Águilas News

Octubre 2020

Maximizando la utilidad de la tecnología

El coronavirus vs la privacidad

Grupo ÁGUILAS
Seguridad Industrial, Comercial y Personal

Una nueva perspectiva de prevención

Por: David Lee / ASIS Capítulo México A.C.

El fenómeno de la inseguridad, que se ha agudizado en la última década en muchos de los países de América Latina, con graves afectaciones económicas y sociales, ha comprometido, como nunca antes, la gobernabilidad democrática y la legitimidad del Estado, afectando la confianza de la ciudadanía en las autoridades y entre los personas mismas.

La comisión de delitos por parte de un individuo, debe contemplarse más allá del contexto situacional en el que se encuentre en el momento mismo de delinquir, desde la perspectiva de lo que ha sido su vida en familia, su educación, trabajo y experiencias, así como del entorno físico y social que lo envuelve y la credibilidad y eficiencia del sistema de justicia que lo rija.

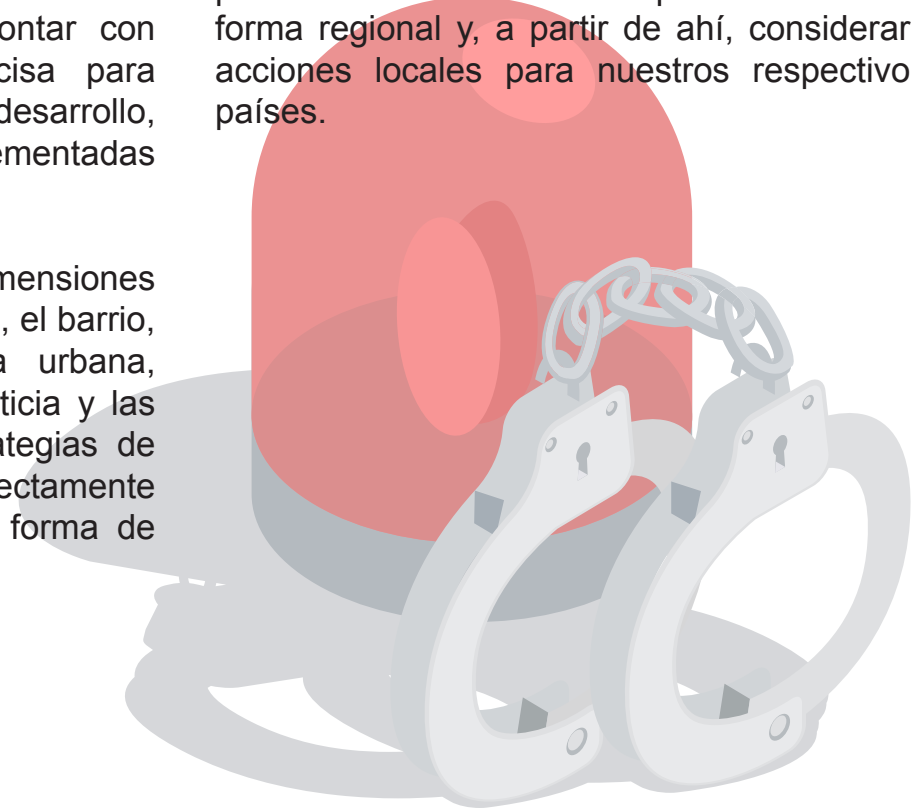
Dentro de ese marco, el diseño de políticas públicas exige el contar con la información confiable y precisa para analizar su viabilidad y evaluar su desarrollo, considerando las acciones implementadas para combatir el crimen.

No obstante, las distintas dimensiones que involucra: la familia, la escuela, el barrio, la comunidad, la infraestructura urbana, las regulaciones, la policía, la justicia y las cárceles, requieren distintas estrategias de intervención que se deben perfectamente conocer para reconocer la mejor forma de realizarlas.

Dichas intervenciones no solo dependen del Estado, sino que deben ser realizadas en conjunto con la ciudadanía, la cual debe jugar, hoy en día, un papel protagónico toda vez que los gobiernos han invertido mayormente en represión que en prevención y, para alcanzar el éxito de ésta última, es indispensable que las personas, a nivel comunitario, colaboren.

De aquí que, para lograr una sociedad formada en materia de prevención, es preciso el contar con una ciudadanía bien informada y con personas que, a través de las organizaciones de la sociedad civil, decidan ser parte de los esfuerzos encaminados a coproducir eso por lo que hoy clamamos todos: seguridad.

En ese sentido, el observar el contexto de América Latina nos ofrece una visión integral, permitiéndonos conocer la problemática de forma regional y, a partir de ahí, considerar acciones locales para nuestros respectivo países.



Maximizando la Utilidad de la Tecnología

Por: Diofanor Rodríguez / Seguridad en América

Los especialistas de seguridad física se encuentran con los últimos avances de la tecnología para la seguridad. Y en el entendido que los dispositivos de seguridad física son cada vez más inteligentes, la pregunta que emerge es: ¿Los profesionales de seguridad física están adquiriendo el conocimiento suficiente para beneficiarse de los avances tecnológicos?

Una pregunta que tal vez para muchos suene ridícula, pero que en temas de seguridad sí es importante tener en cuenta, debido a que muchas veces, se compran equipos que poseen unas características tecnológicas importantes, pero que desafortunadamente son subutilizadas porque no contamos con la expertise para aprovechar al máximo sus características.

Aquí se hace más visible un adagio popular que dice: “Se compran cosas que no se necesitan con dinero que no se tiene, para la gente que no le interesa”, ¿por qué traer a colación este adagio? Es que en seguridad muchas veces se compran elementos de seguridad electrónica sin tener en cuenta las necesidades que posee la instalación, para poder acertar en la compra del equipo apropiado y aprovechar de manera eficiente todas las características técnicas del equipo.

¿Pero por qué sucede esto con frecuencia? Lastimosamente, sucede porque las decisiones de los elementos electrónicos de seguridad se dan por moda y no como el resultado de un concienzudo análisis de riesgos que permita de forma adecuada identificar cuáles son las necesidades que posee la instalación.

Adicional a lo anteriormente expuesto existe un elemento que converge con la seguridad física y es la seguridad informática, por ello el hombre de seguridad moderno deberá aprender sobre el tema y saber si la tecnología que está comprando no pone en riesgo otros de los procesos de la organización, porque muy fácilmente nos podemos convertir en el eslabón más débil de la seguridad.

EL APRENDIZAJE DEBE SER PRIORIDAD

Con elementos de seguridad electrónica ya en desarrollo con inteligencia artificial se hace necesario mantener un aprendizaje constante, entendiendo las necesidades de la seguridad, que sean balanceadas, y pensadas de la mano de la ciberseguridad.

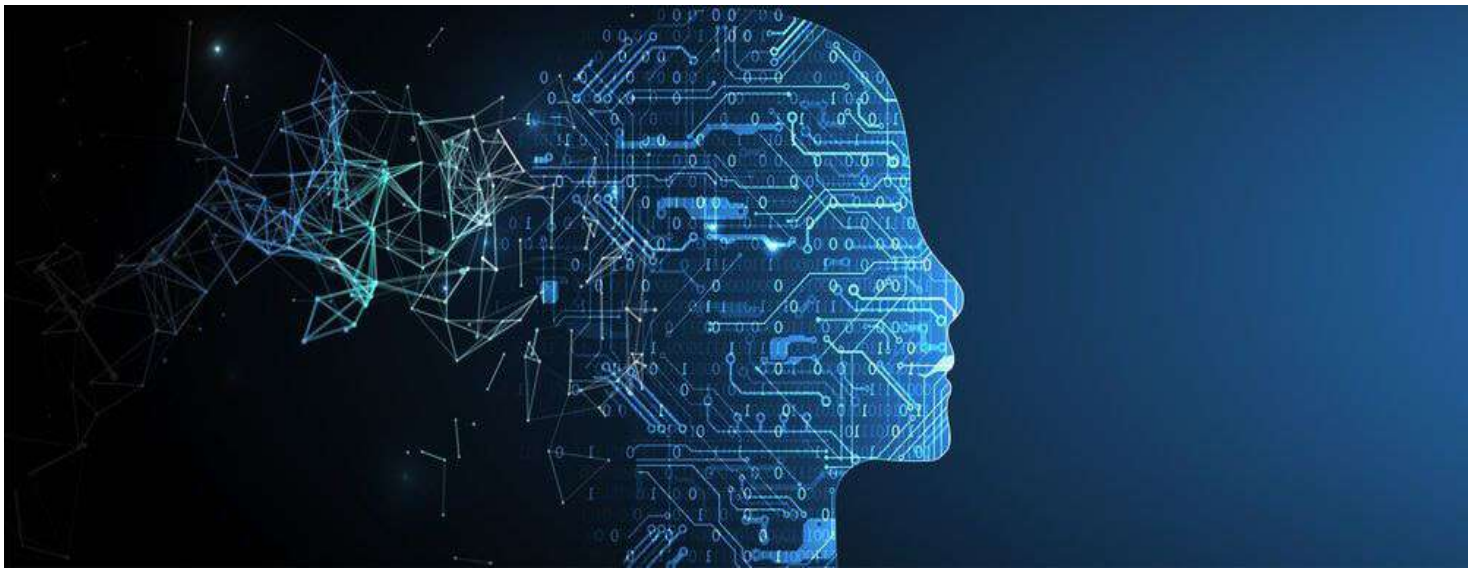
Como podemos ver el panorama cada vez más obliga al profesional de seguridad no sólo a saber de seguridad física, sino que también debe saber de seguridad informática para poder asesorar las organizaciones en la compra de los elementos electrónicos de la seguridad. Con las nuevas tendencias tecnológicas, en videovigilancia, control de accesos, alarmas e integración de todos los sistemas es importante desarrollar un conocimiento de las tecnologías emergentes que ayuden a minimizar los riesgos corporativos y que nos permitan utilizar de forma adecuada sus características y rendimientos.

Y con esto poder dar el balance necesario entre procedimientos, tecnología y personas con el único fin de apoyar a la organización al logro de sus objetivos.

Porque ustedes los profesionales de seguridad estarán de acuerdo conmigo que no hay nada más frustrante que recomendar un sistema de seguridad electrónica y que no cumpla con las necesidades de la organización y no apoya los objetivos corporativos.

Con las ventajas actuales donde la tendencia smart no sólo ha llegado a los objetos que los usuarios utilizan día a día, sino que ya está y podemos ver distintos ejemplos de edificios inteligentes alrededor del mundo, y con esto las organizaciones serán las próximas en acercarse a estas tecnologías. ¿Acaso esto fermentaría nuevos tipos de agresión que reúnan lo digital y lo físico?

Estos elementos presentados nos llevan a realizar una reflexión muy importante frente a la educación y capacitación que estamos recibiendo y entregando a los profesionales de la seguridad.



El coronavirus vs. la privacidad

Por: Eugene Kaspersky / Revista Forbes

En los últimos meses, me han preguntado en varias ocasiones cómo las medidas tomadas por los gobiernos para combatir el coronavirus afectarán nuestra privacidad y la seguridad de los datos personales. Es una pregunta importante, así que decidí compartir mis pensamientos con los lectores de Forbes.

En primer lugar, los estándares de privacidad en cada país en particular son el producto de una larga evolución histórica. Para algunos países, como Estados Unidos, comenzó con la prohibición de escuchas clandestinas en 1769; en Francia, fue la prohibición de la publicación de datos privados, que entró en vigor en 1858. Y en Rusia, por ejemplo, en 1845, se estableció la responsabilidad penal por violar la confidencialidad de la correspondencia, las conversaciones telefónicas y las comunicaciones telegráficas. Sin embargo, al día de hoy, algunos países todavía no tienen una definición legal vinculante de privacidad; Gran Bretaña y Australia, por ejemplo. Entonces, cuando hablamos de medidas de privacidad, debemos tener en cuenta que, en cada país, están determinadas por su historia y cultura, y, desafortunadamente, no podemos hablar de una solución común para todo el mundo.

Las nuevas tecnologías y su desarrollo también siempre han estado relacionados con problemas de privacidad. Hay muchas nuevas tecnologías, servicios y sistemas que realmente disfrutamos y nos hacen la vida mucho más fácil, pero de hecho afectan nuestra privacidad.

Por ejemplo, las tarjetas de crédito o la matrícula de su automóvil: cuando se inventaron, no había problemas con su privacidad, pero ahora tenemos escáneres de matrículas que rastrean su ubicación y velocidad; y tarjetas de crédito, que dan a los bancos acceso a información adicional sobre nuestro paradero y hábitos. Estas son las desventajas de la tecnología.

Y, por supuesto, a medida que Internet se desarrolló, sus primeros usuarios y los primeros ciber-hooligans descubrieron que la red les proporciona un anonimato muy relativo. Nunca fue muy difícil encontrar un usuario específico, pero en los albores de Internet, nadie tenía realmente una razón para hacerlo. Sin embargo, con el crecimiento de la potencia informática, resultó que: a) un usuario de Internet crea una gran cantidad de información en el proceso de uso de la red; b) esta información se vuelve fácil de recopilar y almacenar a bajo costo; y c) el procesamiento de la información puede ser muy rentable, y cuanto mayor sea el nivel de personalización, más costosa será la información. Al mismo tiempo, la comunicación móvil se estaba desarrollando rápidamente y los operadores móviles obtuvieron automáticamente información sobre el paradero exacto de sus usuarios.

Hoy en día, los usuarios de dispositivos móviles e Internet proporcionan voluntariamente sus datos a cambio de servicios “gratuitos” de operadores y proveedores, a menudo sin tener idea de cuánta información se les transmite a terceros, un hábito muy desactualizado en mi opinión.

El modelo económico actual implica la recopilación constante de información sobre la vida privada de los usuarios.

¿Y dónde está el Estado en esta agitación de la privacidad? La función básica del Estado es garantizar la seguridad, y para hacer esto, todos los Estados recopilan y analizan constantemente datos personales. El reclutamiento, la recaudación de impuestos, la emisión de pasaportes, el registro de matrimonios, la investigación de delitos, el espionaje y el análisis epidemiológico son razones diferentes para recopilar y analizar nuestros datos privados.

Los gobiernos poseen los poderes más amplios y la capacidad de "cuidar" de sus ciudadanos. Por ejemplo, hay hasta 17 agencias de inteligencia diferentes trabajando en los Estados Unidos, cada una de las cuales recopila, almacena y analiza enormes cantidades de datos personales. Mientras, en el Reino Unido, están discutiendo el tema de expandir la lista de organizaciones gubernamentales que pueden acceder al tráfico de usuarios sin una orden judicial.

Por otro lado, el Estado también está obligado a proteger los intereses de sus ciudadanos, Es por eso que, en los últimos años, muchos países de todo el mundo han estado trabajando activamente para crear leyes que regulen la recopilación y el uso de datos personales por plataformas digitales, desde el Proyecto de Ley de Protección de Datos Personales de la India hasta el GDPR europeo.

Todas estas leyes tienen como objetivo encontrar un equilibrio entre los intereses de los usuarios, las empresas y el Estado. El problema es que la tecnología y la realidad están cambiando rápidamente, mientras que las leyes cambian lentamente. Al mismo tiempo, el Estado es el mayor consumidor de información sobre la vida privada y el principal defensor de su protección.

¿Qué está sucediendo en relación con la epidemia actual? No se introdujeron nuevas tecnologías que puedan cambiar el enfoque para recopilar información sobre la privacidad durante la pandemia. Si consideramos la pandemia como una amenaza para la seguridad personal y pública, entonces el uso de la tecnología por parte del Estado para el monitoreo y la vigilancia no es sorprendente; por el contrario, ¡es su responsabilidad directa!

En algunas culturas, las personas comparten información con el Estado de manera más voluntaria. Por lo tanto, los éxitos de Corea del Sur, Taiwán y China en la lucha contra el coronavirus se deben en parte al uso activo de aplicaciones y dispositivos para buscar y prevenir el contacto con portadores del virus.

Desafortunadamente, no siempre es fácil encontrar un equilibrio entre el Estado sobrepasando sus poderes y cuidando el bienestar de sus ciudadanos. Sin embargo, en el caso de esta pandemia, cuando las vidas de millones de personas están en riesgo si tengo la opción de elegir entre vigilancia y entierros masivos, elegiré vigilancia. Espero que sea solo un problema temporal y que cuando el mundo vuelva a la normalidad, los Estados traten los datos recopilados de manera responsable y los destruyan.

Por lo tanto, personalmente creo que la preocupación por las "medidas digitales" para combatir la epidemia es el resultado del hecho de que cada vez más usuarios comenzaron a preguntarse qué pasa con sus datos en principio. Cuanto más dependa la sociedad de la tecnología, más usuarios querrán saber quién recopila sus datos. Muestra la necesidad de más transparencia en el mundo digital. La epidemia simplemente agudizó este problema, y dado que superarlo implica un uso aún mayor de la tecnología, es muy importante buscar respuestas y soluciones que ayuden a encontrar y mantener el mismo equilibrio de intereses.

El plan de seguridad que llevaría López Obrador durante sus giras

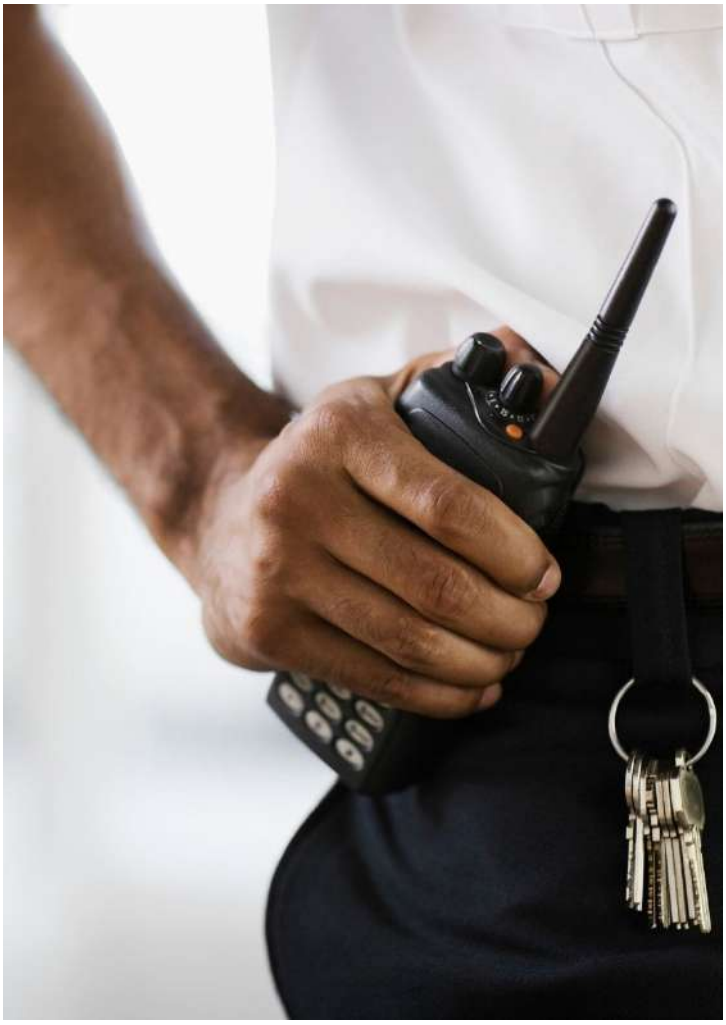
Por: Redacción / Seguridad en América

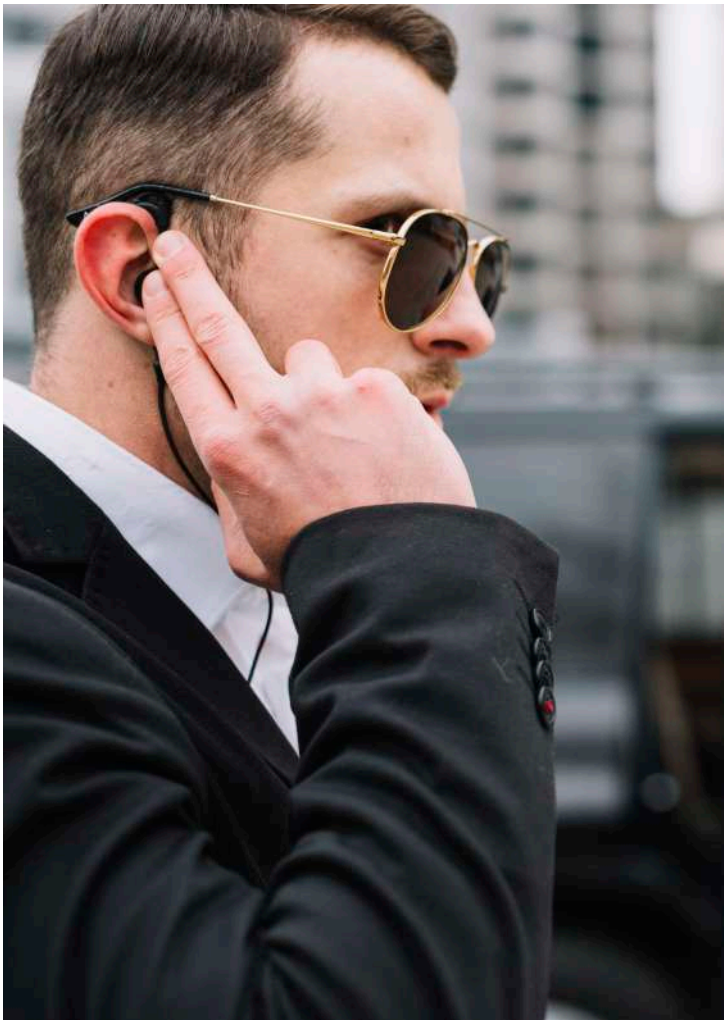
Andrés Manuel López Obrador, presidente de México contaría con un plan estructurado de seguridad para las giras de trabajo que tiene alrededor de la República.

El plan conocido como Operación Barrido y comprendería por lo menos a cinco dependencias gubernamentales del área.

La Secretaría de Seguridad y Protección Ciudadana (SSPC), la de la Defensa Nacional (Sedena), la Marina, la Guardia Nacional, el Centro Nacional de Inteligencia (CNI), la Ayudantía de la Presidencia, entre otras instituciones de seguridad del país, forman parte de este plan.

El presidente es monitoreado constantemente por las instituciones de seguridad e inteligencia. La seguridad con la que cuenta López Obrador responde a los altos niveles de peligrosidad a los que se encuentra expuesto como ejecutivo del país.





Grupo ÁGUILAS

Seguridad Industrial, Comercial y Personal

20 Años haciendo negocios seguros

NUEVAS DIVISIONES

ÁGUILAS LOGÍSTICA

PANOPTIC
Monitoreo Inteligente

Tel. 01 800 838 5155

656 418 0805

ventas@grupoaguilas.com

www.grupoaguilas.com

Sucursales: BAJA CALIFORNIA CHIHUAHUA COAHUILA NUEVO LEÓN PUEBLA SONORA ZACATECAS