



TENDENCIAS CLAVE EN SEGURIDAD PRIVADA

Visión general de los desafíos del sector

Julio César González, experto en administración de la seguridad y conferencista internacional en esta disciplina con más de 15 años de experiencia en cargos directivos y de consultoría en seguridad y protección, opinó, en entrevista para Motorola Solutions, acerca de los retos post COVID-19 y desafíos tecnológicos que presentan las empresas de seguridad privada y vigilancia en Latinoamérica.

¿Cómo ha sido la transformación de las empresas de seguridad privada y vigilancia en los últimos 5 años?

JCG: Ha sido definitivamente una evolución. Las empresas de seguridad privada han venido experimentando cambios importantes, dos bastante tangibles: Primero el involucramiento de nuevas tecnologías para mejorar la gestión de la seguridad de sus clientes. Cómo la vinculación de sistemas de seguridad electrónica como parte de la oferta de seguridad a los clientes, es un aspecto importante puesto que ha comenzado a existir una integración un poco tímida pero prometedora para que comencemos a hablar de sistemas más robustos e integrados de seguridad; sin embargo, aún la tecnología sigue siendo

concebida como un apoyo y no como un elemento determinante en las iniciativas de protección como debería ser. En segunda instancia, la preocupación de la estandarización de procesos e implementación de sistemas de gestión en las empresas; esto es muy positivo y aquellas que han apropiado correctamente esta iniciativa, han visto como definitivamente mejora y dinamiza los procesos internos y tiene un impacto directo en el servicio al cliente la preocupación de la estandarización de procesos e implementación de sistemas de gestión en las empresas; esto es muy positivo y aquellas que han apropiado correctamente esta iniciativa, han visto como definitivamente mejora y dinamiza los procesos internos y tiene un impacto directo en el servicio al cliente



MOTOROLA SOLUTIONS

¿Cómo será la seguridad post COVID-19?

JCG: La seguridad post-COVID 19; tiene dos momentos, la etapa de resiliencia o superación ante la pandemia y la etapa de desconfinamiento definitivo.

Comencemos con la etapa de resiliencia, esta época es la que viviremos en unos meses cuando comencemos a ver el aplanamiento de la curva y la espera de la llegada de una vacuna en procura de lograr la inmunidad.

Al haber menos ingresos, desempleo, más trabajo en casa, menos necesidad de controlar accesos en las oficinas, menos puestos de supervisor, comienza a verse una creciente mejora en la adopción de las tecnologías para desempeñar actividades esenciales para una efectiva migración de servicios de seguridad que sean fácilmente reducibles en la cantidad de personas. Aunque suena un poco brusco entender que existe la posibilidad de generar una reducción de los servicios de vigilancia, lo cual es el ingreso y la esencia de las empresas de vigilancia; es una necesidad sentida de los clientes, dada la situación económica actual.

Ahora, **en la época post COVID-19**, que es el desconfinamiento gradual y la reapertura de todos los sectores económicos y espacios sociales, incluidos los espacios que podrían ser de alto riesgo de hiper contagio, la inseguridad será durante un tiempo y en consecuencia de las dificultades económicas y el desempleo un factor de preocupación de los usuarios. Esta etapa podría llevar al incremento de los servicios de vigilancia y seguridad humana y el retorno gradual de algunos servicios de seguridad privada como respuesta de los factores de inseguridad; sin embargo es claro que la misma demanda de servicios de seguridad humana que en la antigua normalidad no se verá, debemos entender que las empresas aprendieron a funcionar desde la virtualidad, en tal sentido el trabajo semi presencial será un factor que se impondrá y por ende los espacios, las grandes oficinas, sucursales bancarias y en general todo el comercio tendrá una mayor dependencia de las compras digitales. Ahora bien, desde la parte de la tecnología, lo que se observa es el desarrollo de excelentes sistemas de seguridad con unas funcionalidades excepcionales que podrían marcar un cambio disruptivo en el sector de la seguridad.

¿Por qué deberían de invertir en tecnología las empresas de seguridad privada y vigilancia?

JCG: Porque no hay otro camino para evolucionar! Quisiera contar un poco la historia para entender el futuro. Hace 30 años la seguridad privada emergía en los países latinoamericanos a partir de vigilantes con baja formación. Hace 15 años la vigilancia y seguridad privada contaba con mayores bases teóricas con una escuela y academia propia en donde se impartían conocimientos más claros y técnicos tanto para vigilantes como para directivos de la seguridad. Así mismo, la presencia de cámaras y alarmas y sistemas de control para vigilancia comenzaba a ser una necesidad. Ahora bien, en estos 15 años los desarrollos en tecnología, con el auge de la analítica de video y una mayor parametrización de los controles de acceso aunado con la biometría se abre una puerta para pasar de empresas de vigilancia a empresas de base tecnológica, que quiero decir con esto, que **el sector de empresas de vigilancia y seguridad privada deben incorporar una línea fuerte de seguridad electrónica para que al asumir un puesto de vigilancia no se venda sencillamente "X" cantidad de puestos de seguridad, se instalen unas cámaras y ya; sino que**

“La inseguridad será durante un tiempo y en consecuencia de las dificultades económicas y el desempleo un factor de preocupación de los usuarios.”

“Desde la parte de la tecnología, lo que se observa es el desarrollo de excelentes sistemas de seguridad con unas funcionalidades excepcionales que podrían marcar un cambio disruptivo en el sector de la seguridad.”



se haga un diseño dentro de los principios de la seguridad, los riesgos y las necesidades del cliente. Esto da como resultado un sistema de seguridad integral. Pese a que muchos dicen que ya tienen implementados sistemas de seguridad, cuando hago auditorías veo como no se hacen los mantenimientos, el diseño es inadecuado, o la seguridad electrónica la dejan en un segundo plano o incluso que el vigilante tenga unas cámaras y no las pueda monitorear porque está pendiente de desempeñar otras múltiples funciones; es decir poca importancia se le da a un buen sistema de seguridad y esto se vuelve parte del paisaje del vigilante. En conclusión, en la actualidad hay una incipiente cultura que le resta la relevancia que se merece el sistema de seguridad electrónico como principal elemento dentro del sistema de protección.

Planteemos un caso hipotético; ¿qué pasaría si una empresa de tecnología de punta en seguridad electrónica adquiere una empresa de vigilancia? Mi respuesta sería que los diseños de los sistemas de seguridad serían en base tecnológica, altamente efectivos y el aporte y participación humana serían solamente para generar reacción, control y algo de disuasión, es decir, estamos hablando de esquemas de seguridad más eficientes y eficaces en la reducción de costos y riesgos. En el momento que esto pase, definitivamente vamos a tener un cambio disruptivo en la forma de concebir la seguridad. En suma, las empresas de seguridad deben invertir en tecnología porque es la necesidad del mercado, la necesidad de los costos y el futuro cierto. ¿Quién no está dispuesto a tener más seguridad por menos recursos y con la posibilidad de tener el control y la información en tiempo real?

“¿Quién no está dispuesto a tener más seguridad por menos recursos y con la posibilidad de tener el control y la información en tiempo real?”



¿Cuáles son las principales barreras para la adopción de tecnología en el sector?

JCG: El usuario aún no ha aprendido a entender que la tecnología ya le permite muchas funcionalidades. Las empresas de vigilancia tienen que vender más seguridad y menos vigilancia, con esto quiero decir que si sigo vendiendo vigilancia estoy ofreciendo una persona, un servicio costoso, un medio y no una solución efectiva, pero si mezclamos la seguridad humana o menos vigilantes con sistemas de seguridad electrónica adecuados, según la evaluación de los riesgos y las funciones vitales de seguridad, esto dará como resultado un nuevo concepto de sistemas integrales de seguridad. Hoy en día creemos que tener cámaras, alarmas y vigilantes es un sistema integrado de seguridad y no es así, si estos no tienen un diseño adecuado, una fundamentación técnica y una administración basada en riesgos, vulnerabilidades y desempeño, estamos en el ayer, en la antigua realidad.

“Las empresas de vigilancia tienen que vender más seguridad y menos vigilancia.”

¿Cuáles son las herramientas tecnológicas más importantes para el sector?

JCG: La seguridad física tiene unos principios, vamos a hablar de los cuatro más importantes que fundamentan los teóricos. **La seguridad está basada en la detección de amenazas, el retardo de estas amenazas y la neutralización de estas amenazas; todo lo anterior se debe gestionar adecuadamente permitiendo el control y buen funcionamiento.** Actualmente la detección se hace por medios tecnológicos, es decir alarmas perimetrales con sensores de diferentes tecnologías que se esfuerzan cada vez más por lograr la precisión de discernir entre una amenaza y una falsa alarma de tal manera que la fiabilidad es mayor. Por otro lado, circuitos cerrados con analítica de video que cada vez registran mayores atributos en calidad y mayor capacidad de almacenamiento. Hoy en día muchos de estos han migrado a la analítica de video basada en algoritmos y ha sido una evolución muy positiva puesto que hay algoritmos que cada vez son más precisos; sin embargo, me parece que la analítica de video por inteligencia artificial es fundamental, puesto que esto reducirá el error humano.

En estos momentos estoy haciendo una publicación del error humano en el monitoreo de cámaras y para no divulgar antes de tiempo los resultados de esta investigación, puedo anticipar

que una persona en condiciones ideales y monitoreando 8 cámaras tiene una probabilidad cercana al 74% de detectar un evento, esto realmente es bajo si tenemos en consideración que hoy en día los centros de monitoreo y control superan fácilmente las 200 cámaras; entonces la reducción de la capacidad de detección de eventos es sumamente baja y se pierde el sentido de las cámaras; es decir pasamos de la prevención al uso masivo de estos sistemas a la investigación. Acá juegan un papel importantísimo las comunicaciones, son la columna vertebral de todos los demás sistemas de seguridad, la fiabilidad del sistema en muchos casos, sino en todos depende de las comunicaciones. Cómo enlazar los nodos entre ellos, sistemas de seguridad y comunicaciones, se convierte en un atributo diferencial o en la vulnerabilidad del sistema.

“Acá juegan un papel importantísimo las comunicaciones, son la columna vertebral de todos los demás sistemas de seguridad, la fiabilidad del sistema en muchos casos, sino en todos depende de las comunicaciones.”

¿Por qué es importante la comunicación por radio en el sector?

JCG: Las comunicaciones son el eje principal de todo el sistema y pese a esto son invisibles. Por lo general cuando se está planificando cualquier sistema de seguridad se piensa en los atributos de los principios tradicionales del sistema de protección: detección, retardo y respuesta. Sin embargo, la ausencia de las comunicaciones en un sistema de seguridad no permite que absolutamente toda la seguridad funcione integrada y armónicamente. Las comunicaciones permiten los flujos de información para proceder a tomar correctivos, dar aviso de una situación de riesgo, permiten dejar los registros, dejar constancia de actos administrativos u operativos. Como lo dije es vital y hoy vemos cómo interactúa la comunicación con diferentes sistemas alarmas, software, vigilancia, video seguridad y gracias a la fiabilidad de las comunicaciones, la seguridad de la transmisión garantiza que los demás sistemas de seguridad sean o no tan efectivos como el desarrollador o usuario cree.

“Las comunicaciones permiten los flujos de información para proceder a tomar correctivos, dar aviso de una situación de riesgo, permiten dejar los registros, dejar constancia de actos administrativos u operativos.”

Hablando de voz y datos en seguridad, que tan importante considera que son las siguientes características:

JCG:



Monitoreo remoto:

Es altamente necesario para un sistema de seguridad, puesto que permite que los usuarios rompan la barrera de la presencialidad para hacer que los sistemas funcionen de manera efectiva. Esto supone que una muy buena conectividad le va a permitir a una organización tener de manera distante la posibilidad de detectar remotamente cualquier anomalía para la seguridad y tomar los correctivos en tiempo real. En un futuro no muy lejano creería que en las empresas esto se hará por inteligencia artificial.



Localización por GPS:

Permite dejar la trazabilidad de los movimientos, rutas de supervisión, desplazamientos de vehículos con carga crítica, reportar los parámetros que se violen según la configuración, última ubicación reportada de una unidad, ubicación de activos robados.



Alerta de hombre caído:

En situaciones de emergencia, históricamente se ha desconocido la importancia de generar un reporte sin una fuente humana, puesto que la fuente humana es neutralizable, puede ser vulnerable y en estos casos dispositivos que cuenten con este atributo a partir de la posición y ausencia de movimiento de un dispositivo son esenciales para generar alertas importantes para lograr uno de los principios de la seguridad como la reacción o respuesta.



Botón de emergencia:

Al igual que el sistema de hombre caído, este te permite generar una alarma, no podemos admitir un sistema de seguridad que no cuente con dispositivos que garanticen la respuesta ante una situación de emergencia. En este caso el botón de pánico es activado cuando se advierte de una amenaza, y en caso de que la amenaza neutralice a la persona de seguridad, la alerta de Hombre Caído es la solución redundante, es el plan B, es la que no permite que el sistema tenga fallo en su funcionamiento.



Control de rondas:

Muchas de las circunstancias que se presentan en el día a día de la seguridad es por que pensamos que tener un vigilante en un puesto de seguridad es la solución. Déjeme contarle que no siempre es así. Tenemos diversos tipos de puestos de vigilancia y uno de ellos es de recorrido o de supervisión de áreas. Este tipo de puestos de seguridad hacen necesaria una trazabilidad de las actividades que se realizan en cuanto a las áreas críticas que requieren una presencia constante. Le pongo un ejemplo en un Centro Comercial los locales más críticos como bancos, joyerías o cajeros electrónicos. El control de rondas es la solución perfecta para garantizar que ese vigilante o guarda de seguridad pueda realizar con mayor responsabilidad y posibilidad de detección ante una situación amenazante o una condición de inseguridad.



Accesorios manos libres.

Esos pequeños dispositivos nos ayudan a mantener la confidencialidad en las comunicaciones, nos permiten garantizar que nadie de los que está en el entorno se entere de lo que se está transmitiendo. Imagínese el reporte de una situación de riesgo en un centro comercial donde la gente escuche lo que se transmite y comienza a entrar en pánico y genera una alteración colectiva; todo por no tener este dispositivo. O qué tal un escolta que carezca de manos libres, con una mano debe manipular su arma, con la otra debe dominar a su protegido para garantizar una evacuación y control de esta persona; ¿qué sería de un escolta sin manos libres? Pues sencillamente usaría un radio en una mano, su arma en la otra y no podría garantizar el control de la persona que posiblemente esté en shock por la emergencia.



MOTOROLA SOLUTIONS