargo, esta imagen superficial no siempre se traduce en una capacitación adecuada o en un conocimiento profundo de las amenazas contemporáneas y tácticas delictivas.

Por otro lado, el término "escolta" implica un nivel más alto de preparación y profesionalismo. Un escolta debe poseer un perfil íntegro y contar con una formación integral en técnicas de protección. Esto incluye el dominio de habilidades como el combate cuerpo a cuerpo, el uso de armas y la conducción defensiva en vehículos de dos y cuatro ruedas. Además, debe estar al tanto de las últimas tendencias en seguridad y ser capaz de adaptarse rápidamente a situaciones cambiantes. Sin embargo, incluso este rol puede carecer de la profundidad necesaria para abordar todos los aspectos de la protección personal.

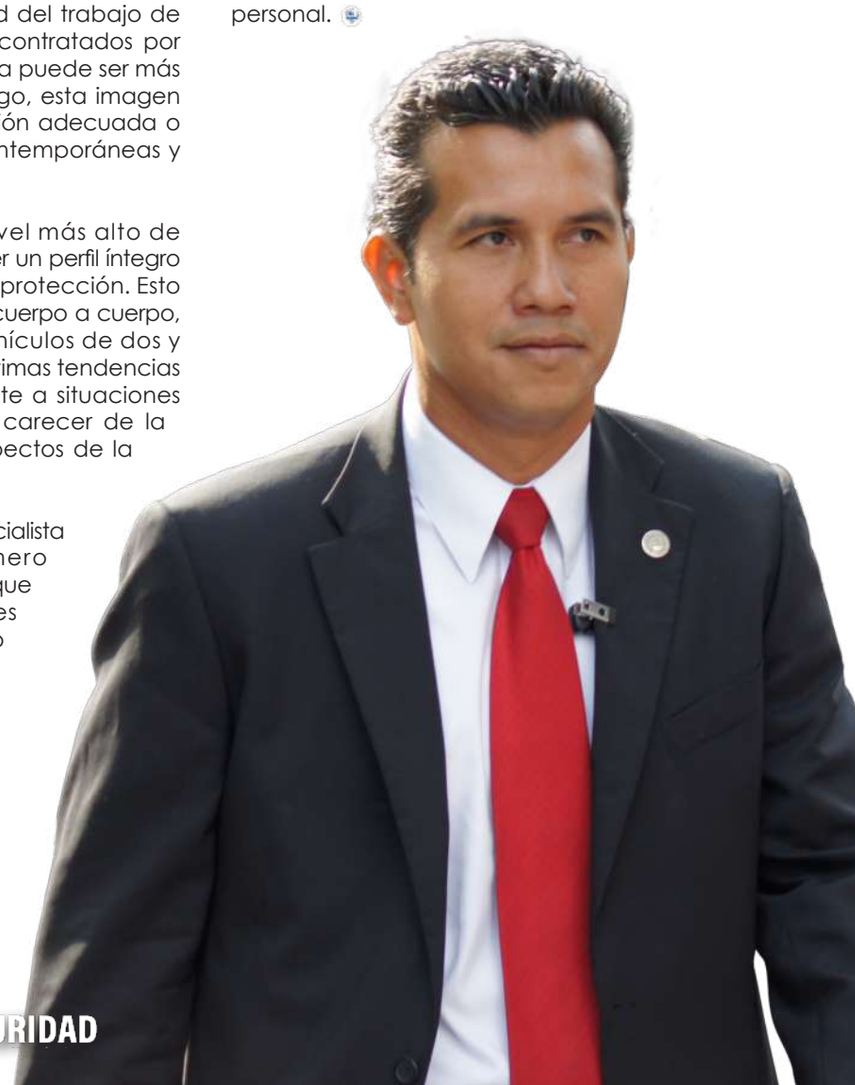
Aquí es donde entra en juego el concepto de "especialista en protección". Esta figura va más allá del mero escolta; es un profesional altamente capacitado que combina conocimientos técnicos con habilidades interpersonales. Un especialista en protección no solo tiene la capacidad de neutralizar amenazas inmediatas, sino que también debe ser capaz de realizar un análisis exhaustivo de riesgos y diseñar estrategias preventivas adaptadas a las necesidades específicas de la persona o entidad que protege. Esto requiere una formación continua y certificaciones reconocidas que respalden su preparación.

Un especialista en protección debe tener una visión global de la seguridad. Esto implica no solo conocer las técnicas de defensa personal y protección física, sino entender aspectos como la gestión de crisis, planificación de rutas seguras y evaluación del entorno. Además, las habilidades blandas son igualmente importantes; trabajo en equipo, liderazgo y comunicación efectiva son fundamentales para garantizar que el especialista pueda coordinarse con otros miembros del equipo de seguridad y actuar con eficacia en situaciones críticas.

La imagen y la presentación personal también juegan un papel crucial en el trabajo del especialista en protección. Dado que este profesional a menudo representa a personas influyentes (PMI/VIP), su comportamiento, dicción y apariencia pueden influir en la percepción pública y en la seguridad general del protegido. Un especialista en protección debe ser capaz de moverse con discreción y elegancia, manteniendo siempre un enfoque profesional.

Aunque los términos "guardaespaldas", "escolta" y "especialista en protección" pueden parecer similares, hay diferencias significativas entre ellos. El especialista en protección es un profesional altamente capacitado que desempeña un papel esencial en la seguridad personal, combinando habilidades técnicas con un enfoque proactivo y estratégico.

En un mundo donde las amenazas son cada vez más complejas, contar con un especialista en protección bien entrenado puede marcar la diferencia entre la seguridad y el riesgo. Por lo tanto, es vital reconocer y valorar esta distinción para garantizar que se tomen decisiones informadas al buscar servicios de protección personal.



GRUPO ALEM

Seguridad Privada Integral S.A. de C.V.

¡Garantizamos su tranquilidad!

Guardias intramuros: Capacitados en diferentes modalidades (condominios, plazas comerciales, fábricas, etc)

Escoltas: Entrenados constantemente y especializados de acuerdo a la actividad del protegido

Custodias: Para todo tipo de transporte de mercancías en tránsito

Rastreo satelital: Vehículos particulares, carga o flotillas

Videovigilancia: Fija, móvil y remota

Análisis de riesgos y vulnerabilidades: Desarrollado por expertos en seguridad física y patrimonial

www.grupoalem.mx

edgar.seguridad.integral@gmail.com

+52 564705 2246

El cielo bajo control criminal: Geopolítica y seguridad ante la era de los drones

Fernando Vaccotti
PhD. CPO.
Miembro por Uruguay del Consejo Consultivo Latino de IFPO.
Articulista invitado

Montevideo, Uruguay.- En el siglo XXI, pocos avances transformaron tan rápido la seguridad internacional, la guerra y el crimen organizado como los drones. Lo que empezó como herramienta civil para agricultura o fotografía, hoy es un instrumento estratégico para Estados, corporaciones militares privadas y organizaciones criminales. Su bajo costo, fácil adquisición y rápida adaptabilidad han modificado doctrinas de combate y dinámicas delictivas, reconfigurando los límites entre seguridad nacional y ciudadana, guerra y crimen.

Revolución militar y criminal

Los drones ofrecen artillería de precisión, vigilancia en tiempo real y capacidad de enjambre, igual de revolucionaria que la pólvora o el tanque. En el terreno delictivo, los grupos criminales los emplean para contrabando, reconocimiento y ataques directos. Se ha creado una industria global de drones y contra-drones en la que conviven Estados, empresas y talleres clandestinos, operando en esa zona gris entre lo legal y lo ilícito.

De Ucrania al mundo

El conflicto en Ucrania es el laboratorio contemporáneo del uso masivo de drones. Un UAV de 500 USD puede destruir equipos que valen millones. Rusia emplea masivamente los Shahed iraníes, y Ucrania produjo millones de drones en 2024-2025. Irán, Turquía y China consolidan su dominio tecnológico, mientras la capacidad de ataque se democratiza: cualquier actor puede golpear infraestructura estratégica a bajo costo, alterando la geopolítica del poder aéreo.

Crimen organizado y drones

En América Latina, los drones se integraron al ecosistema criminal. Sirven para transportar drogas, realizar vigilancia o ejecutar ataques con explosivos, como los del CJNG en México. En cárceles de Brasil, Colombia, Argentina y Uruguay se usan para introducir armas o celulares. En el Reino Unido hubo más de mil 700 incidentes en prisiones, y América Latina sigue esa tendencia. En Michoacán, México, un dron improvisado atacó un helicóptero militar: símbolo del nuevo equilibrio del terror.

Tecnologías emergentes

Los drones FPV permiten cargas mayores y vuelo autónomo con IA. Los navales (USV) exponen la vulnerabilidad de puertos y buques. La evolución tecnológica apunta a mayor autonomía, menor costo y masificación.

La carrera defensiva

El mercado C-UAS (contra drones) supera los 3 mil 500 millones de dólares y crece 20% anual. Las defensas se dividen en:

- **Soft kill:** inhibidores, geocercas y bloqueadores RF.
- **Hard kill:** láseres, escopetas y drones interceptores.
- **Estructurales:** mallas, techos, sensores acústicos.

Pero no basta con derribar drones: es clave desmantelar la red logística que los sustenta, desde los técnicos hasta el mercado negro de baterías y repuestos.

Economía global y poder aéreo

El mercado mundial ronda los 73 mil millones USD y podría duplicarse en 2030. Startups, universidades, milicias y Estados compiten en un mismo ecosistema donde la línea entre innovación y delito es cada vez más difusa.

El impacto geopolítico es evidente: el dron democratiza la capacidad de ataque, permitiendo que un Estado débil o un actor no estatal puedan golpear infraestructura estratégica a bajo costo.

Para concluir, los drones marcan una inflexión estratégica. Si el siglo XX fue el de la supremacía aérea estatal, el XXI democratizó el cielo. En Ucrania reescriben la guerra; en Yemen los hutíes golpean el comercio global; en México los cárteles desafían al Estado; y en las cárceles latinoamericanas son parte del nuevo orden criminal.

El cielo, antes símbolo de soberanía, hoy es un territorio disputado. La tarea urgente de los Estados es blindar infraestructuras, modernizar la inteligencia y anticipar la próxima generación de amenazas autónomas.

No es solo innovación: es una revolución que redefine la seguridad global.

Expodefensa 2025

Feria Internacional de Defensa y Seguridad
International Defense and Security Trade Fair

1st to 3rd DEC 2025

• CORFERIAS-BOGOTÁ, COLOMBIA •

TAKE PART IN
THE MEETING PLACE FOR SECURITY & DEFENSE
IN LATIN AMERICA

230+
Exhibiting companies
from 29 countries

50+
Delegations
from 27 countries
(top decision makers, from governments)

10,000+
Participants
(keys players and buyers)

20
Conferences

100+
journalists

WWW.EXPODEFENSA.COM.CO

Supported by:

Defensa

Organized by:

CODALTEC
CORPORACIÓN DE ALTA TECNOLOGÍA

COGES EVENTS

corferias
Generadores de Oportunidades y Progreso

Autor: José Paulino González.

Nos dijeron que para tener éxito hay que sacrificar el bienestar. Pero eso es mentira.

"Conquista tu Estrés" es una ruta clara, humana y poderosa para alcanzar un alto desempeño sin romperte por dentro.

Sin Burnout. Sin caos interno. Sin desconectarte de ti.

A través de historias reales, ciencia accesible, prácticas corporales y sabiduría ancestral, José Paulino González te guía a reconectar con tu centro y convertir el estrés en tu aliado.

En estas páginas descubrirás cómo:

- Regular tu sistema nervioso de forma simple y convertirlo en tu aliado.
- Leer las señales de tu cuerpo antes de que sea demasiado tarde.
- Ampliar tu ventana de tolerancia y mantener la calma bajo presión.
- Diseñar tu propio protocolo de recuperación, desde lo físico hasta lo emocional.
- Volver a ti, recuperar tu energía y liderar desde tu propósito, con presencia y poder.
- La guía práctica que todo líder necesita para sostener su alto desempeño sin caer en Burnout.

Autor: Carlos Ramírez.

En un mundo donde las amenazas evolucionan y los límites entre lo físico y lo digital se desdibujan, proteger lo esencial ya no puede hacerse desde compartimentos estancos. "Defensa Total" propone un enfoque estratégico, técnico y humano para abordar la convergencia entre seguridad física y ciberseguridad, con foco en infraestructuras críticas.

Este libro no solo recorre marcos normativos, amenazas actuales y tecnologías emergentes, sino que invita a construir una cultura de seguridad convergente, donde las personas, los procesos y la inteligencia se alinean para anticipar riesgos híbridos. Con casos reales, herramientas prácticas y una visión integrada, es una guía imprescindible para quienes lideran, gestionan o auditan entornos de alto impacto.

1. Más que un libro técnico, es una propuesta de transformación: pasar de reaccionar a anticipar, de dividir a integrar, de vigilar a comprender.

salto
INSPIRED ACCESS

SALTO WECOSYSTEM

Impulsando un acceso más inteligente

SALTO lidera la transformación digital en la gestión de accesos e identidades, combinando tecnologías innovadoras con soluciones pensadas para cada necesidad.

Desarrollamos tecnología de vanguardia en control de accesos, gestión de identidades y cerraduras electrónicas, para ofrecer experiencias seguras, confiables y sin fricciones en todo tipo de espacios.

saltosystems.com

Datos de contacto
marketing.cala@saltosystems.com

Centros de comando y control más inteligentes

Conozca como estamos creando los **C4** y **C5i** más robustos y resilientes de Latinoamérica.

- ✔ Mayor coordinación entre agencias, respuestas eficientes
- ✔ Mayor integración de dispositivos y visibilidad de su ciudad
- ✔ Análisis predictivo para toma de decisiones
- ✔ Automatización y mejor agilidad de despacho ante incidentes
- ✔ Certificación NENA 9-1-1

MOTOROLA SOLUTIONS

contactenos@motorolasolutions.com