

REVISTA

# XTREM SECURE

EL MUNDO DE LA SEGURIDAD



**Seguridad Privada**



TECNOLOGÍA DEL FUTURO EN SEGURIDAD

VISITA NUESTRAS REVISTAS DIGITALES

# Multiproseg

A quien **valor** merece





## **V** GUARDIAS **INTRAMUROS**

Ofrecemos un servicio de alta calidad con mejora continua en donde la capacitación constante de los guardias, la supervisión frecuente y la asistencia personalizada forman gran parte de nuestro éxito. Desde la selección estricta del personal hasta la calidad de los uniformes - cuidamos los detalles para satisfacer las necesidades de nuestros clientes.



## **V** CUSTODIA DE **TRANSPORTE**

Nuestro servicio de custodia al transporte se enfoca en la prevención de robos de los bienes. Contamos con el apoyo permanente de nuestro propio Centro de Monitoreo (24/7) y conexiones importantes con las autoridades, permitiéndonos una reacción inmediata en caso de un siniestro.



## **V** SISTEMAS ELECTRÓNICOS DE **SEGURIDAD**

Dependiendo de las estrategias de seguridad definidas, complementamos la protección de nuestro personal con sistemas tecnológicos como Alarmas, Control de Acceso, Videovigilancia, Seguridad Perimetral y GPS, entre otros.



## **V** ANÁLISIS Y EVALUACIÓN DE **RIESGOS**

Elaboramos esquemas de seguridad de acuerdo a las necesidades de cada caso. En el Análisis y Evaluación de Riesgos que realizamos, se valoran las amenazas y vulnerabilidades actuales para generar recomendaciones específicas y soluciones apropiadas.

**¡Contáctanos!**

Av. Armada de México No. 1500 Col. Residencial  
Cafetales Del. Coyoacán, CP 04930, CDMX

☎ 5594.5513 | 5594.5759 | 5603.0497

# EDITORIAL

No hay duda de que los avances tecnológicos ayudan a las industrias a profesionalizarse para alcanzar estándares de servicio cada vez más altos, y la seguridad no es la excepción. Cuando la protección de bienes y vidas humanas están en juego, los proveedores de seguridad deben esforzarse por emplear la tecnología más avanzada para lograr su misión.

Un buen software puede ser el punto de partida ya que provee ciertos niveles de automatización, protección y confianza, y contribuye al profesionalismo y la efectividad del proveedor de seguridad, lo que se traduce, finalmente, en tranquilidad para el cliente.

Con la tecnología móvil se pueden documentar los hallazgos encontrados en las rondas, además de que se pueden respaldar con evidencias fotográficas y video, quedando un testimonio digital de la ubicación y la hora del momento exacto en el que se levanta el reporte. Un sistema de control de rondas de vigilancia con GPS ayuda a planear, monitorear y complementar el trabajo.

Los países más avanzados en temas de seguridad han realizado un esfuerzo sistemático y coordinado para desarrollar capacidades de innovación que puedan interrelacionarse con los mejores avances tecnológicos a nivel militar a partir de la asignación de recursos para la investigación, el recurso humano y una gobernanza adecuada.

En México las empresas que ofrecen productos y servicios de seguridad siguen esforzándose en conseguir las tecnologías de punta para sus clientes, así como las empresas que brindan servicios de profesionalizar a su personal. En Xtrem Secure "El Mundo de la Seguridad" le presentamos a las empresas más profesionales y de confianza para esta encomiable labor, para cualquier duda o comentario no dude en escribir a [cvillatoro@xtremsecure.com.mx](mailto:cvillatoro@xtremsecure.com.mx), nos despedimos por este año, no sin antes desearles de parte de toda la editorial felices y seguras fiestas.

## DIRECTORIO

Noviembre- Diciembre 2019

**César Villatoro Ramírez**  
DIRECTOR GENERAL

**Mariano Botey Hernández**  
DIRECTOR EDITORIAL

**Mayte Caracas**  
GERENTE COMERCIAL

**Jazmín Rodríguez González**  
CREATIVIDAD & DISEÑO

**Voces de Seguridad**  
WEBMASTER

**Victor Cruz García**  
REDACCIÓN

**Publicaciones GBM**  
DISTRIBUCIÓN

Mariano Botey  
Jairo Rojas Campo  
Manuel Sánchez Gómez-Merelo  
David Chong Chong  
Kamila Barca  
Teodoro Serralde Medina  
Edson Yano  
Juan Manuel Harán  
Philippe Verrier

COLABORADORES EN ESTE NÚMERO

52 (55) 7663 3711  
52 (55) 52 07 47 04  
VENTAS

[cvillatoro@xtremsecure.com.mx](mailto:cvillatoro@xtremsecure.com.mx)  
COMENTARIOS



XTREM SECURE, revista dirigida a directivos, ejecutivos, empresarios, políticos y personas encargadas de contratar los productos o servicios de seguridad para su protección personal, casa o negocio.

Los juicios y opiniones de nuestros colaboradores son de carácter estrictamente personal y no representan necesariamente la opinión de nuestra revista. XTREM SECURE es una publicación bimestral de Palabras Aladas, S.A. de C.V.

Se distribuye con circulación controlada y calificada. C2019. Todos los derechos reservados. Prohibida la reproducción total o parcial por cualquier medio, incluso los electrónicos sin autorización por escrito de los editores. La información ha sido obtenida de fuentes que se consideran fidedignas, pero en ningún caso deberá considerarse como recomendación para adquirir o utilizar bienes o servicios. El contenido de los anuncios es responsabilidad del anunciante. Editor responsable: César Leobardo Villatoro Ramirez. No. de Certificado de Reserva otorgado por el Instituto Nacional del Derecho de Autor 04-2008-041411145200-102. No. de Certificado de Licitud de Título 14085. No. de Certificado de Licitud de Contenido 11658. Domicilio de la publicación: Londres 75 Desp 401-E Col. Juárez, C.P. 06600 CDMX, Impreso en Ciudad de México.

Impresora Litho Signus, S.A. de C.V. tiraje 14,500 ejemplares distribuidos en toda la República Mexicana en oficinas y exposiciones. PUBLICIDAD. Para contactar con los ejecutivos de ventas o solicitar información sobre tarifas y espacios publicitarios, comuníquense al Cel. (55) 7663 3711, Tel: 5207 4704, o escriba a: [cvillatoro@xtremsecure.com.mx](mailto:cvillatoro@xtremsecure.com.mx)

# CONTENIDO

NOVIEMBRE - DICIEMBRE - 2019



www.seguridadprivadamx.mx

31

SEGURIDAD PRIVADA



www.seguridadpublica.mx

61

SEGURIDAD PÚBLICA



www.controldeaccesosmx.com

67

CONTROL DE ACCESOS



www.seguridadindustrialmx.com

75

SEGURIDAD INDUSTRIAL



www.ciberseguridadmx.com

81

CIBERSEGURIDAD

SÍGUENOS EN REDES SOCIALES



[www.facebook.com/revistaxtremsecure](https://www.facebook.com/revistaxtremsecure)



[www.twitter.com/xtremsecure](https://www.twitter.com/xtremsecure)



[www.youtube.com/xtremsecure](https://www.youtube.com/xtremsecure)

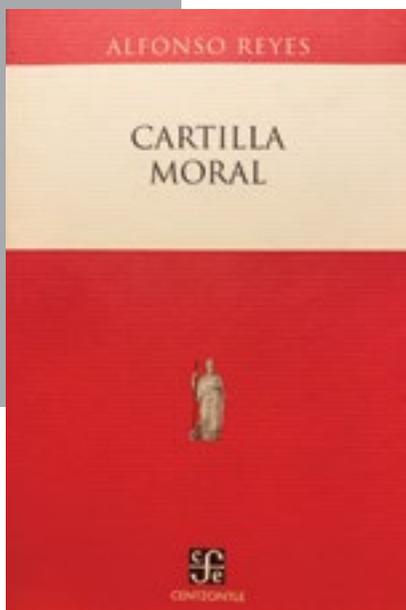
# LA SEGURIDAD DE LEER

Por Mariano Botey, [mboteyh@gmail.com](mailto:mboteyh@gmail.com)



## Cartilla Moral

de Alfonso Reyes, FCE Colc. Centzontle, México, 2004.



Este prodigioso libro aunque comenzó como encargo en 1944, tuvo sus sinistros obstáculos desde el punto de donde parte la sugerencia: “un mínimo de principios morales”; desde luego se fue dando la naturaleza de su tejido, con inquietudes espirituales en ese forraje de “lecciones morales”, hasta verse impreso en 1952: “Cartilla Moral” del helenista Alfonso Reyes; su misma obra escrita con esa agudeza mental es una disyuntiva: hacer esto o hacer lo otro; leer esto o leer lo otro. “El hombre debe educarse para el bien. Esta educación, y las doctrinas en que ella se inspira constituyen la moral o ética”. Acudamos pues a la etimología de cada palabra, que de manera breve y sin quitarle el valor: La palabra “moral” proviene del latín “moris” que significa “de la costumbre”; y la palabra “ética” del griego “ethos” significa “voluntad”. Así son los hilos de calidad de este libro del humanista Alfonso Reyes en su Cartilla Moral, con esa fuerza de voluntad en su pluma, deja impreso esos bienes de

la costumbre; porque al leerlo nos educa y orienta a ser mejores intérpretes de nosotros mismos. “Podemos figurarnos la moral como una Constitución no escrita, cuyos preceptos son de validez universal para todos los pueblos y para todos los hombres. Tales preceptos tienen por objeto asegurar el cumplimiento del bien, encaminando a este fin nuestra conducta”. No hay mejor fórmula de amarse comenzando con “el respeto que cada ser humano se debe a sí mismo, en cuanto es cuerpo y en cuanto es alma”. Reyes como buen promotor de los valores, nos sugiere que no perdamos la capacidad de asombro, como también en no desperdiciar la capacidad de alegría: “El descanso, el esparcimiento y el juego, el buen humor, el sentimiento de lo cómico y aun la ironía, que nos enseña a burlarnos un poco de nosotros mismos, son recursos que aseguran la buena economía del alma, el buen funcionamiento de nuestro espíritu”. El respeto es una regla esencial en todos los sentidos; uno elige en quedarse o moverse, dependiendo ese sentido común, Reyes supo tratar el tema sin faltar al respeto en nadie: “Sobre el amor que une a los miembros de la familia no vale la pena de extenderse, porque es sentimiento espontáneo, sólo es perturbado por caso excepcional. En cuanto al respeto, aunque es de especie diferente, lo mismo debe haberlo de los hijos para con los padres y de los padres para con los hijos, así como entre los hermanos”. Dignifiquemos esa humilde escuela de la vida: nuestro hogar. “Si los padres, que son nuestros primeros y nuestros constantes maestros, se portan indignamente a nuestros ojos, faltan a su deber; pues nos dan malos ejemplos, lejos de educarnos como les corresponde”. A propósito de las fiestas patrias y que nos enorgullece en ser mexicanos pues “El respeto a la patria va acompañado de ese sentimiento que todos llevamos en nuestros corazones y se llama patriotismo: amor a nuestro país, deseo de mejorarlo, confianza en sus futuros destinos. Se ha dicho que quien ignora la historia

patria es extranjero en su tierra. Puede añadirse que quien ignora el deber patrio es extranjero en la humanidad”. “Las palabras “civilización” y “cultura” se usan de muchos modos. Algunos entienden por “civilización” el conjunto de conquistas materiales, descubrimientos prácticos y adelantos técnicos de la humanidad. Y entienden por “cultura” las conquistas semejantes de carácter teórico o en el puro campo del saber y del conocimiento”. Reyes fue un hombre civilizado sin descuido al cultivo de su espíritu; él mismo plantea que no hubiera sido posible las valiosas aplicaciones de la electricidad sin los conocimientos previos “el solo hecho de obrar bien nos permite ser más felices dentro de la sociedad en que vivimos. Esto bien puede considerarse como una ventaja práctica”, no necesitamos premios ni reconocimientos para hacer las cosas bien sino obrar de buena voluntad; así vaya encaminado al crecimiento de su esfuerzo de cada uno por convicción propia. Vaya que Alfonso Reyes sí nos enseña a pensar y reflexionar, como es este ejemplo relacionados a los árboles, ya que alguno de nosotros hemos llegado a cuestionar el daño que le hacen a la naturaleza; a la morada de los seres inteligentes: “Dante, uno de los mayores poetas de la humanidad, supone que, al romper la rama de un árbol, el tronco le reclama y le grita: ¿Por qué me rompes? Este símbolo nos ayuda a entender cómo el hombre de conciencia moral plenamente cultivada siente horror por las mutilaciones y los destrozos”. Si algo tenía Reyes, -y fue magnánimo- fue ofrecer toda su riqueza y bienes espirituales, sin buscar algo a cambio, porque aun en la traición y en las bajezas de algunos de quienes lo rodeaban, siempre ofreció una moral en la cartilla de su corazón: “Un mexicano -educado en las buenas tradiciones de nuestra cortesía- solía decir siempre: Cuando una mano se alarga para pedirme algo, pienso que esa mano puede ser, mañana, la que me ofrezca un vaso de agua en mitad del desierto”

# VIDEOVIGILANCIAMX



REVISTA DIGITAL

ESPECIALIZADA EN VIDEOVIGILANCIA

[www.videovigilanciamx.mx](http://www.videovigilanciamx.mx)

# LANZA AXIS CÁMARA PTZ

## con analítica avanzada

*Se trata de la P5655-E PTZ que incorpora el chip de última generación que mejora la calidad de imagen, con funciones de seguridad más potentes y sistema de compresión de video más eficiente.*



Axis Communications lanza la cámara de red AXIS P5655-E PTZ, un dispositivo de alto rendimiento apta para un amplio abanico de aplicaciones de vigilancia. Incorpora el chip de última generación que mejora la calidad de imagen, tiene funciones de seguridad más potentes, junto con una capacidad superior para la analítica y un sistema de compresión de vídeo mucho más eficiente.

De acuerdo con la compañía, la AXIS P5655-E integra un sensor sensible a la luz y la tecnología WDR Forense, para verlo todo claro, aunque en la escena haya zonas oscuras como iluminadas. Además, gracias a la tecnología Axis Lightfinder 2.0 puede capturar imágenes con poca luz con una mayor saturación de colores e imágenes más nítidas de los objetos en movimiento.



Asimismo, la estabilización de imagen electrónica minimiza los efectos de las vibraciones y las sacudidas. La potencia de procesamiento superior abre la puerta a aplicaciones de analítica avanzadas y el sistema permite elegir entre cuatro perfiles de escena (interior, exterior, forense y tráfico).

"En cada perfil, la cámara optimiza automáticamente el tiempo de exposición, el balance de blancos, la apertura, la nitidez, el contraste y el ruido en función de los requisitos de la escena. El firmware firmado y el arranque seguro evitan la manipulación del firmware y garantizan la instalación únicamente de firmware autorizado. Y si es necesario, el arranque seguro comprueba que la cámara esté totalmente limpia de malware después de un restablecimiento de los ajustes predeterminados de fábrica", indicó la empresa.

### Principales características:

- ▶ HDTV 1080p con zoom óptico de 32x
- ▶ Forensic WDR y Lightfinder 2.0
- ▶ Firmware firmado y arranque seguro
- ▶ Recuperación de enfoque y EIS
- ▶ Zipstream compatible con H.264 y H.265

Para garantizar una instalación flexible, esta cámara incorpora audio bidireccional y cuatro puertos de E/S. Además, la tecnología Zipstream de Axis es compatible con los códecs H.264 y H.265, lo que reduce considerablemente el ancho de banda y la capacidad de almacenamiento necesaria.



# Control de acceso Abierto, flexible y seguro.

Nuestras soluciones de control de acceso son abiertas y se ajustan a sus necesidades. Le dan la libertad de mezclar y combinar el mejor hardware y software e integrarlos perfectamente con otros sistemas, incluyendo su sistema de videovigilancia. Puede usarlos para todo, desde identificación básica y control de entradas, hasta gestión avanzada de acceso. Nuestro portafolio de control de acceso incluye: controladores de puerta de red, estaciones de puerta de red, relés de E/S de red, lectoras de tarjetas y más, todos aportan los beneficios de IP abierta.

[www.axis.com/products/access-control](http://www.axis.com/products/access-control)

**AXIS**<sup>®</sup>  
COMMUNICATIONS



## PANASONIC presenta nuevas **CÁMARAS PTZ** para vigilancia en exteriores con mala iluminación

Los modelos de la serie i-Pro Extreme WV-X6533LN y WV-S6532LN son idóneas para aplicaciones de seguridad preventiva en vías ferroviarias, aeropuertos, infraestructura urbana, estacionamientos y estadios.

Panasonic ha incorporado a su oferta para aplicaciones de seguridad preventiva en grandes espacios de exterior y entornos de iluminación extrema, las cámaras PTZ WV-X6533LN y WV-S6532LN.

Estos modelos forman parte de la serie i-Pro Extreme, ofrecen calidad de video Full HD, tecnologías de detección de escenas y ajuste para capturar la mejor imagen posible. Además, presentan un diseño robusto para operar a la intemperie en condiciones climatológicas extremas o resistir posibles actos de vandalismo.

Pensadas para su instalación en mobiliario urbano, postes, puentes o estructuras al aire libre, Panasonic ha fabricado estas cámaras con altos estándares de resistencia tanto a los efectos del polvo y agua (IP66) como a posibles golpes accidentales o acciones vandálicas (IK10).

Su diseño facilita diferentes opciones de montaje para conseguir la mejor cobertura de imagen, en combinación con el uso de su mecanismo PTZ, lo que permite realizar movimientos horizontales y verticales, además de acercamientos, para que la labor de monitorización sea lo más completa y veloz posible.

Para obtener la mejor calidad de imagen, las cámaras WV-X6533LN y WV-S6532LN cuentan con la tecnología iA (intelligent Auto), que detecta los cambios de escena y el movimiento, para ajustar automáticamente la configuración de la cámara en tiempo real, reduciendo la distorsión y el desenfoque de objetos en movimiento.

Su revestimiento ClearSight evita que las gotas de agua y el polvo se adhieran a la superficie de la lente, lo que asegura la nitidez de imagen necesaria para la identificación de vehículos en movimiento.

La captura de imágenes bajo condiciones extremas de iluminación, como apagones o zonas sin alumbrado público, es un reto que estas cámaras superan al incorporar la tecnología Led IR.

Esta tecnología consigue iluminar a una gran distancia (hasta 350 metros para la WV-X6533LN y 100 metros para la WV-S6532LN) para capturar imágenes monocromáticas muy claras en condiciones de hasta 0 lux.

Por su parte, durante la noche o bajo densas tormentas, la tecnología de Visión Nocturna a Color ayuda a conseguir imágenes a color con muy bajo nivel de ruido en circunstancias de muy baja iluminación (0.001 a 0.015 lux).

El modelo WV-X6533LN cuenta con un lente de alto desempeño para largas distancias pues su poderoso zoom de 40x ofrece una óptima estabilización de imagen, al combinar la función Intelligent Zoom Stabilization con un giroscopio incorporado en la cámara.

Ambos modelos utilizan tecnología de compresión H.265, que reduce el uso de ancho de banda con una eficiencia de hasta el 95%, en comparación con la H.264 convencional, para incrementar el tiempo de grabación y utilizar menos espacio de almacenamiento.

Además, con la función ROI (Region Of Interest) y la codificación Auto VIQS (Variable Image Quality on Specified Area), la cámara detecta y 'aprende' las zonas de movimiento constante para que la imagen de vehículos y personas se mantenga con la mejor calidad, mientras se reduce el uso de ancho de banda.

Las nuevas cámaras incluyen el uso de una licencia del software i-VMD (intelligent Video Motion Detection), que brinda funciones de detección inteligente de cambios en la imagen o situaciones de riesgo en áreas previamente determinadas. Este es capaz de enviar notificaciones de alerta, desde una señal de aviso en la pantalla del operador de monitorización hasta la puesta en marcha de un sistema de alarma.



El centro para el aprendizaje y conocimiento de la seguridad física y en red.

Oportunidad única para ampliar su red de contactos.

El evento de actualización y networking por excelencia!

**2020**

Tel.: +593 2 604 08 06

E-mail: [pr@ipusergrouplatino.com](mailto:pr@ipusergrouplatino.com)

MEDIO ALIADO

EMPRESA  
**XTREM SECURE**  
EL MUNDO DE LA SEGURIDAD



IP-in-Action LIVE

**Bogotá**

Febrero 2020



IP-in-Action LIVE

**Santo Domingo**

Abril 2020



IP-in-Action LIVE

**Guayaquil**

Junio 2020



IP-in-Action LIVE

Ciudad de  
**Guatemala**

Agosto 2020



IP-in-Action LIVE

Ciudad de  
**México**

Octubre 2020



IP-in-Action LIVE

**Lima**

Noviembre 2020



## CÁMARA WIFI

### con panel solar integrado

Por Jairo Rojas Campo

**E**n múltiples ocasiones nos hemos visto en la necesidad de instalar equipos de videovigilancia en puntos de difícil acceso, donde las instalaciones eléctricas son un obstáculo o simplemente son muy costosas de realizar. Es por ello que las cámaras alimentadas por energía solar pueden brindar una solución de costo eficiente.

Dichas cámaras pueden ser usadas en áreas de campo abierto o sitios remotos donde realizar un adecuado tendido de cable es una tarea de alto costo o repetitiva; por ejemplo, en el desarrollo de una obra de construcción ya sea en la misma ciudad o una carretera o en urbanizaciones a campo abierto.

Daremos a conocer las recomendaciones más importantes sobre lo que se debe tener en cuenta y cuáles son las opciones a la hora de pensar en implementar cámaras WiFi con alimentación solar.

#### ¿Cómo son?

Básicamente las cámaras alimentadas por energía solar y a la vez con enlaces WiFi no requieren cableado de alimentación ni de red: utilizan paneles solares de alto rendimiento para su funcionamiento. Algunos fabricantes suministran en un solo conjunto panel, baterías, cámara y módulo de red inalámbrico, y otros ofrecen un kit con elementos separados; este caso permite

escoger o especificar según los requerimientos de duración de batería el panel solar que más se ajuste a la necesidad.

#### ¿Cómo funcionan?

La cámaras con alimentación de energía solar usan paneles de alto grado para la captura de los rayos de luz del sol y convertir esta energía luminica en energía corriente directa (DC). Adicionalmente, incorpora un sistema de regulación y en algunos modelos PoE (Power Over Ethernet) la cual a su vez se usa para energizar la cámara IP y las baterías para garantizar su uso continuo.

En ausencia de luz solar, la cámara sigue funcionando con la energía almacenada en las baterías conectadas al panel solar. Generalmente son cámaras de aplicaciones en exteriores.

Para tener en cuenta, en condiciones de lluvia o días opacos las cámaras siguen funcionando; sin embargo, el rendimiento y la eficiencia de los paneles solares no será igual al de los días soleados y despejados, aspecto importante para determinar su uso en determinados sitios o geografías con condiciones de lluvia constantes.

#### Los beneficios

Facilidad de instalación, prácticamente en cualquier parte, en sitios de difícil acceso.



**20 & 21**  
Febrero 2020



**Descuentos para:**

Socios ALAS, Usuarios finales, Gobierno,  
Asistentes a eventos ALAS y Grupos.

---

 [eventos@alas-la.org](mailto:eventos@alas-la.org)  
 321 615 3368

---

[www.alas-la.org/congresoalas](http://www.alas-la.org/congresoalas)



Esto es un evento de la:



Al no requerir cables de ningún tipo estas pueden ser instaladas en sitios sin puntos de energía cercanos, como en obras en construcción, sembrados, cultivos, establos, vehículos marítimos, aplicaciones móviles o sitios temporales, etc. Son equipos que se instalan con mayor rapidez en cualquier parte; del mismo modo son más fáciles de mantener, solo requieren limpieza y son fáciles de reinstalarse si el sitio de interés cambia.

### Amigables con el Medio Ambiente

Al aprovechar la energía solar no requieren el uso de cables, tuberías, etc., que al mover la cámara de un punto a otro generalmente estos elementos se vuelven desechos.

### Larga vida útil

Estos equipos presentan mayor duración en ambientes exteriores donde existe incidencia de afectaciones eléctricas por descargas atmosféricas. Al no contar con cableado eléctrico ni hacer parte de un circuito eléctrico son equipos menos sensibles a este tipo de afectaciones. Sin embargo, los daños por inducciones eléctricas se pueden presentar con una menor posibilidad, por lo que una correcta puesta a tierra e instalación eléctrica de equipos cercanos sí deben estar garantizados.

Algunas marcas ya ofrecen hasta 25 años de garantía donde los paneles solares pueden producir a lo largo del tiempo hasta el 80% de eficiencia con poco mantenimiento.

### Aspectos a considerar a la hora de comprar cámaras IP con alimentación de Energía Solar

Cuánta energía eléctrica puede producir el panel solar de la cámara está determinado por el tamaño y eficiencia del panel e intensidad de luz solar. Un panel típico para este tipo de aplicación puede producir alrededor de 265 vatios de potencia. Se debe revisar la ficha técnica de la cámara a instalar de modo que se pueda ajustar al consumo de la cámara.

Para obtener el mejor rendimiento de las cámaras, el panel solar debe estar orientado hacia el sol y evitar obstáculos como árboles, pancartas, vallas, etc.

Las baterías recargables son usadas para energizar la cámara en ausencia de corriente eléctrica proveniente del panel cuando la luz solar no está presente. Se recomienda que la capacidad de las baterías sea de al menos 10 veces la capacidad máxima del panel solar, de modo tal que las baterías no se dañen por sobrecarga.

Lo recomendable es consultar al proveedor por el kit (panel, cámara, batería) completo si inicialmente no se tiene la experiencia de implementación de este tipo de soluciones. Si requiere un arreglo de baterías como backup

del sistema, consulte con la fábrica o distribuidor por el modelo o referencia recomendado.

### Transmisión de datos

Lo más práctico para este tipo de aplicaciones es contar con una red WiFi para la conexión de datos de las cámaras. La mayoría de fabricantes ofrecen modelos con protocolo ONVIF con lo cual estos equipos se pueden incorporar a soluciones VMS que operen dicho estándar. Actualmente la mayoría lo permite.

Existen modelos que usan la red de comunicación celular para transmisión de video sobre 3G/4G, lo cual es una solución para casos donde no hay acceso a Internet o la construcción de una red Wifi no es posible pero sí existe buena cobertura de red celular.

### Instalaciones más seguras

Para evitar daños por robo o vandalismo es recomendable que el panel solar no esté ubicado de manera fácil de acceder; puede estar en la parte superior de un poste o sobre el techo de la edificación.

Aproveche las funciones básicas de análisis de video como detección de movimiento, merodeo y funciones de alarma como elementos disuasivos, podría generar alertas visuales o audibles que ahuyenten a posibles agresores del sistema. Se recomienda que en este tipo de aplicaciones se configure la cámara mínimo a 1080p con el fin de poder tener identificación y reconocimiento de detalles a determinada distancia.

Implemente tarjetas de memoria SD para casos de desconexión, las cuales están en los 16 y 32 GB, lo que permitirá conservar datos almacenados mientras se restaura la conectividad con el sistema VMS.

### Conclusiones

El uso de cámaras con paneles solares parece una solución costo eficiente para instalaciones donde los costos de infraestructura son altos o simplemente no se pueden realizar. A la hora de escoger la cámara integrada o conformar un kit aproveche las funcionalidades de la misma y verifique las características de potencia, baterías y la transmisión de datos. Son instalaciones rápidas y permiten la movilidad de equipos con relativa facilidad. 

*Las cámaras son alimentadas por energía solar y a la vez con enlaces WiFi, no requieren cableado de alimentación ni de red*





# ¿PARA QUÉ SIRVE LA VIDEOVIGILANCIA?

Panorama y Perspectiva de su utilidad en Seguridad

*La videovigilancia se ha convertido en una especie de “panacea” para los problemas de seguridad. Cada vez que ocurre algún evento de relevancia, una de las primeras medidas de reacción es “instalar más cámaras”, lo cual crea expectativas que en muchas ocasiones no se cumplen porque, a pesar de “tener más cámaras”, los eventos siguen ocurriendo, de tal manera que la ciudadanía se cuestiona, ¿para qué sirve la videovigilancia?*



Por David Chong Chong

*Secretario General para México de la Corporación Euro Americana de Seguridad, CEAS México. [www.ceasmexico.org.mx](http://www.ceasmexico.org.mx)*

*Correo electrónico: [dchong@ceasmexico.org.mx](mailto:dchong@ceasmexico.org.mx)*

## Panorama

Para evitar desilusiones y decepciones acerca de una propuesta, se debe acotar las expectativas a la realidad, en este caso respecto al uso de la videovigilancia. Para ello, se debe entender que:

1. La videovigilancia es un recurso de tecnología, y por tanto una herramienta que ayuda a hacer el trabajo, pero no hace el trabajo, el cual lo realiza quien utiliza la aportación de este recurso para algún propósito.
2. La función de la videovigilancia es captar las imágenes de hechos que ocurren dentro del campo visual de una cámara y que transmite a una central de monitoreo, donde se almacenan, para un uso posterior, o se proyectan, para un uso inmediato.
3. La aportación de la videovigilancia consiste en fungir como fuente de información visual, imágenes, que son reproducciones imprecisas de una supuesta realidad. “Imprecisas”, porque resultan de la composición funcional de la resolución de la cámara, el ancho de banda del canal, la frecuencia de captación (cuadros por segundo), y la resolución del medio de proyección. Y “supuesta”, porque no existe la certeza de que las imágenes que se reciben en la central de monitoreo sean las que captó la cámara.

En este contexto, se proyectan dos vertientes para el uso de la videovigilancia, ambas igualmente valiosas, pero con diferentes perspectivas:

- Como activador de una reacción ante emergencias, con la Captación de los hechos, para que un recurso de análisis bajo condiciones de apremio, y en última instancia humano, sea capaz de Detectar los problemas y Alertar con oportunidad a las corporaciones de asistencia que tienen la capacidad de Intervenir para atenderlo.



- Para un análisis forense de hechos ocurridos, también aportando la Captación de los hechos, para que un recurso de análisis, en este caso con un enfoque retrospectivo, y en última instancia humano, pueda identificar elementos de apoyo para algún propósito, por ejemplo, la identificación de presuntos responsables en la comisión de delitos.

En consecuencia, la valía de la videovigilancia, en particular por la inversión que representa su instalación, operación y conservación, está determinada por la medida en que logre los objetivos que motivaron su despliegue.

### Perspectiva

La forma más efectiva de valorar es por mediciones, para lo cual se requieren de un conjunto de indicadores, métricas y referentes. Para este propósito, se contempla una valoración inicial de dos aspectos para la videovigilancia:

- La efectividad de captación global, medida por el porcentaje de eventos captados del total de eventos ocurridos en el área, y que depende de la forma en que se usa el recurso para cubrir el área.
- La efectividad de captación de campo o focal, medida por el porcentaje de eventos distinguidos del total de eventos captados, y que depende de las prestaciones técnicas del equipo.

A partir de lo cual se aplican valoraciones específicas para las dos vertientes de uso, en los siguientes términos.

### Como activador de una reacción

En esta vertiente la instalación de cámaras se orienta a evitar que se consumen ciertos hechos, y/o a reducir su recurrencia, la incidencia delictiva en una zona, por ejemplo. Para este propósito, en nuestro País existen ciertos criterios para seleccionar la ubicación de estos recursos en los denominados Puntos de Monitoreo Inteligente, establecidos en la Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Videovigilancia para la Seguridad Pública, emitida por el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública.

Bajo estos criterios, la valoración de utilidad se puede determinar por la efectividad de alertamiento, medida por el porcentaje de eventos de interés captados, con la suficiente oportunidad para que se pueda evitar que se consumen por la intervención de las corporaciones de asistencia, así como por la efectividad de disuasión, medida por la reducción de los índices de ocurrencia y recurrencia de los eventos de interés, por ejemplo, la incidencia delictiva. Con base en esto, la medida de

utilidad será el resultado de la conjunción de ambas valoraciones, que no son mutuamente excluyentes, y considerando, en el primer caso, que el éxito en la atención de las emergencias depende, en última instancia, de la capacidad de respuesta de las corporaciones de asistencia, esto es, que el sistema puede ser útil, aun cuando no se hayan evitado que los hechos se consumen por causas ajenas al mismo.

### Como fuente para análisis forense

En esta vertiente la valoración se enfoca a la utilización de la información visual que aportan, las imágenes, en los siguientes aspectos: la efectividad como fuente de indicios, o la medida en que las imágenes captadas aportan indicios que permiten apoyar el desarrollo de los procesos de investigación de delitos; la efectividad como fuente de evidencias, o la medida en que las imágenes captadas puedan ser utilizadas como evidencias, ya sean auxiliares o plenas, en procesos de procuración de justicia; y la efectividad como fuente para prospectiva, o la medida que las imágenes captadas permiten la identificación de fenómenos inéditos y/o la conformación de medidas preventivas. En este caso, la medida de utilidad será el resultado de la conjunción de estas tres valoraciones, no excluyentes entre sí, y considerando que en todos los casos el éxito en su aprovechamiento dependerá más del trabajo del recurso de análisis.

### Conclusiones

La utilidad de la videovigilancia como activador de una reacción ante emergencias está determinada por la capacidad de detección y alertamiento, lo cual depende del desempeño del recurso de análisis, que en última instancia se refiere al personal. Por ello, la mayor utilidad de la videovigilancia ha sido en la línea del análisis forense, sin duda valiosa para remediar, no para detener, contener ni mucho menos evitar daños.

La medida de la utilidad global de la videovigilancia integra una valoración multifactorial de los aspectos antes descritos, pero disociada de la efectividad de los recursos de análisis, ya sean de naturaleza tecnológica, que por más sofisticados que sean nunca podrán trascender su diseño o su programación, o humanos, falibles por propia naturaleza. Asimismo, considerando la posibilidad de que surjan formas de utilidad no contempladas en la intención original de su instalación. 



# ELECTRÓNICA Y TECNOLOGÍA



REVISTA DIGITAL

ESPECIALIZADA EN ELECTRÓNICA Y TECNOLOGÍA

[www.electronicaytecnologia.com](http://www.electronicaytecnologia.com)



## ALEMANIA se suma al proyecto del LILIUM JET

*La empresa alemana Lilium dio a conocer que el primer prototipo de su taxi aéreo de propulsión eléctrica Lilium Jet realizó su primer vuelo a principio del mes de septiembre*

La nueva empresa alemana Lilium se suma al proyecto de taxi aéreo Lilium Jet dentro del concepto de "movilidad aérea urbana" iniciado por Boeing, Bell y Airbus

En Oberpfaffenhofen, en el sur de Alemania se realizó la primera salida del Lilium en un vuelo libre de 1 minuto.

El Lilium Jet puede despegar y aterrizar verticalmente, y luego pasar a una fase de crucero horizontal. Está propulsado por 36 ventiladores eléctricos basculantes, 24 en las alas y 12 en la nariz. Este no tiene cola ni timones y su control se basa en un sistema de propulsión distribuida.

El fabricante alemán ha expresado que Lilium será capaz de realizar un vuelo autónomo, pero se espera que entre en servicio con un piloto por razones de "regulación y aceptación" por lo que podrá transportar cuatro pasajeros.

Se espera que alcance una velocidad máxima de 300 km/h (161 kt) y un alcance de 161 nm por lo que supera las prestaciones de los competidores en el mercado que han diseñado sus aeronaves para viajes cortos e interurbanos.

Daniel Wiegand, cofundador y director ejecutivo de Lilium, dice: "Hoy estamos dando otro gran paso para hacer realidad la movilidad aérea urbana. En menos de dos años hemos podido diseñar, construir y volar con éxito un avión que servirá como nuestra plantilla para la producción en masa".

El prototipo no está tripulado y pilotado desde el suelo. Leandro Bigarella, jefe de pruebas de vuelo, dice: "Si bien un vuelo inaugural es siempre un momento de verdad para un negocio, el Lilium Jet se desempeñó exactamente como se esperaba y respondió bien a nuestras órdenes.

"Nuestro programa de pruebas de vuelo ahora continuará con maniobras cada vez más complejas a medida que miramos hacia nuestro próximo gran objetivo de lograr el vuelo de transición"- agregó.

Lilium espera que la aeronave y su infraestructura física y de software subyacente estén operativas para 2025, aunque las pruebas comenzarán antes en varios lugares no revelados.

Las pruebas iniciales de vuelo se llevarán a cabo utilizando el prototipo pilotado a distancia y un segundo vehículo tripulado seguirá más adelante. La certificación se prevé para principios de 2020, con los reguladores europeos ya involucrados en el proceso. 





## Integradores de Sistemas Electrónicos de Seguridad



Guadalajara • León • Querétaro • Yucatán  
Monterrey • Puebla • Los Mochis

 Av. Universidad 989 – 401. Col. Del Valle,  
Benito Juárez, 03100. CDMX, Tels. 5685 7830  
5685 7837 01 800 2 COMEXA

 [ventas@comexa.com.mx](mailto:ventas@comexa.com.mx)

- **Diseño de Ingeniería**
- **Servicios**
  - Comissioning
  - Desarrollo e Integración
  - Instalación y Mantenimiento
  - Administración de Proyectos
- **Sistemas**
  - Inteligencia Artificial (IA)
  - Incendio (Detección y Extinción)
  - Control de Accesos (Biometría)
  - CCTV (IP)
  - Central de Monitoreo con reporte directo al C-4 en la Ciudad de México

# EL MERCADO DE LA SEGURIDAD

alcanzará los 167,120 millones de dólares en 2025 sobre sus negocios



*El creciente impacto del IoT y la adopción de sistemas de control de acceso y videovigilancia impulsarán el mercado de la seguridad en los próximos 6 años. Según la consultora Grand View Research, este mercado alcanzará un volumen de negocio de 167,120 millones de dólares en 2025 con crecimientos anuales promedio del 10.3% en este próximo sexenio.*

Según Frédéric Salles, CEO de Matooma, “la seguridad afecta tanto a las empresas (seguridad de los empleados y de los bienes), como a las personas (seguridad del hogar, casa y familia aislada)”.

En los últimos años, el IoT y los dispositivos conectados satisfacen mejor las necesidades de seguridad de todos: cámaras de videovigilancia, desfibriladores cardíacos conectados, dispositivos de teleasistencia conectados, controles de acceso biométricos. El Internet de las Cosas se ha convertido en una tecnología esencial para el desarrollo de este sector.

## El IoT refuerza la seguridad de los bienes y las personas

Los dispositivos conectados permiten una mejor supervisión de las máquinas, anticipar accidentes humanos y materiales, y optimizar el rendimiento y los costos.

### Empresas

El IoT permite que las empresas sean más seguras y más productivas. En relación a los empleados, por ejemplo, si uno o más trabajadores están aislados, es recomendable equiparlos con un sistema de alarma o un detector de caídas para evitar que corran peligro. En el caso de una caída, por ejemplo, el detector conectado envía automáticamente un mensaje a un centro de rescate para una respuesta rápida.

La seguridad de los edificios es otro aspecto clave que deben cuidar las compañías. En este sentido, las alarmas contra incendios conectadas pueden alertar a los bomberos en caso de incendio en el lugar de trabajo. Los controles de acceso biométricos instalados en la entrada de un edificio solo permiten el acceso a los empleados de esa empresa, a través de un análisis rápido de las huellas dactilares.

Además, las cámaras de videovigilancia brindan una visibilidad permanente de las instalaciones.

Por último, la seguridad relativa a los costos es otro aspecto a tener en cuenta. Existen actualmente equipos para controlar el consumo de energía que envían alertas en caso de sobreconsumo.

### Gran público

Entre las principales aplicaciones de seguridad conectada que afectan al usuario final, nos encontramos con:

- Seguridad de la familia: las alarmas contra incendios y las cámaras de videovigilancia también ayudan a las personas a sentirse más seguras en el hogar.
- Seguridad del hogar: la domótica es un buen ejemplo. Gracias a sus peculiaridades, el concepto de 'hogar conectado' comienza a tomar forma (puertas y ventanas que se abren y cierran de forma remota, la luz que se enciende o apaga a distancia, cámaras colocadas en la puerta delantera, etc.).
- Seguridad de los seres queridos aislados: si una persona mayor vive sola y sufre algún percance, un dispositivo de teleasistencia enviará automáticamente un mensaje para solicitar ayuda.
- Seguridad en las ciudades: los desfibriladores cardíacos conectados están cada vez más presentes en lugares públicos de las ciudades.

### Problemáticas de los fabricantes de dispositivos IoT

Más allá de la simple comercialización de dispositivos conectados, el desafío para los actores del mercado de la seguridad no es el mismo.

Frédéric Salles, CEO de Matoma explica que "deben suministrar productos impecables, de hecho, un desfibrilador cardíaco o un brazalete de teleasistencia tienen que funcionar siempre cuando una persona los necesita". El rendimiento de los objetos conectados y la elección de una buena solución de conectividad son dos elementos que no deben pasarse por alto.

### Tarjeta SIM M2M multioperador para mayor seguridad

La tarjeta SIM multioperador es una solución de conectividad que aporta fiabilidad a los dispositivos conectados. Una vez insertada en el objeto, la tarjeta se conecta automáticamente a la mejor red local disponible. Esta tarjeta asegura una conectividad cercana al 100% de los dispositivos IoT. De hecho, esta tarjeta SIM puede conectarse a diferentes redes locales. Por lo tanto, si una de las redes tiene problemas de conexión en un momento determinado, el dispositivo inicia automáticamente un escaneo de las redes disponibles y la tarjeta SIM se conecta a otra red confiable y potente. 

## ¿Cuál será el papel de las computadoras cuánticas en el MACHINE LEARNING?

La Inteligencia Artificial ha sido usada en la sociedad y en especial las empresas, principalmente en una parte llamada machine learning (aprendizaje de máquinas). En este proceso las máquinas acceden a determinados datos y con el uso de estadística y patrones de repetición recibimos resultados. Muchos llegan a ser útiles, otros no dicen nada, pero no suelen ser vistos.

Los humanos poseemos conocimientos que aplicamos a partir de correlaciones y algunas reacciones básicas que nos permiten sobrevivir. Por supuesto, muchas veces eso no quiere decir que haya una causa, pero implica un tipo de pensamiento diferente al de "llenarnos de datos" para mostrar inteligencia. En términos generales, podemos decir que nuestra capacidad nos permite recibir información, retenerla como dato y luego aplicarla a diversos contextos y situaciones.

Sin embargo al introducir una serie de valiosos datos a una máquina no podemos todavía obtener resultados. El mayor problema para obtenerlos es que alrededor de machine learning seguimos encontrando barreras que van desde lo técnico a lo contextual, saber qué puntos de los datos se juntan bajo qué contextos.



Hace décadas las computadoras impresionaban con su capacidad para procesar hojas de ingresos, egresos y otras cosas más. Pero las computadoras no te dicen cómo tener finanzas personales o familiares saludables, de hecho, no muchos sabemos cómo hacerlo. Es por esto que muchos expertos apuestan por las computadoras con procesamiento cuántico para empezar a detectar correlaciones, razonamiento simbólico, puntos de contacto que probablemente

como humanos no lograríamos hacer a escalas masivas.

¿Serán estas computadoras cuánticas las que finalmente nos ayuden a completar el viaje que hay desde el machine learning a la inteligencia artificial? Este campo está muy poco explorado pero el salto de capacidad de procesamiento de las mismas nos permite imaginar escenarios muy prometedores. Será cuestión de esperar. 



blu!

un nuevo producto de  tiLatina

*Diariamente en nuestro país se pierden al menos 17 millones de pesos por el robo de mercancía que sufren los transportistas de carga. En promedio, un camión de carga es robado cada 45 minutos en México, una cifra alarmante si se compara con otros países.*

*Por ejemplo, se calcula, que por cada unidad robada en los Estados Unidos, en México se roban alrededor de 20.*

Según datos oficiales, el costo total de la inseguridad en el autotransporte durante el año pasado ascendió a 43 mil 665 millones de pesos. Como una respuesta a esta grave problemática, ti Latina, una de las empresas de seguridad más prestigiadas en nuestro país, dio a conocer su nuevo producto: **blu!**

El pasado 21 de septiembre, en un evento realizado en los viñedos La Redonda, en el estado de Querétaro, ante clientes e invitados especiales, Ti Latina presentó formalmente blu!, un sistema de seguridad enfocado a la protección del transporte de carga en viajes de punto a punto o de reparto.

Se trata de tecnología 100% mexicana, operada por la plataforma **Axelia**, que actúa de forma autónoma cuando deja de tener contacto con el centro de monitoreo, garantizando así el cumplimiento de los procesos operativos. Además permite comunicarse, vía voz, con el operador.

Otra característica de blu! es la detección casi inmediata de jammers. En poco menos de un minuto, informa al operador el protocolo a seguir y efectúa acciones automáticas, como el paro de motor de la unidad y el bloqueo de la misma, sin que el operador pueda impedirlo.



*Sistema de seguridad autónomo para el transporte de carga.  
Tu carga protegida.*

En caso de robo, el sistema blu! es capaz de emplear algunos elementos disuasivos, como la activación de buzzer, el bloqueo de puertas, cortinas de humo y barreras de sonido.

La plataforma **Axelia**, con la que opera **blu!**, requirió más de siete años de desarrollo y es un excelente ejemplo de lo que es la seguridad inteligente. Este sistema integra el monitoreo de video y convierte cualquier cámara, de cualquier marca, en un detector.

La plataforma permite, además, establecer la geolocalización de un individuo y en caso de suscitarse una emergencia, enviar ayuda. **Axelia** administra y gestiona sistemas de alarma, así como de niebla y otros, permitiendo su activación en cuanto se confirma un evento.

**Axelia** agrega eficacia y valor, si ya se cuenta con un centro de monitoreo pues disminuye costos al requerir un mínimo de personal y es, hoy en día, el único sistema de seguridad accesible que administra GPS, video y alarmas en un solo lugar. Es ideal para la protección de personas, vehículos de transporte, oficinas y hogares.

Con **blu! Ti Latina** se ha anotado un éxito más y se coloca, nuevamente, a la vanguardia en innovaciones tecnológicas enfocadas a la seguridad. Sin duda será ampliamente aceptado por el mercado y muy pronto escucharemos muchas buenas noticias sobre este gran producto. 📺

**Bienvenido blu!**





# Alertan sobre los **ROBOTS ASESINOS**

Por Kamila Barca

La tecnología ha cambiado nuestro día a día, y lejos de ser una distopía, también puede destruir grandes cosas con pequeños movimientos. Hablar de robots asesinos puede dar una sensación de lejanía, pero sin pensar a lo grande, hace sólo unas semanas una de las bases petroleras más importantes del mundo fue atacada por un dron de baja tecnología que estaba en las manos equivocadas.

El presidente de Microsoft insiste en su entrevista en algo similar, puesto que señalaba que algunos drones pueden equiparse con sistemas de armas letales, misiles, bombas o armas de fuego.

El caso de los robots o armas más avanzadas con IA es que pueden ser imparables por culpa de la autonomía implantada en ellos mismos. "No se les debe permitir decidir por sí mismos participar en el combate y a quién matar", insiste Smith.

Además ha hecho un llamamiento especial a una nueva Convención de Ginebra para hablar del peligro del desarrollo de estas armas letales: "La seguridad de los civiles está en riesgo hoy. Necesitamos una acción más urgente, y la necesitamos en forma de una Convención digital de Ginebra, normas que protegerán a los civiles y soldados".

Hasta ahora ha habido 4 Convenciones de Ginebra que intentan regular el derecho internacional humanitario con el objetivo de proteger a las víctimas de conflictos armados. La primera de ellos protege durante la guerra a heridos y enfermos de las fuerzas armadas en campaña, la segunda a las fuerzas armadas en el mar, la tercera a los prisioneros de guerra y la cuarta a personas civiles, incluso en territorios ocupados.

Llevarlo a un terreno tecnológico puede cambiar la historia pero sobre todo tener el control y poder sobre estas armas que ahora mismo no conocen límites.

*El presidente de Microsoft, Brad Smith, considera un asunto de máxima importancia, que debería hablarse en una Convención de Ginebra, el desarrollo de los robots asesinos o las armas con Inteligencia Artificial, tal y como ha comentado en una entrevista con The Telegraph.*

Además, Brad Smith recoge una reflexión en su nuevo libro Tools and Weapons (Herramientas y armas) la necesidad de controlar algo mucho más sensible si cabe: la tecnología de reconocimiento facial.

"Es necesario que haya una nueva ley en este espacio, necesitamos una regulación en el mundo del reconocimiento facial para protegernos contra posibles abusos", explica el mismísimo presidente de una empresa tecnológica cuyas técnicas tiene a su alcance. 





PROYECTOS TI  
Si de convergencia hablamos



01 800 58 10 689



[www.proyectosti.mx](http://www.proyectosti.mx)



[contacto@proyectosti.com.mx](mailto:contacto@proyectosti.com.mx)





## NUEVAS TECNOLOGÍAS en seguridad

*No hay duda de que los avances tecnológicos ayudan a las industrias a profesionalizarse para alcanzar estándares de servicio cada vez más altos, y la seguridad no es la excepción. Cuando la protección de bienes y vidas humanas están en juego, los proveedores de seguridad deben esforzarse por emplear la tecnología más avanzada para lograr su misión.*

Un buen software puede ser el punto de partida ya que provee ciertos niveles de automatización, protección y confianza, y contribuye al profesionalismo y la efectividad del proveedor de seguridad, lo que se traduce, finalmente, en tranquilidad para el cliente.

La tecnología móvil es especialmente útil para la industria de la seguridad ya que este tipo de empresas operan por procesos de vigilancia, donde el personal hace rondines en ciertos horarios con los que se encargan de observar que no haya incidencias, así como de reportar cualquier situación fuera de lo normal.

Con la tecnología móvil se pueden documentar los hallazgos encontrados en las rondas, además de que se pueden respaldar con evidencias fotográficas y video, quedando un testimonio digital de la ubicación y la hora del momento exacto en el que se levanta el reporte. Un sistema de control de rondas de vigilancia con GPS ayuda a planear, monitorear y complementar el trabajo.

Además, en el camino para profesionalizar sus servicios es natural entrar en procesos de certificación de calidad que, como es bien sabido, requieren de estándares definidos y documentación de los registros de gestión de la operación, de donde resulta información relevante para la toma de decisiones.



Los países más avanzados en temas de seguridad han realizado un esfuerzo sistemático y coordinado para desarrollar capacidades de innovación que puedan interrelacionarse con los mejores avances tecnológicos a nivel militar a partir de la asignación de recursos para la investigación, el recurso humano y una gobernanza adecuada.

Actualmente, los temas que se trabajan en seguridad priorizan lo siguiente:

**1.** La seguridad cibernética, que es un elemento clave que permite anticipar las vulnerabilidades a través del fortalecimiento de los sistemas cibernéticos e infraestructura, permite el monitoreo en tiempo real y fortalece la respuesta y recuperación en caso de un ataque o amenaza potencial.

**2.** La inteligencia, que implica en la recolección de los datos, con sus fuentes, análisis, integración y generación de resultados de forma precisa y oportuna es fundamental para la seguridad de cualquier país, para las agencias de inteligencia, cumplimiento legal y autoridades de protección de fronteras y salud.

**3.** Seguridad fronteriza y gestión de identidades, implica la aplicación de la ciencia y la tecnología para mejorar la capacidad de rastrear, identificar y detectar personas, objetos, materiales peligrosos o amenazas que requieren la observación y evaluación de explosivos, agentes químicos, biológicos o radiológicos, enfermedades, narcóticos u otro tipo de materiales o productos peligrosos para la seguridad.

**4.** Las ciencias forenses, son fundamentales para mejorar las capacidades para utilizar la información como apoyo forense, que implica procesamientos efectivos para evitar actividades terroristas y criminales con nuevas tecnologías que permitan trabajar y analizar la situación en el lugar de los hechos para generar información científica, oportuna y precisa, para apoyar la investigación de los sucesos.

*Finalmente la protección, prevención y respuesta al riesgo, implica que se debe estar equipado y preparado para responder de manera efectiva y segura a eventos que puedan alterar la seguridad.*



## Seguridad digital

La **seguridad digital** de la información es una preocupación para todas las personas, gobiernos y empresas del mundo. Cada día aumentan los factores de riesgo que facilitan los cibercrímenes, sin embargo, los avances tecnológicos también se han desarrollado a pasos agigantados y, sobre todo, han ampliado su alcance a un creciente número de personas, el mejor ejemplo de ello son los sistemas de seguridad biométricos.

Actualmente, los usuarios gestionan múltiples cuentas online de servicios y entretenimiento adicionales a sus cuentas de acceso de los dispositivos electrónicos, por lo que diariamente manejan un sinnúmero de contraseñas de seguridad. El problema es que la acción típica de la mayoría de las personas es utilizar una misma contraseña para todas sus cuentas, lo cual favorece su desciframiento y peor aún, el mal uso o robo de su información.

Se estima que para el año 2020, el usuario promedio contará con alrededor de 200 cuentas en línea, lo que se traduce en 200 contraseñas distintas. ¿Cómo afrontar este reto?, una opción es la biométrica, es decir, la tecnología dedicada a medir y analizar datos biológicos como la huella dactilar, las características del ojo, la geometría de la mano, las características faciales y hasta patrones de voz.

En este sentido, el lector de huella digital se ha convertido en uno de los sensores de autenticación más eficaces, accesibles y sencillos de utilizar, por lo que se ha comenzado a integrar en los teléfonos inteligentes.

Esta tecnología funciona con la correspondencia entre la huella digital presionada en el lector y la "imagen" almacenada en el dispositivo, la cual es una representación detallada de la huella, que incluye todos los arcos, curvas y círculos de los poros del dedo.

Según un estudio de Deloitte Global, se calcula que este año habrá más de mil millones de dispositivos equipados con lectores de huellas digitales. Si cada sensor se utiliza en promedio 30 veces al día, implicaría más de 10 billones de pulsaciones al año en todo el mundo.

En contraste con los otros sistemas biométricos, las huellas digitales ofrecen las ventajas de que el sensor funciona en segundos, incluso en la oscuridad, y puede ejecutarse discretamente mientras el usuario camina o realiza otras actividades.

Además, los smartphones que incluyen el lector de huella digital constituyen una herramienta de seguridad integral, debido a que



unifica los tres factores de autenticación esenciales: de conocimiento, inherente y de posesión. El primero se basa en contraseñas, NIP (Número de Identificación Personal) y preguntas de verificación, el segundo consiste en la biometría la cual implica una firma biológica única e irrepetible, y el tercero que está relacionado con la conectividad de los teléfonos, por lo que en caso de robo se pueden rastrear con mayor facilidad e incluso deshabilitarlos de manera remota.

La tecnología biométrica aplicada con propósitos de seguridad, identificación y autenticación, es una herramienta valiosa en la actualidad. Se estima que el 40% de todos los teléfonos inteligentes en países desarrollados incorpora un lector de huella digital y al menos el 80% de los usuarios de estos smartphones utiliza con regularidad este sensor.

Esta situación se perfila como una oportunidad relevante para la adopción general de la biometría en otros entornos de la vida, por lo que es probable que en los

próximos años se alcance un desarrollo de la tecnología biométrica más sofisticado y eficaz.

Adicionalmente, el uso de varios sensores biométricos como clave de autenticación aumentará potencialmente la seguridad de la información y con ello la confianza de los propios usuarios.

Para lograr este avance en materia de seguridad depende de la democratización tecnológica, es decir, a la apuesta de que más personas puedan tener acceso a dispositivos móviles de calidad. Así, el uso cotidiano de la tecnología biométrica será una acción cada vez más familiar para las personas, lo que a su vez promoverá la investigación científica para la mejora de la tecnología biométrica mundial.



*Actualmente una de las preocupaciones de los ciudadanos es la seguridad, tanto en sus hogares como en su trabajo, el transporte, la calle y en prácticamente toda la ciudad. Y es que en los últimos años se han incrementado los asaltos, el vandalismo, los robos de automóviles y otros delitos.*

## Ciudades seguras, una tendencia en la vanguardia tecnológica

Una de las tendencias que está marcando el futuro son las llamadas ciudades seguras, donde la tecnología inteligente cobra un papel importante, con una vigilancia las 24 horas, con sistemas de monitoreo y videovigilancia que ayuden a la prevención y reacción contra algún incidente.

Existen soluciones de videovigilancia para la seguridad de las personas, sus propiedades e instalaciones, los nuevos sistemas inteligentes de cámaras son complementados con otros sistemas que ayudan a integrar varios equipos y soluciones en uno mismo, de esta forma se logra monitorear y analizar en vivo varias zonas de la ciudad.

Adicionalmente, también se encuentran los sistemas de alerta que ayudan a identificar situaciones de alto riesgo para las personas, dando aviso oportuno a los servicios de seguridad.

El costo de reparación en inmuebles y negocios por vandalismo y robo de materiales suele ser muy elevado, otra de las preocupaciones de los ciudadanos mexicanos es la seguridad de sus negocios y mercancías. Ante esto, hemos visto un crecimiento de herramientas tecnológicas que apoyan en la administración, control y vigilancia de los negocios.

Desarrollar aplicaciones de analítica de video que habilitan la vigilancia proactiva, ayuda al personal de seguridad a proteger su propiedad mediante la detección y disuasión de delitos. Las aplicaciones pueden, por ejemplo, detectar intrusos o merodeadores y notificar automáticamente a un vigilante o reproducir un mensaje de audio por un altavoz.

También existen tecnologías de analítica inteligente que proporcionan estadísticas útiles y prácticas que pueden ayudar en el control y administración de las multitudes



en lugares muy concurridos, como lo son las tiendas o supermercados, donde el comercio minorista a través de la analítica puede mejorar la experiencia del cliente, mejorar las ventas, prevenir las pérdidas, optimizar procesos y aumentar los beneficios.

La mayoría de los delitos son investigados horas después de que han sucedido e incluso, muchas veces no se obtiene la información necesaria para dichas investigaciones, es por esto que contar con la tecnología adecuada, los sistemas de vigilancia completos, cámaras de videovigilancia y audio IP conectados a un sistema de monitoreo en vivo es imprescindible.

Los sistemas de videovigilancia inteligente son lo de hoy, el aumento de tendencias tecnológicas como el IoT, Ciberseguridad e Inteligencia Artificial, pueden mejorar el mundo de la vigilancia y ya lo están permitiendo, por ejemplo con dispositivos con grabaciones en 4K, cámaras que permiten identificar en la oscuridad o en condiciones difíciles, son algunos de los cambios actuales que se ha tenido en la industria de la videovigilancia.

Las cámaras de videovigilancia llevan muchos años presentes en nuestras vidas como parte del mobiliario urbano, pero esto ha cambiado de modo vertiginoso, desde las propias cámaras de seguridad que han reducido su tamaño y mejorado la calidad de la imagen, incluso en situaciones de mala visibilidad por el clima o la falta de luz, hasta el no tener que estar pendientes de si se terminan las cintas de las grabadoras o poder ver las imágenes en tiempo real a través del móvil.

Hoy día los circuitos cerrados de televisión han pasado de ser unos simples grabadores de imágenes, o ser una herramienta para el personal de seguridad para vigilar los perímetros desde un centro de control, a disponer de más funcionalidades que no hace muchos años pensaríamos que eran imposibles.

Las nuevas funcionalidades de las cámaras de seguridad son: visión nocturna, visión térmica, mapas de calor, visión telescópica avanzada, conteo de personas, reconocimiento facial, identificación de placas de vehículos y un largo etcétera.

La información que genera la videovigilancia debe ser analizada para no desperdiciar las nuevas funcionalidades de los sistemas. No sólo se trata de dejar constancia de lo que ocurre sino de millones de datos que pueden ofrecer una valiosa información.

La videovigilancia no sólo implica la seguridad de personas, lugares y objetos, ahora también son un elemento indispensable para el control de acceso físico, comunicación bidireccional y la gestión de situaciones de emergencia y, en paralelo, que se pueda manejar desde una distancia considerable. El factor espacio ha dejado de ser un factor primordial.

El Internet de las cosas ha evolucionado, ha dejado de ser un mero concepto para convertirse en una realidad, pero esto conlleva también varios desafíos, sobre todo en cuanto a la ciberseguridad ya que deben conseguirse sistemas bien protegidos para evitar ataques.

## Tecnologías de vigilancia para luchar contra el crimen



*Las cámaras de vigilancia no sólo ayudan a las autoridades en la lucha contra infracciones menores, también han contribuido en ocasiones a esclarecer hechos criminales tan graves como un asesinato o un intento de homicidio sin testigos.*

La aparición de la inteligencia artificial ha hecho aún más sofisticados los actuales sistemas de seguridad, permitiendo incluso monitorear e interpretar los movimientos de los ciudadanos. China es hoy uno de los países más avanzados en esta tecnología, gracias a la potente red de vigilancia que ha montado utilizando la información que proporcionan las 20 millones de cámaras inteligentes que observan sus ciudades y que utilizan complicados algoritmos para saber exactamente lo que tienen que buscar.

El sistema, de nombre Sky Net, puede no sólo atestiguar sobre la comisión de un delito sino también hallar a su autor en cuestión de segundos. Para ello sólo necesita contar con la imagen del sospechoso y cruzar la información que le proporcionan las millones de imágenes que recoge diariamente para saber dónde está e indicárselo a las autoridades.

Sin embargo, este espionaje continuo al que somete Sky Net a los habitantes de ese país, también ha despertado suspicacias ante la presencia de este ojo que todo lo ve, más allá incluso de delitos o crímenes, lo que se considera una intromisión exagerada en la vida de sus ciudadanos.

El debate entre privacidad y seguridad está planteado, y es que vivimos en un estado de exposición permanente, no sólo gracias a estas tecnologías de vigilancia, sino también a la información que nosotros mismos proporcionamos de nuestras vidas y de las de otros a través de Internet y las redes sociales.

Estos datos personales que “regalamos”, de forma consciente o no, son analizados por algoritmos entrenados para elaborar nuevas estrategias de marketing, estudiar nuestro comportamiento o incluso, llevados al extremo, investigar y hasta reproducir una conducta anómala o psicopática.

Quién no ha buscado un determinado producto por Internet y se ha sorprendido luego cuando en su perfil de una red social se le bombardeaba con anuncios al respecto sin que exista relación aparente entre ambos entornos.

En definitiva, vivimos en una sociedad en la quizá sea en el futuro un verdadero artículo de lujo. Y es que la tecnología no deja de avanzar para hacer cada vez más difícil, y hasta imposible, escondernos de esa vigilancia permanente.



## Vigilando todo lo que sucede en el planeta

La aparición de los satélites ha supuesto un cambio definitivo en la forma de observar el mundo, ya que ha permitido mejoras en ámbitos tales como los sistemas de posicionamiento (GPS), la agricultura de precisión, la respuesta de emergencia ante desastres naturales, la vigilancia de infraestructuras e, incluso, el rastreo de fraudes inmobiliarios o el descubrimiento de delitos desde el espacio.

Hasta ahora el mayor obstáculo en la búsqueda de nuevas aplicaciones para esta tecnología era su elevado costo. Sin embargo, esto podría dejar de ser un problema gracias a las soluciones que proporcionan firmas como Planet, que tiene en órbita más de 150 satélites -a los que llama Doves (palomas), con un costo tan reducido como su tamaño: algo así como una caja de zapatos. Estos pequeños observadores toman hasta dos fotografías por segundo del espacio que controlan, lo que hace posible un seguimiento continuo de la transformación de la superficie de la tierra.

Planet trabaja ya con organizaciones como la Asociación de Conservación de la Amazonia, monitoreando por ejemplo la deforestación de su superficie en Perú, o con Amnistía Internacional, en la detección y control de conflictos armados. Incluso algunos periódicos, como USA Today, han solicitado en algunas ocasiones imágenes para buscar pruebas de ataques en ciudades en guerra.

Con este grado de vigilancia, parece imposible que exista algún lugar en el mundo en el que algo pueda ocultarse a estos pequeños observadores que nunca duermen, lo que obliga a aplicar ciertas limitaciones éticas para evitar un uso



malintencionado de la cantidad ingente de información que ofrecen.

Planet asegura que nunca proporciona imágenes que puedan ser utilizadas de forma perjudicial para la sociedad. Y también aplica restricciones para respetar la intimidad de las personas, evitando, por ejemplo, que las figuras humanas puedan ser distinguidas de forma nítida.

## Para proteger la privacidad

La Unión Europea ha alertado sobre temas de seguridad en innovación tecnológica. Los países europeos tienen la obligación de analizar cuáles son los riesgos de seguridad más importantes dependiendo de las características de su nación. Por lo general, se dividen en técnicos (posibles problemas de los equipos y programas informáticos) y jurídicos. Estos últimos exigen una adaptación de la normativa legal de cada país en su relación con terceros países proveedores del servicio.



En octubre de 2019, los países implicados compartieron los riesgos detectados y comenzaron a trabajar en la elaboración de un documento conjunto que proteja mejor a la ciudadanía. La protección de la privacidad y los datos es uno de los pilares fundamentales de esta medida.

El conflicto entre Estados Unidos, Google y Huawei es el resultado directo de la enorme evolución tecnológica de China, la tecnología 5G proviene de este país. La UE no ha apostado por la prohibición, pero sí por alertar a los países que forman parte de ella de que la situación va a cambiar en breve. Al igual que sucediera con la puesta en marcha de las redes 4G, no se busca beneficiar a nadie sino mantener la seguridad.

Y es que decir 5G es apostar por el Internet de las cosas, por la domótica, por los mayores avances tecnológicos y por incluir dispositivos diversos en una casa que hagan la vida más fácil. Este presunto avance no deja de ser como tener a un invitado permanente en la casa, por lo que resulta imprescindible tomar medidas de seguridad para evitar consecuencias imprevisibles.

El sector corporativo deberá saber cómo proteger la empresa y los datos de sus clientes para lograr seguir avanzando. Modernizar sus redes y apostar por la mejor tecnología 5G será el camino para convertir a las compañías en modelos cada día más eficientes.



**MÁS CERCA  
DE NUESTROS LECTORES**

Ahora puedes consultar  
la revista **XTREM SECURE** de  
manera GRATUITA en el:

- Aeropuerto Internacional de la Ciudad de México
- Aeropuerto de Toluca



**TU REFERENCIA EN SEGURIDAD**

f Revista Xtrem Secure

@XtremSecure

[www.xtremsecure.com.mx](http://www.xtremsecure.com.mx)

# **SEGURIDAD PRIVADA**MX



REVISTA DIGITAL

ESPECIALIZADA EN SEGURIDAD PRIVADA

[www.seguridadprivadamx.mx](http://www.seguridadprivadamx.mx)



## Grupo Multisistemas y Universidad Anáhuac **SE UNEN POR LA SEGURIDAD**

*La empresa mexicana de seguridad privada, Grupo Multisistemas, refrendó su acuerdo con la Universidad Anáhuac para seguir desarrollando un Master de Liderazgo e Innovación para empresas de seguridad privada enfocado a capacitar y profesionalizar a mil 200 directivos provenientes de todo el país.*

La alianza entre estas dos instituciones tiene como fin ir un paso adelante en los procesos de tecnología, calidad y mejora continua en los servicios de seguridad privada que la compañía ofrece. Es importante recalcar que la universidad y la compañía de seguridad se asociaron desde hace 23 años.

El curso tendrá entre sus nuevos procesos y temas el análisis delincriminal, cómo opera y se mueve la delincuencia. Además, se enseñará como qué se puede hacer para que los clientes, su patrimonio y su personal estén más seguros.

*“Esto, sin tecnología y sin protocolos, sería insuficiente; trabajamos para que nuestro cliente tenga una seguridad real y total”,* dijo el Lic. Alejandro Desfassiaux, presidente de Grupo Multisistemas de Seguridad Industrial.

En el evento también estuvieron presentes Inocente Fermín Hernández Montealegre, general de Brigada D.E.M. y subjefe de Inteligencia del Estado Mayor de la Secretaría de Defensa Nacional; el Lic. Elías Salomón Nader, CEO de Fármacos Nacionales; el Lic. Raúl Sapién Santos, presidente del Consejo Nacional de Seguridad Privada; el Lic. Gonzalo Martínez de Teresa, director general de Seguridad Privada de la Secretaría de Seguridad y Protección Ciudadana; José Herrera Chávez, comisario jefe y coordinador de SIDEPOL de la Guardia Nacional, y el Mtro. Alfredo Nava Govea, director de la Facultad de Economía y Negocios de la Universidad Anáhuac.



# GECSA

## SEGURIDAD PRIVADA



*SI LO PUEDES PREVER*  
***LO PUEDES RESOLVER***

[www.gecsa.com.mx](http://www.gecsa.com.mx)

01 (55) 5363 2868 | 01 (55) 5373 1761

Calle Limoneros No. 9-A, Col. Valle de San Mateo Naucalpan, Estado de México, C.P. 53240





## UN DÍA SIN

# Seguridad Privada...

*Por Manuel Sánchez Gómez-Merelo, Consultor Internacional de Seguridad*

**E**spaña.- Si un día al despertarnos observáramos que las empresas y profesionales de la seguridad privada dejaron sus puestos y misiones... las armas, la vigilancia, la protección de los bienes y personas... ¿qué pasaría? Pues, sencillamente, que tendríamos un caos de tamaño descomunal.

Un caos por la desaparición sin alternativa de una seguridad privada, donde en por ejemplo en España trabajan, según datos del Ministerio del Interior, más de 1,500 empresas acreditadas, con más de 100,000 profesionales habilitados, y en la que, sólo en el año 2011, se llegaron a realizar más de cuatrocientos mil contratos y más de un millón cien mil servicios, con un resultado en materia de colaboración de más de sesenta mil actuaciones o comunicaciones a las Fuerzas y Cuerpos de Seguridad sobre auxilios, colaboraciones, informaciones y detenidos.

Pero, más allá de unas cifras globales, y a modo simplemente de ejemplo, ¿cómo sería un día normal de actividad en un aeropuerto como el de Madrid donde trabajan más de 600 vigilantes de seguridad, o en el Metro de Barcelona y Madrid donde desarrollan su actividad más de 600 y 1,500 vigilantes de seguridad, respectivamente?

¿Qué pasaría en una Central Nuclear donde hay habitualmente más de 70 vigilantes de seguridad? ¿Y en

los centros comerciales, áreas industriales, polvorines, transporte público, etc.? ¿Cómo se gestionarían grandes eventos culturales o deportivos donde pueden llegar a trabajar más de 500 vigilantes de seguridad en uno solo de ellos?

Igualmente ¿cómo se desarrollarían los más de 9,000 servicios anuales de transporte y custodia de dinero y valores o los más 1,600 transportes de explosivos?, ¿Cómo se realizaría el control y la gestión de más de un millón y medio de sistemas de alarma monitorizados por las centrales de alarmas privadas que generan en conjunto más de 200,000 señales de alarmas falsas o no deseadas?, ¿Quién efectuaría el acompañamiento y protección de personas determinadas? O ¿quién protegería nuestros pesqueros que están faenando en el Océano Índico?

En todo caso, se incrementarían los riesgos de actos violentos, robos, atracos, agresiones, vandalismo, o incluso podría colapsarse la actividad normal en donde las Fuerzas y Cuerpos de Seguridad no podrían ni deberían estar presentes. Y no podrían principalmente porque no poseemos esos recursos, y, sobre todo, no deberían porque, en la mayoría de los casos, son actividades privadas, incluso con ánimo de lucro, en las que no procede poner a disposición esos recursos públicos para nada que vaya más allá de su misión superior de garantizar la seguridad ciudadana.



**GRUPO**  
**M**  **SEC**  
SEGURIDAD PRIVADA ARMADA

**MONITOREO Y SEGURIDAD PRIVADA, S.A DE C.V.**

Viveros de Atizapán No.1 esq. Sor Juana Inés de la Cruz, Col. Viveros de la Loma,  
C.P. 54080, Tlalnepantla, Estado de México

Tels: (01) 55 53901618 | 55 5565 0732 | 55 5556 0812  
comercial@moseg.com.mx

[www.moseg.com.mx](http://www.moseg.com.mx)



### A modo de conclusiones

Es evidente que la sociedad depende de la Seguridad Privada como auxiliar y complementaria de la Seguridad Pública. Su misión, especialmente preventiva, abarca todas aquellas actividades que precisan seguridad preventiva, como son principalmente las infraestructuras de transporte, industriales o comerciales, o, caso especial, el correspondiente a la mayoría de las infraestructuras críticas o estratégicas del país, en las que su seguridad interna y de funcionamiento debe ser costeada por sus propios operadores.

Actividad y competencia aparte tendrán los recursos de Seguridad Pública para garantizar la Seguridad Ciudadana de los entornos correspondientes.

Finalmente, no se hagan lío los que piensen que la especialización y el crecimiento paralelo de la seguridad privada es una forma de privatización de la seguridad pública. El normal desarrollo de la sociedad, presenta nuevas complejidades, retos y demandas que sólo se puede afrontar correctamente con soluciones nuevas y cooperativas. No es eficiente plantear que sea la Seguridad Pública la que preste atención a este vastísimo campo de especialización, sino que los nuevos desafíos han de contar con un sector privado reforzado, bien formado y dotado de medios específicos para realizar su complementaria labor de la mejor manera posible y con la mejor capacitación.

En este sentido, hay un importante capítulo aparte aún nada debatido, y merece la pena subrayar que, para el normal desarrollo de la Seguridad Privada, es imprescindible también una revisión y ampliación rigurosa de los programas de formación básica y de especialización, de todos los niveles profesionales del sector, en lógico acercamiento a los niveles de capacitación que son exigidos en la Seguridad Pública. El incremento de formación y capacitación profesional es una asignatura pendiente imprescindible de modificar y aprobar.

Hay que insistir en un concepto muy básico a tener en cuenta, como es que la Seguridad Humana en general, y la Seguridad Ciudadana en particular, requieren del concurso y cooperación de la Seguridad Pública más la Seguridad Privada, logrando pasar de la simple "acción preventiva" al "compromiso preventivo coordinado", con una seguridad única que aporte sinergias, y sobre la base de los nuevos recursos implantados y en desarrollo, dentro de redes y planes específicos de la Policía y Guardia Civil, arbitrados por el Ministerio del Interior, de quien depende finalmente la regulación y control centralizado de toda la seguridad, incluida la privada. 15

# TALLER

## ESPECIALIZADO EN GERENCIA DE PROYECTOS MITIGACIÓN DE RIESGOS Y DISEÑO DE CONTRAMEDIDAS DE SEGURIDAD EN CADENA DE SUMINISTRO



31000 : 2018



28000:2007



21500:2012





# LA BIBLIOTECA DEL SENSEI

*Como siempre, damos la bienvenida a la gustada sección del maestro, del Sensei, que ya nos tiene acostumbrados a sus recomendaciones de lecturas de gran utilidad. Veamos.*

*En esta ocasión, derivado de nuestra reciente visita al seminario de ASIS Internacional, en Chicago, en los Estados Unidos, quiero compartirles dos libros que me parece son fundamentales para un buen directivo o ejecutivo de seguridad.*

## BUILDING A CORPORATE CULTURE OF SECURITY

*John Sullivant, Editorial Butterworth-Heinemann*



El primero de ellos al cual nos referiremos se denomina "Construyendo una Cultura Corporativa de Seguridad", escrito por John Sullivant. Es un libro que atiende las tendencias más recientes de la seguridad y las necesidades que tenemos de que la seguridad deje de ser un valor agregado.

Las empresas siempre manejan a la seguridad como la última etapa dentro de su proceso de negocio; sin embargo, en este libro, el autor nos da una serie de elementos que son fundamentales para que un ejecutivo de seguridad corporativa pueda ir dando poder, o empoderar, a su área dentro del proceso de negocio, dándole valor a la cadena de negocio al integrar a la seguridad a cualquiera de los procesos de la empresa.

El autor en este texto que tiene 17 capítulos, que van desde el planteamiento de las estrategias para que usted mismo diseñe su línea de vida en la empresa, pasando por la vulnerabilidad y lo que hoy se conoce como el ecosistema empresarial y el ambiente de riesgo o amenazas que lo envuelven.

Hace una referencia muy importante al enfoque de las ciberamenazas que hoy se dan en el mundo. Hace un planteamiento práctico sobre cómo establecer un programa de gestión de riesgos de seguridad dentro de la empresa, obviamente también se refiere a las métricas que pueden utilizar los ejecutivos para medir, en términos reales, la eficiencia y los resultados de la seguridad, y plantea el uso de un modelo amigable para la seguridad, desarrollando perfiles que sean utilizables de los peligros en los que se encuentra la empresa.

Y realmente recorre temas como la preparación de emergencia, desarrollo de protocolos, la apreciación de la seguridad desde la alta dirección, la construcción de las competencias que debería tener tanto el directivo como del personal del área de seguridad, y algo que me pareció fundamental es que él habla de cómo comunicarse efectivamente con los altos directivos de la empresa.

Creo que este es uno de los textos más importante que recientemente se han sacado a la luz para ejecutivos de seguridad.

## SAFEGUARDING INTANGIBLE ASSETS

*Michael D. Moberly, Editorial Butterworth-Heinemann*

El segundo texto se llama "Asegurando los Bienes Intangibles", el autor se llama Michael D. Moberly. Este libro fue editado hace cuatro ó cinco años y nos hace especial referencia a ese cambio de paradigma que estamos teniendo en las organizaciones en donde los bienes tangibles pasan a tener mucho menos impacto en la economía de una empresa. Cada vez más los negocios migran a estos modelos intangibles, como son la información, la imagen, el prestigio, la credibilidad y la reputación.

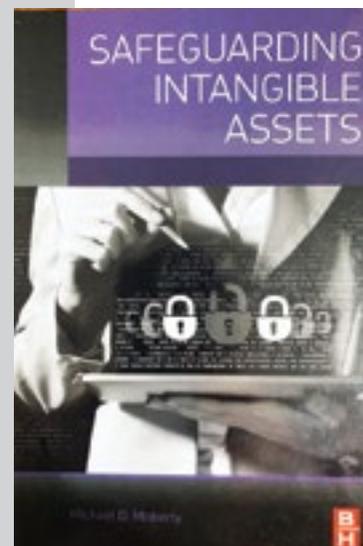
Las empresas están empezando a entender que si alguien ataca sus bienes informáticos no tiene que romper con un camión la malla ciclónica, sólo necesita tener un punto vulnerable, que normalmente es un empleado que accidental o deliberadamente ha roto la cadena de seguridad para atacar a una empresa.

En este libro el autor nos va haciendo referencia, en doce capítulos, de la reflexión de qué son los bienes intangibles. Debemos entender que no sólo estamos hablando de la informática, sino el hecho de que se impacte a la imagen de la empresa, así sea en redes sociales, diciendo que la empresa participa en algún entramado delictivo o discriminatorio, o de malas prácticas de gobierno o empresarial, le puede costar mucho a una organización y nos da reglas para poder gestionar internamente no nada más desde el punto de vista de la seguridad, y eso es lo valioso de este libro, sino que involucra a todas las áreas de la empresa.

Y habla de un factor que es muy importante para el profesional de la seguridad, que debe ser manejado en el día a día en la empresa, que es el proceso de cuidado en la gestión de los bienes intangibles y que debe ser parte de la cultura de las empresas, de la distinción de lo que son los bienes intangibles y la propiedad intelectual de la empresa y entra a un punto fundamental que es medir el desempeño de la seguridad de los bienes intangibles y qué tipo de entrenamiento tiene que recibir, en materia de bienes intangibles todo nuestro personal.

Habla del problema de que los bienes intangibles están mucho más expuestos a problemas desde adentro de la empresa, de las estrategias y del panorama que, a partir del 2015, se veía venir y que se está volviendo realidad.

Creo que este es uno de los textos que pueden abrirle un campo al ejecutivo de seguridad bajo el principio que muchas veces he planteado: no debemos estar donde la pelota está sino donde la pelota va a estar. Tenemos que ver hacia el futuro y tratar de estar listos para enfrentar y ayudar a nuestra empresa a enfrentar eficientemente las nuevas y futuras amenazas. Hasta la próxima.





# DE GUARDIA A GERENTE

## Inicio, Creación, Vida y Crecimiento

Entrevistamos al especialista Hermelindo Rodríguez Sánchez, CPO, CSSM, DSI, Director Nacional de Operaciones en Grupo Garcea Servicios Integrales en Seguridad Privada, y nos habla de sus inicios en la seguridad, desde el nivel de guardia de seguridad hasta llegar a ser gerente de operaciones, al día de hoy cumplió 30 años de forma ininterrumpida en la seguridad y nos platica lo siguiente:

### ¿Cómo llegaste al ámbito de la seguridad?

Por necesidad en el ámbito personal y para cumplir con mis metas, así como coadyuvar en el tema familiar con los gastos de la casa. Salí a la calle a buscar una oportunidad laboral, encontrando el puesto de guardia de seguridad en una empresa líder en la seguridad, mi proceso fue: un día de entrevistas, selección, exámenes médicos y psicológicos, el tercer día fue la contratación final.

### ¿Cómo fue tu desarrollo en la seguridad?

Después de estar 3 meses en una tienda retail, me movieron a otro servicio de retail, para levantar el servicio, porque estaban por cancelar, estuve 2 meses y me regresan al mismo lugar, donde inicié, como jefe de turno y así mismo, subí a jefe de servicio y después a coordinador, en 5 meses ya estaba coordinando a 60 personas en la empresa.

### ¿Cómo fuiste creciendo hasta llegar a ser gerente?

Después de estar como coordinador, el Teniente Raúl Cortés, militar retirado, me designa como supervisor, posición que conservé durante 7 años y posteriormente me nombran Jefe de Operaciones, el grado más alto en las empresas de seguridad en ese tiempo, 1997, después me pasan al área administrativa y estuve como jefe de facturación y cobranza, pero regresó a la operación en un año posterior, y me mandan a la empresa de alarmas como Jefe de Patrullaje, donde estuve un año, para después regresar a la empresa de Guardias, como Gerente de Operaciones, donde tuvimos la oportunidad de trabajar y crecer

con empresas extranjeras como Home Depot, Office Depot y Wal Mart, con quienes tuvimos un crecimiento importante, hasta llegar a tener 5,000 elementos que nos dio el impulso para seguir creciendo con la prestación de servicios de seguridad.

Una vez viajando por toda la república en todas las aperturas de sucursales, me dan el cargo de Gerente de sucursales y posterior viajé a España y Costa Rica para la atención de sucursales fuera del país.

### ¿Cuál es tu pasión en la vida?

Cuando tenía 7 años dedicado a la seguridad, siendo supervisor, me di cuenta que la seguridad era mi futuro y que tenía que realizar mis esfuerzos para lograr un crecimiento laboral, me gustaba mucho el trato con las personas y con los clientes y uno de los orgullos más apasionantes ha sido la virtud de brindar un servicio, un servicio basado en cumplimientos, calidad y compromiso, que ha sido mi mayor fortaleza y reto en mi camino.

### ¿Cuál es tu futuro en la seguridad?

Seguir desarrollando y explotando mis habilidades y conocimientos, para el beneficio de la empresa con la que estoy comprometido en la continuidad del negocio.

### ¿Qué recomiendas a los mandos medios?

Es importante saber de dónde vienes, para saber a dónde vas, por lo que es importante tener los valores, del servicio a las personas y a las empresas, cumplir objetivos y expectativas, contar con la pasión y el gusto a la seguridad, porque brinda beneficios importantes, si me imagine alguna vez estar como autoridad, pero nunca llegar tan lejos, es importante tomar en cuenta a los compañeros, a las personas que te brindan su apoyo, siempre tener la confianza en sí mismo, esa es la clave del éxito y contar con el impulso de la pasión de servir a los demás y ser un modelo de persona para avanzar hacia un cumplimiento, he aprendido que los errores pueden ser tan buenos profesores como el éxito. 



*En el año 2007 inicié la certificación como CPO (Certified Protection Officer) en la IFPO (INTERNATIONAL FOUNDATION OF PROTECTION OFFICER)*



*Colaboré con el Gobierno Federal, a través de la Policía Federal en la División de Gendarmería, como instructor en el Diplomado de Ciclos Productivos.*



¡LA CALIDAD  
NO ESTÁ EN CONTRA  
DEL PRECIO!

UNIFORMES A LA MEDIDA  
PARA EMPRESAS DE SEGURIDAD



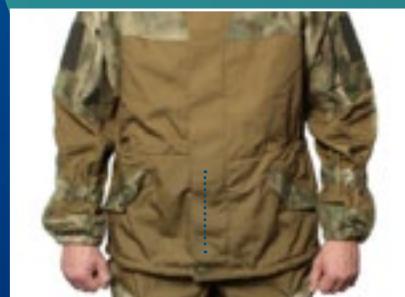
Federal



Privada



Pública



Militar

CLIENTES  
LEALES:



- INFORMES -

Cerrada de Palmira No.14, Francisco Villa, Tlalnepantla, Estado de México,  
C.P. 54059, Tels: (0155) 2873 0771 y (0155) 5082 2968, ventas@uniformesjr.com.mx

[www.uniformesjr.com.mx](http://www.uniformesjr.com.mx)



## FORO ANÁLISIS Y PROSPECTIVA de la Seguridad Privada en México

Por David Chong Chong, [dchong@ceasmexico.org.mx](mailto:dchong@ceasmexico.org.mx)

*El viernes 27 de Septiembre, en el 198º Aniversario de la Consumación de la Independencia de México, se realizó el Foro “Análisis y Prospectiva de la Seguridad Privada en México”, organizado por la Comisión de Defensa Nacional del Senado de la República, como parte de una serie que se inició en Noviembre de 2018 con el Foro “La Seguridad Nacional; Desafíos y Oportunidades en el Contexto del Nuevo Régimen 2018-2024”, así como en febrero del presente año con el Foro “Retos y Propuestas para la Seguridad en México”.*



Este Foro ha sido convocado con el propósito de analizar las problemáticas que afectan a este Sector, que aporta entre el 1.4%, de acuerdo con cifras oficiales, y el 2.2%, de acuerdo a estimaciones por el mercado de prestadores irregulares, del P.I.B., y representa una fuente de empleo para más de 750 mil familias, así como recabar propuestas para su solución, con una óptica de espacio de expresión abierta e incluyente a todos los participantes e interesados en este ámbito.

Al dar la bienvenida a los participantes en la apertura del Foro, el Senador J. Félix Salgado Macedonio, Presidente de la Comisión de Defensa



Nacional, enfatizó la importancia de la Seguridad Privada como un recurso auxiliar del Estado en su responsabilidad y compromiso ante el enfático reclamo social en materia de Seguridad. Asimismo destacó que, si bien existe un gran problema para el Sector por la diversidad de regulaciones y su repercusión en términos de múltiple tributación, el mayor problema es “la división y dispersión de visiones y posiciones, incluso al grado de la descalificación peyorativa (una empresa irregular, mal llamadas “patito”, no necesariamente es ilegal, porque están establecidas legalmente como mercantiles), que existe entre sus actores, empresas, asociaciones y autoridades, cada una atendiendo a sus intereses, muchas veces de manera excluyente y afectándose entre sí”.

Finalmente reiteró que se convocó a este Foro “con plena conciencia de la responsabilidad constitucional del Estado para brindar seguridad a la ciudadanía, invitándolos a dejar atrás las divisiones y confrontaciones, y trabajar de manera integrada por fortalecer a este tan importante sector para la gobernabilidad y la prosperidad de México como Nación”.

Durante el Foro se desarrollaron 4 mesas de Trabajo con la participación de ponentes de diversas empresas y organizaciones, como CONESPRYSIR, CEAS México, CONAMEX, SAP, IVAGIR, UNAM, ELD, CELA, FCPyS, TECNAVIX, ALAS Internacional, SKYMEDUZA, UFESP, Grupo SABE, Top Securus y Becley Abogados.

En la Mesa 1 se abordó el tema de la Profesionalización, destacando la importancia del desarrollo del capital humano por la naturaleza y repercusión de sus responsabilidades profesionales y

sociales, pero también el aspecto de sus condiciones y derechos laborales.

Siguiendo con el programa, en la Mesa 2 se planteó el tema de la Tecnología aplicada a la operación de los servicios enfatizando el impacto de la innovación que rebasa la regulación existente y las responsabilidades que conlleva, destacando los tópicos del uso y regulación de los Sistemas Aéreos de Pilotaje Remoto (RPAS por sus siglas en inglés de Remotely Piloted Aircraft Systems, y conocidos como “drones”), así como los sistemas de anti-bloqueo de comunicaciones (“antijammers”).

Por lo que respecta a la Mesa 3 se aboco al tema de la diversidad regulatoria que prevalece en el País, lo cual dificulta y encarece su ejercicio, al mismo tiempo que fomenta la irregularidad en los prestadores de estos servicios.

En la Mesa 4 se abordó la necesidad de contar con una legislación que facilite y propicie el desarrollo del Sector, con una amplia participación de todos sus actores, prestadores y usuarios de los servicios, con una visión incluyente.

Al término de la sesión, el Senador Salgado Macedonio anunció la presentación de un proyecto de iniciativa para la regulación de los servicios de Seguridad Privada, orientada a unificar e integrar las diversas regulaciones existentes y con una visión incluyente y de acuerdo con los lineamientos de austeridad y eficiencia propuestas para el Nuevo Régimen. Asimismo, reiteró la invitación a participar en la construcción de consensos y acuerdo en beneficio del Sector de la Seguridad Privada, y de la Sociedad a la que se pretende servir. **AS**





## URGE NUEVA LEY en Materia de Seguridad Privada, ASUME

Una propuesta para reformar la Ley fue entregada en abril de 2018 y aún está a discusión en la Cámara de Diputados. Con ella se busca generar una mayor eficiencia y control en el sector.

Para Armando Zúñiga Salinas, Coordinador General de Asociaciones de Seguridad Unidas por México (ASUME), con la nueva Ley General de Seguridad Privada se propone evitar la doble tributación de las empresas, así como promover la profesionalización de los elementos, la regulación de la tecnología en la seguridad privada y erradicar la corrupción.

Y aclaró que: “Con esta ley se busca tener el piso parejo para todas las empresas, y que la seguridad privada sea un ejemplo para todos los empresarios, para ello se busca tener las mejores prácticas para poder impulsar la profesionalización del sector”.

“Combatir la informalidad en el ámbito de la protección privada es una forma de proteger al pueblo. Por eso, la Ley General de Seguridad Privada es una meta clave para nuestro sector”.

Esta regulación plantea la creación de un comité y un registro único para todas las organizaciones del país, eliminando los registros federal, estatal y municipal, dejando la tarea a un órgano desconcentrado.

“El proyecto de ley, que tenemos trabajando desde hace casi 5 años, en la legislatura pasada, ya fue aprobado por el Senado, pero se quedó en la Cámara de Diputados. Por los tiempos legislativos ya no se alcanzó a votar. Entonces esperamos que se instalara la nueva legislatura y desde que se instaló buscamos a la presidenta de la Comisión de Seguridad Pública, la diputada Juanita Guerra, que afortunadamente nos ha atendido y nos ha escuchado”.

“Por muchas razones no se ha podido llevar nuestro proyecto de Ley a votación, además de que hay muchos cambios. Estaba adecuada para el gobierno anterior, pero cambiaron algunas cosas, por ejemplo, la Comisión Nacional de Seguridad ya no existe, ahora es la Secretaría de Seguridad y Protección Ciudadana. De hecho se tienen que hacer muchos cambios, y es en lo que estamos trabajando”.

“Gracias a que ASUME forma parte del Consejo Coordinador Empresarial, hay unas mesas de trabajo, que se llaman mesas beta, en donde se están trabajando 10 puntos que preocupan a los empresarios en temas de seguridad, por ejemplo, el tema de la seguridad turística, o el tema del robo a transporte y, afortunadamente, entre esos 10 puntos logramos subir el tema de la iniciativa de ley”.

“Yo creo que muy pronto podremos tener la iniciativa de Ley con los cambios que se tengan que hacer, más la reforma constitucional. Es importante la participación de ASUME por la representación que tiene hoy de 32 asociaciones que representan a todo el sector de la seguridad. ASUME se encarga de coordinar con cada una de las asociaciones, o con cada uno de los rubros, por ejemplo, con los blindajes, o con el rastreo vehicular, para que esta Ley enfocada no solamente a los oficiales de seguridad, sino también en la necesidades del sector de la tecnología en seguridad, de normar los blindajes, en fin, de todo lo que abarca el sector de la seguridad privada”.

“Como sector creo que tenemos dos objetivos principales, el primero es la Ley de Seguridad Privada, y el segundo es la Cámara de la industria del sector, esos son los dos grandes objetivos que nos hemos planteado, y afortunadamente hemos recibido buenas respuestas de los empresarios”.



# A SUME

Agrupaciones de Seguridad Unidas por México

## PRINCIPALES OBJETIVOS

Fortalecer al sector en la cúpula empresarial.

Impulsar la Ley General de Seguridad Privada y la Cámara de la Industria.

Participación destacada de la seguridad en proyectos de desarrollo económico y social.



[asumeseguridad.org](http://asumeseguridad.org)





Carlos Seoane Noroña, especialista antisequestro

## SESIÓN MENSUAL DE AMEXSI

### Panorama 2020: Secuestro, Radiografía de México

*El pasado 26 de septiembre se realizó la novena sesión mensual de la AMEXSI de este año. Fue una de las sesiones más concurridas y, de acuerdo con lo informado por el presidente del organismo, Arturo Martínez Avalos, la membresía sigue creciendo.*



En esta ocasión el conferencista invitado fue Carlos Seoane Noroña, sin duda una de las máximas autoridades cuando se habla del secuestro en nuestro país. En su intervención, el especialista aseguró que: “el panorama esperanzador que nos daba la disminución del delito de secuestro se ha oscurecido. Durante el año, mes con mes se había presentado una disminución constante en este delito, pero después hubo un fuerte incremento”.

“Cada mes rompemos récord en violencia y crecen prácticamente todos los delitos de alto impacto. El secuestro no fue la excepción, se incrementó 23.9% respecto al mes de abril, al pasar de 117 carpetas de investigación iniciadas en el mes de abril a 145 carpetas de investigación iniciadas en el mes de mayo”.

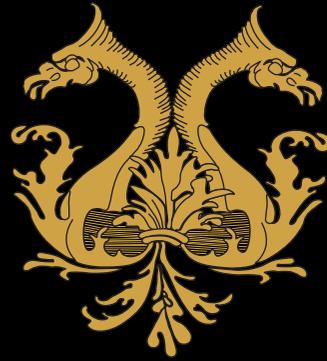
Sin embargo, persiste una disminución de 19.4% si comparamos los primeros 6 meses del gobierno de Enrique Peña Nieto, donde ocurrieron 1,206 secuestros, con los primeros 6 meses del gobierno de Andrés Manuel López Obrador, donde ocurrieron 971.

La concentración del delito de secuestro en algunas entidades es alarmante, 7 de cada 10 secuestros ocurren en Veracruz, Estado de México, Ciudad de México, Puebla, Tamaulipas, Morelos y Guerrero. En la Ciudad de México, el delito de secuestro ha repuntado 103.4% en lo que va del año, si lo comparamos con los primeros cinco meses de 2018.

# 10 años

## Gracias por tu confianza

CONTAMOS CON COBERTURA  
A NIVEL NACIONAL



SEGURIDAD PRIVADA

▶ VIGILANCIA  
INTRAMUROS

▶ CUSTODIAS

▶ SEGURIDAD  
ELECTRÓNICA

▶ MONITOREO Y RASTREO  
VEHICULAR



Tel. (0155) 5916-5931

laadukalmekak@hotmail.com • laadu@laadusp.com

cpromo@laadusp.com • ventas@laadusp.com

*“ La experiencia  
está anclada al plan  
maestro del cuerpo ”*

[www.laadusp.com](http://www.laadusp.com)



El número de carpetas de investigación por secuestro en la CDMX pasó de 7, entre enero y abril de 2018, a 26 en el mismo periodo de este año. Tan sólo en enero, la Procuraduría General de Justicia capitalina abrió 16 indagatorias por este delito. Todos los casos fueron de tipo "extorsivo". Esto significa que la CDMX ya es la cuarta entidad a nivel nacional con los mayores índices delictivos en secuestro, según datos del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP).

Y a nivel nacional, las cifras de plagios también van al alza, mientras el año pasado hubo 361 carpetas de investigación iniciadas en el fuero común, este año sumaron 463, por lo que el promedio diario pasó de tres a cuatro plagios.

De acuerdo con cifras de la organización Alto al Secuestro, la alcaldía Cuauhtémoc tiene el mayor número de plagios, con 13 privaciones ilegales a la libertad, seguido de

Iztapalapa, con 11 delitos, y en tercer lugar se encuentra la Gustavo A. Madero, con siete secuestros.

La entidad con más secuestros entre enero y abril de este año fue Veracruz, con 133, cifra 150.9 por ciento mayor a la registrada por la entidad en el mismo lapso de 2018, cuando acumuló 53. Los únicos estados libres de secuestro en dicho periodo fueron Baja California Sur, Durango y Yucatán.

"Las penas mínimas por secuestro de 1955 a 2014 se incrementaron de 5 a 40 años de prisión, y la pena máxima aumentó 100 años, pasó de 40 a 140 años. Pero, ¿eso ha hecho que el secuestro baje? ¿sirven 500 años de condena para disuadir a los delincuentes? Obviamente no".

"¿Y cuál es el panorama para 2020? Hay dos caminos: opción A, sigue igual que como estamos de mal; opción B, algo pasa y milagrosamente nos curamos".





# CERTIFÍCATE COMO



**INICIO**  
**19 NOVIEMBRE 2019**  
**FINALIZA**  
**07 DE ABRIL 2020**



**DURACIÓN**  
**30 SESIONES**  
**MARTES Y JUEVES**  
**DE 5 A 9 PM**

## EL ÚNICO PROGRAMA EN MÉXICO QUE INCLUYE

- Desde la página web del Capítulo se podrá visualizar la bibliografía en línea oficial de la certificación -**POA® (Protection of Assets®)** - en **ESPAÑOL** sin ningún costo extra, se cuenta además con los **ESTÁNDARES** y **GUÍAS** como complementos para el estudio de cada **TEMÁTICA**.
- Podrás personalizar tu estudio con planeadores, actividades de reforzamiento, guías breves de aprendizaje.
- **GRUPOS DE ESTUDIO** mensuales liderados por Profesionales Certificados.
- Constancia de participación de ASIS Capítulo México.
- **REVIEW FINAL** con examen simulacro.

## INVERSIÓN

	SOCIO ASIS MX	SOCIOS OTROS CAPITULOS (ASIS INTERNACIONAL, ALAS, ASUME, AMEXSI)	COLABORADOR DE SOCIO	NO SOCIO
<b>PRESENCIAL</b>	\$24,000.00 NETOS	\$26,000.00 + IVA	\$27,000.00 + IVA	\$28,000.00 + IVA
<b>EN LÍNEA</b>	\$14,000.00 NETOS	\$16,000.00 + IVA	\$17,000.00 + IVA	\$18,000.00 + IVA

### CUPO LIMITADO.

Aparta tu lugar con el **15%** del monto total antes del **18 de octubre**.



**AULAS DE  
CAPACITACIÓN**  
**FINDES - AV. PASEO DE  
LA REFORMA #403.**



En caso de que no puedas ASIStir, no olvides solicitar tu **ID** para conectarte a través de **zoom**, no te pierdas de las sesiones teóricas en tiempo y forma.

Para continuar con tu proceso de **CERTIFICACIÓN** se tiene que cubrir la cuota de examen ante **Prometric**:

Socios ASIS Internacional | ASIS  
Capítulo México: **335 USD\***  
No Socios: **485 USD\***

\* Estos montos se pueden considerar dentro de tu cotización.

\*\* También puedes cubrirlo a 3 meses sin intereses con tarjetas participantes.

**INSCRÍBETE HOY, PIDE INFORMES CON:**  
**FABIOLA CADENA | CAPACITACION@ASIS.ORG.MX |**  
**PAOLA HERRERA | FORMACION@ASIS.ORG.MX | 55 1321 1289**



Lic. Saturnino Soria Pérez, Director General de SEPSISA Seguridad Privada

## SEPSISA

experiencia que da confianza

*SEPSISA es, sin lugar a dudas, una empresa consolidada, en junio pasado cumplió 15 años de actividades en el mercado nacional. Para hablarnos un poco más en detalle sobre esta exitosa compañía, platicamos hace unos días con Saturnino Soria, socio fundador y director general de la empresa. Esto es algo de lo que comentó:*

“SEPSISA como cualquier otra empresa, tiene su complejidad. Al ser una empresa del rubro de la seguridad, ser prestadores de servicio y que trabaja con capital humano, puede aumentar un poco el grado de complejidad, pero la verdad es que ésta es una profesión que me genera mucha satisfacción. Me gusta hacer lo que hago. Al igual que el resto de los socios, estoy contento del lugar al que hemos llegado”.

Sobre sus clientes nos dijo: “Algo en lo que no hemos incursionado es el tema de bares, centros nocturnos y casinos, pero fuera de eso estamos en toda la industria, la verdad es que donde nos hacen el favor de invitarnos en proyectos de seguridad, nos sentimos muy complacidos y vamos con todo el gusto por trabajar. No podemos decir que tenemos una

especialidad como tal, pero tenemos experiencia de varios años en diferentes campos”:

“Industria aeroportuaria, ferroviaria, automotriz, boutiques, salud, centros comerciales, hoteles, maquila, laboratorios, marítimo, residencial, corporativo, y de instituciones educativas, donde venimos trabajando por más de 13 años y hemos desarrollado diversas “estrategias de seguridad” para reducir los riesgos.





¿Y cómo le ha hecho **SEPSISA** para competir y crecer en este mercado?: “Pues no hay otra más que constancia, trabajo, profesionalismo, y estar siempre muy cerca del socio comercial. Algo que nos ha funcionado mucho es la cercanía que tenemos con nuestros principales, el estar siempre pendiente de ellos, el asistir a reuniones de trabajo de manera sistemática, el escuchar las críticas constructivas y ver cómo podemos trabajar en esas áreas de mejora continua. Quizá el no ser tan grande, como los enormes corporativos transnacionales que existen, te permite ser más ágil”.

“Hoy **SEPSISA** se está diversificando en temas de seguridad, estamos haciendo fuertes inversiones en temas de seguridad electrónica. Durante muchos años **SEPSISA** se enfocó en lo que son guardias intramuros, en 2018 y 2019 tuvimos un detonante muy importante en temas de custodia, custodia de transporte, y se hicieron inversiones también muy fuertes en la adquisición de patrullas y eso nos ha permitido incursionar en una forma mucho más directa en este sector”.

“En seguridad electrónica también estamos invirtiendo muchos recursos, tanto en alarmas como en el CIL, que es nuestro Centro de Inteligencia Logística, un pequeño búnquer aislado de nuestras instalaciones para poder tener esa independencia que requiere. Y

también invertimos en temas de monitoreo de GPS y de transporte, también en circuitos cerrados. Ya existe, y se sigue apuntalando, un área de tecnología y seguridad electrónica”.

“¿Dónde nos vemos en los próximos años? Evidentemente tenemos planes de expansión a nivel nacional, y se está pensando a mediano plazo, abrir una sucursal probablemente en Centro y Sudamérica, porque algunos de nuestros socios comerciales que tienen operaciones allá nos están invitando, y han sido insistentes en que requieren y les gustaría que nosotros les diéramos el servicio en las instalaciones que tienen en Latinoamérica. Creo que todavía no es el momento, en el corto plazo es seguir teniendo una expansión importante en el territorio nacional”.

“Hoy no podemos pensar de manera aislada en un guardia sin un apoyo tecnológico, o en tecnología sin el apoyo humano. El tema es la seguridad integral, y más en los tiempos que estamos viviendo, hoy tenemos que trabajar completamente en la prevención, y no nada más las empresas, sino la ciudadanía en general, o sea, generar una cultura de autoprotección y de seguridad integral, tanto en trayectos en la calle, como en los hogares, o en nuestros trabajos y en las empresas”.





## SECURITY WEEK LATAM ASIS 2019



*Del 13 al 17 de octubre pasado se llevó a cabo, en el marco del 25° aniversario de ASIS Capítulo México, la Security Week LATAM ASIS 2019, en el Centro Citibanamex de Ciudad de México.*

El evento tuvo por objetivo brindar a los profesionales de la seguridad de la región un espacio para compartir experiencias, mejores prácticas, discutir y exponer avances, problemáticas y estrategias, que abonen a su proceso de actualización y profesionalización continua.

El evento contó con la participación de más de 500 asistentes en las diferentes modalidades del programa académico, incluyendo casi 60 conferencias. En la zona de expo estuvieron presentes más de 30 marcas.

Durante el desayuno inaugural, Pedro Sanabria, presidente del Capítulo, dio la bienvenida a los asistentes y llamó a las compañías del sector a transformarse, a convertirse en verdaderos líderes en protección, beneficiando con ello al mercado, y al país. Y recordó que el principal objetivo del evento era construir el diálogo e intercambiar experiencias para enriquecer el conocimiento en la industria y fomentar la capacitación.

Por su parte, Enrique Tapia, vicepresidente regional senior de ASIS International para México, Centroamérica y el Caribe, felicitó a los organizadores por su gran desempeño y destacó la labor del Capítulo, y aseguró que ha convertido a la región en la más activa y pujante a nivel mundial.

A nombre de IPS, empresa patrocinadora del desayuno, Jorge Uribe, su director comercial, destacó la importancia de seguir apoyando a la organización y se comprometió a

Tu seguridad  
desde una  
nueva  
perspectiva





continuar haciéndolo: “De nada sirve que en México operen muchas empresas de seguridad si no cumplen con la ley. Nosotros sí cumplimos y no debemos permitir que nos confundan. Por eso, revisemos con lupa nuestros procesos y no permitamos que se desprestigie el mercado”.

El conferencista invitado en esta ocasión fue Santiago Roel, director de Semáforo Delictivo, que presentó el “Panorama de la seguridad en México”. La organización que preside cuenta con información detallada sobre el estado que guarda la seguridad en el país, cifras alimentadas con las denuncias ciudadanas, así como de los esfuerzos de transparencia de las autoridades.

El especialista destacó la importancia de la percepción de la inseguridad: “No hay mejor medidor que la opinión de los vecinos que llevan años viviendo en una misma zona” y aseguró que la mitad de los estados del país han registrado un aumento en la percepción de seguridad, siendo Baja California Sur y Sinaloa los primeros.

Sin embargo, sólo han descendido dos tipos de delitos: el robo de vehículos, con un 12%, y el robo en casa habitación, un 2%. Mientras tanto, todos los demás delitos aumentaron, en algunos casos con subidas alarmantes, como en el caso de la extorsión, que aumentó un 36%, el narcomenudeo, 22%, la violación, 11% y secuestro, 9%.

En cuanto a homicidios, aseguró que este es uno de los flagelos que más impactan al país y reveló que el

año 2018 fue uno de los peores de la historia a nivel nacional, ya que se registró un incremento importante: “El 80% de los homicidios que se registran en México son por causas del crimen organizado. Hay una pésima política de drogas y se está atacando un mercado a balazos, cuando lo que se requiere es una regulación adecuada”.

El resto del programa académico de la Security Week abordó temas de gran interés, como migración y conformación de pandillas, ciberseguridad en la 4ª revolución industrial, Seguridad en instalaciones vitales, nuevos retos de la seguridad en la cadena de suministros de la Ciudad de México, phishing, el arte de robar información y el efecto del nuevo sistema penal acusatorio en el sistema penitenciario.

Con gran éxito se presentaron también diversos paneles con el formato de ASIS Talks, como el realizado por Miguel Ángel Champo, socio director de Multiproseg, que presentó su ponencia sobre “Seguridad en Hospitales Gubernamentales (presupuesto cero)”, Gabriel Bernal, que habló de “La importancia de vigilar la rentabilidad del negocio: grande vs. productivo”, y Juan Antonio Arámbula, que lo hizo sobre la profesionalización del sector.

Hubo también dos conferencias magistrales, la primera de ellas a cargo de Santiago Nieto Castillo, actual titular de la Unidad de Inteligencia Financiera de la SHCP y que llevó por título “Memorias de un Fiscal Incómodo”.





La segunda, con la que se dio por terminada la jornada, fue un diálogo entre expertos, con la participación del primer comandante de la Guardia Nacional, Luis Rodríguez Bucio, y el investigador y académico Javier Olivas.

El Gral. Rodríguez Bucio aseguró que hacerle frente a la inseguridad es el principal reto, pues el reclamo en amplias zonas del país para recuperar la normalidad en la vida cotidiana va acompañada de una serie de medidas que son fundamentales para el funcionamiento de la Guardia Nacional.

Reducir el número de delitos es uno de los principales objetivos, por un lado se cuenta con el despliegue de elementos, por otro la estrategia buscará fortalecer la investigación y prevenir delitos ayudados por la división científica, inteligencia y antidrogas que se suman con la incorporación de la Policía Federal.



La Guardia Nacional tendrá que enfrentar grupos criminales de diferente nivel de organización y alcance territorial, adoptando estrategias de penetración territorial incorporando en sus actividades la lucha contra el robo de combustible, la extorsión, el secuestro y el feminicidio, realizando diversos análisis y estudios en distintos niveles, desde lo nacional, estatal, regional, municipal, y hasta por colonias, barrios y calles.

*En resumen, el Security Week LATAM ASIS 2019 fue todo un éxito, y sin duda coloca la vara muy alta para tratar de igualar, y posiblemente superar, este tipo de eventos en el futuro. Felicidades a todos los organizadores, fue un verdadero privilegio participar en éste, que sin duda, fue el evento del año.*





# ASIS INTERNACIONAL

## Global Security Exchange (GSX) 2019 en Chicago

*ASIS Internacional, la asociación más grande del mundo para profesionales en la gestión de seguridad, realizó el pasado mes de septiembre su conferencia anual: Global Security Exchange (GSX) 2019, en la ciudad de Chicago, en los Estados Unidos.*

**E**l evento, al que asistieron más de 3 mil profesionales de la seguridad de todo el mundo, contó con un extenso programa con más de 250 sesiones educativas, conferencias y sesiones generales, y un piso de exhibición con más de 550 expositores de la industria de la seguridad.

Christina Duffey, presidenta de ASIS Internacional, afirmó que: "GSX marca el comienzo de un enfoque reinventado de la educación, las exposiciones y la creación de redes, combinando estos aspectos en nuevas oportunidades y eventos. Sólo ASIS tiene la experiencia, el alcance global y el poder colectivo y la experiencia de sus miembros para convocar un evento de esta magnitud y calidad".

La formación educativa se centró en una gran cantidad de temas relevantes de seguridad global, incluida la violencia en el lugar de trabajo, los planes de operaciones de emergencia, la resistencia crítica de la infraestructura, las amenazas cibernéticas que enfrentan el gobierno, las corporaciones y los ciudadanos, las mujeres en seguridad, la investigación en línea y en las redes sociales.

Una sesión sobre ciberseguridad incluyó una revisión de los tipos de ciberataques y cómo protegerse de ellos. El surgimiento de las redes 5G fue un punto destacado en la sesión, ya que los presentadores señalaron que si bien la tecnología traerá nuevos beneficios de los dispositivos interconectados, también abrirá nuevas vías para los piratas informáticos.

ASIS Internacional, fundada en 1955, es la organización de membresía más grande del mundo para profesionales de la seguridad. Cuenta con cientos de capítulos en todo el mundo y es reconocida como la principal fuente de aprendizaje, redes, estándares e investigación en la materia.

A través de sus certificaciones, ASIS garantiza que sus miembros y la comunidad de seguridad tengan acceso a la inteligencia y los recursos necesarios para proteger a su gente, propiedad y activos.

Al entrar a su 65 aniversario, ASIS transformó su tradicional Seminario y Exhibición anual en el Global Security Exchange, el evento más completo del mundo para profesionales de la seguridad, dedicado a abordar los cambios acelerados en toda la industria con un enfoque en aprendizaje inmersivo, redes revitalizadas y un piso de exhibición reinventado.

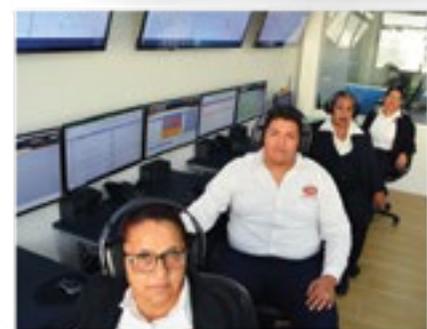
Con el GSX ASIS Internacional sigue dedicado a expandir y enriquecer el intercambio de conocimientos, las mejores prácticas y las conexiones entre pares para que los profesionales de seguridad en todas las disciplinas, y en todas las etapas de su carrera, puedan obtener acceso a la información y los recursos que necesitan para tener éxito. 



**CORPORATIVO**



su **seguridad** tranquilidad **y** satisfacción



### **NUESTROS SERVICIOS**

- > GUARDIAS INTRAMUROS
- > PROTECCIÓN A EJECUTIVOS
- > CUSTODIA DE TRANSPORTES
- > SEGURIDAD EN EVENTOS
- > ESTUDIOS DE SEGURIDAD
- > CENTRAL DE MONITOREO PROPIA

### **SEGURIDAD ELECTRÓNICA**

- > CCTV
- > ALARMAS
- > CONTROL DE ACCESOS
- > PROTECCIÓN PERIMETRAL
- > SISTEMAS CONTRA INCENDIOS
- > LOCALIZACIÓN SATELITAL GPS/GPRS

**Servicios de calidad  
en forma continua y  
permanente**

**Comprometidos con  
nuestros clientes en obtener  
su total satisfacción**

**Empresa conformada  
por profesionales con  
amplia experiencia**

Tels: (55) 55-32-48-30, (55) 56-72-86-92 y (55) 24-55-59-15 Y 16  
Miguel Laurent 1695 Col. Letrán Valle, Alcaldía Benito Juárez, C.P. 03650, Ciudad de México  
seguridad@zncorporativo.com | direccion@zncorporativo.com

**[www.zncorporativo.com](http://www.zncorporativo.com)**



# PROBLEMÁTICA DE REGISTRO NACIONAL

## de Empresas, Personal y Equipo de Seguridad Privada

Por Teodoro Serralde Medina  
teodoro@serraldeconsultores.com

### Registro de Personal Operativo de Seguridad Privada

Es obligación de las empresas de seguridad privada, de acuerdo a lo que establece el artículo 32, fracciones XVI y XX, de la Ley Federal de Seguridad Privada lo siguiente:

- a. Consultar los antecedentes policiales del personal que se pretenda contratar para prestar servicios de seguridad privada.
- b. Inscribir al personal operativo, previamente consultado, en el Registro Nacional de Personal de Seguridad Pública (RNPSP).
- c. Solicitar al personal operativo que utilicen la cédula de identificación expedida por la Dirección General de Seguridad Privada.

La razón por la que se inscribe el personal operativo de seguridad privada en el Registro Nacional de Personal de Seguridad Pública es porque la Ley General del Sistema Nacional de Seguridad Pública en su artículo 151, les otorga el carácter de auxiliares a los prestadores de servicios de seguridad privada, en particular a su personal de carácter operativo, es decir, son considerados parte del Sistema Nacional de Seguridad Pública, por lo tanto deben inscribirse.

### Registro Nacional de Personal de Seguridad Pública

El Registro Nacional de Personal de Seguridad Pública se encuentra dentro del sistema informático denominado "Plataforma México". Dentro del apartado de seguridad privada se encuentran módulos que corresponden al registro de la Dirección General de Seguridad Privada, así como de cada una de las entidades federativas.

Dada la naturaleza del Registro no es posible inscribir a una persona en dos o más entidades de la república en el Registro Nacional de Personal de Seguridad Pública, toda vez que un elemento no puede estar al mismo tiempo en dos corporaciones.

### Registro Nacional de Empresas, Personal y Equipo de Seguridad Privada

En términos del artículo 12 de la Ley Federal de Seguridad Privada, los elementos operativos deben estar identificados en el Registro Nacional de Empresas, Personal y Equipo de Seguridad Privada. Esta se trata de una base de datos distinta al Registro Nacional de Personal de Seguridad Pública.

### Registros Estatales de Seguridad Privada

La mayoría de las legislaciones estatales y/o reglamentos especiales que regulan la prestación de los servicios de

seguridad privada contemplan la creación de Registros Estatales de Seguridad Privada. Este tipo de legislaciones y/o reglamentos contemplan la inscripción del personal operativo en el Registro Estatal de aquellas empresas que cuentan con permiso de la localidad.

De la misma forma, es importante resaltar que se trata de un Registro distinto al Registro Nacional de Personal de Seguridad Pública, así como del Registro Nacional de Empresas, Personal y Equipo de Seguridad Privada.

### Obligación de Registro Federal y Estatal

El artículo 150 de la Ley General del Sistema Nacional de Seguridad Pública establece que los prestadores de servicios que presenten servicios en dos o más entidades federativas deben tener la autorización de la Secretaría (de Gobernación). También señala la obligación de que las empresas cuenten con la legislación local, es decir, tener permiso local y registrar a su personal. En la mayoría de las legislaciones o reglamentos que regulan los servicios de seguridad privada en las entidades federativas contemplan la creación de registros estatales de prestadores de servicios.

### Problemática de Registro de Personal Operativo

La Problemática que existe respecto a la Inscripción de Personal Operativo de las prestadoras de servicios de seguridad privada en el país, se resume en lo siguiente.

**a.** Los Reguladores Estatales obligan a las empresas de seguridad privada a Registrar al Personal Operativo en sus "Registros Locales".

**b.** En la mayoría de los casos, los reguladores estatales no cuentan con una base de datos estatal (Registro estatal) y toman como base el Registro Nacional de Personal de Seguridad Pública.

**c.** Los Reguladores Estatales cobran derechos por la inscripción local.

**d.** Existe confusión entre Reguladores Estatales y Prestadores de Servicios ya que consideran que el pago que realizan es por la inscripción en el Registro Nacional de Personal de Seguridad Pública, siendo que es por la inscripción en el Registro Local

**e.** En el caso de las empresas con autorización federal, aun cuando ya se encuentre inscrito el personal operativo en el Registro Nacional de Personal de Seguridad Pública, deben cumplir con la inscripción del personal en el Registro Estatal.



**f.** Dada la forma en que se diseñó el módulo de personal de seguridad privada del Registro Nacional de Personal de Seguridad Pública, no existe la posibilidad de señalar al personal operativo en dos o más entidades federativas.

**g.** Lo anterior genera la problemática de establecer prioridades de registro (quien lo realice en primer lugar conserva la adscripción), en lugar de complementar lugares de adscripción del personal.

**h.** Los Reguladores Estatales establecen requisitos superiores a la Ley Federal de Seguridad Privada para registro de personal operativo.

Derivado de lo anterior, las empresas de seguridad privada se enfrentan a problemáticas administrativas para dar cumplimiento a sus obligaciones de registro de personal, tanto a nivel Federal como en el ámbito estatal, toda vez que tienen que replicar el proceso de inscripción hasta 33 veces, además de que el pago por registro también debe realizarse en cada entidad y en la Dirección General de Seguridad Privada.

La problemática de registro expuesta se replica para el registro de empresas y de equipo que utilizan en la prestación de los servicios.

Para mayor ilustración de lo anterior, se presenta la siguiente gráfica:



## 1.1. DATOS NACIONALES<sup>1</sup>

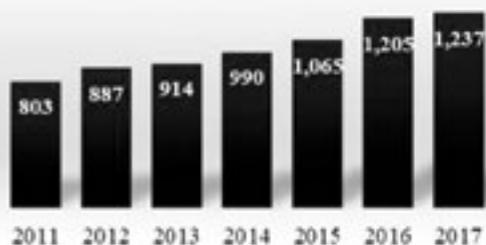
### EMPRESAS CON REGISTRO ESTATAL

ENTIDAD	2017	2018
01) Aguascalientes	64	78
02) Baja California	238	246
03) Baja California Sur	62	68
04) Campeche	53	48
05) Coahuila	122	131
06) Colima	94	110
07) Chiapas	73	88
08) Chihuahua	224	178
09) Ciudad de México	760	832
10) Durango	41	49
11) Guanajuato	168	192
12) Guerrero	82	87
13) Hidalgo	35	49
14) Jalisco	240	294
15) Estado de México	241	269
16) Michoacán	70	60
17) Morelos	128	133
18) Nayarit	45	54
19) Nuevo León	422	461
20) Oaxaca	47	52
21) Puebla	152	173
22) Querétaro	101	151
23) Quintana Roo	146	162
24) San Luis Potosí	89	100
25) Sinaloa	96	90
26) Sonora	96	43
27) Tabasco	54	53
28) Tamaulipas	10	6
29) Tlaxcala	16	15
30) Veracruz	61	25
31) Yucatán	102	104
32) Zacatecas	75	65
<b>TOTAL NACIONAL</b>	<b>4,207</b>	<b>4,466</b>

### PERSONAL OPERATIVO ESTATAL

ENTIDAD	2016	2017	2018
01) Aguascalientes	779	449	167
02) Baja California	8,582	7,427	7,210
03) Baja California Sur	865	985	805
04) Campeche	769	772	978
05) Coahuila	3,066	3,995	4,043
06) Colima	1,654	1,751	1,897
07) Chiapas	2,005	1,978	2,218
08) Chihuahua	5,708	5,413	5,704
09) Ciudad de México	17,122	18,592	19,121
10) Durango	545	581	588
11) Guanajuato	3,821	3,954	3,756
12) Guerrero	1,308	1,262	1,216
13) Hidalgo	778	269	120
14) Jalisco	1,289	1,121	1,541
15) Estado de México	1,974	2,063	1,877
16) Michoacán	1,712	1,607	1,198
17) Morelos	3,046	2,747	2,221
18) Nayarit	508	592	685
19) Nuevo León	6,742	3,792	3,900
20) Oaxaca	843	764	650
21) Puebla	1,781	1,725	1,525
22) Querétaro	4,691	5,157	5,719
23) Quintana Roo	5,582	6,361	7,199
24) San Luis Potosí	2,011	2,040	1,958
25) Sinaloa	2,461	2,815	2,394
26) Sonora	1,392	1,546	1,561
27) Tabasco	245	341	386
28) Tamaulipas	3,001	2,796	1,989
29) Tlaxcala	280	298	215
30) Veracruz	1,457	1,376	1,150
31) Yucatán	1,227	1,052	1,024
32) Zacatecas	339	311	215
<b>TOTAL NACIONAL</b>	<b>87,583</b>	<b>85,932</b>	<b>85,230</b>

### Empresas con autorización federal



### Personal operativo con autorización federal



1. Fuente de datos Dirección General de Seguridad Privada, Comisión Nacional de Seguridad, Secretaría de Gobernación. Cuadros de creación propia. AS



**Consultoría de Servicios Jurídicos especializada en regulación de prestadores de servicios de Seguridad Privada, Tecnologías de la Información, así como de estrategia corporativa y administrativa.**

**Contamos con amplia experiencia en materias:**

- Corporativa
- Administrativa
- Protección de Datos Personales,
- Comercio Electrónico, Mercantil y Laboral.



Servicios profesionales jurídicos y administrativos de la más alta calidad



Firma de regulación jurídica con la mejor y alta calidad en la prestación de servicios jurídicos y administrativos



Nuestros servicios jurídicos se basan en el trabajo profesional y responsable

**[www.serralde.com](http://www.serralde.com)**

Ignacio Allende 283A, Colonia Clavería, Alcaldía Azcapotzalco, CDMX  
Teléfono (55) 70906639 (55) 70907385 | Correo teodoro@serraldeconsultores.com

# ATENCIÓN A CLIENTES ¿Tema olvidado?



El pasado 18 de julio se realizó el interesante Webinar organizado y dirigido a miembros de la AMEXSI. En esta ocasión, este interesante ejercicio de comunicación estuvo a cargo de Eduardo Barrón Rivera, CPP, DSI.

El tema fue la atención a clientes: “Todo tiene raíz en la atención que damos al cliente, la correspondencia que tengamos con él, la empatía con sus necesidades. Muchas veces el cliente nos plantea algún problema que ellos tienen, alguna necesidad que les surge, y nosotros no somos empáticos y decimos “este cuate está loco” o “es una jalada lo que nos está pidiendo” pero no nos ponemos en sus zapatos para poder pensar que tal vez es algo que a él le están pidiendo y que para su empresa es importante y nosotros no somos empáticos y lo vemos con desdén”.

Por eso son muy importantes los tiempos de atención: “El tiempo que nosotros le damos de respuesta a nuestros clientes es vital. Luego nos mandan un mensaje y lo vemos tres o cuatro horas después, o nos están llamando y no tomamos la llamada, o si es miércoles, les decimos que nos vemos el lunes, sin ponernos a pensar que si él está llamando con urgencia, no podemos darle hasta 5 días para tener la respuesta que andan buscando. Eso es, desde la perspectiva del cliente, algo grosero”.

“Hay diferentes conceptos de la seguridad, pero el que a mí me gusta usar es aquel que dice que la seguridad es un sentimiento, y por tanto, es pensar en qué parámetros está la relación con la empresa que me está brindando seguridad. A lo mejor nosotros mandamos guardias o patrullas, o todos los recursos técnicos, y sin embargo el cliente nos dice “Oye, tu servicio no está funcionando” porque él no siente la atención, o la seguridad en el servicio que le estamos prestando. Entonces todos los esfuerzos que hagamos están fracasando”.

“Una vez vendido el servicio, ¿quién se encarga de dar seguimiento? ¿Qué debemos hacer para ser siempre la primera opción de nuestros clientes? Generalmente es el coordinador operativo el que da seguimiento a nuestros clientes, pero cuántos de ellos están realmente capacitados para hacerlo, cuántos de nuestros jefes operativos, supervisores, jefes de servicio, los vemos con desdén y no nos sentamos nunca en una mesa para intentar darles una visión ejecutiva de lo que es el servicio al cliente y ellos no lo entienden”.

“Como usuario, de repente es frustrante que cuando tienes alguna necesidad y tu empresa prestadora de servicio no es empática y lejos de darte una solución te da un cuestionamiento, o un reclamo, o de plano te dice “lo que tú me estás pidiendo es absurdo”. Y no, lo que nosotros debemos hacer no es cuestionar, sino ofrecer alternativas. Dicen por ahí que una buena atención al cliente puede hacer más competitiva a tu empresa que un excelente precio o la calidad en el producto”.

“Regularmente metemos al aula a nuestro personal para darles temas como manejo de armas, o un intento como de liderazgo, manejo de crisis, pero nunca los sentaste a darle una competencia para que pudiera hablar con su cliente, para que pudiera darle respuestas sensatas a su cliente, para que pudiera escuchar a su cliente y una vez que tenga las cosas en orden, llevarlo de la mano y proponerle innovación, cambio de estrategias y hacerle ver que le aporta valor a la relación, que no le vende nada más el servicio sino que le aporta valor y que le da una competencia a nivel interno de su área, que hace brillar el área de seguridad en su empresa, y ser ya no su proveedor, sino cambiar la estrategia, cambiar la visión de ser un proveedor a ser un socio estratégico del negocio”.



*Protegerte, nuestro Compromiso*

Generamos ahorros importantes al adaptarnos a tus diversas locaciones, ya que contamos con protocolos que hacen efectiva nuestra adaptabilidad geográfica.



Nuestra capacidad de adaptación a las diferentes plazas y costumbres, hace posible entregar un servicio con la calidad que necesitas.

### **NUESTROS SERVICIOS**

Protección Ejecutiva • Seguridad Intramuros  
Custodia de Bienes • Seguridad Electrónica  
Geolocalización GPS • Monitoreo de Alarmas  
Videovigilancia • Administración de Riesgos  
Protección Perimetral

**Contamos con 32  
sucursales a  
nivel nacional a tu  
servicio**

[www.mspv.com.mx](http://www.mspv.com.mx)



**ASIS**

**AMEXSI**



Tel: 52.155.5399.9937, Correos: [ventas@mspv.com.mx](mailto:ventas@mspv.com.mx) y [info@mspv.com.mx](mailto:info@mspv.com.mx)  
Edificio Corporativo en Lago Superior No. 25, Col. Tacuba, Alcaldía de Miguel Hidalgo, C.P. 11410, CDMX.

# DIRECTORIO DE SEGURIDAD



**ABASTECEDOR PRINCIPAL NACIONAL, S.A. DE C.V.**

No. de Autorización. DGSP/020-11/1687  
La Rioja Número 2979, Col. Providencia  
1ra. 2da. y 3ra. Secc., C.P. 44630,  
Guadalajara, Jalisco.

Tel. (33) 36425110 / 36412350 / 36415684  
direccion@aprinosa.com / www.aprinosa.com



**LK SEGURIDAD PRIVADA, S.A. DE C.V.**

No de Autorización. DGSP/119-07/926  
Hacienda de Tepalcates No.57,  
Col. Hacienda el Rosario, C.P. 02420,  
Alcaldía Azcapotzalco, Ciudad de México.

Tel. 5916 5931  
Laadu\_kalmekak@hotmail.com / www.laadusp.com



**MULTIPROSEG, S.A. DE C.V.**

No. de Autorización DGSP/090-16/3023  
Av. Armada de México No. 1500,  
Residencial Cafetales, C.P. 80220,  
Alcaldía Coyoacán, Ciudad de México.

Tel. 01(55) 5594 5513  
info@multiproseg.com / www.multiproseg.com



**INTERNATIONAL PRIVATE SECURITY DE MEXICO, S.A. DE C.V.**

No. de Autorización DGSP/008-12/1940  
General Ignacio Zaragoza Número 768,  
Col. Aviación Civil, C.P. 15740,  
Alcaldía Venustiano Carranza, Ciudad de México.

Tel. (55) 63786621  
www.grupoipsmexico.com



**CORPORATIVO INALARM, S.A. DE C.V.**

No. de Autorización DGSP/115/11/1751  
Rey Maxtla No. 213, Col. San Francisco  
Tetecala, C.P. 02730, Alcaldía Azcapotzalco,  
Ciudad de México.

Tel. (55) 5354 5670  
www.inalarm.mx



**SERVICIOS ESPECIALIZADOS EN SEGURIDAD PRIVADA SEPSISA, S.A. DE C.V.**

No. de Autorización DGSP/277-12/2152  
Calzada de Las Bombas No. 121,  
Col. Ex-Hacienda, Coapa, C.P. 04980,  
Alcaldía Coyoacán, Ciudad de México.

Tel. (55) 5662 6284 (55) 5662 6039, (33) 1562 6604 y (33) 3658 4548  
www.sepsisa.com.mx



**GRUPO EMPRESARIAL CASA, S.A. DE C.V.**

No. de Autorización DGSP/144-05/669  
Limoneros No. 9-A, Fraccionamiento  
Valle de San Mateo, C.P. 53240, Naucalpan,  
Estado de México.

Tel. 5373 1761 y 5363 2868  
ventas@gecsa.com.mx / www.gecsa.com.mx



**PROTECCIÓN Y ALARMAS PRIVADAS, S.A. DE C.V.**

No. de Autorización DGSP/026-01/163  
Río Culiacán No. 203 Poniente,  
Col. Guadalupe, C.P. 80220,  
Culiacán, Sinaloa.

Tel. 01(800) 727 7472  
atencionclientes@paprisa.com.mx / www.paprisa.com.mx



**ICP RANGER SWAT MEXICO, S.A. DE C.V.**

No. de Autorización. DGSP/250-17/3397  
Av. Invierno Número 11, Col. Ángel Zimbron,  
C.P. 02099, Alcaldía Azcapotzalco,  
Ciudad de México.

Tel. (55) 5561535  
contacto@rangerswat.com.mx / www.rangerswat.com.mx



**GUARDIAN CONTRACTORS, S.A. DE C.V.**

No. de Autorización DGSP/015-15/2798  
Av. Sayil Num. Mz. 5, Lt. 2, Col. Zona  
Federal Supermanzana 6a, C.P. 77503,  
Benito Juárez, Quintana Roo.

Tel. (998) 2677473, 229 937 9284  
contacto@guardian.org.mx / www.guardian.org.mx

# **SEGURIDAD PUBLICA**



**REVISTA DIGITAL**

ESPECIALIZADA EN SEGURIDAD PÚBLICA

[www.seguridadpublica.mx](http://www.seguridadpublica.mx)



## ARMA NO LETAL

que usa ondas sonoras

Se ha desarrollado un instrumento, en forma de arma, que tiene como función dispersar multitudes. Esta nueva "arma" ha sido pensada y puesta en práctica junto con las fuerzas militares y policiales de China. Como se indica en el sitio web del Instituto Técnico de Física y Química de la academia, las autoridades podrán utilizar un equipo que utilice ondas focalizadas de sonido de baja frecuencia.

El "efecto biológico" del dispositivo causará una incomodidad extrema, con vibraciones en los tímpanos, ojos, estómago, hígado y cerebro, dijeron científicos.

Los estudios de 1940 descubrieron que la energía sonora de baja frecuencia podría, dependiendo de la intensidad y la exposición, causar mareos, dolor de cabeza, vómitos, espasmos intestinales, defecación involuntaria, daños en los órganos y ataques cardíacos.



### China crea un arma sónica portátil, pero aún no la ha usado en Hong Kong

Las armasónicas son típicamente grandes y deben montarse en vehículos. Incluso el desarrollo chino, que no tiene partes móviles, estos equipos eran alimentados con electricidad para conducir una bobina magnética para generar energía. Eso significaba que necesitaban una fuente de energía grande y estable.

El gobierno chino lanzó el programa de armasónicas en 2017. Sin embargo, es poco probable que su conclusión esté relacionada con los meses de protestas antigubernamentales en Hong Kong.

Según el profesor Xie Xiujuan, responsable del diseño, el dispositivo es alimentado por un recipiente en forma de tubo que contiene un gas inerte. Cuando se calienta, las partículas de gas vibran y se emite un sonido profundo y monótono.

El prototipo pasó pruebas de campo, de terceros y el equipo del proyecto terminó su evaluación de los efectos del dispositivo en el cuerpo, dijo la academia.

El 4 de septiembre, un panel de científicos e ingenieros representantes del Ministerio de Ciencia y tecnología se reunió en Pekín y aprobó un proyecto desarrollado por el equipo de la Xie para la producción masiva.

### Con aspecto de rifle, se puede usar en cualquier escenario

En una foto del sitio web del instituto, el dispositivo puede verse sobre una mesa de reunión. Además de la capacidad de ser portátil, esta nueva arma parece un rifle, con cargador, gatillo y cañón.

Aunque había mucho interés en el tema, los científicos implicados se negaron a revelar detalles. Por lo tanto, todavía no se sabe nada sobre la frecuencia del dispositivo o su alcance efectivo. Además, Xie Xiujuan también se negó a comentar sus usos sin la aprobación de las autoridades superiores. 

**“TECNOLOGÍAS NO LETALES,  
TECNOLOGÍAS MENOS LESIVAS”**



**PISTOLA NO LETAL  
MODELO TIGGER**



**PISTOLAS  
ELÉCTRICAS NO  
LETALES**



**ESCUDO  
ELÉCTRICO**



**Soluciones  
para el Sistema  
Penitenciario**

Correo: [ventas@aprinosa.net](mailto:ventas@aprinosa.net)

Tel: (52) 333 6412350

Tel: (52) 333 6415684

Whatsapp: (52) 333 7007721

EMPRESA 100% MEXICANA

**[www.aprinosa.net](http://www.aprinosa.net)**



## LONDRES PRUEBA ESCÁNERES CORPORALES en el metro para detectar armas y explosivos

La policía londinense comienza a desplegar a modo de prueba una serie de escáneres corporales diseñados para poder detectar pistolas, cuchillos y diferentes dispositivos explosivos que puedan llevar los usuarios del metro ocultos bajo la ropa. Este ensayo, que está financiado por el Ministerio del Interior, tendrá lugar en la estación de Stratford, al este de la ciudad, y forma parte de una nueva ofensiva que se está llevando a cabo en la capital para acabar con los altos índices de violencia, según informa Evening Standard.

Los escáneres de la firma Thruvision que están usando los miembros de la British Transport Police (BTP) trabajan revelando objetos ocultos bajo las prendas de ropa de los usuarios, una forma de detectar a potenciales sospechosos que funciona gracias a una tecnología de imagen térmica que permite detectar elementos ocultos. Así, estas cámaras son capaces de rastrear a 2,000 personas cada hora y permiten a los cuerpos de seguridad conocer el tamaño, la forma y la ubicación de cualquier tipo de arma o elemento que pueda dar lugar a sospechas.

### Escanean desde 9 metros

La particularidad de estos escáneres corporales es que pueden dar una visión de cada uno de los pasajeros a

una distancia de algo más de 9 metros (30 pies), mientras estos están subiendo o bajando una escalera automática o pasando por los tornos de acceso y salida del suburbano londinense. Además, este sistema posibilita hacer estos controles sin que los usuarios analizados tengan que parar o ralentizar su trayecto, ni requerir una búsqueda manual, según las palabras de su inventor.

La prueba servirá a la policía para mostrar y analizar cómo los oficiales pueden usar la tecnología para identificar si algún individuo porta un cuchillo o algún otro tipo de arma y, con ello, reducir de forma potencial los controvertidos controles aleatorios que estaba llevando a cabo la British Transport Police en los últimos tiempos.

Esta tecnología, la cual ya está en uso desde el año pasado en el metro de Los Ángeles y que ha convertido a este suburbano en el primer sistema de transporte público en adoptarla, estará en manos de la British Transport Police, aunque contará con el apoyo de la Metropolitan Police. Al respecto de la prueba en la capital europea, el Ministro de la Policía, Kit Malthouse, dijo que estaban "haciendo todo lo posible en una batalla contra el crimen con arma blanca en Londres y en todo el país".

# INVIERTEN COMERCIOS

## hasta 50 mil pesos en seguridad



**M**exicali, Baja California.- Hasta 50 mil pesos en equipamiento de seguridad gastan algunos comercios para protegerse de la delincuencia, señaló el presidente de la Cámara Nacional de Comercio (Canaco), Juan Ramón López Naranjo.

Señaló que durante los últimos años ha incrementado la inversión de los comerciantes en materia de seguridad, sobre todo en todo lo relacionado con la tecnología.

Esto mediante la compra de alarmas, botones de seguridad, cámaras de video y audio vigilancia, que asegura ayudan a inhibir la entrada de delincuentes a los locales comerciales.

“Creo que ha habido un incremento en el hábito de autoprotegerse” comentó “creo que en parte a eso se debe también la disminución que ha habido en el robo y la delincuencia en los comercios”.

López Naranjo también resaltó que la disminución en los costos de las tecnologías también ha permitido a los comerciantes acceder a este tipo de aditamentos.

Por otra parte, resaltó que durante este año se ha visto una reducción en los casos de robo e inseguridad a comercios de al menos un 11%, hecho que relaciona a la implementación de estas medidas de seguridad por parte de los empresarios. **JS**

## Reunión con

# ANTAD

**C**ampeche.- Para dar seguimiento a los programas de combate al delito de robo, específicamente el denominado farderismo, en tiendas departamentales y de autoservicio, el titular del Consejo Estatal de Seguridad Pública (CESP) Manuel Lanz Novelo, encabezó la reunión con los representantes y encargados de la seguridad de los supermercados y tiendas departamentales pertenecientes a la Asociación Nacional de Tiendas de Autoservicio y Departamentales (ANTAD).

Durante el encuentro, fueron presentadas estadísticas que indican la disminución de la incidencia delictiva en los negocios, como resultado del trabajo coordinado con las instancias de seguridad pública y de procuración de justicia.

También acordaron reforzar las medidas para prevenir conductas inadecuadas y delictivas, dentro y fuera de los establecimientos



comerciales, mediante pláticas y cursos de prevención del delito a empleados y asociados.

Lanz Novelo, igual presentó información sobre el Registro Público Vehicular (REPUVE) que consiste en el control público de vehículos, previo cumplimiento del proceso de validación de información, y que además de ser instrumento de información, otorga seguridad pública y jurídica a los trámites que sean realizados con vehículos que circulen en territorio estatal y nacional.

Igual señaló que el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública mantiene a Campeche como el Estado con menor incidencia delictiva, por lo que exhortó a los presentes a no bajar la guardia y desde sus respectivos ámbitos de competencia, continuar fortaleciendo los esfuerzos contra la delincuencia.

Finalmente dijo que estas reuniones se harán extensivas a diferentes puntos del estado para fortalecer las estrategias de seguridad en toda la entidad. **JS**



## VIGILAN ZONAS MÁS CONFLICTIVAS

### con 225 cámaras

*“Para poder determinar en dónde se iban instalar estas cámaras, dimos prioridad a las zonas que tienen mayor incidencia delictiva”, comentó.*



Tijuana, México.- A pocos días de concluir el 22 Ayuntamiento de Tijuana, el Gobierno Municipal adquirió un sistema de videovigilancia conformado por 225 cámaras.

El secretario de Seguridad Pública Municipal (SSPM), Marco Antonio Sotomayor Amezcua, informó que el Municipio invirtió más de 26 millones 473 mil pesos en este proyecto con el que se busca reducir los índices delictivos.

Detalló que las cámaras comenzaron a operar en el mes de septiembre y se ubican en las colonias donde existe mayor inseguridad.

El titular de la SSPM recordó que administraciones pasadas instalaron cámaras, pero orientadas al primer cuadro de la ciudad sobre todo en Zona del Río, y en esta ocasión será en comunidades de la Zona Este.

Explicó que las cámaras están enlazadas al Centro de Control y Mando (C2) y al Centro de Control, Comando, Comunicación y Cómputo (C4).

Resaltó que además 50 comercios en distintas partes de la ciudad compraron cámaras de vigilancia que están integradas al Sistema de Vigilancia Urbana, con lo que suman 800 cámaras funcionando en diferentes puntos de Tijuana.

Los dispositivos en negocios, dijo Sotomayor Amezcua, han dado resultados como la atención de 20 mil 204 reportes y se ha logrado detener a 12 mil 118 personas por falta al Bando de Policía y 409 delincuentes. Además atendieron 3 mil 62 reportes relacionados con vialidades y hechos de tránsito.

El presidente municipal, Juan Manuel Gastélum Buenrostro, consideró que la compra de cámaras ayudará a la prevención.

“Para nosotros es importante dejarle a Tijuana todo listo para que la nueva autoridad en cuanto pueda adquiera más cámaras, más patrullas, contrate más policías”, añadió.

El Primer Edil aclaró que en esta ocasión no habrá problemas con las cámaras como en el pasado que no había quien diera mantenimiento e hiciera el monitoreo, porque al ser una compra final el personal del C2 las usará y atenderá. 

# CONTROL L

DE **ACCESOS** MX



REVISTA DIGITAL

ESPECIALIZADA EN CONTROL DE ACCESOS

[www.controldeaccesosmx.com](http://www.controldeaccesosmx.com)



## DEMIA agrega Inteligencia Artificial a Morphowave Compact

París, France.- Con más de 40 años de experiencia IDEMIA ha fusionado con éxito los beneficios de la IA con su experiencia en principios biométricos fundamentales. Esta inversión continua en I + D ha llevado al siguiente gran avance en la identificación de huellas dactilares, ampliando aún más los límites con el Morphowave Compact mejorado, ahora impulsado por IA.

IDEMIA lanzó por primera vez un dispositivo biométrico de control de acceso sin fricción altamente seguro con Morphowave hace varios años, respondiendo con éxito a la demanda del mercado en la industria. La tecnología de huellas digitales 3D sin contacto ha sido adoptada por organizaciones de todo el mundo, ya que los clientes comprenden la importancia y el valor de la identificación biométrica positiva combinada con un alto rendimiento y conveniencia. Según IDEMIA, el lanzamiento de Morphowave Compact el año pasado ha reforzado esta posición de liderazgo. En línea con la estrategia de IDEMIA para permitir el acceso sin fricción a todas partes, este cambio de juego para la industria se ha adoptado rápidamente en una amplia gama de verticales.

En esta última actualización, el nuevo motor biométrico integrado basado en IA de IDEMIA ofrece un aumento del 85% en la velocidad de coincidencia, lo que se traduce en un aumento del rendimiento del 25% de más de 50 personas por minuto por punto de acceso. Los algoritmos aumentan aún

más la precisión de coincidencia, permiten una mayor capacidad (hasta 100,000 usuarios para la identificación de uno a muchos) y brindan un beneficio particular cuando se trata de las huellas digitales más desafiantes.

Los clientes nuevos y existentes de Morphowave Compact pueden aprovechar esta última actualización, lo que demuestra el compromiso de IDEMIA no solo con el desarrollo del mercado, sino también con la presentación de un socio confiable a largo plazo en soluciones de seguridad biométrica.

"La tecnología está evolucionando a un ritmo increíble y constantemente desafía y redefine las prácticas de los clientes. En IDEMIA, la innovación y ampliar los límites es parte de nuestro ADN. Esta última innovación es otro paso hacia el futuro de la identificación biométrica y nos permite seguir siendo un líder en identidad aumentada". Comentó Yves Portalier, vicepresidente ejecutivo de la unidad de negocios Connected Objects en Idemia. 

# CINCO FACTORES CLAVE

## que impulsan el mercado de control de acceso

**D**ublín, Irlanda y Parsippany NJ (EE. UU.).- La percepción y la realidad del crecimiento en el mercado de control de acceso ciertamente han cambiado en los últimos años. Lo que una vez fue conocido por su trayectoria lenta y conservadora ahora se ha transformado en una industria que está experimentando un desarrollo acelerado, con las últimas predicciones que predicen que el mercado global crecerá a un estimado de alrededor de \$ 16 mil millones de dólares para el final de ese período de tiempo. Aquí, Vanderbilt ofrece una visión de los cinco factores principales que podrían estar contribuyendo a este crecimiento.

Como es común en cualquier segmento de la industria de la seguridad, este crecimiento puede atribuirse a una serie de factores, y cada uno juega un papel importante en la evolución general del mercado. Aquí echamos un vistazo a los cinco primeros:

### Amenazas crecientes

Los objetivos suaves de todo el mundo, como instalaciones educativas, lugares, centros comerciales, centros de transporte y más, continúan enfrentando el desafío de mantenerse preparados para la creciente importancia y frecuencia de las amenazas. Y uno de los primeros métodos de protección que a menudo viene a la mente para estas instalaciones es asegurar el perímetro del edificio o campus, lo que lleva a un aumento en el uso de soluciones de control de acceso que mejoran la seguridad y permiten cierres rápidos con solo presionar un botón.

### Tecnología avanzada

La aparición de la nube e Internet de las cosas (IoT) ha impactado positivamente en toda la industria de la seguridad en su conjunto, y esto sin duda incluye el mercado de control de acceso. Estas tecnologías inteligentes han abierto nuevas posibilidades para los sistemas tradicionales de control de acceso del pasado,



como la supervisión remota, las instalaciones menos engorrosas y la gestión / informes centrales. Además, la tecnología como las credenciales móviles y la biometría ofrecen opciones emocionantes e innovadoras para las soluciones de control de acceso, impulsando el crecimiento del mercado a través del interés en la conveniencia de estas características.

### ACAAS

Uno de los beneficios clave que la nube crea para el mercado de control de acceso es el modelo de control de acceso como servicio (ACaaS), del cual estamos viendo una alta adopción, particularmente en las pequeñas y medianas empresas (PYMES) - y por lo tanto está facilitando la expansión del mercado. Las pequeñas y medianas empresas están aprovechando la capacidad de entregar la administración del sistema a un integrador, beneficiándose de ahorros de costos, soporte continuo y escalabilidad.

### Integraciones

La tecnología de plataforma abierta ha dado lugar a la integración perfecta de los sistemas de control de acceso con otras soluciones, alentando el crecimiento del mercado al permitir que las organizaciones obtengan una funcionalidad adicional de sus inversiones en tecnología. Las empresas pueden converger sin problemas su control de acceso con cámaras de vigilancia, sistemas de gestión de video (VMS), plataformas de intrusión y más, lo que les permite invertir en una solución que puede abordar múltiples necesidades.

### Funcionalidad agregada

Aunque el control de acceso se utiliza principalmente para fines de seguridad, a medida que estos sistemas se vuelven más inteligentes y capaces de comprometerse con otras operaciones fuera de la seguridad, su valor aumenta y, por lo tanto, conduce al crecimiento del mercado. Por ejemplo, un sistema de control de acceso puede integrarse con un sistema de gestión de edificios para bloquear / desbloquear puertas para un evento, encender / apagar luces o controlar la temperatura.

En los próximos años, a medida que la tecnología avance y se vuelva más inteligente, Vanderbilt espera ver que estas tendencias continúen impulsando el mercado de control de acceso, y encuentra alentador ver cuán lejos ha llegado el mercado. ■

# MERCADO BIOMÉTRICO DE RECONOCIMIENTO DE VOZ

## de EE. UU. Impulsado por el sector bancario

*Se espera que el creciente número de usuarios de aplicaciones de banca móvil para transacciones bancarias influya positivamente en el crecimiento del mercado estadounidense en el futuro cercano. Un aumento alarmante en las actividades bancarias fraudulentas en los Estados Unidos, según los investigadores. Es un factor importante que impulsa la adopción de medidas de seguridad de alta gama, como la biometría basada en voz, en las organizaciones bancarias.*



Los Angeles, Ca (EE. UU.).- Se espera que la demanda del mercado de reconocimiento de voz de los EE. UU. alcance 733.3 millones de unidades para 2025, registrando un 16.5% CAGR de 2019 a 2025 según un nuevo estudio realizado por Grand View Research, Inc. La creciente demanda de aplicaciones de autoservicio como las basadas en voz, se prevé que la identificación biométrica en el sector bancario impulsará el crecimiento del mercado en un futuro próximo.

La integración de la tecnología en los automóviles está ganando popularidad en todo el mundo, ya que numerosos países están desarrollando estrictas regulaciones de conducción, como la prohibición del uso de teléfonos celulares mientras se conducen vehículos. Se estima que para 2020, más del 50% de los automóviles del mundo estarán equipados con sistemas de reconocimiento de voz en el automóvil con características como hacer una llamada o cambiar la música usando comandos verbales. También es probable que la tendencia sea fuerte en los EE. UU., Lo que impulsará el mercado de EE. UU. Para el reconocimiento de voz.

Además de esto, los comandos de voz ayudan a los conductores a mantener la vista en la carretera incluso cuando acceden a aplicaciones como la navegación del automóvil o el sistema de información y entretenimiento del automóvil mientras conducen. Mientras que la entrada del destino de voz ayuda a los conductores a seguir la ruta correctamente mientras vigilan la carretera, ingresar datos manualmente en un sistema de navegación puede generar riesgos de seguridad significativos. Debido a la creciente demanda a nivel mundial, los fabricantes de dispositivos de consumo se están centrando en innovar sus productos al habilitar comandos verbales en ellos. Se espera que esta tendencia acelere el crecimiento del mercado de reconocimiento de voz de EE. UU. Durante el período de pronóstico.

Otros hallazgos clave del informe sugieren que la vertical automotriz representó una participación de mercado significativa en el mercado de EE. UU. Para el reconocimiento de voz en 2018 debido a la creciente popularidad de los sistemas de información y entretenimiento en el automóvil habilitados por comandos verbales. La tecnología también se usa cada vez más en la industria automotriz para mejorar los sistemas de navegación verbal, como actualizar al conductor del automóvil con las condiciones del tráfico en la ruta y también sugerir rutas alternativas.

Se espera que la vertical bancaria y financiera registre la CAGR más alta durante el período de pronóstico debido a la creciente adopción de autenticación biométrica basada en voz para realizar transacciones bancarias. Varios institutos financieros como HSBC y Wells Fargo están en proceso de habilitar funciones de comando verbal en sus aplicaciones bancarias.

Además, las aplicaciones en la vertical del consumidor están ganando terreno y es probable que la vertical sea testigo de prometedoras perspectivas de crecimiento durante el período de pronóstico. Los sistemas de seguridad avanzados se están integrando cada vez más con la tecnología de reconocimiento de voz para ayudar al usuario a dar comandos verbales para actividades tales como ajustar los termostatos, encender y apagar las luces e identificar a los residentes e informar a los intrusos.

Los analistas nombran algunos de los principales proveedores de soluciones de reconocimiento de voz de EE. UU. En el informe, incluidos: Advanced Voice Recognition System, Inc., Agnitio S.L. (subsidiaria de Nuance Communications Inc.), Amazon.com, Inc., Apple Inc. y Baidu, Inc. 



## TECNOLOGÍAS DE IDENTIFICACIÓN CONFIABLES permiten a integradores crear experiencias conectadas más inteligentes

*Edson Yano, gerente de ventas de la unidad IDT de HID Global para América Latina.*



Las identificaciones confiables se están volviendo uno de los elementos fundamentales para crear entornos que conecten de manera más efectiva a las personas, los lugares y las cosas de una organización. Los integradores que adopten las ventajas de las identificaciones confiables ayudarán a sus clientes a redefinir la experiencia de los usuarios utilizando una combinación de tecnologías como el IoT (internet de las cosas), la nube y los dispositivos móviles. De igual manera, los integradores también desean soluciones de credenciales más unificadas y mejorar de forma significativa numerosos servicios en el lugar de trabajo y procesos empresariales mediante herramientas de análisis avanzadas.

### El móvil: un punto de inflexión

El control de acceso móvil va ganando popularidad a medida que las soluciones van madurando y se integran con otros sistemas. Hasta hace poco, el concepto de una credencial alojada en un dispositivo móvil constituía un nicho para un pequeño segmento del mercado. Sin embargo, su contribución a una mayor eficiencia operativa, una mejor experiencia de usuario y un mejor nivel de seguridad, así como la capacidad de integrarse con otros sistemas, ha posicionado el acceso móvil como una excelente opción para muchas organizaciones en el mercado de consumo. La demanda será mayor en las siguientes operaciones: abrir puertas con un teléfono inteligente, usar un dispositivo móvil como medio de autenticación en aplicaciones -como la verificación de identidad para proteger su uso en la banca en línea o el acceso a una red digital-, o portar una identificación (como la licencia de conducción) en un teléfono.

Cuanto más medios físicos móviles existan para portar identificaciones confiables, mucho mejor; de este modo, las organizaciones podrán emplear esta solución en la más amplia gama de casos prácticos. Los relojes inteligentes y dispositivos biométricos personales son las prendas electrónicas más comúnmente empleadas en el entorno empresarial actual. El incremento del uso de prendas y accesorios electrónicos en soluciones de acceso empresarial sigue estando a la orden del día. Estos dispositivos se están volviendo más inteligentes y su uso más frecuente en un número cada vez más amplio de aplicaciones.

Otros beneficios del acceso móvil se harán evidentes, especialmente a medida que las soluciones se vayan integrando en todos los edificios y centros empresariales. La tecnología demostrará su capacidad de mejorar la comodidad del usuario a gran escala. Asimismo, la migración a la verificación de identificaciones a través de teléfonos móviles también revelará una tendencia hacia la cohesión digital, en la que todo esté interconectado y disponible en una aplicación; desde la verificación en el inicio de sesión en una cuenta bancaria o en una red virtual privada (RVP) hasta el uso de un teléfono como licencia de conducción móvil o para verificar la autenticidad de una credencial física.

La adopción de estos avances tecnológicos no se ha limitado a las credenciales móviles; la migración de facto que se ha dado desde el protocolo Wiegand al estándar del protocolo de dispositivo abierto supervisado (OSDP, por sus siglas en inglés) también va en camino a convertirse en un factor importante para el control de acceso. La sonada exposición de las vulnerabilidades del antiguo protocolo Wiegand, junto con el deseo de lograr una experiencia más conectada en la gestión de los lectores, ha impulsado la demanda del estándar OSDP.

Aunque la comunicación de campo cercano (NFC, por sus siglas en inglés) es una alternativa atractiva que vale la pena considerar en el futuro para el control de acceso, Bluetooth sigue siendo el único estándar de comunicación predominante que es compatible con diversas plataformas para el acceso móvil en la actualidad. Sin embargo, las organizaciones que hoy en día invierten en infraestructura están considerando adquirir lectores que admitan ambos estándares de comunicación para poder estar preparadas en adoptar nuevas experiencias a medida que vayan ocurriendo cambios en la industria de los dispositivos móviles. La tecnología de los lectores de control de acceso también se adaptará para aprovechar la potencia de la tecnología móvil y las plataformas en la nube. Las organizaciones usarán un dispositivo móvil para

aprovisionar lectores, inspeccionar los lectores instalados y detectar su configuración actual, actualizarlos con nuevas prestaciones y/o revocar el acceso a ellos.

## La adopción cada vez mayor de la nube

Uno de los aspectos que impulsa la adopción de la nube es que su seguridad ha logrado una mejora significativa. A medida que crece la confianza en estas plataformas, aumenta la demanda de soluciones de identificación confiable en la nube y del aprovechamiento de sus numerosas ventajas. La adopción aumentará a medida que se difunda más el conocimiento sobre la facilidad de implementación, flexibilidad, opciones de conectividad y beneficios de productividad que trae la nube.

Las plataformas en la nube constituirán la columna vertebral para incorporar tecnologías nuevas y emergentes, a la vez que mejorarán la manera en que se ofrecen las soluciones de identificación. También brindarán a las organizaciones mayor flexibilidad para actualizar su infraestructura de seguridad, escalarla a la par del crecimiento de la organización, mejorar la eficiencia y adoptar nuevos modelos de servicios gestionados de menor costo.

Las plataformas en la nube propiciarán el uso de nuevas soluciones que amplíen el abanico de opciones de las organizaciones para aprovechar al máximo sus inversiones. Entre las opciones más atractivas se encuentran las soluciones que ofrecen servicios de localización para hacer seguimiento de activos y para que las organizaciones tengan más información sobre cómo se utilizan sus edificios y así poder optimizar el lugar de trabajo. Las organizaciones están adoptando tecnologías que amplían las posibilidades de interacción y trabajo de los ocupantes e inquilinos de los edificios en nuevos espacios de trabajo inteligentes. Además, estas innovaciones permiten a los responsables de la planta física de las compañías proporcionar de forma proactiva un entorno de trabajo más seguro, lograr una experiencia más inteligente en el mantenimiento de los equipos de los edificios y cumplir con un sinnúmero de normativas de inspección locales y federales.

Un beneficio adicional de la nube es que genera la oportunidad de implementar nuevos modelos de servicios gestionados. Por ejemplo, ya hay en el mercado plataformas de emisión en la nube de tarjetas de identificación que ofrecen a los usuarios la opción de arrendar hardware, software y otros recursos, cuyos costos son agrupados en una oferta de servicio que se factura en cuotas anuales o mensuales. El modelo de servicio no solo reduce varios niveles de costos en los programas, sino que además permite a los administradores escalar fácilmente la oficina de emisión de identificaciones para que se adapte a las prestaciones de las tecnologías futuras o a las cambiantes demandas de volumen. Los administradores tienen la opción de encargar a agencias de impresión comercial la producción de grandes lotes de tarjetas durante los períodos de mayor demanda. En general, los servicios en la nube ofrecen todos los beneficios de control y visualización centralizada del proceso de emisión, además de la opción de realizar impresiones distribuidas o por lotes y al mismo tiempo mejorar la comodidad del usuario.

Este modelo es particularmente atractivo para grandes centros de salud y campus universitarios. En el sector universitario, desde hace tiempo las tarjetas de identificación en los campus han permitido a los usuarios comprar comidas, prestar libros de la biblioteca y abrir puertas de dormitorios, entre muchos otros usos. No obstante, estas instituciones están entendiendo los beneficios que trae adoptar la nube para actualizar la forma de emitir las identificaciones de la población universitaria. En lugar de emitir tarjetas usando una o más estaciones de trabajo PC, cada una de las cuales está conectada a una impresora cercana, las universidades están migrando a soluciones en la nube para lograr una nueva experiencia de emisión remota de tarjetas. Este cambio también está transformando las impresoras de tarjetas de identificación en dispositivos periféricos dentro del internet de las cosas confiables (IoT por sus siglas en inglés).

## Experiencias más conectadas en el IoT

Hoy más que nunca, los teléfonos inteligentes que portan identificaciones confiables están permitiendo una gama cada vez más amplia de prestaciones



seguras en la gestión de edificios inteligentes, las cuales se pueden usar sin importar dónde se encuentre el usuario y conectan el mundo de las personas con el mundo de las cosas. Por ejemplo, una nueva clase de soluciones de seguridad vuelve confiables las etiquetas NFC, las cuales pueden adherirse luego a llaves mecánicas y estas ubicarse en diferentes puntos de una planta física para que, por ejemplo, la entrega de llaves se pueda automatizar y los guardias que estén haciendo las rondas de vigilancia puedan registrar su presencia en un punto de control de seguridad mediante la autenticación en la nube.

Los integradores pueden combinar esta misma tecnología con soluciones de software de gestión computarizada de mantenimiento (CMMS, por sus siglas en inglés). Estas permiten transacciones seguras entre equipos de seguridad y de protección contra incendios y sistemas de mantenimiento en línea, lo cual ayuda a simplificar los procesos de seguridad y protección contra incendios y facilitar el cumplimiento de la normatividad local.

Hoy en día, el uso de las balizas BLE, los servicios en la nube y las redes móviles actuales, también ha reducido significativamente los costos de infraestructura que acarrea la implementación de aplicaciones IoT en edificios inteligentes. Los servicios de localización de BLE a Wi-Fi posibilitan a los encargados de la planta física de las compañías visualizar en tiempo real cuándo se está utilizando un área específica durante la jornada laboral, lo cual les permite planificar los espacios y la utilización general del edificio (desde oficinas independientes y espacios de trabajo compartidos hasta salas de conferencias de gran demanda). Por ejemplo, los ocupantes y visitantes de los edificios pueden desplazarse fácilmente por las instalaciones utilizando servicios de localización que los orienten con indicaciones, lo que facilita la colaboración, la ubicación de los miembros del personal y la búsqueda instantánea de espacios para reuniones. Las innovaciones en IoT también pueden agregar un nivel de seguridad adicional al permitir a los responsables de la planta física de la compañía autorizar el acceso a zonas específicas, de acceso restringido, en un determinado espacio, planta de producción o cualquier área que requiera un nivel adicional de seguridad zonificada.

Hay muchas oportunidades para que los integradores de sistemas ayuden a sus clientes a aprovechar estas prestaciones en diversos mercados verticales y en función de sus diversos requerimientos. Por ejemplo, las instituciones de atención médica necesitarán servicios de localización en tiempo real para optimizar los flujos de trabajo en los departamentos de emergencias y en las operaciones clínicas y para ofrecer orientación a los pacientes y visitantes que circulan por los hospitales.

Los sistemas de control de acceso también se están expandiendo para crear entornos donde sea posible conocer mejor las actividades desarrolladas por el personal en industrias como el petróleo y el gas, donde es fundamental que los equipos de seguridad conozcan la ubicación precisa de los empleados en situaciones de emergencia o cuando un trabajador ha sufrido un accidente o desmayo ("hombre caído").

### La comodidad de la convergencia

Otra área en la que los integradores de sistemas pueden brindar un valor agregado es en ofrecer la comodidad de un sistema de seguridad física e informática que converja en una única credencial. De la misma manera en que los usuarios están gravitando hacia las soluciones móviles, en parte porque les gusta la forma en que estas interconectan



a su mundo digital, también las empresas, universidades e instituciones de salud están adoptando las credenciales convergentes. Los clientes desean hacer mucho más con sus credenciales de identificación confiables que solo abrir puertas.

La noción de las credenciales derivadas también ayudará a impulsar la convergencia. Estas credenciales, cuyo uso inicial estaba restringido al gobierno de los EE. UU., se derivan de una tarjeta física, se almacenan en un token de software y están protegidas con la protección de hardware de un dispositivo móvil. Este tipo de credenciales también facilitará el uso de dispositivos móviles para la seguridad física e informática. Los pioneros de esta tecnología en la industria financiera, de energía, en otras industrias sujetas a reglamentación y en los gobiernos internacionales, usarán estas soluciones para proteger el acceso a edificios, correos electrónicos, sitios web y redes privadas virtuales (RVP).

La convergencia también impulsará la adopción de la gestión unificada del ciclo de vida de las identificaciones. Va en aumento la demanda de soluciones de gestión de identidad y de acceso físico (PIAM, por sus siglas en inglés) que conecten múltiples y distintos sistemas de control de acceso físico (PACS) de las compañías y los sistemas de seguridad informática a otras partes de los ecosistemas informáticos, como los directorios de usuarios y los sistemas de recursos humanos.

Estas soluciones también permiten que el sistema de control de acceso físico se conecte a sistemas de emisión de tarjetas en la nube y a cerraduras inalámbricas, así como a servicios de localización. Esto mejora la eficiencia y la seguridad al estandarizar la gestión de identificaciones de los empleados, contratistas, visitantes, inquilinos y proveedores. Las soluciones de gestión de identidad y de acceso físico también constituyen un puente entre los edificios inteligentes y el personal que se contrata en la actualidad, de naturaleza más fluida y flexible.

Uno de los primeros ejemplos de la potencia de las credenciales convergentes se encuentra en la atención médica. Las organizaciones están utilizando un modelo en la nube para proporcionar identificaciones y llevar a cabo la autenticación en el control de acceso físico y lógico y gestionar los sistemas de prescripciones electrónicas de sustancias controladas (EPCS por sus siglas en inglés). Esta y otras industrias migrarán cada vez más a sistemas que reúnan todo lo relacionado con la gestión de identificaciones en un sistema unificado capaz de otorgar y gestionar derechos de acceso.

Las nuevas soluciones de identificación confiables tendrán un impacto radical en el papel que desempeñarán los integradores de sistemas en el futuro, ya que el aumento de las oportunidades les permitirá agregar más servicios a sus portafolios. En el futuro, los continuos avances en seguridad y tecnologías de identificación darán lugar a entornos más inteligentes que brindarán una experiencia de identificación integral y segura. Los integradores de sistemas serán un enlace fundamental en la cadena de valor para garantizar este modelo, basado en la experiencia, que prioriza la protección de personas y activos en el futuro. ■



# ORIGINS PRIVATE SECURITY S.A. DE C.V.



**SEGURIDAD**



**PREVENCIÓN**



**CONFIANZA**



Marsella No. 60, Int. 103,  
Colonia Juárez, Alcaldía Cuauhtémoc,  
Ciudad de México, C.P. 06600

Telefónos:

**5207 6828 / 3603 3189**

[www.seguridad-privada.com.mx](http://www.seguridad-privada.com.mx)



# SEGURIDAD INDUSTRIAL



REVISTA DIGITAL

ESPECIALIZADA EN SEGURIDAD INDUSTRIAL

[www.seguridadindustrialmx.com](http://www.seguridadindustrialmx.com)



## SAFESTART

# la Neurociencia y la Cultura de la Prevención en Seguridad

*“El error humano provoca el 95 por ciento de los accidentes por descuido, errores, falta de concentración o distracción. Por lo que es necesario empezar a trabajar el subconsciente en las capacitaciones que realizan las empresas a través de las Técnicas de Reducción de Errores Críticos (TREC) del método de SafeStart”, Señaló Crowe.*



Paul Crowe, consultor y master trainer SafeStart, realizó el Webinar *“Neurociencia por detrás de los Factores Humanos”*, y destacó el surgimiento de una Tercera Generación de la seguridad, que se enfoca en el desarrollo de hábitos y habilidades de seguridad para disminuir errores críticos. Con la corroboración de la neurociencia, el foco fue demostrar la eficacia del autocuidado.

Paul indicó que las empresas para evitar accidentes realizan cursos y entrenamientos de seguridad tradicionales, buscan disciplinar sus trabajadores con programas muy reactivos que normalmente no ubican el error humano, perteneciendo a lo que se denomina la 1ª y 2ª generación de seguridad.

La 3ª generación fomenta una cultura de protección que va mucho más allá de las generaciones anteriores, lo que implica hacer un cambio de abajo hacia arriba del individuo, es decir, trabajar desde el subconsciente en sus hábitos y habilidades más seguras, haciendo con que los riesgos y las respuestas a ellos, también sean detectados automáticamente.

Sugirió que evitemos hacer las cosas en el modo *“piloto automático”*, es decir, debemos concientizarnos de la dimensión de lo que puede costar un error, que no solo tiene que ver con la empresa, con la rentabilidad, sino con la vida de una persona y el impacto en la familia.

En el webinar destacó que la Tercera Generación de Seguridad es el trabajo y compromiso, un cambio interno de un proceso subconsciente. Con el método SafeStart proporcionamos herramientas para que la gente tenga los *“ojos y mente en la tarea”*.

*“Si no cambiamos la percepción de peligro de las personas, nada cambiará a largo plazo, los viejos hábitos prevalecerán; la mente subconsciente necesita una perspectiva diferente para poder *“re-cablear”* sus respuestas a los peligros del día a día”,* destacó Paul Crowe.

La presentación se realizó el 11 de septiembre y contó con la presencia de personas de México, Perú, Colombia, Argentina, Bolivia, Brasil y otros países de Centro y Sudamérica. 🇲🇽



## EXPO FIRE

# PROTECTION MÉXICO 2019

*Los días 1 y 2 de octubre se realizó la Expo Fire Protection, un evento especializado para la industria de la protección contra incendio que combina una exposición, que presenta sistemas de protección, detección, alarma, extintores, protección personal y capacitación, así como amplia gama de proveedores de servicios, como ingeniería, instalación, mantenimiento y puesta en marcha. Además, el Congreso Internacional de dos días de conferencias y paneles de alto nivel con temas relevantes en seguridad y protección contra incendio.*



La Expo Fire Protection & International Congress significa un gran paso para sensibilizar y concientizar acerca de la impostergable necesidad de actualizar y fortalecer el marco regulatorio en materia de seguridad humana y protección contra incendio.

En México aún es incipiente la cultura de la prevención contra incendios. De 2015 a 2018 se registraron 54 mil siniestros de este tipo, cuyas pérdidas representan el 8% del Producto Interno Bruto (PBI) del país generado en un año. Frente a este panorama, se requiere de una regulación homologada que genere riquezas y proteja vidas.

Durante la inauguración del evento, Juan Carlos Camacho, presidente de Asociación Mexicana de Rociadores Automáticos Contra Incendio (AMRACI), aseguró que “los siniestros por fuego tienen mayores víctimas y daños que



un huracán o un sismo, pero se producen de manera aislada, por lo que no provocan noticias de primera plana. En los últimos cinco años, en el territorio mexicano se han registrado alrededor de 25 mil heridos; 19 mil evacuados; 14 mil damnificados; y 93% de los pacientes fueron atendidos en hospitales públicos, debido a los incendios”.

“Esto refleja la insuficiente infraestructura para resolver este problema, en ocasiones se requiere acudir a otro país para atender heridos por quemaduras, el índice de pérdidas humanas es más del doble que en países desarrollados, donde se ha modernizado la regulación contra la protección contra incendios”.

A raíz del terremoto de 1985 se modificaron las reglas de construcción de los edificios. A la fecha, aseguró el presidente de la organización, se cuenta con un reglamento de construcción adecuado, pero éste debe estar alineado a un esquema de protección civil específicamente en la prevención de incendios.

Por su parte, David Morales, presidente del Consejo Nacional de Protección Contra Incendios (Conapci), indicó que las nuevas construcciones se están enfocando hacia lo sustentable, sin embargo, esto genera nuevos desafíos en materia de seguridad y las normas existentes son inadecuadas. Al año, en México se registra un 10% de aumento en el número de incendios.

En el evento, también estuvo Alfonso Güati Rojas Sánchez, director general de Normas de la Secretaría de Economía, quien ofreció reunirse con las asociaciones del sector a fin de que se revise la normatividad contra incendios para crear un mejor modelo de industria y seguridad de cara a 2020.

La AMRACI, con el respaldo de otros organismos del sector, incluido el Cuerpo de Bomberos de la CDMX, anunció la realización de la 5ª Campaña de Prevención y Protección Contra Incendios, que tiene como objetivo fomentar una cultura para lograr un México sin víctimas de fuego, y que se llevó a cabo del 30 de septiembre al 4 de octubre. 



## ¿QUÉ SIGNIFICA EL COLOR DE CASCO DE SEGURIDAD?

**E**s bien sabido que toda persona cuya labor se ubique en una zona de riesgo, debe usar un casco de protección, lo que no se conoce a ciencia cierta es la categoría de los cascos, los cuales diferencian el cargo de cada persona por su color.

Es necesario conocer antes de adquirir los cascos de seguridad, cuál será el rol de cada quien en la obra y una vez teniendo conocimiento de éste, elegir el color indicado para cada quien.

No existe una normativa legal u oficial al respecto, más bien, dependerá de cada empresa esta elección. Lo que sí es oficial son las reglas básicas no escritas al momento de identificar los colores de los cascos de los trabajadores. Por norma general, se asocian los colores más llamativos con las tareas más riesgosas.

Así, tenemos que la asignación de color de casco de seguridad más común es esta:

**Amarillo:** Para todo tipo de trabajo de obra, como operarios en construcción o albañiles.

**Naranja:** Lo suelen usar los equipos de carretera, los nuevos trabajadores y ayudantes.

**Rojo:** Para personal de seguridad, bomberos o brigadas de emergencia.

**Verde:** Lo usan inspectores de seguridad, servicios médicos e higiene. Ocasionalmente lo usan los hormigoneros, visitantes a la obra, nuevos trabajadores o personal de prueba.

**Blanco:** Lo utilizan los gerentes, jefes de obra, supervisores, ingenieros, capataces, arquitectos, personal administrativo o topógrafos.

**Azul:** Usualmente lo utilizan carpinteros, encofradores y operadores técnicos, incluidos los técnicos electricistas; también para estudiantes en prácticas, asesores técnicos y también visitas.

**Gris:** Básicamente lo utilizan visitantes.

**Café:** Soldadores y otros trabajadores con aplicaciones de alto calor. También en industrias petroquímicas.

**Dorado:** Para las visitas más importantes: dueños y autoridades.

**Rosa:** Algunas empresas los usan para aquellos trabajadores que se han olvidado su propio casco; se utiliza como una forma ligera de castigo. En algunas otras empresas simplemente los utilizan las mujeres o incluso el personal administrativo que no está expuesto a un gran riesgo.

Así es como se clasifica usualmente la gama cromática del color de casco de seguridad, el cual ciertamente es básico y es mejor utilizar cualquiera a ninguno. Es un elemento de seguridad que puede salvar la vida de los elementos que forman parte de un objetivo, que deben respetar no solamente las reglas de su empleador, sino resguardar su integridad. 

*En toda zona de construcción existen roles que deben de tomarse, respetarse y darse a conocer con los demás participantes para el correcto flujo de comunicación, que en ocasiones no es verbal dadas las condiciones ambientales.*





## COPARMEX

# Protección Civil en la Ciudad de México

**E**n lo que va de este año muchos temas relacionados con la protección civil en la Ciudad de México han cambiado. Para entender un poco mejor este nuevo panorama, hace algunos días visitamos a Armando Aguilar Hirata, presidente de la Comisión de Seguridad e Higiene y Protección Civil de la COPARMEX Ciudad de México. Esto fue lo que nos dijo:

“La legislación en materia de protección civil era otra hasta antes del pasado 5 de junio, que es cuando se expide la Nueva Ley de Gestión Integral de Riesgo y Protección Civil. La anterior ley, llamada Ley del Sistema de Protección Civil del Distrito Federal, publicada en el 2014, era muy complicada y muy opresiva. Las delegaciones se convertían en juez, parte y verdugo en materia de protección civil. Más del 90% de las empresas de la ciudad estaban obligadas a presentar un programa de protección civil, pero el problema es que era un mero trámite, no tenía otra función”.

“Y es que era un trámite integrador porque tenías que presentar cosas como el visto bueno de seguridad de operación, éste debía generarlo un especialista que se llama director responsable de obra, y para poder obtenerlo, la empresa debía contar primero con un registro, después con un documento que se llama alineación y número oficial y después contar con un registro catastral, sólo para estar seguros de que realmente estás ahí y pagas impuestos. Bueno, pues esa no es la función de la protección civil”.

“Durante la administración de Mancera se legisló para que fuera obligatorio para todas las empresas y negocios presentar un programa de protección civil, que era sólo un documento, un trámite. Era muy caro y engorroso de cumplir por lo que aparecieron infinidad de “gestores” o “coyotes” que sólo contribuyeron a aumentar la corrupción”.

“Esto estuvo ocurriendo desde que se creó la primera Ley del Sistema de Protección Civil, por ahí del 2012. La primera ley

de protección civil de la ciudad aparece en 1998 con la primera asamblea y desde entonces el deporte favorito de los diputados ha sido cambiarla cada tres años. Una ley que dura sólo tres años es imposible de cumplir porque tienes que comunicarla, la ley tiene que socializarse y después se empieza a cumplir”.

“Para el año 2017 logramos que se eliminara todo esto, ese fue uno de los principales logros de la COPARMEX para el sector productivo de la ciudad. Logramos eliminar ese impuesto que era totalmente inútil, era un impuesto que no generaba más que problemas”.

“La COPARMEX Ciudad de México, a través de su comisión, está constantemente tratando de influir, de ayudar, a que la legislación de la ciudad no impacte a las empresas de manera negativa. Sabemos que tenemos que cumplir con la ley, sabemos que tenemos que ser empresas seguras, sabemos que tenemos que buscar el bien común. Estamos en la ciudad más peligrosa del mundo, hay un catálogo de 42 amenazas que pueden ocurrir, y de esas 42 amenazas, 38 pueden ocurrir en la Ciudad de México, y es algo de lo que no estamos consientes. El estar preparado contra esas 38 amenazas es una obligación del dueño de la empresa, primero porque es su empresa, y la continuidad de operación, la continuidad del negocio, es obligación del, o los dueños”.

“La nueva ley, la Ley de Gestión Integral de Riesgos y Protección Civil, que está vigente en este momento, se publica el día 5 de junio de este año, y entra en vigor el 5 de agosto. Tiene muchas cosas que a mí en lo particular me parecen muy buenas. Con la ley anterior, el 90% de las empresas de la ciudad debían presentar el trámite. En este momento, muy probablemente ese 90% no tendrá que hacerlo más. Se cambió diametralmente el enfoque, que estaba basado en un riesgo teórico por cercanía, y se cambió a una situación de actividad comercial”.

# CIBERSEGURIDADMX



REVISTA DIGITAL  
ESPECIALIZADA EN CIBERSEGURIDAD

[www.ciberseguridadmx.com](http://www.ciberseguridadmx.com)



## UTILIZAN AI PARA IMITAR LA VOZ DEL CEO DE UNA COMPAÑÍA y robar 220 mil euros

Por Juan Manuel Harán

El pasado 30 de agosto Wall Street Journal publicó la historia de un caso que ocurrió en marzo de este año en el que criminales utilizaron un software basado en inteligencia artificial (IA) para imitar la voz del CEO de una empresa de energía alemana y así llevar adelante un engaño que permitió a los estafadores robar 220,000 euros.

Según explicó el medio, los estafadores utilizaron esta tecnología para suplantar la identidad del director ejecutivo de una multinacional alemana y engañar al CEO de una de sus sedes en Reino Unido, quien creyó que estaba hablando telefónicamente con su jefe y aseguró haber reconocido el ligero acento alemán en su voz. Así, el supuesto CEO de la firma alemana solicitó al CEO de la sede británica realizar un pago urgente a un proveedor de Hungría.

Los estafadores volvieron a comunicarse con la víctima haciéndose pasar nuevamente por el CEO alemán para asegurarle que la transferencia sería reembolsada y, por si fuera poco, lo contactaron en una tercera oportunidad –antes del supuesto reembolso- para solicitar una tercera transferencia en calidad de urgente. En ese momento, el director ejecutivo de la sede británica comenzó a sospechar y se rehusó a realizar la transferencia.

Según explicó el especialista en ciberseguridad de ESET, Jake Moore, es de esperarse que en el futuro cercano veamos un gran incremento de ciberdelitos en los que se utiliza el aprendizaje automático (del inglés, machine learning). De hecho, “ya hemos

visto DeepFakes imitando a celebridades y otras figuras públicas en video”, explicó Moore a un medio británico. Si bien la creación de piezas convincentes a través de video demanda más tiempo y recursos, “para producir voces falsas solo se necesitan unas pocas grabaciones, y en la medida en que el poder de procesamiento de los equipos aumenta comenzaremos a ver que estas piezas serán cada vez más fáciles de crear”, agregó el especialista de ESET.

En el capítulo “Las máquinas aprenden, los humanos no tanto”, del informe Tendencias en el campo de la ciberseguridad para el 2019 elaborado por ESET, la investigadora en seguridad, Lysa Myers, analizó el escenario del aprendizaje automático e hizo especial hincapié en la importancia de tener presente que es más que factible que los cibercriminales adopten el uso del machine learning para llevar a cabo sus objetivos -que en la mayoría de los casos es robar dinero u otros bienes de valor-, sobre todo los grupos de cibercriminales financiados por algún Estado.

Facebook junto compañías como Microsoft y distintas universidades de los Estados Unidos ya se han percatado de esta tendencia creciente y han manifestado su preocupación con el anuncio del lanzamiento del desafío “Deepfake Detection Challenge (DFDC)”; una iniciativa que busca contrarrestar el fenómeno creciente de las deepfakes y que premiará a quien sea capaz de desarrollar una tecnología que pueda ser utilizada por cualquiera y que tenga la capacidad de detectar el uso de inteligencia artificial para generar videos adulterados.

La divulgación de casos como el de la estafa que dio a conocer Wall Street Journal son de utilidad para generar conciencia y para estar mejor preparado para enfrentar lo que puede significar una tendencia y una de las posibles formas de evolución de las técnicas de ingeniería social. En este sentido, para prevenir ser víctima de una estafa en la cual se imite la voz de una persona de confianza, Moore asegura que hay algunas medidas que se pueden tener en cuenta para minimizar los riesgos de caer en el engaño. En primer lugar, saber que es posible que alguien logre suplantar la identidad de una persona legítima al imitar su voz. Una vez que sabemos que esto es posible podemos, por ejemplo, incluir algunas medidas de verificación antes de realizar una transferencia de dinero. Por ejemplo, corroborar que el número entrante es el de la persona que dice ser y comunicarle a la persona que llama que usted le devolverá el llamado; por supuesto, marcando de manera manual el número de teléfono que tiene en su agenda. 📞



## Función “**ELIMINAR PARA TODOS**” de WhatsApp no elimina archivos enviados a usuarios de iPhone

Por Juan Manuel Harán

La opción que ofrece WhatsApp y que permite eliminar mensajes enviados para que el destinatario no pueda verlos no funciona como muchos esperan. Al parecer, los archivos multimedia (fotos, videos, etc) que son enviados a usuarios de iPhone que tengan la configuración por defecto de la app no son eliminados del dispositivo cuando quien envía el mensaje decide borrarlos para que el destinatario no los vea, lo cual genera una falsa sensación de privacidad.

En este sentido, a pesar de que la persona que envía el mensaje quiera eliminarlo y la aplicación despliegue el mensaje “el mensaje ha sido eliminado”, el mismo aún está disponible en el dispositivo iOS al cual se envió, explica en un artículo TheHackerNews.

Este inconveniente no está presente en dispositivos Android, donde la función de volver para atrás y eliminar un archivo que se envió funciona correctamente y el contenido se eliminará del dispositivo del remitente o de los remitentes; en caso de ser enviado a un grupo.

Según publicó el medio, el hallazgo de este problema de privacidad es obra del consultor en seguridad Shitesh Sachan, quien explicó que la funcionalidad de WhatsApp para iOS no ha sido diseñada para eliminar mensajes multimedia recibidos que fueron guardados en Camera Roll de los dispositivos iPhone, mientras que en dispositivos Android los archivos enviados sí se eliminarán desde la galería en la cual son guardados por defecto.

En su configuración por defecto, la app de mensajería automáticamente guarda todas las imágenes y videos que se reciben a través de WhatsApp en Camera Roll de los dispositivos iPhone y la galería de imágenes de Android; una opción que puede desactivarse desde la configuración de WhatsApp.

Una vez que la compañía recibió el reporte por parte de Sachan acerca de este inconveniente, la misma aseguró que no realizará cambios para intentar resolverlo, alegando que la función “Eliminar para todos” fue pensada para eliminar mensajes dentro de WhatsApp y que no ofrece garantías de que un archivo será eliminado de manera permanente, aunque dijo que en el futuro podría hacer cambios en esta funcionalidad y en cómo está implementada, publicó el medio. 📞



# CIBERSEGURIDAD

## ¿Qué tan segura es tu seguridad?

Por Philippe Verrier



Las cámaras de seguridad IP y otros dispositivos de seguridad están, por su propia naturaleza, conectados a Internet. Esto es lo que permite a los usuarios acceder a ellos de forma remota y a los fabricantes realizar actualizaciones del software sin tener que hacer una visita a domicilio. Pero esta característica también puede ser el talón de Aquiles si no se cuentan con las medidas indicadas para proteger nuestros sistemas de seguridad física.

Cuando un dispositivo de control de acceso o cámara, dentro del Internet de las cosas (IoT), no está asegurado adecuadamente, cualquier persona puede acceder a ellos, no solamente las personas a las cuales se les ha dado acceso. Del mismo modo, las comunicaciones no cifradas entre un servidor y la aplicación del cliente, o el firmware desactualizado, pueden ser explotados por los ciberdelincuentes, lo que pone en riesgos la red de toda una organización.

### Un gran reto para la industria de la seguridad física

Según la firma analista de la industria, Gartner, para 2020 más del 25 por ciento de los ataques cibernéticos en las empresas involucrarán dispositivos IoT. Más del 60 por ciento de los ataques cibernéticos son en medianas y pequeñas empresas y estas últimas son particularmente vulnerables, pues en su mayoría, no pueden mantener sus negocios más allá de los seis meses posteriores a un ciberataque importante.

De acuerdo con expertos en ciberseguridad, México es una de las naciones más atacadas del mundo, ubicándose dentro de los 10 primeros lugares. Los principales riesgos que existen son: robo de datos de usuarios, pérdida o eliminación de información, robo de identidad, fraude o extorsión, secuestro de información, e interrupción de servicios.

Los ataques a grandes empresas también generan grandes pérdidas. Según un estudio de 2018 realizado por IBM y el Instituto Ponemon, la violación de datos

promedio le cuesta a las compañías \$ 3.86 millones y las violaciones a gran escala pueden superar los \$ 350 millones.

Lo anterior es posible, dada la cantidad de personas que hay con dispositivos y acceso a internet, la falta de educación sobre seguridad informática, la cercanía con países como Estados Unidos y, sobre todo, la ausencia de una legislación mexicana que castigue este tipo de delitos, lo que propicia que los cibercriminales tengan en la mira empresas establecidas en el territorio.

De acuerdo con la Procuraduría General de la República, la pérdida estimada por ciberataques a empresas mexicanas tan solo en 2017 fue de \$7,700 millones de dólares. Según la corredora de seguros Lockton México, en 2018 se detectaron 25,000 millones de intentos que pretendieron vulnerar los sistemas para acceder a la información de empresas.

"Cuando se trata de proteger nuestro sistema de seguridad no podemos permitirnos correr ningún riesgo, los fabricantes de seguridad física y los desarrolladores de software hemos establecido una multitud de formas de protección contra las amenazas cibernéticas y no nos detenemos allí", señala Philippe Verrier, Gerente de Programas de Mercadeo de Genetec, empresa líder innovadora en sistemas de seguridad de arquitectura abierta basados en redes IP. "Constantemente nos esforzamos porque nuestras soluciones realmente brinden la protección necesaria", indica Philippe.

### ¿Cómo obtienen acceso los cibercriminales a un sistema de seguridad?

Los ciberdelincuentes pueden explotar fácilmente una cámara mal asegurada, las comunicaciones no cifradas entre un servidor y una aplicación cliente o un firmware desactualizado. Los ataques de ransomware son particularmente costosos y se sabe que se dirigen a sistemas que ejecutan software común pero desactualizado.

Con demasiada frecuencia, las personas son el eslabón más débil cuando se trata de violaciones de seguridad cibernética. Los empleados que no

cambian las contraseñas predeterminadas en los dispositivos IoT es una manera fácil para que los ciberdelincuentes oportunistas obtengan acceso a su sistema. Los ataques de fuerza bruta consisten en delincuentes que adivinan las contraseñas, el rastreo de paquetes captura el tráfico de la red y los ataques de intermediarios escuchan las comunicaciones entre dos sistemas, utilizando la información obtenida para su beneficio.

La mayoría de las soluciones de seguridad física están siempre evolucionando con nuevos dispositivos que se agregan para expandir el sistema o reemplazar productos obsoletos o rotos. El proceso de agregar nuevos equipos, quizás de un fabricante diferente con estándares menos seguros, es otra oportunidad para una vulnerabilidad.

### ¿Qué elementos debe tener una solución de ciberseguridad?

Una de las formas más importantes para combatir las amenazas cibernéticas es con un plan. Las empresas deben capacitar y educar a sus colaboradores sobre la importancia de las mejores prácticas y las exigencias de cumplir con las

Cuando sus datos están encriptados, incluso si una persona no autorizada, entidad o ciberdelincuente obtiene acceso a ellos, no podrán leerlos ni comprenderlos.

### Autenticación

La autenticación es el proceso de determinar primero si una entidad-usuario, servidor o aplicación cliente es quien dice ser, seguido de la verificación de si esa entidad debería acceder a un sistema y de qué manera. Dependiendo de la configuración, la autenticación puede ocurrir en el lado del cliente o del servidor, o en ambos extremos. La autenticación del lado del cliente usa combinaciones de nombre de usuario y contraseña, tokens y otras técnicas, mientras que la autenticación del lado del servidor usa certificados para identificar a terceros confiables. La autenticación de dos factores se refiere a dos formas de autenticación utilizadas en combinación. La autenticación es una herramienta importante para protección de datos pues evita que lleguen a manos equivocadas. Impide el acceso no autorizado y garantiza que solo el personal de seguridad sea, de hecho, el que acceda al sistema cuando



políticas de la empresa. "Elegir un integrador de sistemas que recomiende solo a los fabricantes más confiables y enfatice la importancia de la ciberseguridad es un buen comienzo", señala Philippe Verrier, de Genetec, y agrega: "Juntos, deben desarrollar una solución que implemente múltiples capas de ciberseguridad, incluido el cifrado, la autenticación y la autorización para sus sistemas comerciales y de seguridad críticos".

### Cifrado de extremo a extremo

El cifrado es el proceso a través del cual los datos se codifican para que permanezcan ocultos o inaccesibles para usuarios no autorizados. Ayuda a proteger la información privada, los datos confidenciales y puede mejorar la seguridad de la comunicación entre las aplicaciones cliente y los servidores.

inicie sesión. Esto significa que los piratas informáticos no pueden pretender ser un servidor de seguridad para tomar el control, manipular o copiar datos sensibles.

### Autorización

La autorización es la función que permite a los administradores del sistema de seguridad especificar los derechos y privilegios de acceso del usuario u operador. Los administradores restringen el alcance de la actividad en un sistema otorgando derechos de acceso a grupos de individuos para recursos, datos o aplicaciones, definiendo lo que los usuarios pueden hacer con estos recursos. Cuando los administradores gestionan lo que su personal puede ver y hacer, están garantizando la seguridad de los datos transmitidos y almacenados dentro del sistema de seguridad. Esta es una

forma clave de aumentar la seguridad del sistema en su conjunto, así como mejorar la seguridad de los otros sistemas conectados a este.

## Nunca se puede ser complaciente cuando se trata de ciberseguridad

Con informes casi diarios de otro hack o violación de seguridad, muchos están comenzando a sufrir fatiga de conciencia de seguridad cibernética. Sin embargo, nadie puede darse el lujo de ser complaciente en la guerra contra los cibercriminales. Una vez que haya hecho e invertido en una estrategia de ciberseguridad, es importante mantenerse alerta.

**1**.- Solo elija fabricantes de productos de seguridad confiables y de buena reputación que estén comprometidos a proteger su organización de las amenazas cibernéticas. Hay una serie de requisitos gubernamentales y organizacionales cuando se trata de protección de la información y privacidad.

**2**.- Una empresa que se toma en serio la seguridad cibernética también realizará sus propias pruebas de penetración. Las pruebas de penetración deben realizarse de forma recurrente para detectar cualquier vulnerabilidad.

**3**.- Al trabajar con un integrador de sistemas para desarrollar o mantener una solución de seguridad física, éste debe considerar la ciberseguridad como una prioridad y solo debe recomendar productos de fabricantes confiables que también se comprometan a proteger su sistema.

**4**.- Para mitigar riesgos financieros, algunas empresas están recurriendo al seguro de responsabilidad cibernética. Es un tipo relativamente nuevo de cobertura que ofrecen las compañías de seguros para proteger a las empresas contra amenazas basadas en Internet y violaciones de datos.

*"El seguro de responsabilidad cibernética dará tranquilidad a los integradores y permitirá a las empresas acceder a fondos para gestionar una respuesta de ataque cibernético y mantener el negocio en funcionamiento", indica Philippe.*

La contratación de seguros que ofrecen una cobertura contra ataques cibernéticos aumentó en un 300% el año pasado en México. Robo de información, cobertura por pérdidas al interrumpirse operaciones en el negocio por un ataque cibernético y multas impuestas por órganos reguladores a empresas afectadas son de las principales pólizas contratadas.

*"La ciberseguridad se está convirtiendo en uno de los principales riesgos comerciales para organizaciones de todos los tamaños. Asegúrese de elegir proveedores confiables que utilicen múltiples capas de defensa, como cifrado, autenticación y autorización, así como pruebas de penetración y trabajar con integradores de sistemas que se comprometan a proporcionar protección continua contra amenazas cibernéticas pues de esto dependerá en gran medida el éxito de su negocio", finalizó Philippe Verrier.*



# ÍNDICE DE ANUNCIANTES



IPS

MOSEG

TI LATINA

Portada

MULTIPROSEG

2da. Forros / Pág. 3

AXIS

Pág. 7

IP USERGROUP

Pág. 9

ALAS

Pág. 11

COMEXA

Pág. 17

PROYECTOS TI

Pág. 23

XTREM SECURE

Pág. 30

GECSA

Pág. 33

MOSEG

Pág. 35

CSCS

Pág. 36

UNIFORMES JR

Pág. 39

ASUME

Pág. 43

LK SEGURIDAD PRIVADA

Pág. 45

ASIS

Pág. 47

IPS

Pág. 51

ZN CORPORATIVO

Pág. 55

SERRALDE

Pág. 59

APRINSA

Pág. 63

ORIGINS

Pág. 74

RANGER SWAT MÉXICO

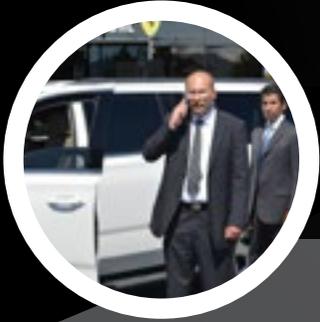
Pág. 88 -3ra. de Forros

SEPSISA

Contraportada



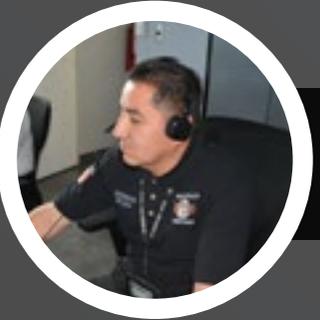
# RANGER SWAT MÉXICO



Servicio de transporte a Ejecutivos



Servicio de Custodias



Servicio de GPS y Rastreo Satelital



Servicio de Escoltas



Servicio de Intramuros



# Detecto, Visualizo y Actúo

52 (55) 5347 2741

[contacto@rangerswat.com.mx](mailto:contacto@rangerswat.com.mx)



Av. Invierno #11, Col. Ángel Zimbrón, Alcaldía Azcapotzalco, C.P. 02910.



*El camino a la excelencia comienza por la seguridad.\**