

MÁS SEGURIDAD

Magazine



4ever

PROJECTS

EL INTEGRADOR GIGANTE de América

Edición 155 | Año 17 | Marzo-Abril 2025



México y Latam / precio \$60.00MX



ORION

LA INNOVADORA SOLUCIÓN DE
ROSTRO COMO CREDENCIAL



Garantice un acceso seguro con la tecnología de reconocimiento facial más avanzada. Permita a los usuarios acceder utilizando sólo la cara como credencial única, eliminando la necesidad de llaves físicas, tarjetas de acceso o credenciales móviles. Salto Orion agiliza y optimiza el proceso de acceso, mejorando la seguridad al eliminar el riesgo de pérdida o robo de credenciales. Con Orion, puede obtener un control total sobre instalaciones de cualquier tamaño, todo desde una única fuente.



Aplicación

Potente tecnología de reconocimiento facial que redefine la forma en que las personas acceden a los espacios.



Tecnología

Orion simplifica el reconocimiento facial, garantizando un funcionamiento rápido, preciso y sin contacto.



Capacidades

Orion ya está integrado en Salto Space, la plataforma de control de acceso inteligente todo en uno.



Prestaciones

Orion ofrece un tiempo de respuesta rápido, que permite a los usuarios acceder a cualquier punto de entrada de Salto rápidamente y sin problemas en menos de un segundo.



HUMBERTO MEJÍA HERNÁNDEZ
DIRECCIÓN GENERAL
humberto@revistamasseguridad.com.mx

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

BEATRIZ CANALES HERNÁNDEZ
COORDINACIÓN EDITORIAL
edicion@revistamasseguridad.com.mx

LUZ GONZÁLEZ MEDINA
COORDINACIÓN DISEÑO
diseno@revistamasseguridad.com.mx

TERESA RAMÍREZ OJEDA
INFORMACIÓN
redaccion@revistamasseguridad.com.mx

SARA MEJÍA CASTRO
DESARROLLO DE NEGOCIOS LATAM
negocios@revistamasseguridad.com.mx

FREY NICACIO DÍAZ GÜIZA
DESARROLLO DE NEGOCIOS COLOMBIA
ventas@revistamasseguridad.com.mx

CARMEN CHAMORRO
CORRESPONSAL ESPAÑA
corresponsal@globaldefense.com.mx

OSCAR TENORIO COLÓN
ADMINISTRACIÓN Y CONTABILIDAD
contabilidad@revistamasseguridad.com.mx

JORGE MERCADO ABONCE
SERVICIOS JURÍDICOS INTEGRALES
ANAZALDO-MARTÍNEZ-MERCADO
DIRECCIÓN JURÍDICA
juridico@revistamasseguridad.com.mx

ASISTENCIA A CLIENTES
atencion@revistamasseguridad.com.mx

CONTACTO
Tel: +52 55 1894 7067
WhatsApp: (+52) 55 1894 7067
asistencia@revistamasseguridad.com.mx
atencion@msglobal.com.mx

SIGUENOS EN:

-  Revista más seguridad
-  @revmasseguridad
-  revistamasseguridad
-  Revista más seguridad
-  @revmasseguridad
-  Revista más seguridad

Revista Más Seguridad Año 17, No 155, Marzo/Abril 2025, Publicación mensual 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 5555272279 / +52 5528732719.
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: PPI5-5134 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.

Crece ecosistema de integradores y arquitectura de seguridad

Los integradores de tecnologías de seguridad en México y LATAM, desempeñan un rol fundamental en la protección de infraestructuras y datos.

Las empresas integradoras juegan un rol fundamental en la protección de infraestructuras y datos, ofreciendo soluciones adaptadas a las necesidades cambiantes del mercado y contribuyendo al fortalecimiento de la seguridad en la región.

En el panorama de la seguridad electrónica en México y América Latina, las empresas integradoras juegan un papel estratégico por ofrecer soluciones completas que combinan diversos sistemas y herramientas de vanguardia, para proteger activos y garantizar la continuidad operativa de las organizaciones en múltiples sectores.

Los integradores, no solo implementan tecnologías avanzadas, sino que también diseñan estrategias adaptadas a las necesidades específicas de cada cliente, abarcando aspectos como la seguridad física y la ciberseguridad.

Algunos ejemplos destacados son las firmas mexicanas dedicadas a brindar soluciones de automatización, monitoreo y seguridad para hogares y oficinas, que utilizan tecnologías de punta para crear entornos eficientes y seguros, permitiendo a sus clientes tener visibilidad y control en todo momento sobre sus espacios.

Otras empresas relevantes se especializan en proyectos y sistemas de seguridad integral para organizaciones industriales, comerciales y de servicios. Ofrecen soluciones que incluyen protección anti-intrusión, videovigilancia, control de acceso y ciberseguridad, adaptándose a las exigencias normativas más rigurosas y garantizando la confianza de sus clientes.

En el ámbito de la ciberseguridad, existen firmas relevantes con divisiones para seguridad, consolidando al sector en México y América Latina. Servicios como monitoreo y detección de amenazas, inteligencia cibernética y protección de infraestructuras críticas, contribuyen significativamente a la gestión de riesgos digitales en la región.

La creciente demanda de soluciones de seguridad integradas ha impulsado a muchas empresas a innovar y adaptarse a las nuevas amenazas y desafíos. Según un informe de Gartner, se espera que para 2025, el 70% de las organizaciones que inviertan en seguridad busquen tecnologías con monitoreo en tiempo real, Inteligencia Artificial para la detección de amenazas y automatización de sistemas de seguridad.

Los integradores de tecnologías de seguridad en México y LATAM, desempeñan un rol fundamental en la protección de infraestructuras y datos, ofreciendo soluciones adaptadas a las necesidades cambiantes del mercado y contribuyendo al fortalecimiento de la seguridad en la región.

Los profesionales de LATAM

Amplia experiencia en el campo de la seguridad integral, comenzó en el campo de la Prevención de Riesgos Laborales con experiencia en Servicios de Prevención públicos como técnico especialista en PRL, con notable experiencia en la investigación de accidentes laborales desde un punto de vista judicial, formándose como Perito Judicial en esta materia de la Seguridad laboral y fundando la Asociación Profesional de Expertos en Riesgos y Accidentes Laborales APERAL.

Cursó estudios en la Universidad Antonio de Nebrija obteniendo el título de Director de Seguridad y la posterior habilitación como Director y Jefe de Seguridad Privada por el Ministerio del Interior. También en la docencia en varias especialidades para el Personal de Seguridad Privada. Es Máster en Criminalística por la Universidad Internacional Isabel I de Castilla y con varias especialidades como Perito.

Es miembro de la Sociedad Española de Criminología y Ciencias Forenses y la Sociedad Española de Derecho de la Seguridad así como miembro de la Asociación Española de Antropología y Odontología Forense. Es Presidente de ADISPO y Vicepresidente de AIMCSE, Vocal del Turno de Peritos de ADISPO. Presidente y fundador del Foro Iberoamericano de Seguridad y Emergencias.

Ostenta distintos reconocimientos profesionales y académicos del ámbito de la seguridad pública y privada. Más de 25 años trabajando en el área de la seguridad integral y en el campo de la investigación. 🌐



Francisco Javier González Fuentes
España



• Escucha —  —



**NUESTRO
PODCAST**

a través de Spotify



MÁS SEGURIDAD
Magazine

SUMARIO

- 6 Nueva web de displays Hikvision**
- 8 Videovigilancia inteligente con Uniview**
- 12 HID transforma espacios corporativos**
- 16 Factor humano como clave de la seguridad SafeStar**

22 4everSecure el integrador gigante de América

- 25 Evolucionan SISA la seguridad en México**
- 26 Optex, fibra óptica para protección de grandes sitios**
- 28 Computare, mente maestra de la seguridad electrónica**

Top Firms de Integradoras

30



Humberto Mejía Hernández, DSE.

Rancho Izaguirre: El “Auschwitz mexicano”

Los escandalosos y macabros hallazgos en el Rancho Izaguirre, en Teuchitlán, Jalisco, evidencian el horror que se ha instalado en México. Los crematorios y el adiestramiento forzado de personas desaparecidas no son hechos aislados, sino expresiones de una maquinaria de exterminio. Estas prácticas obligan a preguntar ¿quiénes son los responsables de esta violencia: un cártel del narcotráfico o un grupo terrorista? Pero el gobierno federal sigue en su letargo. Medios de información internacionales afirman que el Rancho Izaguirre es el “Auschwitz mexicano”. Vergonzosa la comparación.

El hallazgo realizado por Guerreros Buscadores y Madres Buscadoras (ambas organizaciones de Jalisco) es tal vez el último eslabón de una larga lucha de las familias de personas desaparecidas que desde hace décadas han impulsado procesos de búsqueda y develado el horror que vivimos en México. La Fiscalía de Jalisco no ha demostrado voluntad para investigar estos crímenes.

También es cierto que los campos de exterminio y reclutamiento como el de Teuchitlán, no pueden operar sin un marco de protección gubernamental que los permita. No se trata solo de cárteles operando en la clandestinidad, sino de una estructura donde el Estado mismo facilita (o ignora estas prácticas). Esta realidad obliga a replantear: ¿Será narcoterrorismo aunque el gobierno de Claudia Sheinbaum lo niegue?

La desaparición y el exterminio no son meros efectos colaterales de la “guerra contra el narcotráfico”, sino procesos integrados en un modelo de acumulación, despojo, control territorial, extracción de rentas y disciplinamiento social.

En días recientes, después de que la Fiscalía estatal afirmó que no encontró más tras los allanamientos, el grupo Guerreros Buscadores de Jalisco denunció que ahí, además de un campo de adiestramiento del Cártel de Jalisco Nueva Generación (CJNG), había hornos crematorios para desaparecer los cuerpos de las víctimas de esta organización criminal. La Presidenta, Claudia Sheinbaum, ya se pronunció y pidió “esperar a los resultados”. Por su parte, el Secretario de Seguridad y Protección Ciudadana, Omar García Harfuch, dio a conocer avances en la investigación del “supuesto ‘campo de exterminio’ de Teuchitlán, esto luego de la detención en la Ciudad de México de José Gregorio “N”, alias “El Lastra”, integrante del Cartel Jalisco Nueva Generación (CJNG) encargado del reclutamiento de víctimas para convertirlos en sicarios.

El funcionario reveló que el crimen organizado solía contactar a sus víctimas por redes sociales y ya en grupos cerrados de mensajería, describía las actividades a realizar. Algunas de estas publicaciones referían ofertas de trabajo como guardias de seguridad con un pago de 4 mil a 12 mil pesos semanales. Una vez que las víctimas accedían, eran citadas en centrales de autobuses y de ahí trasladadas al campo de adiestramiento en el Rancho Izaguirre.

Debido a que se detectaron perfiles en redes sociales y cuentas donde ofrecían falsas ofertas de empleo, la dependencia a su cargo ya dio de baja 39 páginas de reclutamiento y siguen la pista a otras más. “Después del niño ahogado”...

El Estado ha tenido un papel que va desde la omisión hasta la complicidad. La militarización de la seguridad ciudadana no ha reducido la violencia, sino ha fortalecido a las redes de macrocriminalidad al integrarlas dentro de las estructuras estatales. Empresas y redes económicas, tanto legales como ilegales, sostienen estas dinámicas a través del lavado de dinero y la explotación de territorios y personas. La impunidad es el hilo conductor de esta estructura. La pregunta es: ¿podría clasificarse como narcoterrorismo? 🇲🇽

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

Tour Internacional 2025

MÁS SEGURIDAD
Magazine



Sigue la cobertura informativa en redes sociales, sitio web y revista

CALENDARIO

CURSOS ALAS 2025



MAR 11 - 14  Video Vigilancia	ABR 22 - 25  Control de Acceso	MAY 27 - 30  Inteligencia Artificial en Seguridad	JUN 17 - 20  Alarmas y Detección de Intrusión	JUL 22 - 25  Operadores de Cuartos de Control
AGO 19 - 22  Evaluación de Riesgos de Seguridad	SEP 23 - 26  Ventas para la Industria de la Seguridad	OCT 28 - 31  Gerencia de Proyectos	NOV 25 - 28  Video Vigilancia	DIC 9 - 12  Operadores de Cuartos de Control

Este curso y muchos más los puedes disfrutar en la modalidad InCompany

Alarmas y Detección de Incendios • Alarmas y Detección de Intrusión • Ciberseguridad para Alta Gerencia • Ciberseguridad y Protección de Activos Digitales • Control de Acceso • Drones en Seguridad • Evaluación de Riesgos de Seguridad • Evaluación del Retorno de la Inversión • Fundamentos de Seguridad Electrónica • Gerencia de Proyectos • Integración de Sistemas de Seguridad • Inteligencia Artificial en Seguridad • Management 3.0 • Operadores de Cuartos de Control • Redes IP e Inalámbricas • Seguridad Perimetral • Ventas para la Industria de la Seguridad • Video Vigilancia •

www.alas-la.org



ASOCIACIÓN
LATINOAMERICANA
DE SEGURIDAD

Si eres Socio ASIS,
obtendrás puntos CPEs
en esta actividad



CRISTIAN MOLINA
Coordinador de Cursos
Whatsapp:
+57 321 6153367



Nueva web de displays



- *Tecnología y soluciones a la medida para LATAM.*
- *"Queremos que este portal sea una referencia para quienes buscan soluciones avanzadas y adaptadas a las necesidades del mercado latinoamericano"*

La empresa mundial en soluciones de videovigilancia y tecnología de pantallas, Hikvision, anuncia el lanzamiento de su nueva página web para América Latina: <https://display.hikvision.com/es-la/>. Este nuevo portal está diseñado para ofrecer información detallada sobre las últimas innovaciones en pantallas y displays, abarcando múltiples sectores industriales y comerciales en la región.

El sitio web se enfoca en mostrar las capacidades avanzadas de las soluciones de pantallas LED de Hikvision, así como en brindar a los usuarios una experiencia digital intuitiva, con acceso a especificaciones técnicas, tendencias del mercado y casos de éxito locales.



Fran Sánchez, Marcom director en Hikvision México, destacó que la nueva plataforma digital nace como respuesta a la creciente demanda de soluciones tecnológicas de alta calidad en América Latina: “La tecnología fue el principal catalizador para la creación de este sitio web. Nuestro objetivo es proporcionar un espacio digital donde los usuarios puedan conocer a fondo nuestras soluciones de pantallas LED de ultra alta definición, displays con eficiencia energética optimizada y alternativas personalizadas para diversos escenarios y necesidades específicas. El portal está diseñado para profesionales, empresas y entusiastas de la tecnología en toda la región”.

Subraya que el lanzamiento de este portal es parte de la estrategia de la compañía para consolidar su presencia en América Latina, una región en constante crecimiento tecnológico. Con oficinas locales y un equipo de expertos, la empresa reafirma su compromiso de ofrecer soluciones innovadoras y un servicio al cliente excepcional.

El portal ofrece un extenso catálogo de soluciones adaptadas a diferentes industrias, incluyendo sistemas de señalización digital para retail, pantallas interactivas para educación, soluciones para empresas, Videowall LED, señalización digital y monitores industriales de alto rendimiento, entre las que destacan:

- **Pantallas LED:** Ideales para señalización digital en retail, centros comerciales y eventos masivos.

- **Pantallas planas interactivas:** Perfectas para entornos educativos y empresariales que buscan fomentar la colaboración y el aprendizaje activo.
- **Publicidad digital:** Soluciones para optimizar campañas de marketing con pantallas de alto impacto visual.
- **Dispositivo de videoconferencia:** Equipos que mejoran la conectividad y la eficiencia en las comunicaciones corporativas.
- **Paredes de video LCD:** Diseñadas para centros de control, seguridad y monitoreo de alta demanda.
- **Software especializado:** Herramientas para la gestión eficiente de contenidos en displays digitales.

El nuevo sitio web de Hikvision no solo se enfoca en la venta de productos, sino que también se posiciona como una fuente de información confiable y actualizada para la industria tecnológica en América Latina.

El portal contará con artículos técnicos, estudios de caso y noticias sobre las últimas tendencias en pantallas y displays:



“Queremos que este portal sea una referencia para quienes buscan soluciones avanzadas y adaptadas a las necesidades del mercado latinoamericano. Además, se actualizará regularmente con contenido relevante que ayude a nuestros socios y clientes a tomar decisiones más informadas”, concluye Fran Sánchez. 🌐



Fran Sánchez
Marcom Director
en Hikvision México

DESCARGA Y ÚNETE A LA COMUNIDAD DE



Hik-Partner Pro

Asistente comercial de seguridad
en la punta de sus dedos.

Noticias y
promociones

Obtenga
ingresos
adicionales

Mantenimiento
remoto



- Accede a información y beneficios exclusivos.
- Utiliza herramientas y funciones para potenciar tu negocio.
- Brinda servicios de valor agregado.



Escanea el **código QR** para
descargar la aplicación
Hik-Partner Pro.



Consulta el portal en
www.hik-partner.com



@HikvisionMx
www.hikvision.com/mx

Hikvision México
sales.mexico@hikvision.com



significa videovigilancia inteligente al alcance de todos

- La firma crece 30% anual y equipa proyectos de videovigilancia en todo el país.
- OwlView permite visión nocturna totalmente a color sin necesidad de infrarrojo.
- All View ofrece vigilancia panorámica 360° ideal para espacios de alto tráfico.

Hoy la seguridad es una necesidad y una exigencia diaria, la tecnología juega un papel determinante. En ese escenario, Uniview (UNV) se ha consolidado como uno de jugadores más importantes en soluciones de videovigilancia. Y en México, su crecimiento es tan acelerado como contundente.

“Estamos creciendo a un ritmo de 150% anual en el país”, afirma Roberto Ávila, gerente comercial de UNV en territorio mexicano.

“Hace más de cinco años decidimos tener presencia directa en México, y hoy nuestros productos están instalados en miles de puntos estratégicos, en diferentes alcaldías de la Ciudad de México hasta megaproyectos en estados como Guanajuato, Sonora, Mérida y Oaxaca”.

Visión a color, incluso en la oscuridad total.

Entre sus desarrollos más disruptivos, destaca OwlView, una tecnología de visión nocturna a color que redefine el estándar de vigilancia. A diferencia de otras marcas, UNV ha desarrollado sensores más grandes que permiten capturar la luz con una gran eficiencia.



“La quinta generación de nuestras cámaras nocturnas permite ver en total oscuridad como si fuera de día”, explica Ávila, “incluso sin infrarrojo, se activa una luz blanca que mantiene la imagen completamente nítida y a color. Es impresionante: parece que estás viendo una escena a las 2 de la tarde”.

Esta tecnología está disponible desde su gama de entrada Easy, hasta sus líneas más robustas Prime y Pro, permitiendo que la innovación sea accesible para todo tipo de cliente, desde un pequeño negocio hasta un centro de monitoreo urbano.

Asimismo, en la línea de productos más recientes, UNV también ha lanzado la tecnología OwlView Ultra, una solución de videovigilancia panorámica con múltiples lentes que permite observar 360° sin puntos ciegos. Esta cámara está pensada para espacios abiertos y de alto tráfico, como estadios, aeropuertos y centros comerciales.

“Este producto combina múltiples ángulos en una sola imagen fluida. Es ideal para aquellos proyectos donde no se puede perder detalle... Y lo mejor, es que su integración con sistemas de gestión de video profesionales (VMS) como Genetec, Milestone, Axxon o ISS nos permite competir al tú por tú con marcas occidentales a un costo significativamente más bajo”.



Soluciones para todo tipo de industria

El portafolio de UNV México abarca sectores tan diversos como:

- Gobierno y ciudades inteligentes (Safe City)
- Retail y centros comerciales
- Banca, educación, hospitales y hoteles
- Logística, estadios y desarrollos habitacionales

Para cada caso, la marca ofrece soluciones adaptadas a las necesidades reales del cliente: cámaras con analítica integrada, detección de rostros, reconocimiento de placas, sistemas PTZ con zoom óptico 45X y gestión integral a través de sus centros de control, que incluyen videowalls, controladores, joysticks y software de gestión.

UNV también ha pensado en las pequeñas y medianas empresas, así como en distribuidores locales. Su línea Uniarch ofrece videovigilancia profesional con excelente desempeño a precios altamente competitivos: “Queremos democratizar el acceso a la seguridad de calidad”, sostiene Ávila.

El éxito de UNV no solo se mide en tecnología, sino en el respaldo que brinda a sus aliados. Su programa UNV Partner Program ofrece certificaciones, equipos demo, descuentos escalonados y soporte técnico. Además, acompaña directamente a los integradores desde la planeación hasta el cierre del proyecto.

“Hemos trabajado con más de 2 mil integradores en México, desde pequeños instaladores hasta firmas especializadas en seguridad pública. Nuestro compromiso es ayudarlos a cerrar proyectos, incluso con desarrollo personalizado vía SDKs o APIs de nuestras cámaras”.

Una marca con visión de futuro. Entre los planes inmediatos de la firma está el fortalecimiento de su presencia en hospitales, universidades y soluciones de control de acceso, así como un impulso en pantallas LED y centros de visualización para vigilancia y monitoreo.

“Estamos aquí para ofrecer soluciones reales, potentes y rentables. Desde una tienda de barrio hasta una ciudad completa, nuestro compromiso es brindar tecnología de videovigilancia accesible, confiable y avanzada”, concluye Roberto Ávila.



Roberto Ávila
gerente de proyectos
en Uniview (UNV)

univ | Todo con **W**ise-ISP

Familia de Producto **owlView**

Ve Maravillas de Noche

owlView

Potencia impresionante, precio increíble

Sensor de hasta 1/1.8", apertura de hasta F1.0, tecnología Wise-ISP

• 2/4/5/8MP



owlView Plus

Noche más nítida, visión más inteligente

Sensor supergrande de hasta 1/1.2", mejorado en imagen, hardware y funciones inteligentes, ideal para más proyectos y escenarios de aplicación

• 4/8MP

owlView PTZ

Navega toda la noche, mantiene alerta y brillante

Imagen mejorada, incluso con zoom, panorámica e inclinación

• 4MP



**Primero & Exclusivo
en Industria**

Protección sin compromisos:

AJAX Systems

Proteger los espacios exteriores siempre es más difícil que proteger los interiores. A menudo es difícil ajustar el ángulo del detector para que no haya ángulos muertos y el aparato no capte zonas innecesarias. Las soluciones que no requieren un mantenimiento constante, como cambiar las pilas cada mes, también valen su peso en oro. Aunque pueda parecer inalcanzable encontrar la solución perfecta, Ajax lo hace posible.

En el Ajax Special Event: Multiverse, la marca presentó MotionCam Outdoor HighMount (PhOD) Jeweller. Con su amplia cobertura, protección avanzada contra sabotajes y filtro de interferencia térmica, está diseñado para que la seguridad en exteriores sea sencilla y fiable. El dispositivo puede instalarse a alturas de 2 a 4 m. Sus nuevas funciones impresionarán a los instaladores y simplificarán su trabajo.

Elemento central de las torres de alarma móviles

El MotionCam Outdoor HighMount (PhOD) Jeweller es muy eficaz cuando se utiliza como componente principal de una torre de seguridad. Es una solución ideal para proteger ubicaciones temporales, como obras, almacenes temporales, espacios para eventos u otras zonas sin acceso a la red eléctrica. Se montan varios detectores en una estructura de soporte para proporcionar una visión de 360 grados. Los detectores de movimiento pueden conectarse al Hub BP Jeweller, alimentarse con una batería externa y combinarse con la sirena exterior.

Esta configuración crea un sistema totalmente autónomo para detectar intrusiones e iniciar alertas que llamen la atención. Ya existen ejemplos de éxito de este tipo de torres de seguridad entre los productos de Ajax Ready desarrollados en colaboración con socios.

No hay por qué preocuparse con la verificación de alarmas

Cuando un intruso entra en la zona protegida, el sistema activa una alarma inmediatamente. Dependiendo de la configuración, la alarma va seguida de una serie de hasta cinco fotos. Las imágenes se muestran en aplicaciones Ajax a los usuarios que tienen los derechos de acceso adecuados. Existen los siguientes tipos de fotoverificación:

- **Foto por alarma:** las imágenes se capturan automáticamente cuando se detecta movimiento.
- **Foto por programación:** las imágenes que se toman a varios intervalos especificados.
- **Foto por escenario:** las imágenes se capturan cuando un dispositivo específico del sistema activa una alarma.
- **Foto bajo demanda:** las imágenes se pueden tomar en cualquier momento o cuando el sistema está armado.

La función de verificación de fotos funciona mejor cuando el dispositivo está instalado en un ángulo de visión óptimo. Para que el instalador disponga de la máxima flexibilidad a la hora de colocar correctamente el detector, es esencial contar con un soporte de montaje fiable.

Instalación sin complicaciones

El proceso de instalación de MotionCam Outdoor HighMount (PhOD) Jeweller es lo más sencillo e intuitivo posible. Este detector de movimiento se instala únicamente con un soporte giratorio metálico duradero.

Solución fiable para montar el detector en paredes exteriores.

En la aplicación Ajax PRO, los instaladores pueden comprobar el campo de visión de la cámara y la zona de detección máxima con la opción Área de detección de movimiento. Permite al instalador hacer una foto de prueba para comprobar el campo de visión de la cámara. La foto de prueba ayuda a ajustar el ángulo de inclinación y la posición horizontal del detector. Compruebe el funcionamiento del aparato y determine con precisión el sector en el que detecta el movimiento.



Protección antisabotaje avanzada

El sabotaje es una de las mayores amenazas para cualquier sistema de seguridad. Cuando se manipula un dispositivo, todo el sistema puede verse comprometido. Por eso, el MotionCam Outdoor HighMount (PhOD) Jeweller cuenta con protección avanzada contra sabotajes para ir un paso por delante de los intrusos. El dispositivo utiliza varias capas de protección contra sabotajes:

- **El magnetómetro** detecta el movimiento o los intentos de mover el dispositivo. Si el campo magnético cambia, se envían notificaciones instantáneas a los usuarios y a la empresa de vigilancia.
- **La alarma antisabotaje** se activa si el dispositivo se separa de la superficie o si se pone en peligro la integridad de su carcasa. El sistema notifica instantáneamente a la compañía de seguridad y a los usuarios sobre cualquier intento de intrusión.
- **El sistema antienmascaramiento** detecta los intentos de bloquear la lente pintando, pegando con cinta adhesiva o colocando un obstáculo delante de la zona sensible del sensor de movimiento del detector.
- **El sondeo periódico** garantiza que el detector permanezca conectado al Hub, mientras que el cifrado de datos protege la información transmitida.

Autonomía excepcional y rendimiento estable en frío y calor

El detector funciona hasta tres años con las pilas preinstaladas. Esto reduce la necesidad de mantenimiento frecuente y disminuye los costes de explotación. También existe la opción de conectar una fuente de alimentación externa de 12-24 V. Cuando se conecta la alimentación externa, las pilas preinstaladas se utilizan como reserva. Esto garantiza el funcionamiento ininterrumpido del aparato.

El detector funciona a temperaturas comprendidas entre -25 °C y +60 °C. Es eficaz tanto en condiciones de calor extremo como de frío glacial. La carcasa con clasificación IP55 protege el dispositivo del polvo y el agua. La cubierta protectora preinstalada proporciona una protección adicional contra la lluvia y la nieve. Esto hace que el detector sea adecuado para propiedades expuestas a condiciones climáticas adversas. 🌧️

Mujeres en tecnología, transformando la industria:



- *Gracias a políticas de igualdad y programas de capacitación y mentoría, la marca ha logrado consolidar un entorno donde las mujeres pueden crecer profesionalmente y asumir mayores responsabilidades dentro de la organización.*

El 8 de marzo se conmemora el Día Internacional de la Mujer, una fecha clave para reconocer los avances en equidad de género y visibilizar los retos a los que las mujeres aún se enfrentan. No obstante, en el sector de la tecnología en seguridad, las mujeres han ganado cada vez más espacios de liderazgo, demostrando su talento y compromiso con la innovación.



Mariana Ramírez, gerente de Marketing para Latinoamérica de Axis Communications.



Denith García, gerente de Ventas Internas de Axis Communications.

En este contexto, Axis Communications se ha posicionado como una empresa que promueve la inclusión y el empoderamiento femenino dentro de la industria. En Latinoamérica, la empresa de origen sueco cuenta con el 54% de mujeres en posiciones de liderazgo o gerenciales, lo que destaca su compromiso con la equidad y el desarrollo profesional de su equipo femenino.

Uno de los pilares de la empresa en la región es la promoción de líderes dentro de su organización. Actualmente, el 25% de las mujeres en la empresa ostentan el título de "Team Lead" o son responsables de equipos, lo que evidencia la confianza de la compañía en su talento y capacidad de gestión.

"Estas iniciativas de Axis Communications han hecho que las mujeres hayan sido reconocidas en sus roles dentro de la organización y permiten el apoyo continuo para el crecimiento integral de la mujer, como la equidad de género. El ejemplo de esto es el nombramiento como embajadoras del Women in Security Forum (WISF) de la Security Industry Association (SIA), a Denith García, gerente de Ventas Internas y a una servidora", afirmó Mariana Ramírez, gerente de Marketing para Latinoamérica.

Estos datos son relevantes en una industria históricamente dominada por hombres, donde la representación femenina en roles estratégicos aún es limitada. Gracias a políticas de igualdad y programas de capacitación y mentoría, Axis Communications ha

logrado consolidar un entorno donde las mujeres pueden crecer profesionalmente y asumir mayores responsabilidades dentro de la organización. Además del liderazgo, el impacto de las mujeres en LATAM se extiende a áreas clave del negocio. Dentro de la empresa, el 30% de las empleadas forman parte de puestos técnico-comerciales, desempeñando funciones esenciales para la innovación y el crecimiento de la misma.

Otro aspecto fundamental en el impulso del talento femenino es la representación generacional. Un 36% de las mujeres que conforman el equipo de Axis pertenecen a la generación millennial o centennial, lo que indica una apuesta por el talento joven y el desarrollo de nuevas habilidades dentro de la organización.

El compromiso de la empresa con la equidad de género también se refleja en la inversión en su talento femenino. Tan solo en 2024, la empresa destinó el 55% de su presupuesto de desarrollo a mujeres, consolidando así su apuesta por la capacitación, el crecimiento profesional y el fortalecimiento de sus habilidades clave.

"Este trabajo que se desarrolla desde la compañía, es el reflejo al compromiso de reducir la brecha de género en la industria de seguridad y tecnología, con el objetivo de construir un entorno en el que las mujeres puedan liderar y transformar este sector" asegura Denith García, gerente de Ventas Internas.

Esta iniciativa refuerza el mensaje, de que la inclusión no es solo una meta, sino una acción constante dentro de la compañía. En este Día de la Mujer, Axis Communications no solo celebra los logros de su equipo femenino, sino que reafirma su compromiso con una industria más equitativa y diversa, donde las mujeres sigan siendo protagonistas del cambio. 🌟



En América Latina, la transformación hacia edificios inteligentes está ganando impulso. Seguido por la creciente necesidad de modernizar espacios corporativos y gubernamentales, se proyecta que este mercado alcance un valor de 16,47 mil millones de USD en 2032 en la región, según un estudio de Informes de Expertos. Este aumento responde a desafíos como la adaptación a modelos de trabajo híbrido, la optimización de recursos y el cumplimiento de objetivos de sostenibilidad.

En este contexto, los estándares abiertos juegan un papel estratégico. En 2020, el OSDP (Open Supervised Device Protocol), se convirtió en un estándar reconocido por la Comisión Electrotécnica Internacional (IEC), desarrado por la SIA, para mejorar la integración entre productos de control de acceso y seguridad, este protocolo abierto está impulsando innovaciones en el sector inmobiliario corporativo, especialmente en el ámbito de los edificios inteligentes, donde la conectividad y la interoperabilidad son fundamentales para su funcionamiento.

Estándares abiertos: la base para una interoperabilidad eficaz

La interoperabilidad es el corazón de los edificios inteligentes modernos, y los estándares abiertos son el motor que hace posible esta conexión fluida entre tecnologías de diferentes proveedores; estos protocolos permiten que los sistemas trabajen en conjunto, eliminando las barreras impuestas por soluciones propietarias.

Transformación de espacios corporativos:



- *El poder de los estándares abiertos para edificios inteligentes*

El protocolo OSDP fue desarrollado para garantizar una integración eficiente entre dispositivos de control de acceso y soluciones de seguridad, independientemente de la marca o el fabricante. Aprovechando las últimas tecnologías de cifrado ofrecidas por OSDP (que garantizan la seguridad), los sistemas pueden combinarse fácilmente para satisfacer necesidades comerciales, operativas y laborales específicas. Esto se potencia si los fabricantes ofrecen APIs abiertas y kits de desarrollo de software para proveedores de soluciones e instaladores de terceros, lo que facilita la integración y el despliegue del sistema.

De este modo, la adopción de estándares abiertos tiene un impacto directo en el desarrollo de edificios inteligentes al permitir que múltiples sistemas, como control de acceso, HVAC, iluminación y gestión de espacios, se integren en una sola plataforma, mejorando la experiencia del usuario y optimizando la operación de las instalaciones al reducir costos funcionales y simplificar su mantenimiento.

Al integrar el control de acceso con este amplio ecosistema (particularmente mediante el uso de teléfonos inteligentes que aprovechan Apple y Google Wallets como dispositivo principal) se mejora la seguridad de los ocupantes y se transforma radicalmente

la experiencia del usuario, tanto para el personal como para los visitantes. El interés en estas soluciones queda evidenciado en el Informe sobre el estado del control de acceso físico 2024, de HID, según el cual, el 43 % de los encuestados identificó a los edificios inteligentes y los espacios de trabajo flexibles como una de las tres tendencias principales que están transformando la industria del control de acceso, solo superadas por la implementación de tecnologías sin contacto (48 %) y el acceso mediante aplicaciones móviles (44 %). Además, cerca del 32 % de los participantes destacó la integración con otras funciones empresariales como una de las tendencias más relevantes del sector. Además, al eliminar la dependencia de un único proveedor, los estándares abiertos brindan a las organizaciones mayor libertad para escalar sus sistemas o adaptarse a nuevas necesidades tecnológicas, sin incurrir en costos significativos de reemplazo. En mercados en crecimiento como el latinoamericano, esta flexibilidad es básica para garantizar que las inversiones en tecnología puedan evolucionar junto con las demandas empresariales.

Tecnología de punta para aumentar la eficiencia corporativa

El avance hacia estándares abiertos sustenta la convergencia tecnológica en la región, haciendo que el control de acceso pase de ser únicamente un medio para evitar el ingreso de personas no autorizadas, a convertirse en un aspecto imprescindible para el uso eficiente de los edificios.

El mercado actual ofrece tecnologías como Identity Positioning, que transforma la gestión de espacios y recursos en las empresas. Esta solución, clave en el crecimiento de edificios inteligentes en América Latina, mejora la eficiencia operativa y optimiza recursos mediante el uso de dispositivos móviles y credenciales digitales. Permite rastrear en tiempo real la ubicación de empleados sin afectar su privacidad ni recolectar datos personales. Identity Positioning monitorea la ocupación de espacios, integrándose con sistemas como HVAC e iluminación para reducir costos energéticos. Además, fortalece la seguridad con controles de acceso basados en ubicación y autorizaciones. 📍



Luis Yanez
gerente de desarrollo
de negocios SaaS de HID.

Guía sobre tecnologías de reconocimiento facial:



- *Muchas soluciones modernas se centran en el análisis estadístico y el reconocimiento de patrones, en lugar de la identificación individual.*

En el dinámico panorama actual de la seguridad en América Latina, el reconocimiento facial se ha convertido en un término de moda que a menudo genera preocupaciones sobre la privacidad y la protección de datos. Sin embargo, muchos profesionales de la seguridad pueden no ser conscientes de que el ‘reconocimiento facial’ es un término general que abarca diversas tecnologías, cada una con aplicaciones específicas e implicaciones en materia de privacidad.

Veamos qué significan realmente estas tecnologías para los distribuidores, integradores y usuarios finales de sistemas de seguridad.

En esencia, la tecnología de reconocimiento facial re-identifica o verifica a las personas en función de sus rasgos faciales, que en este caso se utilizan como datos biométricos. Sin embargo, no todos los sistemas biométricos se basan en características únicas de identificación, algunos analizan atributos generales, como el estilo de vello facial o marcas distintivas; estos rasgos, conocidos como biometría blanda, pueden contribuir a la identificación, pero no son lo suficientemente específicos como para verificar de manera única la identidad de una persona por sí solos. Si bien las aplicaciones del reconocimiento facial van desde el control de acceso hasta la prevención del crimen y la investigación, su implementación varía ampliamente según las necesidades específicas. Los sistemas modernos incorporan sólidas medidas de seguridad, como el cifrado de datos y estrictas políticas de retención, para garantizar el manejo responsable de cualquier información personal identificable (PII).

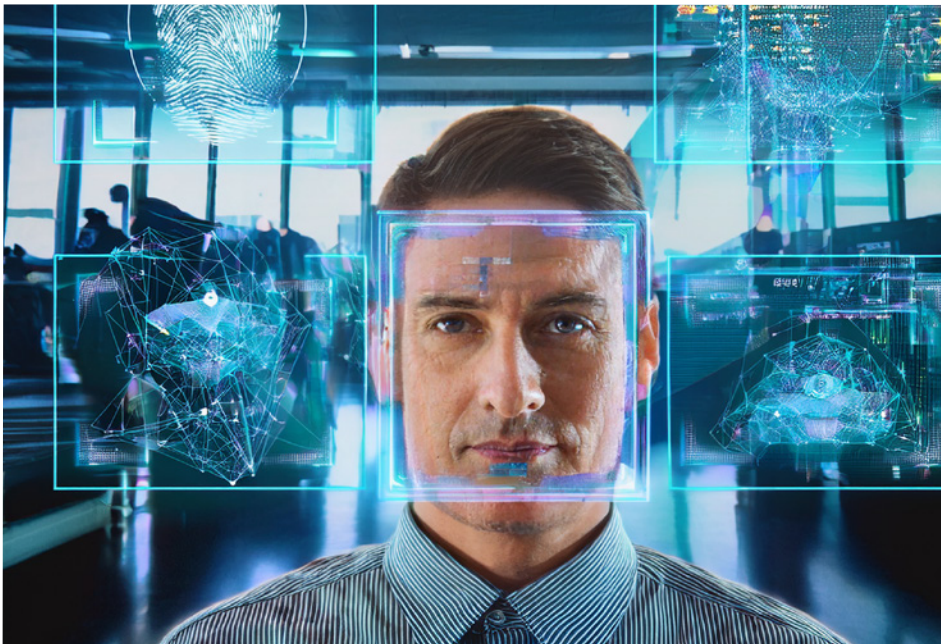
De acuerdo con un estudio de informes de expertos, el mercado de la biometría en América Latina experimentará un crecimiento anual compuesto del 12,30 % entre 2024 y 2032 y, ahora, con el apoyo de la Inteligencia Artificial, se espera que avance aún más.

Comprensión de las tecnologías clave y sus aplicaciones el mundo del reconocimiento facial abarca diversas tecnologías, cada una con propósitos específicos. A continuación, se presenta un desglose detallado de estas tecnologías y sus aplicaciones en el mundo real.

Tecnologías Clave de Reconocimiento Facial

Verificación Facial (1:1): Compara un rostro con una identidad declarada. Ejemplo: Control de pasaportes en aeropuertos.

Identificación Facial (1 a muchos): Busca un rostro en una base de datos. Ejemplo: Localizar a un niño desaparecido en un aeropuerto.



Re-identificación Facial (Muchos a muchos): Rastrea movimientos anónimos entre ubicaciones. Ejemplo: Análisis de tiempo en secciones de una tienda.

1. **Reconocimiento en tiempo real:** Procesa video en vivo para alertas inmediatas. Ejemplo: Detectar personas vetadas en eventos masivos.
2. **Reconocimiento posterior al evento:** Analiza grabaciones tras un suceso. Ejemplo: Identificar sospechosos en videos de seguridad.
3. **Biometría:** Usa rasgos únicos (rostro, huella, iris) para identificación. Ejemplo: Desbloqueo de teléfonos o acceso seguro.
4. **Biometría dura:** Rasgos únicos como iris o huellas. Ejemplo: Seguridad aeroportuaria.
5. **Biometría blanda:** Atributos generales (altura, complexión) para apoyo. Ejemplo: Identificación parcial en videos borrosos.
6. **Similitud de apariencia:** Rastrea por ropa o accesorios, no biométrica. Ejemplo: Análisis de clientes en tiendas.
7. **Detección de prueba de vida:** Verifica que sea una persona real. Ejemplo: Pagos móviles con gestos.
8. **Representación matemática:** Convierte rostros en números no reversibles. Ejemplo: Almacenamiento seguro sin imágenes reales.

Privacidad y seguridad

Los sistemas modernos protegen datos con:

- Aislamiento y cifrado de plantillas biométricas.
- Anonimización en representaciones matemáticas.
- Eliminación automática tras uso.
- Controles segmentados para acceso seguro.



Barry Norton,
vicepresidente de IA
centrada en el ser
humano para
Milestone Systems.

Daños graves por la falta de regulación en prevención de incendios en México y LATAM

- *Presentó Latam PCI, AMRACI y CONAPCI, estudio del estado de la regulación sobre Protección Contra Incendios en Latinoamérica.*
- *La protección contra incendio es una actividad que tiene un impacto transversal en todas las actividades económicas de los sectores productivos.*

Más del 50% de los incendios en el mundo suceden en Latinoamérica por falta de una regulación adecuada. México y América Latina en general se encuentran en grave peligro de sufrir serias tragedias provocadas por incendios urbanos, señala el estudio de la Red Latinoamericana de Protección contra Incendios (Latam PCI), la Asociación Mexicana de Rociadores Automáticos Contra Incendios (AMRACI) y el Consejo Nacional de Protección Contra Incendio (CONAPCI).

Evento transmitido en vivo por streaming, realizado simultáneamente en 12 países miembros de Latam PCI, se presentó desde México el segundo estudio sobre este tema. En él se destacó la ausencia de un marco regulatorio común entre las naciones de la región, lo que plantea desafíos significativos. Además, ofreció un análisis detallado del panorama normativo en diversos países, permitiendo comprender los avances y obstáculos que enfrenta nuestra industria.

En el estudio, México resultó último lugar de clasificación de ocupaciones y en sexto por debajo de países como Argentina, Brasil, Perú y Ecuador, en medios de protección contra incendio dejando ver la brecha pendiente que existe en nuestro país para la salvaguarda de la vida de las personas y la protección de la infraestructura.

La protección contra incendio es una actividad que tiene un impacto transversal en todas las actividades económicas de los sectores productivos debido a los distintos riesgos que, por la naturaleza de cada proceso, materiales almacenados o simplemente por la cantidad de personas en un mismo lugar, representan un verdadero riesgo para la salvaguarda de la vida de las personas, continuidad de operaciones y por tanto a la competitividad del país.

En los últimos años México ha avanzado en muchos aspectos: crecimiento demográfico, mayor infraestructura, nuevos métodos constructivos, incorporación de novedades tecnológicas, lo que representa mayores riesgos; sin embargo, no así los avances normativos y los incendios han ido en aumento. El estudio también señala la importancia de avanzar hacia un marco regulatorio más sólido, unificado y adaptado a la realidad de cada país.

Dicho estudio señala la disparidad en la regulación que existe actualmente. Por ejemplo, señala que:

- [El gran incendio de Valparaíso](#) (Chile, 2014) que causó 15 muertos, dejó a 11 mil personas sin hogar y destruyó más de 2.500 viviendas.
- [El fuego en la discoteca Kiss en Santa María, Brasil](#) (27 de enero de 2013), provocó la muerte de 242 personas y dejó más de 600 heridos.
- [El siniestro en el hotel República Cromañón](#), en Buenos Aires, Argentina (30 de diciembre de 2004), dejó 194 muertos y más de 1.400 heridos.
- [La conflagración del supermercado Ycuá Bolaños en Asunción](#), Paraguay (1 de agosto de 2004) con un saldo devastador de 396 muertos y más de 500 heridos.
- [Todas las quemas forestales en la Amazonia](#) que alcanzaron niveles críticos en 2019, con más de 74 mil focos de fuego.
- [El incendio de la Guardería ABC](#) que ocurrió el 5 de junio de 2009 en Hermosillo, Sonora, México. En el incendio fallecieron 49 niños y 106 resultaron heridos, todos de entre cinco meses y cinco años.

Tales tragedias se deben a la falta de armonización: la ausencia de un marco regulatorio común entre los países que limita el intercambio de buenas prácticas y debilita la efectividad de las estrategias regionales.

Ante ello, Latam PCI y sus asociados AMRACI y CONAPCI, hacen un llamado al Congreso de la Unión, a las secretarías de economía, del Trabajo y Previsión Social, así como a la Coordinación Nacional de Protección Civil, a sumar esfuerzos y voluntad política para generar políticas públicas que garanticen a nivel nacional la “Seguridad Humana y Protección de Incendios”, a través de una legislación moderna, clara, prescriptiva que pueda ser inspeccionada oportunamente.

Considera también urgente la realización de campañas educativas a gran escala, orientadas a concientizar a la población sobre la importancia de la prevención y sus beneficios, promoviendo una cultura de seguridad contra incendios. Están AMRACI-CONAPCI listos para colaborar en esta importante tarea autoridades, instituciones y expertos de la industria para construir un futuro más seguro para todos.



Prevención inteligente:



- **Tecnología que detecta incendios antes de que sea tarde.**
- **Los incendios urbanos en México tienen diversas causas, desde materiales inflamables en la construcción hasta fallas eléctricas y accidentes involuntarios.**

En un mundo donde el cambio climático y el crecimiento urbano incrementan el riesgo de incendios, proteger hogares y empresas se ha vuelto una prioridad. En este escenario, TVCenlínea.com, especialista en soluciones tecnológicas de seguridad, refuerza su oferta con sistemas inteligentes contra incendios en alianza con Dahua, ofreciendo sistemas innovadores que previenen siniestros y garantizan la seguridad de personas y activos.



En México, los incendios urbanos tienen diversas causas, desde materiales inflamables en la construcción hasta fallas eléctricas y accidentes involuntarios.

De acuerdo con el Consejo Nacional de Protección contra Incendios (CONAPCI), el 55.6% de estos incidentes ocurren en viviendas, 34.1% en comercios y usos mixtos, y el resto en hoteles, oficinas e industrias.

Así, la tecnología juega un papel clave en la prevención y respuesta ante incendios. “En TVCenlínea.com, no solo vendemos productos, ofrecemos tranquilidad. Nuestra misión es poner la tecnología al servicio de la seguridad para que nuestros clientes tengan la confianza de que están protegidos”, señaló Baltazar Zúñiga, fundador y director de ventas.

La prevención de incendios va más allá de la vigilancia tradicional. El mercado de sensores de seguridad en América del Norte alcanzará los 3.8 mil millones de dólares en 2029, con una tasa de crecimiento anual del 6.13% según cifras de Mordor Intelligence. Este crecimiento refleja la creciente adopción de herramientas como las de TVC y Dahua, que integran alarmas interconectadas, conectividad inalámbrica y monitoreo remoto para detectar incendios en sus primeras etapas y activar respuestas automáticas.

Desde el hogar hasta grandes corporativos, estas alternativas permiten actuar de inmediato. Los sistemas de CCTV de Dahua facilitan el monitoreo en tiempo real, mientras que la sincronización con alarmas inteligentes permite alertar simultáneamente a todos los ocupantes de un inmueble. Además, la plataforma Wisualarm, basada en la nube, brinda a propietarios y administradores la capacidad de gestionar dispositivos y visualizar datos desde cualquier ubicación.

Para edificios empresariales, contar con tecnología direccionable y sistemas integrados de CCTV y alarma contra incendios es fundamental. Estas tecnologías permiten localizar con precisión el origen del siniestro, minimizar daños y reducir tiempos de respuesta. Además, ofrecen escalabilidad flexible para adaptarse al crecimiento de la infraestructura y funciones de autoprueba que optimizan el mantenimiento.

“No se trata solo de cumplir con regulaciones, sino de proteger lo que realmente importa: la gente, los activos y la continuidad del negocio”, agregó Zúñiga.



Primer Foro Internacional de Factores Humanos:

- **SafeStart capacita a más de cuatro millones de trabajadores en 60 países**
- **con una metodología centrada en el factor humano.**
- **El 95% de los accidentes laborales tienen origen en errores por prisa, fatiga o frustración.**

SafeStart capacita a más de cuatro millones de trabajadores en 60 países con una metodología centrada en el factor humano. El 95% de los accidentes laborales tienen origen en errores por prisa, fatiga o frustración.

Una metodología nacida hace más de tres décadas ha ganado fuerza al poner el foco donde pocos lo hacen: en la mente y el comportamiento humano, inmerso en un mundo empresarial cada vez más automatizado, donde los indicadores de seguridad laboral suelen estar dominados por protocolos, tecnología y procedimientos.

SafeStart International, con presencia en más de 60 países y una trayectoria de más de 30 años, ha capacitado a más de 4 millones de trabajadores en más de cuatro mil empresas a nivel global. Su propuesta: reducir los accidentes laborales, entendiendo primero por qué los humanos cometemos errores.

“Nosotros vamos más allá de las políticas y herramientas. Trabajamos sobre esos momentos de inatención que pueden derivar en un accidente. El error humano no es un problema técnico, es un problema humano, y se puede reducir con conciencia y entrenamiento”, afirma Adrián Javier Monsiváis, Territory Manager y Team Leader de SafeStart para México.

La metodología, desarrollada por el canadiense Larry Wilson, CEO y fundador de SafeStart, se ha traducido a más de 33 idiomas y ha sido implementada con éxito en sectores como minería, manufactura, energía, logística, salud y agroindustria. El programa parte de una pregunta tan simple como poderosa: ¿Por qué una persona con experiencia, capacitada, comete un error que puede costarle la vida?

La respuesta, según Wilson, está en cuatro estados mentales que se repiten una y otra vez en los accidentes: prisa, frustración, fatiga y complacencia. Estos influyen en la toma de decisiones y en la capacidad de atención, factores críticos para evitar lesiones.

“Siempre proyectamos crecimiento, pero lo hacemos con estrategias de inversión que permitan a todo tipo de empresas acceder al programa. Hemos duplicado proyectos desde 2023”, añade Monsiváis.



SafeStart no limita su alcance a las instalaciones de trabajo, ya que su visión es integral y continua. La seguridad no termina al salir del turno, también se trata de conducir con atención, cuidar a la familia, prevenir errores en casa.

Según datos de la propia organización, el 95% de los accidentes, dentro y fuera del trabajo, tienen como causa el error humano. Por ello, la metodología no sólo beneficia a la empresa, sino también al trabajador y su entorno familiar.

México, epicentro de la conversación. Como parte de su expansión en América Latina, SafeStart International celebrará el próximo 15 y 16 de mayo en la Ciudad de México, el primer Foro Internacional de Factores Humanos, encuentro de dos días enfocado en líderes de seguridad, calidad, mantenimiento, recursos humanos y operaciones. “El foro está dirigido a quienes toman decisiones estratégicas en las empresas. Queremos hablar de neurociencia, cambio de paradigmas y comunicación interna, pero sobre todo queremos cambiar la forma en que vemos los errores”, explica Monsiváis.

El evento contará con ponencias magistrales de expertos internacionales, entre ellos el propio Larry Wilson. También se realizarán mesas de trabajo, paneles de discusión y se entregará un reconocimiento a una empresa destacada por la implementación exitosa de la metodología. “México es un mercado estratégico. Hay inversión extranjera, crecimiento constante y también nuevos retos. Este foro busca dar respuesta a esas necesidades con un enfoque moderno y humano”, concluye el ejecutivo.

La firma propone una nueva narrativa: la del liderazgo consciente, el error como parte natural del ser humano y la prevención como cultura cotidiana. Porque al final, como recuerda uno de los principios del programa, la seguridad no es un manual, es una decisión que tomamos todos los días. 🌱



Adrián Javier Monsiváis
Territory Manager y Team Leader
de SafeStart para México.

Centro Nacional de Preparación para Incidentes y Estrategia para la ciberseguridad (NISC) de Japón

- La actualización de esta política en 2022 y un compromiso continuo con la cooperación internacional, Japón refuerza su posición como un actor clave en la seguridad del ciberespacio.



Dr. Gustavo Guzmán Hernández
gguzmanh01@gmail.com
Tw @GustavoG_Kc
México

Articulista invitado

Como parte de los esfuerzos y estrategias de los estados nación, para proteger las operaciones cibernéticas y sus infraestructuras críticas y digitales, los países están transformando procesos y metodologías para el desarrollo de capacidades. Desde los CSIRT's (Cyber Security Incident Response Team) y los CERT's (Community Emergency Response Team) se liderean las estrategias de seguridad cibernética de las naciones. En esta ocasión, hablaremos sobre el NISC (National Center of Incident readiness and Strategy for Cybersecurity) de Japón.

El NISC de Japón, como otros centros nacionales alrededor del mundo, ha reconocido en su momento actividades no autorizadas dentro de sus sistemas. En LATAM dos de los casos más recientes fueron el caso de la Secretaría de la Defensa Nacional de México (SEDENA) y el caso del Comando Conjunto de las Fuerzas Armadas del Perú, ambos en el 2022.

El NISC es un organismo de gran importancia en la seguridad de Japón, ya que tiene como objetivo principal coordinar y promover políticas de ciberseguridad a nivel nacional, actuando como punto focal en la colaboración intra-gubernamental y fomentando alianzas entre la industria, el mundo académico y los sectores público y privado.

Entre sus funciones destacadas encontramos: Formulación de estrategias de ciberseguridad: Desarrolla la Estrategia de Ciberseguridad de Japón, que establece las directrices básicas de las políticas de ciberseguridad para aproximadamente tres años. Esta estrategia busca garantizar un ciberespacio libre, justo y seguro, contribuyendo al desarrollo socioeconómico sostenible y a la seguridad nacional.

Protección de infraestructuras críticas: Implementa políticas para asegurar la continuidad de servicios esenciales, realizando ejercicios transversales anuales que verifican y mejoran las capacidades de respuesta ante incidentes de las organizaciones involucradas.



- **Cooperación internacional:** Participa en reuniones y talleres con países de la ASEAN y otras naciones para fortalecer la colaboración en materia de ciberseguridad, compartiendo información y mejores prácticas.
- **Operación del GSOC:** Coordina el Equipo de Coordinación de Operaciones de Seguridad.
- **Gubernamental (GSOC):** que monitorea y responde rápidamente a incidentes de seguridad en las redes gubernamentales, operando las 24 horas del día.

El NISC desempeña un papel clave en la ciberseguridad gubernamental de Japón, estableciendo los Estándares Comunes sobre Medidas de Seguridad de la Información como referencia obligatoria para todas las agencias y supervisando su cumplimiento mediante auditorías. Además, opera el Equipo de Coordinación de Operaciones de Seguridad Gubernamental (GSOC), un sistema de monitoreo en tiempo real que no solo detecta y analiza comunicaciones maliciosas en las redes gubernamentales, sino que también facilita el intercambio de información entre entidades. Ante amenazas como señales sospechosas o malware, el GSOC emite alertas y proporciona asesoramiento inmediato, fortaleciendo la resiliencia cibernética del gobierno japonés.

Consideraciones finales

El NISC se ha consolidado como un pilar fundamental en la ciberseguridad de Japón, garantizando la resiliencia de sus infraestructuras críticas y promoviendo un entorno digital seguro a nivel global. Desde 2005, su Política de Ciberseguridad para la Protección de Infraestructuras Críticas ha servido como hoja de ruta para fortalecer la defensa de 14 sectores estratégicos mediante cinco ejes clave: respuesta ante incidentes, principios de seguridad, intercambio de información, gestión de riesgos y fortalecimiento estructural.

Con la actualización de esta política en 2022 y un compromiso continuo con la cooperación internacional, Japón refuerza su posición como un actor clave en la seguridad del ciberespacio, colaborando con aliados y organizaciones afines para enfrentar amenazas emergentes con estrategias innovadoras y coordinadas. 🌐

Referencias:

National Center of Incident Readiness and Strategy for Cybersecurity. (n.d.). National Center of Incident Readiness and Strategy for Cybersecurity. Retrieved March 9, 2025, from <https://www.nisc.go.jp/eng/index.html>

Seguridad en impresión: La clave para proteger datos empresariales

- *A través de un enfoque integral, ambas compañías garantizan que los equipos de impresión sean un punto seguro dentro de la infraestructura tecnológica de las organizaciones.*
- *Solución que eleve la eficiencia de tu empresa mientras refuerza la seguridad de tu información.*

En un mundo cada vez más digital e interconectado, la seguridad de la información se ha convertido en una prioridad para las organizaciones. La creciente sofisticación de los ataques cibernéticos y la facilidad con la que pueden ejecutarse ponen en riesgo datos sensibles, afectando la operatividad y reputación de las empresas. A pesar de ello, muchas organizaciones solo reaccionan ante las amenazas después de sufrir una brecha de seguridad.

Ante este panorama, Alldora Latinoamérica y Lexmark, han unido fuerzas para ofrecer Servicios Administrados de Impresión (MPS) que no solo optimizan la gestión documental, sino que también refuerzan la protección de la información empresarial. A través de un enfoque integral, ambas compañías garantizan que los equipos de impresión sean un punto seguro dentro de la infraestructura tecnológica de las organizaciones, reduciendo vulnerabilidades y minimizando riesgos cibernéticos.



Impresión segura desde la raíz

La seguridad en la impresión va más allá de restringir accesos o encriptar documentos. Alldora y Lexmark adoptan un enfoque de protección en tres niveles:

- **Seguridad del dispositivo:** Equipos con mecanismos avanzados de autenticación, control de acceso y configuraciones protegidas para evitar alteraciones no autorizadas.

- **Seguridad de la flota:** Monitoreo y administración centralizada de todos los dispositivos para garantizar que cumplan con los estándares de ciberseguridad.
- **Seguridad en la red:** Protección de la información desde su origen hasta su destino, asegurando la integridad y confidencialidad de los datos que circulan a través de los sistemas de impresión.

Las impresoras y multifuncionales Lexmark no solo destacan por su capacidad de automatizar flujos de trabajo, sino también por su robustez en seguridad. Cuentan con configuraciones avanzadas que protegen el dispositivo como si fuera un servidor o una PC, asegurando que solo usuarios autorizados puedan acceder y gestionar la información.

Estándares de seguridad

Como parte del enfoque integral en seguridad, Lexmark cumple con certificaciones reconocidas a nivel gubernamental e industrial. Estas certificaciones han sido validadas por organismos independientes de prestigio, garantizando el cumplimiento de los más altos estándares en la protección de la información.



Regulación y cumplimiento en seguridad

El equipo de seguridad de Lexmark se encarga de garantizar la confidencialidad, integridad y disponibilidad de los datos. Su enfoque integral permite a los clientes proteger información sensible mediante soluciones seguras, certificadas y adaptadas a diversos sectores.

Protección inteligente para un entorno digital seguro

Hoy más que nunca, las empresas necesitan soluciones tecnológicas que no solo optimicen sus procesos, sino que también protejan su activo más valioso: la información.

Si buscas una solución que eleve la eficiencia de tu empresa mientras refuerza la seguridad de tu información, te invitamos a conocer más sobre cómo Alldora y Lexmark pueden ayudarte a lograrlo.

<https://www.alldora.com.mx/>
https://www.lexmark.com/es_mx.html



ACOMPÁÑANOS A NUESTRAS REUNIONES MENSUALES

14 ENERO		11 FEBRERO		4 MARZO		1 ABRIL	TU MARCA AQUI
6 MAYO						24 JUNIO	
8 JULIO						5 AGOSTO	TU MARCA AQUI
2 SEPTIEMBRE						7 OCTUBRE	
11 NOVIEMBRE	TU MARCA AQUI					2 DICIEMBRE	

AFÍLIATE Y SÉ PARTE DE NUESTRA COMUNIDAD

ASIS
INTERNATIONAL

**MEMBRESÍA
INTERNACIONAL**

125 USD

ASIS
INTERNATIONAL | CAPÍTULO
MÉXICO 217

**MEMBRESÍA
CAPÍTULO MÉXICO**

\$5,650 MXN

ASIS
INTERNATIONAL | CAPÍTULO
MÉXICO 217

**RENOVACIÓN
CAPÍTULO MÉXICO**

\$3,750 MXN

Contáctanos en Linktree*



#ASISxTlyPARATI

Los costos de seguridad de TI son una preocupación en las corporaciones

- *Asociación consolidada como la única organización empresarial que exige y ofrece estrictos estándares técnicos, de calidad y operatividad a sus socios.*
- *AMBA ha resuelto exitosamente toda clase de necesidades de seguridad de los compradores mexicanos e incluso del exterior.*



Dr. Antonio Celso Ribeiro Brasileiro,
PhD, Doctor en Filosofía en Ciencias de la Seguridad
Internacional, Cambridge International University,
Inglaterra. Presidente de Brasileiro INTERISK.
abrasiliano@brasiliano.com.br
Brasil

Articulista Invitado

São Paulo, Brasil.- El Informe de Costos de Seguridad de TI de Kaspersky revela que la protección de entornos tecnológicos complejos, en términos de costos, es la mayor preocupación relacionada con la seguridad de TI en casi la mitad de las empresas (48%) en Brasil. El estudio también muestra que los problemas con la protección de datos, como la exposición de la información corporativa o de los clientes (38%), seguidos de la pérdida de productividad debido al tiempo de inactividad (36%), son la segunda y tercera preocupaciones más importantes, respectivamente.

Según el informe, el costo de la protección de entornos tecnológicos complejos (48%) es la mayor preocupación corporativa causada por la ineficacia de la seguridad informática en las empresas brasileñas. Según los encuestados, los dos principales factores que derivan de este problema son los incidentes con dispositivos conectados que no son computadoras, como los sistemas de control industrial y el Internet de las Cosas (IoT); seguido de la dificultad de gestionar la seguridad en diferentes plataformas. Es decir, las empresas no cuentan con un Sistema Integrado de Seguridad de la Información, Cibernética y Privacidad, llamado SISICP, para un mayor control y efectividad.

La integración de las tres funciones da como resultado una mayor adaptación y rapidez en las respuestas, en mi opinión esta es una de las grandes debilidades del mercado. Esto supondría un cambio de paradigma. También porque la Norma ISO de la Familia 27000 ya se ha integrado como una mejor práctica, por lo que el mercado debería seguir este vector de seguridad.

La exposición/pérdida de datos corporativos o de clientes (39%) es el segundo mayor “dolor de cabeza” para los empresarios brasileños. Entre los principales problemas de TI que generan este desafío, los encuestados indicaron la pérdida física de dispositivos o medios que contienen datos, seguida de la fuga de sistemas internos causada por ciberataques o problemas ocurridos por los empleados, como errores intencionales o negligencia de la política de ciberseguridad.

La tercera mayor preocupación brasileña debido a la ineficacia de la seguridad informática es el tiempo de inactividad/pérdida de productividad, reportado por el 36% de las empresas. Las empresas se enfrentan a este problema principalmente debido al largo período requerido para detectar, responder y neutralizar las amenazas.





La innovación tecnológica ha venido a simplificar la operación, pero siempre ha hecho más compleja la infraestructura de la organización. En los últimos años, las amenazas y los ataques también se han vuelto más complejos. Cualquiera que piense que la seguridad digital corporativa no seguiría el mismo camino se equivoca. Hoy en día, los firewalls y los antivirus por sí solos no son suficientes para garantizar la protección de las empresas. Es por ello que surgen las nuevas tecnologías y aún es necesario contar con profesionales capacitados y buenos procesos para cubrir cada detalle de la infraestructura.



La evidencia de que las organizaciones no protegen adecuadamente sus operaciones es el miedo a las fugas de datos y al alto tiempo de inactividad. Una buena estrategia de ciberseguridad tiene como objetivo asegurar el funcionamiento de la empresa y mitigar los impactos de los ataques a la misma.

Si hay ineficiencia o pérdida, significa que hay fallas en la protección. Esta relación directa pone de manifiesto que vale más la pena invertir en prevención que en remediación. Para ello, tiene que existir un proceso estructurado de gestión de riesgos, donde la primera premisa sería identificar sus vulnerabilidades y riesgos en las diversas actividades de la empresa. La prevención y mitigación de los problemas mencionados en la encuesta es que las empresas evolucionen su visión en seguridad informática, integrada con la ciberseguridad y la privacidad.

No debería haber una segregación de la función de seguridad de las tres disciplinas, ya que la dirección estratégica es garantizar la continuidad de la operación. Las empresas, a través de un SISICP, contarían con un proceso de gestión de riesgos en TI, Cibernética y Privacidad, con métricas específicas, hablar el mismo lenguaje que la integración redundaría en mayor asertividad, mayor anticipación de riesgos y, como consecuencia, una mayor respuesta adaptada a problemas reales.

No es posible resolver problemas complejos de forma sencilla. Por lo tanto, el primer paso es mapear cómo se creó la infraestructura de la empresa y evaluar si el modelo actual es el mejor desde el punto de vista de la seguridad. Teniendo en cuenta las áreas industriales y de IoT citadas en la encuesta, se debe evaluar si es posible segmentar la red para evitar que un ataque tenga acceso libre a todos los dispositivos. En las plantas de fabricación es bastante posible, pero en un entorno hospitalario es más complejo. Una vez que la organización tiene claro cómo está organizada la estructura, se debe pensar en cómo proteger a cada grupo y buscar la manera de optimizarlo.

La visión moderna de la ciberseguridad tiene en cuenta las peculiaridades del negocio y exige un conocimiento robusto de la estrategia de protección. El punto principal aquí es que las organizaciones no necesitan tener expertos internos y deben buscar el apoyo de expertos en el mercado. También existen tecnologías que ayudan a automatizar las acciones de seguridad mediante inteligencia artificial.

Tanto la externalización como la automatización son clave para la eficacia del SISICP. **¡Piensa en esta posibilidad!**



El integrador gigante de América

- *Liderando como la empresa integradora número uno de seguridad en México.*
- *Dos décadas marcando el rumbo de la inteligencia operativa y la vigilancia avanzada.*
- *Del C2 al C7i: una revolución mexicana que ya inspira al mundo.*

Con dos décadas de trayectoria en México, 4everSecure se erige como el líder indiscutible en integración de seguridad, transformando cada proyecto en una sinfonía de precisión tecnológica, visión estratégica e impacto social. Centros de comando con Inteligencia Artificial, plataformas conectadas con agencias globales y soluciones diseñadas para anticiparse al delito consolidan su prestigio. La firma es hoy sinónimo de confianza, innovación y resultados medibles. No es solo tecnología: es poder operativo en tiempo real.

Desde su fundación en 2013, 4everSecure ha redefinido el estándar de la industria de la seguridad en México y América Latina. Con más de 11 años de experiencia, esta empresa mexicana se ha consolidado como la integradora número uno del país, gracias a su capacidad de ejecución, visión estratégica y su enfoque en soluciones reales, disruptivas y confiables.

Bajo el liderazgo del ingeniero Julio Zacarías, 4everSecure se ha convertido en un verdadero gigante de América, caracterizándose por su enfoque innovador, audaz y disruptivo, que rompe los esquemas tradicionales del sector. La empresa va más allá de ofrecer sistemas de vigilancia. Diseña e implementa soluciones comprobables, orientadas a la reducción real de la delincuencia y sustentadas en inteligencia, análisis de datos, ciberseguridad y protocolos operativos que marcan la diferencia.

Con presencia en 304 centros de monitoreo en todo México, ha participado en cada uno con ingeniería, diseño, implementación, operación y mejora continua. Además, es líder en la migración tecnológica de sistemas tradicionales.

Uno de sus mayores logros ha sido la creación del primer C7i municipal de América Latina, en Ecatepec, un centro de comando que integra Inteligencia Artificial, big data, reconocimiento facial a escala masiva, análisis de comportamiento, identificación vehicular y una capacidad de respuesta inmediata sin paralelo. Esta solución destaca tanto por su infraestructura como por su eficacia operativa en la disminución de delitos.



Además, 4everSecure ha desarrollado proyectos insignia que trascienden el ámbito tradicional de la seguridad. Entre ellos se encuentra la creación del primer C4 de la Mujer “Red Violeta”, un centro especializado en proteger y reaccionar ante situaciones de riesgo para mujeres, integrando herramientas tecnológicas, atención inmediata y protocolos de asistencia coordinada. Asimismo, es pionero en el diseño del primer C4 del Agua, un centro de control orientado a monitorear el uso, distribución y eficiencia del recurso hídrico, aplicando analítica, sensores inteligentes y respuesta operativa ante fugas, obstrucciones o anomalías en el sistema.

Como parte de su estrategia de interconexión e inteligencia compartida, 4everSecure también ha creado a lo largo del país diversas Salas de Fusión, pequeñas pero poderosas centrales de monitoreo que operan como nodos estratégicos. Estas salas están diseñadas para compartir y recibir información en tiempo real con entidades internacionales como el FBI, la CIA, Interpol, entre otras agencias, posicionando a México como un actor relevante en la red global de seguridad e inteligencia.



Una de las preguntas más frecuentes en la industria es:
¿Por qué 4everSecure tiene éxito donde otros no lo tuvieron?

La respuesta es sencilla: no siempre buscan “inventar el hilo negro”. Analiza con profundidad lo que otros integradores hicieron bien y mal, corrigen errores, ajusta detalles, perfeccionan procesos, y eso marca la diferencia. Es un modelo basado en el aprendizaje real y en el compromiso con el resultado, no con la apariencia.

Otra prueba de su liderazgo técnico es que, en múltiples ocasiones, empresas de gran renombre en la industria terminan subcontratando los servicios de 4everSecure para ejecutar o corregir proyectos estratégicos. Esta práctica, aunque pocas veces se hace público, evidencia el alto nivel de especialización, confianza y eficiencia que la firma mexicana representa, incluso para sus propios competidores.

A diferencia de muchas empresas del sector, 4everSecure no se limita a ofrecer soluciones comerciales genéricas. Su filosofía se basa en romper con los esquemas tradicionales de la industria, desmarcándose de los proyectos que no generan impactos reales o medibles. Para ellos, la seguridad no es un producto, sino una estrategia estructurada, auditable y comprobable. Tan es así que, en múltiples ocasiones, han sido llamados a fungir como auditores independientes en proyectos de seguridad donde no existen métricas



claras de resultado o impacto, aportando experiencia técnica, metodología y visión crítica para elevar los estándares operativos.

4everSecure ha sido evaluada y reconocida por la Secretaría de Marina, como una de las instituciones más exigentes en materia de seguridad. Actualmente trabaja en proyectos especiales en puntos estratégicos del país, apoyando en zonas de alta prioridad para la seguridad nacional.

A nivel internacional, su impacto no se detiene. Han participado en proyectos en Colombia, Guatemala, Estados Unidos y próximamente se expandirá hacia África, llevando su modelo de seguridad inteligente a nuevos territorios que buscan soluciones modernas, funcionales y confiables.

El impacto visual y funcional de sus soluciones es simplemente impresionante.



Su plataforma de Inteligencia Artificial incluye reconocimiento facial avanzado, detección automática de placas, analítica vehicular, conteo de personas, monitoreo con Inteligencia Artificial y su más reciente innovación: búsqueda de personas por tatuajes. Además, ha desarrollado tecnologías de seguridad como el exoesqueleto conectado, que emite alertas en tiempo real ante situaciones críticas. Todo esto demuestra que la visión de 4everSecure supera ampliamente a la industria.

Su tecnología está respaldada por certificaciones internacionales y ha sido aplicada en instituciones de clase mundial como el Pentágono, el Ejército y la Defensa Nacional de EE.UU., e incluso en entornos de alto riesgo como SpaceX, donde sus sistemas protegen y monitorean instalaciones críticas con los más altos estándares de exigencia.

Pero más allá de la tecnología, 4everSecure también cree en la transformación social. Impulsa programas de sensibilización y capacitación ciudadana, así como colaboraciones con universidades y centros de innovación para formar a las nuevas generaciones en temas de ciberseguridad, ética tecnológica y vigilancia inteligente.

Y su visión no se detiene en el presente. De cara a 2030, 4everSecure proyecta transformar más de 400 centros de monitoreo en América Latina y liderar el desarrollo de una plataforma continental de seguridad integrada, con analítica en la nube, interoperabilidad entre países y algoritmos predictivos que puedan anticiparse al delito.

En México, Fiscalías han adoptado sus soluciones como parte central de su estrategia digital y operativa, demostrando que 4everSecure no solo ofrece tecnología, sino resultados medibles y confiables.

4everSecure es más que una empresa de seguridad: es el futuro presente de la protección ciudadana. Por eso, en esta edición de **Más Seguridad**, se le reconoce en la portada como lo que es: el gigante de América. 🌐



Julio Zacarías
CEO de 4everSecure.

Diseño de portada:
DgCreative

De CONALEP a corporativos: así transforma



la seguridad en México

- *Integra Inteligencia Artificial, videovigilancia y control de accesos en soluciones personalizadas de seguridad.*
- *Proyecta su expansión hacia América Latina y Estados Unidos en 2025.*
- *Sus sistemas ya protegen hogares y más de 1,500 sucursales corporativas a nivel nacional.*

En sólo tres años, SISA, Soluciones Integrales en Sistemas de Alarma y CCTV, ya es un actor clave en el mercado de la seguridad electrónica en México, como firma integradora, fundada en mayo de 2022, ésta joven empresa ha construido una reputación sólida a partir de su capacidad para combinar tecnología avanzada con un enfoque personalizado hacia cada cliente.

Al frente se encuentra Alfredo Sánchez Cruz, director general, quien explica que la clave del éxito, ha sido ofrecer soluciones de alta especialización que responden a las exigencias de distintos sectores, desde empresas privadas hasta instituciones educativas y organismos gubernamentales.

“Somos una empresa comprometida con la innovación. Nos especializamos en integrar sistemas complejos de seguridad para que trabajen de forma coordinada, bajo una misma plataforma y con una capacidad de respuesta en tiempo real”, explica Alfredo Sánchez.

El concepto de integración en seguridad electrónica no se limita a colocar cámaras o alarmas. SISA, es una empresa de tecnología dedicada a integrar diferentes tipos de sistemas de alarma, videovigilancia, control de accesos, sensores, detección de incendios, alertamiento sísmico, entre otras tecnologías en una sola red inteligente que permite control total desde un punto central. Este enfoque, según Sánchez Cruz, ha sido fundamental para garantizar eficiencia operativa y mayor seguridad.

Su portafolio abarca desde la consultoría y planificación de sistemas de seguridad, hasta la instalación, configuración, soporte técnico y mantenimiento predictivo, preventivo y correctivo. La empresa también ofrece soluciones en videoconferencia, automatización industrial y diseño de sonido, así como sistemas de alerta sísmica que operan en sincronía con la red oficial de la Ciudad de México.

Presencia multisectorial: SISA atiende diversos sectores con soluciones diseñadas a la medida.

En el ámbito corporativo, implementa sistemas de control de accesos y videovigilancia para mejorar la seguridad operativa. En instituciones educativas y de salud, desarrolla protocolos de emergencia y tecnologías adaptadas a entornos sensibles. Para el sector residencial, ofrece soluciones inteligentes con soporte técnico continuo.

También ha tenido una fuerte incursión en el sector retail, optimizando operaciones de seguridad en tiendas y centros comerciales, así como en infraestructura crítica y entidades gubernamentales, donde la protección debe ser de alta confiabilidad.



Aliados tecnológicos. Para lograr un elevado nivel de personalización y cobertura, SISA trabaja de manera directa con las marcas más reconocidas del sector:

- **UNV (Uniview):** especializada en cámaras IP y gestión de seguridad unificada.
- **Hikvision y Dahua:** empresas mundiales en videovigilancia, cuyas tecnologías permiten análisis en tiempo real y monitoreo inteligente.
- **ZKTeco:** pionera en soluciones de control de acceso biométrico.
- **Maxhub:** ideal para la integración de soluciones audiovisuales y colaboración digital.
- **DMP:** con sistemas avanzados de alarmas y monitoreo en tiempo real.

Estas alianzas no sólo garantizan acceso a tecnología de punta, sino también una capacitación constante y soporte especializado, gracias a relaciones directas con fabricantes y distribuidores.

Cabe desatacar que uno de los proyectos más importantes que ha gestionado SISA, es el mantenimiento nacional de más de 1,500 sucursales de varias cadenas corporativas, una operación que puso a prueba su capacidad de gestión logística y cobertura técnica.

Por otro lado, uno de sus trabajos más emblemáticos ha sido la instalación de aulas video-educativas en CONALEP CDMX, mediante sistemas de videoconferencia y pantallas que han mejorado la competitividad de los estudiantes al facilitar el acceso a contenidos digitales en tiempo real.

Para 2025, la empresa se ha fijado convertirse en un referente continental en soluciones de seguridad electrónica, apostando por Inteligencia Artificial, gestión remota y soluciones para ciudades inteligentes. Además, reforzará su oferta en videoconferencias, educación digital y automatización industrial, respondiendo así a las nuevas exigencias del mundo postpandemia.



Alfredo Sánchez Cruz
Director general de SISA,
Soluciones Integrales en
Sistemas de Alarma y CCTV.



Tecnología de fibra óptica para protección de grandes sitios

- *Útil para la protección de cercas, rejas, muros o combinaciones diversas de barrera físicas que se utilizan habitualmente en entornos de alta seguridad.*
- *La serie EchoPoint™ utiliza un avanzado algoritmo de clasificación de reconocimiento de patrones para ayudar a analizar los tipos de intrusiones.*

Las soluciones perimetrales de fibra óptica utilizan fibras sensibles a las vibraciones que se integran en barreras físicas, como mallas o muros, o se entierran bajo tierra. La fibra óptica detecta cambios de presión, vibraciones o movimientos causados por un intruso que intenta escalar, cortar, perforar o traspasar el perímetro. Al detectar vibraciones o movimientos cuando un intruso intenta traspasar el perímetro, estos sistemas proporcionan alertas tempranas que permiten a los equipos de seguridad responder rápidamente antes de que se produzca la intrusión, mitigando la amenaza posible.

Las soluciones de fibra óptica de OPTEX son especialmente útiles para la protección de cercas, rejas, muros o combinaciones diversas de barrera físicas que se utilizan habitualmente en entornos de alta seguridad, como centrales eléctricas, prisiones, bases militares y aeropuertos. La serie EchoPoint™ DAS utiliza la tecnología de fibra óptica más avanzada en la actualidad y ofrece una opción en aplicaciones donde haya necesidad de enterrarse, montarse en mallas, muros o implementarse en modo híbrido, proporcionando un método de detección discreto y a prueba de manipulaciones para proteger lugares sensibles sin necesidad de equipos visibles, eliminando puntos de falla sobre el perímetro.

Los sistemas de fibra óptica son extremadamente resistentes a los daños ambientales, particularmente a la inducción por tormentas eléctricas, campos EM o RFI, incluso son intrínsecamente seguros, lo que los hace muy fiables en entornos difíciles y condiciones adversas.

Localización precisa de puntos hasta 100 km

La serie EchoPoint™ utiliza algoritmos de detección inteligentes para localizar con precisión la ubicación de una intrusión de +/- 6 m en un rango de hasta 100 km. La localización del punto se ve favorecida por la zonificación virtual que se configura para dividir el sistema en múltiples áreas de detección definidas por software que pueden oscilar entre 10m-100k. Esta detección altamente precisa y fiable hace que los sensores sean ideales para proteger grandes perímetros y lugares de seguridad de alto riesgo en los que es fundamental localizar e identificar el punto exacto de intrusión.

Algoritmos avanzados y clasificación

Los sistemas EchoPoint™ utilizan un avanzado algoritmo de clasificación de reconocimiento de patrones para ayudar a



analizar los tipos de intrusiones. En una aplicación de vallado, puede clasificar y reconocer los intentos de intrusión, como el corte en la cerca, escalamientos, o trepar por encima apoyándose de una escalera, lo que puede ser útil para determinar cualquier punto débil o predecir el comportamiento futuro del intruso. En una aplicación enterrada, el EchoPoint puede identificar si las vibraciones son causadas por pisadas humanas, o por excavación manual, con máquinas o paso de vehículos. Del mismo modo, esta información puede utilizarse para mejorar la configuración de seguridad, fortaleciendo aún más un emplazamiento.

Facilidad de uso y fiabilidad

Los sensores Echo Point se han diseñado pensando tanto en su facilidad de uso como en su alta fiabilidad. Nos hemos asegurado de que el EchoPoint sea fácil de instalar, ajustar y gestionar con una interfaz fácil de usar y sencilla, lo que hace que todo el sistema sea muy fácil de manejar. Está altamente automatizado y la resolución de problemas puede realizarse fácilmente dentro o fuera de las instalaciones, lo que le ofrece más opciones.

Lo que lo diferencia son las funciones de tolerancia a cortes y redundancia del sistema para evitar fallos del sistema y resistir intentos de manipulación, que no siempre se encuentran en otros sensores de fibra óptica. Las medidas de redundancia de sistema garantizan que, en caso de fallo de un procesador, el segundo procesador tomaría automáticamente el relevo para asegurarse de que el sistema sigue operativo y el perímetro se mantenga activo.



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)



La mente maestra detrás de la seguridad electrónica en México



- 20 años desafiando los límites de la seguridad electrónica y la ciberseguridad.
- Premio ALAS por innovación tecnológica en musicales de gran formato.
- Más de 140 cursos y certificaciones, anualmente para garantizar soluciones de vanguardia

Computare de México integra video-vigilancia, control de accesos, alarmas, ciberseguridad y más, creando ecosistemas inteligentes que trabajan de manera conjunta para anticipar y neutralizar riesgos antes de que sucedan.

Con dos décadas de existencia, Computare de México ha revolucionado la integración de seguridad electrónica y ciberseguridad, convirtiéndose en un referente en el sector. No solo instala tecnología, crea estrategias de seguridad a la medida, basadas en un análisis técnico profundo, innovación y certificaciones de clase mundial.

“Nacimos en 2005 integrando solo soluciones de videovigilancia y evolucionamos hasta ser una firma con presencia en sectores de alto nivel técnico. Hoy, garantizamos soluciones inteligentes que protegen lo más valioso para una persona o empresa”, destaca Oscar Tenorio Colón, CEO de Computare.

A la fecha, la empresa desarrolla soluciones 360° que van desde el análisis y diseño estratégico hasta la implementación y soporte continuo, integrando sistemas complejos como videovigilancia, alarmas contra intrusión e incendio, control de accesos, centrales de monitoreo, enlaces inalámbricos, ciberseguridad y telefonía IP.

“En Computare, la transformación es constante. En 2022, incorporamos la ciberseguridad como una pieza clave de nuestras soluciones, integrando las tecnologías más avanzadas para proteger tanto los activos físicos como digitales. Integramos tecnología que no solo protege, sino que predice y responde, afirma Oscar Tenorio”.

A diferencia de otros integradores, no solo conectan dispositivos, diseñan soluciones estratégicas que protegen y anticipan. “Lo que hacemos es comprender tu operación, anticipar riesgos y diseñar sistemas que trabajen en conjunto para proteger tu futuro. Cada proyecto es único. Analizamos tus necesidades reales y creamos arquitecturas tecnológicas personalizadas que fusionan control de accesos, videovigilancia, analítica y más, creando un ecosistema integral que responde con inteligencia”, subraya Oscar Tenorio.

Una de sus ventajas competitivas es la capacidad de integrar soluciones de seguridad con inteligencia y personalización. En lugar de simplemente conectar dispositivos, se entiende el contexto de cada cliente, se anticipan los riesgos y se crea una infraestructura tecnológica que trabaja de manera conjunta para proteger tanto lo físico como lo digital”, afirma el directivo.

La firma ha ejecutado proyectos emblemáticos desde grandes producciones teatrales hasta industria farmacéutica, sus clientes han experimentado mejoras tangibles en eficiencia operativa, reducción de costos y protección integral.

Mención aparte merece el trabajo con la productora GOU Producciones del afamado productor teatral



Alejandro Gou, donde integraron tecnología de video en musicales de gran formato; como Hoy No Me Puedo Levantar, Billy Eliot, Spamalot, Mentiras El Musical, Timbiriche El Musical, entre otros.

“En musicales de gran formato si nuestro sistema de seguimiento de obra falla, impacta a la producción. Probamos más de 40 modelos de cámaras de diferentes fabricantes, hasta encontrar la que ofrecía cero delay, se adaptara a cambios de iluminación extremos y tuviera buen performance. Fue un reto técnico y artístico”.

También destaca su participación con Grupo Gayosso, donde diseñó una red nacional de monitoreo para sus funerarias, y con una farmacéutica de alto perfil, cumpliendo normas de sanidad, secreto y protocolos industriales estrictos.

“En Computare, no solo trabajamos con marcas premium como Axis, Pelco, Hikvision, Mobotix, NVT, Hochiki, HID, CISCO, Grandstream y muchas más; nos aseguramos de dominar cada una. No vendemos tecnología solo por su nombre, somos expertos certificados en cada una de ellas. ¡La diferencia no está solo en las marcas, está en el conocimiento y la excelencia con la que las implementamos!”, aclara el CEO.

Su relación con distribuidores y fabricantes es directa, lo que le permite ofrecer mejores garantías, acceso a stock y tiempos de entrega competitivos, incluso en proyectos de gran escala.

Aunque aún no han expandido operaciones fuera de México, están en negociaciones con un proyecto en Colombia. Su visión para 2025 se enfoca en evaluar el verdadero potencial de la Inteligencia Artificial en la integración de soluciones de seguridad electrónica, y en reforzar su vínculo con fabricantes líderes.

“No nos conformamos con la innovación estándar, vamos más allá. Las marcas pueden seguir innovando, pero nosotros buscamos romper los límites. Nos apasiona hacer realidad lo que otros solo sueñan: transformar una cámara de videovigilancia en un poderoso aliado estratégico que no solo muestra una imagen, sino que automatiza procesos, optimiza costos y mejora la experiencia del cliente”. Oscar Tenorio advierte sobre la proliferación de integradores poco preparados al señalar que “muchos venden kits armados sin analizar las necesidades reales del cliente. Eso no es integración, eso es improvisación. Nosotros creemos en la profesionalización como camino para hacer crecer todo el sector”.

Computare de México representa una evolución del integrador tradicional hacia una consultoría tecnológica completa con metodologías sólidas, formación constante y una mirada crítica a la industria.



Oscar Tenorio Colón
CEO de Computare

SEGURIDAD INTELIGENTE

"La seguridad no espera. Protege tu empresa con tecnología que anticipa, responde y evoluciona."

- ✓ Sistemas de videovigilancia
- ✓ Control de acceso
- ✓ Alarmas de intrusión e incendio
- ✓ Seguridad Perimetral
- ✓ Centros de datos
- ✓ Centrales de monitoreo
- ✓ Ciberseguridad

Contáctanos

☎ +52 55 8840-9787

🌐 computare@computare.mx



Empresas Integradoras en México



	Empresa	Ciudad
1	4everSecure	CDMX
2	SISA, Soluciones Integrales en Sistemas de Alarma y CCTV	CDMX
3	Computare de México	CDMX
4	7 Sistemas de Seguridad Privada	CDMX
5	A & P Seguridad	CDMX
6	ACEBSA	CDMX
7	Inmobiliaria Elemento 360	CDMX
8	Highlight	CDMX
9	Hi-Tech Systems	San Luis Potosí
10	ICTSA Impulsora Comercial en Telecomunicaciones	CDMX
11	Identatronics	CDMX
12	ISAT	CDMX
13	Multisistemas de Seguridad Industrial	CDMX
14	Omni Equipos Especiales	Puebla
15	Transmisión y Recepción	CDMX
16	Tritech technologies	Nuevo León
17	Vempro	Tamaulipas
18	VANTEC Global (Vanguardia Tecnológica en Soluciones JCRA)	Estado de México
19	Vilsa	CDMX
20	VIP System	CDMX
21	Convergint	CDMX
22	Quality Estándar Technology	Estado de México
23	Soluciones Entelequia	Tamaulipas
24	Rissp TI	CDMX
25	Allied Universal	CDMX
26	Andamase Engeneering & Developing	Tabasco
27	Apollocom	Estado de México
28	Argos	CDMX

Empresas Integradoras en LATAM



	Empresa	País
1	Alarmas Digitales Modernas	Guatemala
2	Alarmas y Sistemas de Seguridad (ASIS Corp)	Guatemala
3	Alarmec	Guatemala
4	Allied Integration Systems	Guatemala
5	Enditel	Costa Rica
6	Evisecurity	Costa Rica
7	Grupo VMA	Costa Rica
8	Ibux - ESPH	Costa Rica
9	IP-Panamá	Panamá
10	MDM Secutities	Panamá
11	Multiservicios VP	Guatemala
12	Onen BrainHunters	Panamá
13	Tracking Security Panamá	Panama
14	Tri Points International Security, Inc.	Panamá
15	Ultra de Nicaragua	Nicaragua
16	Umbrella TSG	Panamá
17	Vosmedia	Guatemala
18	VTG	Guatemala
19	Watchower Security	Nicaragua
20	Xtreme Security	Panamá
21	Teleworks	Honduras
22	Soluciones Seguras	Guatemala
23	TAS Seguridad	Guatemala
24	DC Adonay	Costa Rica
25	VAS Technology	Costa Rica
26	Panama Pacífico	Panamá
27	Ultranic	Nicaragua
28	Grupo Intec	El Salvador

Distribuidores mayoristas en seguridad integral



- Videovigilancia e inteligencia artificial a través de video
- Control de acceso peatonal, vehicular y sistemas de inspección
- Seguridad, videovigilancia e IA en el transporte
- Monitores, LCD y Videowall
- Productos de videoconferencia y pantallas interactivas
- Alarmas e intrusión
- Smart home y productos de consumo

 Calle Salaverry, 1067, Colonia Residencial Zacatenco, Alcaldía Gustavo A. Madero, Código Postal 07369, Ciudad de México.

 ventas@pimecsa.com.mx
 +52 55 1560 7789

MÁS SEGURIDAD

Magazine



Síguenos



Revista Más Seguridad



Revista Más Seguridad



@revmasseguridad



[revmasseguridad](https://www.instagram.com/revmasseguridad)



Revista Más Seguridad

La seguridad somos todos

#PorTuSeguridad

Participación de la mujer en la formación sobre seguridad

- **Beneficios y ventajas.** La seguridad ya no es solo un terreno de hombres; es un espacio donde la diversidad se traduce en mayor eficacia y mejores resultados para todos.



Lic. María Esther Cruz Pérez
DSI. Siprosi Corporativo,
Tesorera de AMEXSI A.C.
México

Articulista Invitada

Hablar de lo que una mujer representa, es siempre una labor difícil de explicar en todas sus dimensiones en tan poco espacio. Desde mis inicios de labor docente, pude constatar la importancia para bien o mal del papel de la mujer en la familia y en la sociedad.

Hoy, por los giros que da la vida, me encuentro inmersa en la seguridad, manteniéndome en una posición de observadora de profesionales en seguridad que muestran gran interés en crecer a través de estudios y certificaciones. Me llama la atención y ver con mucho gusto como, de ser programas exclusivos para hombres, ahora existen grupos en que llega a haber una participación igualitaria de grandes y exitosas mujeres, las cuales cada vez más son reconocidas como auténticas profesionales de alto nivel en la industria.

Antes, cuando se pensaba en seguridad, tradicionalmente imaginamos fuerza, disciplina y autoridad, cualidades que durante mucho tiempo se han atribuido principalmente a los hombres. Sin embargo, la creciente presencia de mujeres en este campo ha demostrado que la seguridad es mucho más que una cuestión de fuerza bruta; es una disciplina que exige inteligencia, agilidad, intuición y habilidades estratégicas.

Es evidente que, con el aumento femenino en los grupos de formación especializada en la seguridad, el desempeño y productividad se incrementa notablemente, pues al agregar el punto de vista femenino a lo que ya los hombres aportan, el resultado es siempre una mayor posibilidad de éxito en los planes y operativos de seguridad.

Desde una perspectiva externa, el papel de la mujer en la seguridad no solo ha roto estereotipos, sino que ha elevado el estándar del desempeño en este ámbito.

Cuando las mujeres están tomando algún programa de estudio, resulta evidente un cambio en la dinámica de los grupos, ya que aportan un enfoque integral a la seguridad, gracias a su aguda capacidad de observación y análisis. Suelen detectar detalles que pueden pasar desapercibidos, evaluar riesgos desde una perspectiva más amplia y anticipar amenazas con mayor precisión y este análisis ayuda a los hombres a tener una mirada diferente.

Otro aspecto en el que las mujeres destacan es la gestión de crisis, ya que suelen demostrar un alto nivel de control emocional en situaciones de presión, lo que les permite tomar decisiones rápidas y efectivas sin perder la calma. Además, su capacidad para comunicarse con claridad y empatía contribuye a resolver conflictos de manera más estratégica, reduciendo la necesidad del uso de la fuerza y promoviendo soluciones más inteligentes.

Las mujeres aportan un enfoque integral a la seguridad gracias a su aguda capacidad de observación y análisis. Suelen detectar detalles que pueden pasar desapercibidos, evaluar riesgos desde una perspectiva más amplia y anticipar amenazas con mayor precisión. Estos instintos son particularmente valiosos en la seguridad preventiva, donde la anticipación es clave para evitar incidentes antes de que ocurran.

La inclusión de la mujer en la seguridad no solo fortalece el desempeño de los equipos, sino que también mejora la percepción de la seguridad en la sociedad. Su presencia genera confianza y demuestra que la protección no se basa exclusivamente en la fuerza, sino en la capacidad de adaptación, el pensamiento estratégico y la empatía.

Si bien todavía hay barreras por superar, el impacto de la mujer en la seguridad es innegable. Su instinto de protección, combinado con habilidades estratégicas y emocionales, no solo enriquece el campo, sino que lo transforma, haciéndolo más eficiente, humano y adaptable a los desafíos del mundo moderno. La seguridad ya no es solo un terreno de hombres; es un espacio donde la diversidad se traduce en mayor eficacia y mejores resultados para todos.

Por eso aseguro, que si en algún momento tienen la oportunidad de participar en programas de formación donde concurren asistentes de ambos sexos, les auguro una experiencia más enriquecedora y exitosa. 🌟



Urge Ley General efectiva para la industria de la seguridad privada:



- **La regulación actual fragmenta al sector, fomenta la informalidad y pone en riesgo la seguridad pública y privada en México.**
- **La falta de una ley genera permite que incluso, el crimen organizado utilice la figura de empresas de seguridad privada como fachada.**

Las Agrupaciones de Seguridad Unidas por México (ASUME) hacen un llamado urgente al Congreso de la Unión para corregir las deficiencias estructurales que hoy afectan al sector en el país. Esto, tras la reciente aprobación en la Comisión de Seguridad Ciudadana de la Cámara de Diputados de dos dictámenes sobre seguridad pública que, lejos de resolver el problema de fondo, profundizan la confusión normativa al mantener un diseño de competencias ambiguo y una sobrerregulación insostenible.

Una distribución de competencias ineficaz

La iniciativa de Ley General del Sistema Nacional de Seguridad Pública aprobada en la Comisión es tibia e inconsistente, ya que subordina a la Federación frente a los estados, generando duplicidades y contradicciones legales. De acuerdo con la propuesta, la Federación regula a las empresas que operan en más de una entidad, mientras que los estados supervisan a las locales, pero, al mismo tiempo, la iniciativa exige a las empresas tramitar autorizaciones federales y luego cumplir con regulaciones estatales que suelen ser excesivas o contradictorias.

“Hoy enfrentamos un marco jurídico obsoleto y fragmentado, con una Ley Federal que ya no responde a la realidad del país, 32 leyes estatales y cientos de reglamentos municipales que se contraponen entre sí. Hemos identificado más de 500 contradicciones que generan incertidumbre jurídica y limitan el desarrollo del sector formal,” afirmó Armando Zúñiga Salinas, presidente de ASUME.

Una ley general pendiente y un entorno propicio para la informalidad

Desde hace años, el Congreso mantiene una deuda pendiente: la expedición de la Ley General de Seguridad Privada. Esta omisión ha generado vacíos normativos que fomentan la competencia desleal y dificultan el control efectivo sobre las empresas irregulares.

“Nos preocupa profundamente que esta situación permita que incluso el crimen organizado utilice la figura de empresas de seguridad privada como fachada, al operar sin supervisión ni controles eficaces”, alertó Zúñiga Salinas. La seguridad privada es un sector clave para la estabilidad económica y laboral del país, hoy genera alrededor de 450 mil empleos formales, lo que representa cerca del 2% de los registros del IMSS, y agrupa a más de 8 mil empleadores.



ASUME sostiene que la solución es clara: expedir una Ley General de Seguridad Privada que unifique criterios, elimine la dispersión normativa y permita establecer una regulación nacional clara, moderna y funcional.

El sector formal exige que esta nueva legislación:

- Elimine requisitos inconstitucionales, como los exámenes de control de confianza.
- Clarifique las competencias entre Federación y estados, evitando la duplicidad de regulaciones.
- Reconozca la labor coadyuvante de la seguridad privada, sin confundirla con funciones de autoridad pública.
- Diferencie las reglas según los tipos de servicios, considerando la diversidad del sector (seguridad tecnológica, transporte de valores, protección ejecutiva, etc.).

Una industria lista para ser aliada del Estado

“México no puede seguir operando bajo un esquema normativo que incentiva la informalidad y deja sin herramientas a las autoridades para sancionar a quienes incumplen. Necesitamos una ley moderna y eficaz que fomente la profesionalización, la transparencia y la colaboración con el Estado”, concluyó Zúñiga Salinas. 🌐

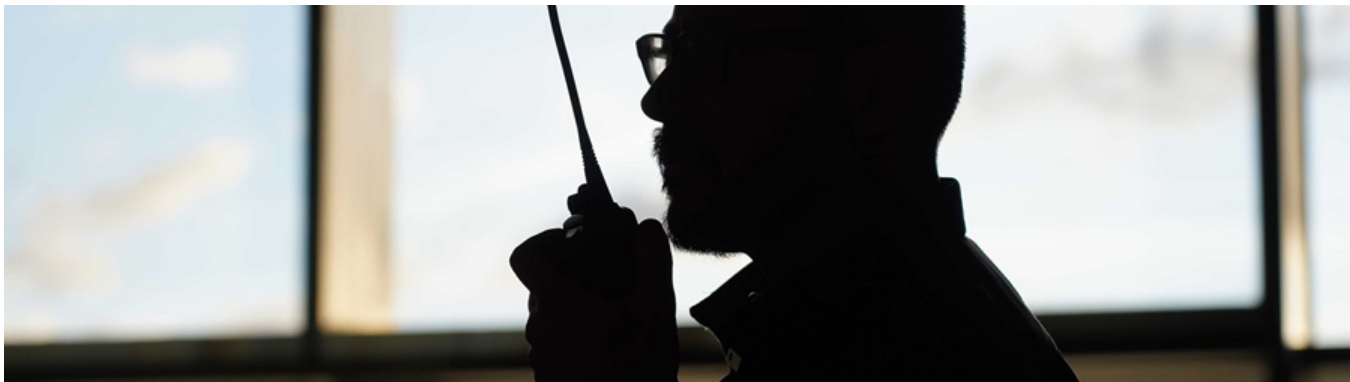


Armando Zúñiga Salinas,
presidente de ASUME.

Liderazgo en seguridad

▪ Transformando desafíos en rentabilidad.

Parte 1 de 2



José Ruíz
CEOCPP® PCI® PSP® CLSD® ASIS
Internacional, director de Seguridad en
Four Seasons Hotels and Resorts, con
más de 20 años de experiencia.
México

Articlista Invitado

El poder de un líder en momentos decisivos

Un buen líder no solo administra, también inspira, guía, y transforma. En un sector tan crucial como la industria de la hospitalidad en México, que en 2023 representó más del 14% del PIB nacional, el liderazgo en seguridad es la columna vertebral que sostiene la confianza de clientes, inversionistas y colaboradores. Ahora, en comparación con el mundo solo quiero que des un vistazo a la importancia que representa el sector en nuestro país comparado con el resto del mundo: “estudio del ciclo 2023” (UN Tourism, WTTC y Latinometrics):



Para reflexionar sobre el nivel de experticia y liderazgo que la industria necesita de nosotros ahora mismo, ¿cierto?

El liderazgo efectivo tiene un impacto profundo:

- **Retiene talento:** Equipos conectados con el propósito de la organización son más comprometidos y resilientes.
- **Atrae talento:** Una sólida reputación como líder, genera confianza,

atrayendo a los mejores profesionales.

- **Impulsa el desempeño:** Expectativas claras y entornos justos potencian equipos de alto rendimiento.
- **Alinea estratégicamente:** Líderes que sincronizan esfuerzos con objetivos globales logran resultados extraordinarios.

Pero ser un líder no es solo cuestión de habilidades técnicas. Requiere método, empatía y visión.

Lecciones del huracán Otis: Liderazgo bajo presión

En 2023, el huracán Otis impactó Acapulco con una fuerza devastadora, dejando en su estela destrucción e incertidumbre. Sin embargo, en medio del caos, emergieron historias de resiliencia que nos enseñan lo que realmente significa liderar. Un ejemplo notable fue el de Mario Franco, director de seguridad de Schneider Electric, quien se enfrentó al desafío de proteger tanto a su equipo como a las operaciones de la empresa en medio de una crisis sin precedentes. Mario, reconocido por su enfoque metódico y su liderazgo humano, logró coordinar una respuesta efectiva que no solo minimizó las pérdidas, sino que fortaleció la reputación de la empresa como un referente en resiliencia empresarial.

Su conferencia “Cuando la Adversidad Golpea: Lecciones de Resiliencia Empresarial Frente al huracán Otis” ha sido una fuente de inspiración para muchos. Si aún no has tenido la oportunidad de escucharla, te recomiendo seguir su trabajo y explorar sus artículos. Mario nos recuerda que un líder no solo actúa en el momento de la emergencia, sino que prepara a su organización para enfrentar lo inesperado con anticipación y confianza. (Continuará) 🌐

Intervenir sin Fracturar

▪ *El arte de la investigación en la cultura organizacional.*



Pedro Oré

Miembro de ASIS Internacional. Oficial Certificado de Protección - CPO. Oficial Certificado en Investigaciones CIO. Máster en Gestión y Dirección de Equipos. Profesional en Administración de Negocios Internacionales. Oficial de Mar de la Marina de Guerra del Perú. Perú

Articlista Invitado

Lima, Perú.- En el mundo corporativo, la confianza es como el oxígeno: invisible, esencial y solo notamos su ausencia cuando ya estamos asfixiándonos. Sin embargo; incluso en las organizaciones con la cultura más robusta, donde el “Great Place to Work” no es solo un slogan, pueden crearse grietas en forma de deshonestidad. El reto es claro: ¿Cómo investigar sin que la organización termine convertida en un campo de batalla de sospechas y paranoia?

Enfrentar un caso de fraude, robo de información o conflicto de intereses es un ejercicio de precisión. Un investigador corporativo debe parecerse más a un cirujano que a un leñador. Mientras el leñador ataca con fuerza y corta indiscriminadamente, el cirujano disecciona con pulcritud, eliminando solo lo que daña sin afectar lo saludable. La pregunta es: ¿Nuestras investigaciones son “bisturí” o “hacha”?

Tratamiento quirúrgico de la información: No todo dato es relevante, no toda conversación es útil y no toda evidencia es definitiva. La tentación de hacer “barridos masivos” de información solo genera pánico. Más vale una prueba concreta que cien hipótesis.

Entrevistas con método, no con martillo: Los entrevistados no son enemigos en un interrogatorio policial. Preguntas bien diseñadas, lenguaje neutral y un enfoque de curiosidad genuina son más efectivos que la presión agresiva. Un testimonio obtenido por miedo es poco confiable y perjudicial para el ambiente laboral.

Restaurar, no solo sancionar: No toda falta es un caso perdido. Las mejores organizaciones tienen protocolos no solo para castigar, sino también para redirigir. En ciertos casos, medidas correctivas pueden ser más valiosas que una simple terminación laboral. El equipo de seguridad corporativa debe ser visto como guardianes de la integridad y no como agentes de persecución. La confianza



Según la “Association of Certified Fraud Examiners (ACFE)”, el 5% de los ingresos corporativos se pierde anualmente por fraudes internos, un dato alarmante que justifica cualquier esfuerzo por identificar riesgos. Sin embargo; otro estudio de “Harvard Business Review” señala que, en empresas con culturas de alta confianza, los empleados son un 50% más productivos y tienen 76% más compromiso. Esto significa que una mala gestión de las investigaciones podría acabar costando más de lo que pretendemos recuperar.

Los procesos de investigación mal gestionados generan efectos secundarios peores que el problema original. La clave es aplicar lo que llamaremos transparencia estratégica: ser abiertos sobre los valores que guían la investigación, pero sin exponer innecesariamente la dinámica interna. Debido a esto debemos tener en cuenta las siguientes premisas: No convertir la sospecha en clima laboral: La peor estrategia es hacer sentir a todos como posibles delincuentes. Si la investigación se filtra o se maneja con secretismo excesivo, el rumor se vuelve un virus organizacional. La comunicación clara sobre las políticas y procedimientos evita el miedo irracional.

se construye cuando la gente percibe que la seguridad protege y no ataca. El éxito de una investigación no está solo en descubrir la verdad, sino en garantizar que el proceso no desmorone la cultura organizacional.

Si queremos empresas en las que las personas trabajen con orgullo y sin temor, la seguridad debe ser parte de la solución y no del problema.

La verdadera habilidad en las investigaciones corporativas no está en encontrar culpables, sino en encontrar la verdad sin que la empresa se rompa en el intento. 🌐

Gestión de la seguridad corporativa.

Habilidades blandas

- *La integración efectiva de estas competencias interpersonales y comunicativas no solo mejora la protección de los activos organizacionales, sino que también incrementa la productividad y el bienestar general del personal.*

Parte 2 de 2



Alfredo Yuncoza

Presidente del Hispanic Advisory Board de IFPO. Director Senior de Smart Risk Consulting. Presidente del Security College US. Presidente de Arcus Group C.A.
Email: a_yuncoza@yahoo.com
ayuncoza@gmail.com
Skype: alfredo.yuncoza
Twitter: @alfredoyuncoza
Venezuela

Articlista Invitado

Caracas Venezuela.- En la edición anterior se mencionaba sobre como las habilidades blandas constituyen un activo estratégico para los profesionales de la gestión de la seguridad corporativa. En esta segunda parte, seguiremos abordando la siguiente parte de estas diez habilidades en el perfil profesional de la seguridad corporativa.

Trabajo en equipo

La gestión efectiva de riesgos requiere un enfoque colaborativo que supere las barreras entre departamentos. Al promover la colaboración multidisciplinaria, las organizaciones pueden identificar y mitigar de manera más eficiente las amenazas a la seguridad. Esta sinergia no solo facilita el intercambio de conocimientos y experiencias, sino que también optimiza la utilización de recursos, lo que conduce a una gestión de riesgo más integral y proactiva.

Provocar un entorno donde diferentes áreas trabajen en conjunto permite a las organizaciones abordar los riesgos desde múltiples perspectivas, enriqueciendo así el proceso de toma de decisiones. Al integrar diversas disciplinas y habilidades, se fortalece la capacidad para anticipar y responder a los desafíos, garantizando una protección más robusta y efectiva frente a posibles incidentes.

Creatividad e innovación

En un entorno empresarial caracterizado por su constante evolución y por la aparición de nuevas amenazas, la capacidad de generar ideas originales y de implementar soluciones disruptivas es crucial. Estas prácticas permiten a las organizaciones anticiparse a los riesgos emergentes, y también fortalecen su resiliencia, asegurando que puedan adaptarse y prosperar en un contexto de incertidumbre.

Fomentar un ambiente que facilite la expresión de ideas innovadoras y que promueva una cultura de aprendizaje continuo se convierte en un imperativo estratégico para las empresas que buscan mantenerse a la vanguardia en seguridad. La creación de espacios donde los colaboradores se sientan motivados a compartir sus perspectivas y a experimentar con nuevas propuestas es fundamental para impulsar la innovación. De este modo, las organizaciones no solo mejoran sus protocolos de seguridad, sino que también desarrollan una mentalidad proactiva que les permite enfrentar los desafíos del futuro con confianza y eficacia.



Gestión del tiempo

Es un pilar fundamental en la construcción de una postura de seguridad corporativa proactiva. Al integrar la gestión del tiempo en las estrategias de seguridad, las organizaciones pueden optimizar la asignación de recursos, priorizar las tareas críticas, y responder de manera más eficiente ante incidentes.

A través de técnicas como el análisis de riesgos basado en el tiempo, la planificación de contingencias detalladas y la implementación de sistemas de monitoreo proactivos, es posible identificar y mitigar proactivamente las amenazas a la seguridad. Además, al fomentar una cultura de seguridad en la que la gestión del tiempo sea una prioridad, las organizaciones pueden fortalecer su resiliencia y minimizar el impacto de los incidentes inevitables.

En última instancia, la gestión del tiempo no solo es una herramienta operativa, sino una estrategia estratégica para proteger los activos más valiosos de la organización.

Persuasión e influencia

Los líderes transformacionales se distinguen por su capacidad para influir y persuadir a otros hacia el logro de una visión compartida. Esta habilidad facilita la implementación efectiva de iniciativas de mejora continua, así como también es crucial para cultivar una cultura de seguridad proactiva dentro de las organizaciones. Al articular una visión clara y convincente, estos líderes son capaces de motivar e inspirar a sus equipos, fomentando un entorno en el que cada miembro se siente valorado y comprometido con los objetivos comunes.

Por otra parte, los líderes transformacionales empoderan a sus colaboradores para que tomen decisiones informadas y asuman la responsabilidad de su propio entorno laboral. Este enfoque no solo mejora la moral del equipo, sino que también promueve una mayor participación en las prácticas de seguridad, lo que a su vez conduce a resultados excepcionales. Al integrar estos principios en su liderazgo, se establece un ciclo virtuoso donde la confianza y la colaboración se traducen en un desempeño superior en materia de seguridad, beneficiando tanto a los empleados como a la organización en su conjunto.



En resumen, las habilidades blandas representan un recurso fundamental para los profesionales involucrados en la gestión de la seguridad corporativa. La integración efectiva de estas competencias interpersonales y comunicativas no solo mejora la protección

de los activos organizacionales, sino que también incrementa la productividad y el bienestar general del personal. Estas habilidades permiten a los profesionales establecer relaciones más sólidas y colaborativas dentro de la organización, lo que resulta en una respuesta más ágil y efectiva ante situaciones de riesgo.

Además, al promover una cultura de seguridad proactiva, los especialistas en seguridad contribuyen de manera significativa al cumplimiento de los objetivos estratégicos de la empresa. La capacidad de comunicarse claramente, resolver conflictos y liderar equipos es esencial para implementar políticas que sean aceptadas y adoptadas por todos los niveles de la organización. Este enfoque no solo minimiza las vulnerabilidades, sino que también fomenta un ambiente laboral donde todos los empleados se sienten responsables y comprometidos con la seguridad.

En consecuencia, el desarrollo y fortalecimiento de habilidades blandas en el ámbito de la gestión de seguridad corporativa no deben ser subestimados. Invertir en la capacitación en estas áreas puede resultar en una mejora sustancial en la eficacia operativa y en el clima organizacional, lo que a su vez se traduce en un mayor éxito en el cumplimiento de las metas empresariales a largo plazo.



Rostros invisibles:

La esclavitud del presente

- *La esclavitud representa la supresión absoluta de la libertad y la dignidad, convirtiendo a una persona en un objeto y negándole su condición de ser humano.*



Edison Cadena Ayala
MSC, CPO, CPOI, CSSM
gerente de la empresa
SEINNATIONAL CIA. LTDA.
Ecuador

Articlista Invitado

Quito, Ecuador.- A pesar de los avances sociales y políticos, la esclavitud no es un fenómeno del pasado. Aunque parezca inaudito en la actualidad, millones de personas viven atrapadas en redes de explotación, desde el tráfico humano hasta condiciones laborales injustas, donde el crimen organizado juega un papel crucial en su perpetuación moderna, actuando como una red estructurada que facilita y se beneficia de estas prácticas. En muchos casos, estas organizaciones controlan actividades como tráfico de personas, explotación sexual y trabajo forzoso.

Se estima que, en Latinoamérica, hasta el 70% de los casos de esclavitud moderna están vinculados a grupos del crimen organizado. Secuestran a mujeres y niñas para la prostitución forzada, mientras que hombres y niños son explotados en trabajos forzados. Además, estas redes suelen operar de manera transnacional, aprovechando la corrupción y la falta de regulación para expandir sus actividades.



De acuerdo con datos recientes de la Organización Internacional del Trabajo (OIT) y otras organizaciones, más de 40 millones de personas son víctimas de esclavitud moderna. Esta cifra incluye mujeres, niños y comunidades vulnerables que enfrentan niveles extremos de explotación. Las regiones más afectadas suelen ser aquellas con altos índices de pobreza, conflicto armado o falta de regulación laboral.

El crimen organizado también utiliza la esclavitud moderna como una fuente de ingresos significativa, ya sea directamente a través de la explotación de personas o mediante el control de cadenas de suministro ilegales. Esto incluye desde la agricultura hasta la construcción, donde las víctimas son obligadas a trabajar en condiciones inhumanas.

La esclavitud moderna, lejos de ser erradicada, persiste como una realidad devastadora que afecta a millones de personas en todo el mundo. Aunque los rostros de las víctimas puedan estar ocultos tras estadísticas y fronteras, sus historias revelan el verdadero alcance de este flagelo contemporáneo.

Hoy, el concepto de esclavitud moderna se extiende más allá de las cadenas físicas. Sus tentáculos se extienden a todos los niveles donde los jóvenes y en especial adolescentes son presa de su influjo debido a la promesa de encontrar la tan ansiada fama y riqueza inmediata.

En un mundo interconectado, la demanda de productos y servicios a bajos costos perpetúa prácticas laborales deshumanizantes. Las cadenas de suministro en sectores como moda, deporte, tecnología y agricultura, frecuentemente ocultan las condiciones de trabajo indignas, lo que convierte a los consumidores en agentes inconscientes de esta esclavitud.

Es importante destacar que estas prácticas modernas de esclavitud no siempre son visibles. Muchas víctimas son ocultadas detrás de normativas débiles, prácticas culturales o la indiferencia social. Este anonimato amplifica el desafío de erradicar el problema, porque ignora el sufrimiento humano.

La esclavitud moderna es una tragedia silenciosa que afecta a millones de personas en todo el mundo. Aunque a menudo pasa desapercibida, sus rostros están entre nosotros: en nuestras comunidades, en las cadenas de suministro que sustentan la vida diaria y en las desgarradoras historias de quienes padecen estas condiciones. Este fenómeno no solo desafía los derechos humanos, sino que también cuestiona los valores éticos y morales como sociedad.

Erradicar este flagelo exige una respuesta colectiva, un esfuerzo conjunto de gobiernos, empresas, organizaciones civiles y ciudadanos. No basta con legislar; es necesario transformar las mentalidades que perpetúan la explotación, como el consumo irreflexivo de bienes vinculados a prácticas abusivas.

La responsabilidad es compartida. Cada denuncia, cada apoyo a iniciativas que combatan la trata y la explotación, es un paso hacia un mundo más justo y equitativo. Este esfuerzo colectivo debe recordarnos que el cambio comienza con cada uno de nosotros.

La esclavitud del presente no define nuestro futuro. Soñar con un mundo donde la libertad y la dignidad sean universales es posible, pero solo si nos comprometemos a convertir los derechos humanos en una prioridad inquebrantable. 🌐



CUMBRE INTERNACIONAL DE LA MUJER CON SEGURIDAD CIMS 2025

"FIRMEZA Y LIDERAZGO"



CIBERSEGURIDAD
Y PREVENCIÓN DE FRAUDES



VIOLENCIA DE GÉNERO
Y AUTOPROTECCIÓN



ADMINISTRACIÓN DE LA SEGURIDAD
CIUDADANA



CRIMEN ORGANIZADO
Y SU AFECTACIÓN A LA SOCIEDAD



GENERACIÓN DE ESPACIOS DE TRABAJO
SEGUROS Y SALUDABLES

CON EL APOYO DE

CONSEJO
VIOLETA



Warmi

Verónica Villamarín



EMPODERATE
y conquistamos tus objetivos

PATROCINAN



CORPORACIÓN CPTD REGIÓN
ICA CHAPTER



MÁS SEGURIDAD
Magazine



Fundación
Rafael Ruiz Calatrava



Su protección, es nuestro compromiso.
SECURITY DOCTORS ECUADOR

IPS
GESTIÓN

IPS
ACADEMIA



UNIVERSITARIO
SEDE AMBATO
JAPON
AMOR AL CONOCIMIENTO



29 y 30 de mayo del 2025



La Quinta by Wyndham
Quito

ORGANIZA:



593 983509271



info.seigrus@gmail.com

Seguridad & Resiliencia

• “No hay seguridad en esta tierra, sólo hay oportunidad”. Douglas MacArthur.



Dra. Mercedes Escudero Carmona

Presidenta de CPTED México ICA Chapter.

Analista especialista, comentarista, conferencista y ponente internacional en temas de seguridad humana, seguridad, prevención del delito y violencia en diferentes ciudades y países.

México

Articulista Invitada

En un mundo cada vez más interconectado y expuesto a riesgos complejos, la seguridad ya no puede concebirse únicamente como la prevención de amenazas. La capacidad de adaptarse, recuperarse y aprender de los incidentes se ha vuelto crucial. Aquí es donde la resiliencia emerge como un concepto clave, especialmente cuando se considera el marco normativo de diversas normas ISO.

¿Qué es la Resiliencia?

Es la capacidad de adaptación de un ser vivo frente a un agente perturbador o un estado o situación adversos. Asimismo, se considera que es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido.

En seguridad, la resiliencia se puede definir como “un proceso dinámico donde las influencias del ambiente y del individuo interactúan en una relación recíproca que tiene como resultado la adaptación positiva de la persona en contextos de gran desafío.” Fuente: Melillo y Suárez, 2002.

La resiliencia, en términos de seguridad, se refiere a la habilidad de una organización, comunidad o sistema para:

- **Anticipar y prepararse:** identificar y evaluar los riesgos potenciales, y desarrollar planes de contingencia.
- **Resistir y absorber:** minimizar el impacto de los incidentes y mantener la funcionalidad durante situaciones adversas.
- **Recuperarse y adaptarse:** restaurar las operaciones normales lo más rápido posible y aprender de la experiencia para fortalecer la seguridad a largo plazo.

Semántica de la Resiliencia:

Es interesante explorar cómo la resiliencia se relaciona y se diferencia de conceptos como la desiliencia, la desistencia y la resistencia. Aunque todos estos términos comparten una conexión con la capacidad de enfrentar la adversidad, cada uno tiene matices semánticos distintos.



Resistencia:

Es la acción o capacidad de aguantar, tolerar u oponerse.

Su definición queda sujeta a la disciplina en la cual sea aplicada. El término proviene del latín resistētia. Está compuesto por el prefijo “re”, que explica la intensificación de la propia acción, y del verbo “sistere”, que deriva del verbo stare, que se traduce como ‘mantenerse o estar en pie’.

Desiliencia:

Situación de vulnerabilidad donde un individuo o grupo social presenta unas circunstancias desfavorables determinadas por unos niveles inadecuados de adaptación.

La relación de equilibrio entre fortalezas y debilidades a nivel interfactorial es precisamente lo que determina la caracterización de la vulnerabilidad.

Desistencia:

Hace alusión como la acción y efecto de abandonar, desistir, renunciar, ceder, dejar o abdicar mediante un derecho, empresa o intento por alguna causa o motivo o de un proceso.

En resumen:

- **La resiliencia implica adaptación y crecimiento.**
- **La desiliencia es la pérdida de esa capacidad.**
- **La desistencia implica abandono.**
- **La resistencia implica soportar.**

Estos conceptos, aunque relacionados, tienen implicaciones distintas en cómo entendemos y afrontamos la adversidad.

Las normas de la International Organization for Standardization (ISO) proporcionan un marco sólido para la gestión de la seguridad y la resiliencia. Es importante destacar que existe la norma respectiva para entender que es la Resiliencia Organizacional:

ISO 22316:2017 Seguridad y resiliencia (Resiliencia organizacional) Principios y atributos:

- Esta norma ofrece directrices para mejorar la capacidad de una organización para sobrevivir y prosperar en un entorno cambiante.
- Enfatiza la importancia de comprender el contexto, liderar con visión y valores, y fomentar una cultura de aprendizaje.
- Proporcionar un marco de referencia que ofrece un lenguaje común para la gestión de la resiliencia organizacional, facilitando la comunicación y la colaboración entre diferentes áreas de la organización.
- Busca asegurar la continuidad de las operaciones de la organización en un entorno cada vez más complejo e incierto.

En esta norma la resiliencia organizacional se define como la habilidad para absorber y adaptarse en un entorno en constante cambio para cumplir sus objetivos y prosperar.

Los principios que nos propone la norma son los siguientes:

Comportamiento alineado con la visión, misión y valores.

- Entendimiento del contexto.
- Absorber, adaptarse y responder efectivamente al cambio.
- Buen gobierno y gestión.
- Diversidad de habilidades, liderazgo, conocimiento y experiencia
- Coordinación de todas las áreas.
- Gestión del riesgo.

Disciplinas de gestión relevantes:

- Gestión de la seguridad de la información.
- Gestión de la seguridad física.
- Gestión de la ciberseguridad.
- Gestión de la salud y la seguridad.

Resiliencia & Seguridad:

La resiliencia se sustenta en la interacción existente entre las personas su seguridad y el entorno. Específicamente en el plano de las intervenciones de tipo social. Es por esta razón que se afirma que:

“La forma de evaluar la situación y a las personas no es por lo que concibe en momentos buenos y de conveniencia, sino por lo que hace en momentos de combate y controversia”.

Para Boris Cyrulnik la Resiliencia es:

- Iniciar un nuevo desarrollo después de un trauma.
- La capacidad del ser humano para reponerse de un trauma y, sin quedar marcado de por vida, ser feliz.

Lo complicado es descubrir qué condiciones la permiten avanzar, es decir, la «securización», la recuperación, las relaciones y la cultura.

La securización se refiere al hecho de dotar de la seguridad necesaria a algo, hecho de hacerlo seguro o protegerlo con los medios pertinentes.

Por otra parte, el proceso de securización tiene el efecto de hacer creer que la seguridad nunca es suficiente, quizás más difícil de observar, aunque de altísimo impacto en las personas. Junto a la privatización del espacio público se genera la sensación de falsa seguridad en los usuarios, ya que supone que en espacios controlados o cerrados se puede estar más seguros.

La resiliencia en los términos explicados proporciona una nueva partida de comprensión y habilidad para entender y enfrentar ciertos pasos o eventos particulares de la vida en cualquier organización, destacan:

- **Procesos de cambio organizacional y cultural**, en los cuales se pone a prueba la capacidad individual de cada persona para hacer frente de los retos.
- **Procesos de adaptación a demandas del entorno**, que conlleven cambios en las prácticas de seguridad tradicionales.
- **Procesos de reducción o de reasignación de personal**, que obligan a generar nuevas formas de diferenciar el trabajo de seguridad según habilidades y competencias de las personas.

Existe el Modelo de Resiliencia Organizacional que propone la International Consortium of Organizational Resilience (ICOR), el cual consta de 3 dimensiones, 9 estrategias y 16 comportamientos. Cada organización es única por lo cual la forma en que se



implemente la resiliencia organizacional exclusiva de cada organización. Hay estudios que han demostrado que existen atributos y comportamientos comunes que han sobrevivido y prosperado en tiempos de cambio e incertidumbre en diversas organizaciones.

Este Modelo se basa en la norma ISO 22316:2017 y ofrece un enfoque estructurado para mejorar la capacidad de una organización para sobrevivir y prosperar ante cambios y desafíos. A continuación, se detallan los aspectos clave de este modelo: Asimismo, se apoya en tres pilares interconectados que, en conjunto, fortalecen la resiliencia organizacional:

1.-Conciencia de la Situación (Situational Awareness):

- Implica la capacidad de la organización para comprender su entorno interno y externo, identificar riesgos y oportunidades, y anticipar posibles cambios.
- Esto se logra a través de:
 - Monitoreo continuo del entorno.
 - Análisis de riesgos y oportunidades.
 - Desarrollo de escenarios futuros.
 - Recopilación y análisis de información relevante.
 - Comunicación efectiva de la información.
 - Toma de decisiones informadas.

2.- Gestión de la Vulnerabilidad (Vulnerability Management):

- Se enfoca en la capacidad de la organización para identificar y reducir sus vulnerabilidades, tanto internas como externas.
- Esto se logra a través de:
 - Evaluación de la vulnerabilidad de los activos críticos.
 - Implementación de medidas de protección y mitigación.
 - Desarrollo de planes de contingencia.
 - Priorización de riesgos.
 - Asignación de recursos adecuados.
 - Pruebas y simulacros de planes de contingencia.

3.- Capacidad de Adaptación (Adaptive Capacity):

- Se refiere a la capacidad de la organización para adaptarse y responder de manera efectiva a los cambios y desafíos.
- Esto se logra a través de:
 - Flexibilidad y agilidad en la toma de decisiones.
 - Promoción de la innovación y la creatividad.
 - Aprendizaje continuo y mejora.
 - Colaboración y comunicación abierta.
 - Tolerancia al cambio y la incertidumbre.
 - Capacidad de recuperación y aprendizaje de los errores.

Importancia del Modelo:

- Proporciona un marco integral para la gestión de la resiliencia organizacional.
- Ayuda a las organizaciones a identificar y abordar sus vulnerabilidades.
- Fomenta la capacidad de adaptación y respuesta ante situaciones de crisis.
- Contribuye a la continuidad del negocio y la protección de los activos.

En resumen, el modelo de resiliencia organizacional propuesto por ICOR, basado en la ISO 22316:2017, es una herramienta valiosa para cualquier organización que busque fortalecer su capacidad para enfrentar los desafíos del entorno actual y futuro. 🌐

Liderazgo y talento femenino en seguridad: Impulsando el futuro del sector

• “Las mujeres que entienden su poder son las que transforman el mundo”. Robin Sharm



Milagros Céspedes Álvarez,
Coach PNL, Directora y Fundadora hace 22 años, del Centro de Estudios de Seguridad para Latinoamérica www.ceslatam.com. Involucrada en el mundo de seguridad desde hace 32 años. Miembro del Consejo Fundador de la Comunidad de Women In Security LAC de ASIS Internacional
Perú

Articulista Invitada

Lima, Perú.- El avance de las mujeres en la industria de la seguridad ha sido valioso en las últimas décadas, enriqueciendo el sector con talento, habilidades y competencias que impulsan su crecimiento y diversificación. Su participación en sectores clave como ciberseguridad, minería y cadena logística, son algunos en los que se ha experimentado un crecimiento significativo en los últimos años, impulsado por iniciativas que promueven la diversidad, equidad y la inclusión.

En Ciberseguridad el incremento ha aportado nuevas perspectivas en la protección de datos y sistemas. Al año 2023, el 37,4% de las mujeres poseen competencias digitales avanzadas. (Fuente: Revista Cloud Computing).

La gran minería es otro sector que viene promoviendo prácticas más sostenibles e inclusivas y la participación activa de mujeres en operaciones y gestión ha tenido un incremento importante. En Chile, por ejemplo, se observa un aumento de 8,9% en 2018 a 21,8% en el 2024, lo que equivale a aproximadamente 11 mil mujeres en el sector. (Fuente: Portal Minero). Otro ejemplo es la cadena logística, donde las mujeres representan el 41% de la fuerza laboral total, aunque solo ocupen el 31% de los puestos de primera línea. (Fuente: Mundo de la logística).

En el sector de la seguridad, el Observatorio Mujer y Seguridad de España en su tercer estudio publicado en marzo de 2024, destacó que las mujeres ocupaban el 15% de los puestos de trabajo en



seguridad privada (Fuente: Seguritecnia). El trabajo del Observatorio, así como de otras organizaciones y sectores, ha sido fundamental en la promoción de la igualdad de género en la seguridad. Mi felicitación sincera a quienes continúan trabajando para aumentar la representación femenina y abordar las barreras que aún existen en el sector.

Entre las varias organizaciones que se dedican a empoderar a las mujeres en la industria de la seguridad y sectores afines quiero destacar:

Women in Security (WIS) de ASIS International: Comunidad global que proporciona una plataforma para compartir conocimientos, desarrollar habilidades y establecer redes profesionales, promoviendo crecimiento y visibilidad en el sector. En especial la comunidad Latam & Caribbean ha hecho un trabajo magnífico con cinco foros y diversas actividades en los últimos años.

Nosotras en Seguridad: Grupo argentino que trabaja para fortalecer la presencia femenina en el ámbito de la seguridad, ofreciendo espacios de formación, intercambio y apoyo.

Foro de Mujeres en Seguridad de SIA (Security Industry Association): Foro que se centra en promover el liderazgo femenino en la industria de la seguridad, proporcionando recursos, mentorías y oportunidades de networking para impulsar la carrera de las mujeres en el rubro.

Women in Cybersecurity (WiCyS): Fomenta la participación femenina en ciberseguridad a través de mentorías, becas y eventos de networking.

International Women in Mining (IWIM): Apoya a mujeres en la minería, proporcionando recursos y oportunidades de desarrollo profesional.

Women in Logistics and Transport (WiLAT): Promueve el liderazgo femenino en logística



y transporte mediante programas de capacitación y mentoría. El incremento de organizaciones de apoyo y de mujeres en la industria, no solo refleja un avance en cifras, sino también el impacto en la forma en que se gestiona y lidera la seguridad en las organizaciones, aportando nuevas perspectivas, estrategias innovadoras y un enfoque más integral en la toma de decisiones, fortaleciendo así la resiliencia y eficacia.

La capacidad de las mujeres para trabajar en entornos complejos, adaptarse rápidamente a los cambios y gestionar crisis con inteligencia emocional y empatía son clave para mejorar la respuesta ante incidentes y la gestión de riesgos. Además, las mujeres destacan por su enfoque colaborativo, su habilidad para la comunicación efectiva y la construcción de equipos sólidos, promoviendo una cultura de confianza y seguridad.

El talento, liderazgo, habilidades y competencias que las mujeres aportan a la industria de la seguridad y sectores relacionados son fundamentales para su crecimiento y evolución. Las organizaciones que apoyan y promueven la participación femenina desempeñan un papel crucial en la construcción de un entorno más inclusivo y eficiente.

Sin embargo, todavía tenemos barreras que romper. A pesar de varios años de trabajo constante y del éxito alcanzado con cada foro WIS LAC, este año no tendremos nuestra VI edición, habiendo

demostrado ser un espacio de crecimiento, reconocimiento y avance para las mujeres en seguridad. Esto refuerza la necesidad de seguir impulsando la igualdad de oportunidades y de asegurar que el camino que hemos construido con tanto esfuerzo y éxito no solo continúe, sino que también inspire a las próximas generaciones.

Es momento de que las empresas y líderes del sector reconozcan el valor estratégico de la diversidad y trabajen activamente para eliminar prejuicios y abrir más espacios para las mujeres en roles de liderazgo y toma de decisiones.

La seguridad no puede fortalecerse completamente si seguimos dejando de lado el talento disponible. Fomentar la diversidad de género no solo impulsa el éxito organizacional, sino que además garantiza un enfoque más integral y resiliente para enfrentar los desafíos futuros y asegurar el desarrollo sostenible de nuestras industrias. 🌐



Competencia vs cooperación y complemento

• *Mujeres transformando la seguridad global.*



Sonia Beatriz Andrade

CPP por ASIS Internacional con especialización en gerencia de riesgos y seguros, así como en gerencia de Seguridad y Salud en el Trabajo. Miembro del Consejo fundador de WIS LATAM. Colombia

Articulista Invitada

Nacimiento de WIS LATAM

Bogotá, Colombia. - En un mundo en constante cambio, seis mujeres de diferentes países y profesiones unimos fuerzas para demostrar cómo podemos liderar caminos hacia la paz y la sostenibilidad. Con un propósito común, reunimos ideas y esfuerzos para potenciar y visibilizar el impacto de las mujeres a través de los pilares de WIS (Women in Security): Promover, Inspirar y Apoyar. Así nació WIS LATAM, una red que visualiza a cientos de mujeres dedicadas o influyentes en la práctica de la seguridad, no solo como profesión, sino como objetivo de vida, abarcando sectores públicos, privados y comunitarios.

Impacto de los foros

Hoy nos preparamos para el VI IFORO WIS LATAM en Ciudad de México, tras los exitosos foros realizados en Lima, Cartagena, Cancún, Río de Janeiro y Panamá, que dejaron huella por su impacto. WIS LATAM, además, ha fomentado intercambios de experiencias y conocimientos, consolidándose como un modelo que motiva la transformación.

Camino del CO: Una nueva visión

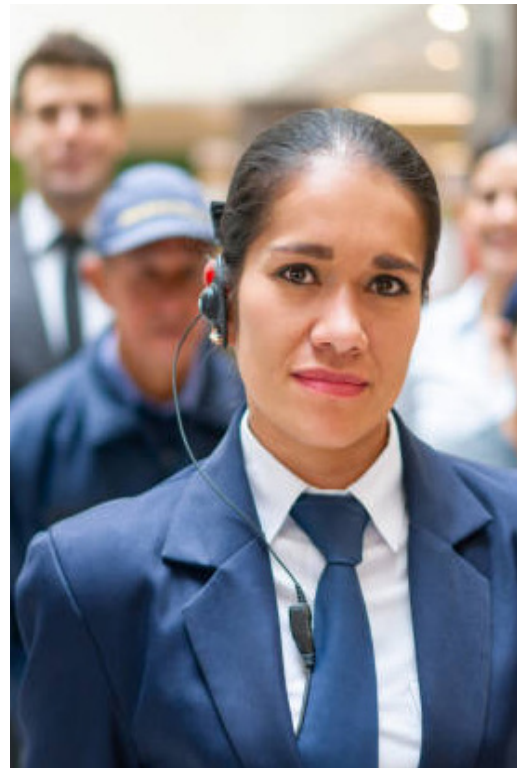
Como miembro activo y del consejo fundador, creo en el “camino del CO”: CONFIANZA, COMPLEMENTO Y COOPERACIÓN, principios esenciales para construir comunidades sostenibles.

Unidas por un propósito mayor

Esta filosofía no solo abarca la relación entre géneros, sino también entre mujeres. La cooperación significa reconocer y valorar las fortalezas de cada persona, mientras que el complemento impulsa unir capacidades en lugar de competir, creando resultados más grandes y significativos.

Derribando barreras invisibles

Tanto las emociones invisibles como los prejuicios o inseguridades pueden generar barreras y bloquear ideas, en WIS LATAM hemos demostrado que la confianza y empatía



pueden transformar estos obstáculos en oportunidades, fomentando unión y entendimiento mutuo.

Impacto del CO

La cooperación y el complemento han generado resultados tangibles: Desde comunidades resilientes hasta el éxito de los foros internacionales. Este camino inspira a mujeres y hombres a redefinir el liderazgo como un acto de colaboración y propósito. El camino del CO será liderado por WIS LATAM mediante estrategias de conciliación y entendimiento, evita procesos de agresión o minusvalía entre hacías, o desde nosotras. Este enfoque ha inspirado comunidades de mujeres resilientes en Colombia, África y Siria, y será parte del propósito de WIS LATAM liderando la transformación.

La invitación está abierta para formar parte de este propósito colectivo, con una visión de transformación global. ¡Juntos podemos construir un futuro más inclusivo! Mujeres y hombres a cooperar no a competir. 🌐

Tecnología que protege



**Un espacio donde
usted podrá:**

- **Posicionar su marca** entre los líderes que mueven la industria.
- **Generar contactos** clave para nuevas oportunidades de negocio.
- **Participar** en la mayor red de networking del sector.



Reserve su stand en
securityfaircolombia.com
o escaneando el código QR



GREMIOS ALIADOS



ORGANIZAN



MEDIOS ALIADOS



El futuro de la seguridad: Adaptación, tecnología y vocación de servicio

- *Al hacer de la seguridad un servicio proactivo y centrado en las soluciones, no solo contribuimos a la mejora continua de nuestra industria, sino que también ayudamos a construir un mundo mejor.*



Ing. María Constanza Tabernero,
gerente general de Grupo
Pucara, CPP, PCI, EMBA.
Argentina

Articlista Invitado

Buenos Aires, Argentina.- El 2025 se presenta como un año clave para el sector de la seguridad, donde la capacidad de adaptación y la generación de soluciones innovadoras serán determinantes para el éxito. La incorporación de tecnología jugará un papel crucial en este crecimiento, impactando directamente en la eficiencia, prevención y capacidad de respuesta de los servicios de seguridad.

¿Cómo están evolucionando los servicios de seguridad? La seguridad ya no puede ser vista como un costo o un servicio estático basado únicamente en la reducción del valor hora del guardia, la implementación mínima de tecnología o la ausencia de un proceso de mejora continua (PDCA). Tampoco puede permitirse la falta de capacitación o el uso inadecuado de herramientas de Prevención del Delito a través del Diseño Ambiental (CPTED).

Hoy, la seguridad debe concebirse como un servicio dinámico y estratégico, capaz de anticiparse a las necesidades de la organización y de cada individuo. Debe operar de manera constante, proactiva y en tiempo real, ajustándose a los cambios operativos, regulatorios y tecnológicos para mantenerse eficiente y alineado con cada entorno.

Un servicio de calidad implica más que solo presencia; requiere vocación de servicio:

- Ser útil, identificando y resolviendo necesidades antes de que se conviertan en problemas.
- Dar el máximo, desde guardias y supervisores hasta técnicos y equipos de soporte.
- Optimizar la tecnología, sacando el mayor provecho de cada implementación de hardware y software.

Evolucionar sin perder la esencia. Estamos en un momento ideal para evolucionar, manteniendo un equilibrio entre innovación y estabilidad. No debemos permitir que los grandes avances tecnológicos opaquen la mejora continua de lo que ya funciona. La seguridad debe avanzar al ritmo de la tecnología, pero sin descuidar sus pilares fundamentales:

- Procedimientos sólidos y bien definidos
- Capacitación constante del personal
- Asignación adecuada de guardias según cada necesidad

La verdadera evolución no es solo adaptarse a lo nuevo, sino también perfeccionar lo que ya tenemos.

2025: El año de brindar soluciones

¿Y qué pasa si ampliamos este compromiso de servicio un poco más?

En nuestra empresa, hemos definido el 2025 como el año de brindar soluciones. Nos comprometemos a transformar nuestra vocación de servicio en una generación constante de soluciones, no solo en el ámbito laboral, sino también en nuestra vida familiar y social.

Creemos firmemente que, al hacer de la seguridad un servicio proactivo y centrado en las soluciones, no solo contribuimos a la mejora continua de nuestra industria, sino que también ayudamos a construir un mundo mejor. 

La ambivalencia de la seguridad aeroportuaria en Brasil

▪ *La revisión periódica de los procedimientos, la evolución tecnológica combinada con la especialización profesional, serán siempre la mejor combinación para el sector de la seguridad.*



Bruno Vidal
Soldado de reserva de segunda clase, graduado en Gerencia de Seguridad Privada con especialización en MBA en Seguridad. Posee diversas titulaciones, otorgadas por el Grupo de Estudios Técnicos de Seguridad de la Universidad de São Paulo (GETS-USP). Es Bombero de Rescate de Aeródromo en el Aeropuerto Internacional de Salvador. Protección y postgrado en seguridad de la aviación y seguridad de vuelo.
Brasil

Articlista Invitado

El control de acceso es una medida de seguridad básica para filtrar el flujo de personas. En los aeropuertos se exigen credenciales de acceso tanto a los empleados como al público que acuda a acceder a zonas controladas, además de restringir el ingreso de personas no identificadas. El uso de circuito cerrado de televisión (CCTV) es un recurso material ampliamente utilizado en la actualidad, especialmente en activos de gran escala, como son los recintos aeroportuarios. Las cámaras de vigilancia fortalecen el sistema de seguridad al proporcionar una mayor cobertura de monitoreo de la que sería posible con solo recursos humanos. Además, fortalecen puntos de mayor sensibilidad en todo el ecosistema a proteger. Las cámaras, a su vez, también contribuyen a la recogida de pruebas materiales relativas al esclarecimiento de los delitos y al registro de los hechos.

El impacto del 11 de septiembre y la evolución de AVSEC

El hecho de que el atentado del 11 de septiembre de 2001, perpetrado por un grupo armado no estatal, se convirtiera en un punto de inflexión para la seguridad de la aviación (AVSEC) en todo el mundo. Además de las revisiones procedimentales, hubo importantes inversiones en recursos tecnológicos para solidificar mejor las acciones de seguridad, en particular, en los canales de inspección de pasajeros. Sin embargo, en el trinomio que sustenta el sector seguridad, los recursos humanos son los que más pueden comprometer y afectar negativamente la aceptabilidad de los resultados. Fallas, episodios de corrupción, mala capacitación y descuidos en el cumplimiento de los procedimientos pueden derivar en escenarios de inestabilidad y situaciones de crisis.

São Paulo, Brasil.- Las mejoras vendrán mediante el avance de los recursos materiales y la revisión de los procedimientos. Nuevas aplicaciones para incrementar la seguridad y protección en el escenario aeroportuario brasileño siempre serán bienvenidas, pero no debemos olvidarnos de considerar la capacitación continua de los recursos humanos, a continuación una perspectiva del autor.

La seguridad como base de la eficiencia aeroportuaria

La seguridad aeroportuaria, constituida por los protocolos de security y safety, es un factor muy importante para el correcto funcionamiento de los sistemas de prevención de actos ilícitos y la salvaguardia de los pasajeros y la infraestructura. Brasil, como Estado miembro de la Organización de Aviación Civil Internacional (OACI), ejecuta sus exigencias legislativas a través de la Agencia Nacional de Aviación Civil¹ (ANAC). Como se mencionó, las acciones de seguridad tienen como finalidad asegurar la integridad de los activos tangibles e intangibles, que en este caso van desde el control de acceso hasta la revisión de equipaje, salvaguardando a quienes pasan por las instalaciones, ya sean pasajeros o empleados, hasta prevenir amenazas terroristas y otros actos ilícitos.

Protocolos de seguridad y control de acceso

Son muchos los escenarios a los que están expuestos los aeropuertos y algunos protocolos acaban demostrando ser más robustos que otros a la hora de mitigar riesgos y contener amenazas. Dicho esto, abordaremos algunas dicotomías pertinentes a ciertas capas de seguridad que podemos encontrar en los aeropuertos, de manera inespecífica.





Siguiendo con el tema del atentado perpetrado por un grupo extremista a las Torres Gemelas del World Trade Center, podemos constatar la mejora en los protocolos antiterroristas. Aunque Brasil no está en la mira de estos grupos, en lo que a eso respecta, el país adopta los protocolos dictados internacionalmente a través de las directrices de la OACI. Podemos encontrar estas adopciones con mayor latencia en los aeropuertos más concurridos, fundamentalmente aquellos con vuelos internacionales.

Debilidades en áreas externas y perimetrales
Por otro lado, existe cierta fragilidad en los procesos de seguridad en áreas externas y perimetrales. En algunos aeropuertos el acceso a zonas restringidas carece de vigilancia. Como ejemplo, podemos recordar el robo ocurrido en el Aeropuerto Hugo Cantergiani, en Caxias do Sul (RS/Brasil), que resultó en la incautación de 144 millones de reales y la muerte de un policía militar y uno de los delincuentes. El alcance limitado de la interoperabilidad entre sectores corrobora resultados como éste.

El papel de los Bomberos de los aeropuertos y otros profesionales de emergencias. Así como la seguridad (security) se enfoca en las cuestiones de protección contra actos de interferencia ilícita, la protección (safety) se centra en la infraestructura aeroportuaria, en la prevención de accidentes y de la integridad física de las personas, ya sean pasajeros o empleados del aeropuerto. Un pilar importante en el ecosistema de la aviación es la figura de los bomberos de aeródromo que conforman el servicio de emergencia junto con otros profesionales.

Los bomberos de aeródromo, que integran el Servicio de Salvamento y Extinción de Incendios (SESCINC), tienen como base de acción la respuesta oportuna a las emergencias aeronáuticas, la protección del entorno aeroportuario y el restablecimiento de su operatividad, y no menos importante, la salvaguarda de vidas.

Otros profesionales que también apoyan las actuaciones de emergencia son los bomberos

y, claramente, los miembros del Puesto de Atención Prehospitalaria (PAPH). Los bomberos están capacitados para combatir incendios, brindar primeros auxilios y realizar acciones de evacuación hasta que lleguen los profesionales especializados. Los profesionales del PAPH son los principales responsables de la atención prehospitalaria en el recinto aeroportuario, con el objetivo de estabilizar la situación. Estos actores corroboran los primeros niveles de respuesta para salvaguardar vidas hasta la atención hospitalaria efectiva.

El papel del Inspector de Patio en la seguridad aeroportuaria

Hablando de seguridad en el entorno aeroportuario, no podíamos dejar de mencionar la imagen del Inspector de Patio. Este miembro muy importante es responsable de monitorear el Área de Seguridad Restringida (ARS), garantizando que las operaciones del aeropuerto ocurran de acuerdo con el Reglamento de Aviación Civil Brasileño (RBAC) y las normas de seguridad específicas del recinto aeroportuario en el que se encuentra. El Inspector de Patio, en situaciones de emergencia, brinda asistencia coordinada, buscando garantizar acciones de respuesta.

Desafíos en los aeropuertos más pequeños y la resolución N° 753 de la ANAC

A pesar de estos activos de seguridad, los aeropuertos más pequeños aún presentan cierta carencia de infraestructura, lo que puede dar lugar a una respuesta insuficiente en casos de emergencias complejas o a un aumento del tráfico aéreo por encima del nivel esperado. Por estas y otras cuestiones, la ANAC dictó el 8 de agosto de 2024, la resolución N° 753, que tiene por objeto “soluciones técnicas para mejorar la seguridad de la aviación civil frente a actos de interferencia ilícita (security), elevar los niveles de seguridad operacional (safety), mejorar la experiencia de los servicios prestados a los pasajeros y mejorar la capacidad aeroportuaria mediante la modernización tecnológica de los equipos y procedimientos aeroportuarios”.

Fortalecimiento de pilares

Según se indica en la resolución, las mejoras vendrán mediante la mejora de los recursos materiales y la revisión de los procedimientos. Nuevas aplicaciones para mejorar la seguridad y protección en el escenario aeroportuario brasileño siempre serán bienvenidas, pero no debemos olvidarnos de considerar la capacitación continua de los recursos humanos. La revisión periódica de los procedimientos, la evolución tecnológica —especialmente ahora, en la era de la Inteligencia Artificial— combinada con la especialización profesional, serán siempre la mejor combinación para el sector de la seguridad. 🌐

Referencia:

¹ La Agencia Nacional de Aviación Civil (ANAC) es un organismo regulador federal responsable de regular y supervisar las actividades de aviación civil en Brasil, tanto en sus aspectos económicos como en la seguridad técnica del sector.

CIBERSEGURIDAD
SEGURIDAD
SAFETY
REDES
FIRE



**SEGURI
EXPO
ECUADOR**

XI Feria internacional de seguridad



QUITO 5 JUNIO 2020
CENTRO DE CONVENCIONES
METROPOLITANO DE QUITO 6 JUNIO 2025

seguriexpoecuador



**11ava
edición**

www.exposeguridadecuador.com
info@myestrategia.com

**MEMBER
SEGU
EXPO
NEXUS**

RED DE CONEXIONES & NEGOCIOS PARA
PROFESIONALES Y EMPRESAS DE LA
INDUSTRIA DE LA SEGURIDAD EN
LATINOAMERICA

**CIBERSEGURIDAD
SEGURIDAD
SAFETY
REDES
FIRE**

EXPO
SEGURIDAD
& TELECOM
CENTROAMERICA



Feria internacional de seguridad



**CIUDAD DE 10-11
GUATEMALA ABRIL**

CENTRO DE CONVENCIONES HOTEL BARCELÓ GUATEMALA



FERIA INTERNACIONAL DE
TECNOLOGÍAS EN
SEGURIDAD, REDES Y
TELECOMUNICACIONES

Exposeguridad centroamerica



GUATEMALA

FERIAS
CONGRESOS
MARKETING

Silar
Global



MEMBER
SEGU
EXPO
NEXUS

RED DE CONEXIONES & NEGOCIOS PARA
PROFESIONALES Y EMPRESAS DE LA
INDUSTRIA DE LA SEGURIDAD EN
LATINOAMERICA

www.exposeguridadcentroamerica.com
info@myestrategia.com