Nº 80 diciembre 2022

2023 nuevo año con objetivos más allá de la seguridad ciudadana

Estamos ante un nuevo año lleno de retos más allá de la simple seguridad ciudadana. Un año 2023 que podríamos definir como el de la disrupción.

Así, las crisis nos empujan al cambio de las seguridades como una cuestión de pura supervivencia, y sobrevivir requiere cambiar e innovar. El 2023 va a ser un año de crisis y serán momentos para la innovación. El economista austriaco Joseph Schumpeter caracterizó en 1942 los procesos de innovación como olas de destrucción creativa.

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad

Estamos ante un año donde hemos de revisar y reinventar nuestra cultura de seguridad basada en la aplicación de la inteligencia, la seguridad desde el diseño, con adecuada aplicación de medios y tecnologías innovadoras, comportamientos y hábitos renovados y un especial intercambio y colaboración de la seguridad pública y privada.

Todo ello, pensando en la seguridad humana, concepto surgido a principios de la década de los 90, en referencia a la seguridad de las personas basada en su desarrollo y derechos.

Nueva perspectiva y desafíos para la seguridad

Desde una perspectiva general una serie de desafíos se presentan con especial dinámica de inestabilidad global e inseguridad para los próximos meses: la potencial recesión económica, la inflación y las tensiones sociopolíticas. Tres grandes amenazas que generarán incertidumbre y cambios en la forma de cómo las organizaciones se han de preparan para funcionar y lograr sus objetivos de mediano y largo plazo.

Por tanto, la necesidad de protegerse ante las distintas amenazas y riesgos de ataque en clara expansión, seguirá impulsando en 2023 la inversión y el gasto empresarial e institucional en seguridad y gestión del riesgo.

Un ejemplo es el nuevo reto de seguir implantando un modelo híbrido de trabajo, combinando la presencia con el trabajo fuera de ella, con todo lo que esto implica para la seguridad de las organizaciones y la vulnerabilidad de sus datos y procedimientos, lo que obliga, además, a reforzar su seguridad con soluciones de protección automatizada para un control y verificación estricta en todo momento de acceso en cada solicitud de los usuarios.

Todo ello, en un entorno donde la guerra de Ucrania y sus recientes amenazas, sabotajes y consecuencias está provocando un nuevo planteamiento de Seguridad Global y de Protección de Infraestructuras Críticas en el ámbito de la Unión Europea, donde se ponen de manifiesto nuevos retos y exigencias para la Seguridad Pública y Privada y su especial integración operativa, que requieren de una revisión y actualización de medios tecnológicos y medidas organizativas para dar respuesta a los consiguientes riesgos y amenazas.

Así, una especial referencia es la agenda de lucha contra el terrorismo de la UE adoptada en 2020 que se basa en las políticas existentes y presenta iniciativas para garantizar la protección física y ciber de los espacios públicos y las infraestructuras críticas.

En este sentido, España ha sido durante 2022 protagonista en materia de seguridad internacional debido al éxito de la cumbre de la Organización del Tratado del Atlántico Norte (OTAN) celebrada en Madrid.

Con todo y por ello, para estar a la altura de esos objetivos, hemos de redefinir las políticas de seguridad, crear una nueva cultura de seguridad integral e integrada, establecer los mecanismos de control y gestión de la seguridad física y lógica, monitorear el sistema de seguridad y, sobre todo, hacer hincapié en la resiliencia.

Nuevas exigencias de seguridad en la Unión Europea

El Consejo de la UE ha adoptado legislación para un elevado nivel común de ciberseguridad en toda la Unión, a fin de seguir mejorando la resiliencia y las capacidades de respuesta a incidentes de los sectores público y privado y de la UE en su conjunto.

La nueva Directiva, denominada «NIS2», sustituirá a la actual Directiva sobre seguridad de las redes y sistemas de información (Directiva NIS).

Además, la nueva Directiva se ha adaptado a la legislación sectorial específica, en particular el Reglamento sobre resiliencia operativa digital para el sector financiero (DORA) y la Directiva sobre la resiliencia de las entidades críticas (RCE), para proporcionar claridad jurídica y garantizar la coherencia entre las NIS2 y estos actos.

Los nuevos desafíos que sugiere el nuevo contexto global de riesgos y amenazas requieren soluciones de seguridad innovadoras, que incorporen a la inteligencia y la tecnología como bases de una estrategia de seguridad global necesaria para operar en las organizaciones y la sociedad en su conjunto

Así, hemos de establecer una redefinición para avanzar en la Seguridad Global de un mundo de retos colectivos y futuro incierto, con necesidad de entender las nuevas dinámicas sociales, económicas, energéticas y tecnológicas en el desarrollo de ese amplio concepto que es la seguridad global que va a definir el presente y futuro próximo.

Nuevos medios y tecnologías de seguridad

Sobre la base de los nuevos desafíos la tendencia es a que más organizaciones migrarán a la nube y adoptarán una implementación híbrida de sus sistemas de seguridad. Y, a medida que más organizaciones avancen en la prueba de aplicaciones en la nube, comprenderán rápidamente los beneficios de la nube híbrida, lo que producirá un impulso aún mayor en la adopción de tecnologías en el nuevo año.

Igualmente, las analíticas de video serán más viables para implementaciones a gran escala como respuesta a la fuerte demanda de soluciones de técnicas de inteligencia artificial y, como continuación del poder de la analítica más organizaciones estarán en disposición de invertir en su mejora del control y la seguridad.

También la modernización del control de acceso será una prioridad para las organizaciones situándola en la parte superior de la lista de inversiones en tecnología de seguridad física.

Las implementaciones de nube híbrida impulsarán la demanda de dispositivos conectados a la nube ya que algunas organizaciones optan por conservar los dispositivos de seguridad y las inversiones en infraestructura que no están preparadas para la nube.

Por tanto, la unificación e integración del sistema de seguridad, los sistemas de análisis de video, la modernización del control de acceso, el avance de la nube híbrida y la ciberseguridad encabezan la lista de prioridades ante los nuevos retos.

La inteligencia en seguridad mejora la seguridad pública

La realidad indica, una vez más, que hemos de seguir avanzando en esa nueva cultura de Seguridad Basada en el Comportamiento (SBC) que surgió, en las últimas décadas del siglo pasado, como una alternativa para motivar a las personas a generar hábitos seguros, dado que las vías clásicas para cambiar el comportamiento de la gente habían fracasado de cara al objetivo de disminuir los errores y los accidentes.

Según estudios de la época, dicho enfoque nos permitió aprender mucho sobre el comportamiento humano y lograr mejores resultados en los indicadores de accidentalidad y otro tipo de eventos, aunque cuando se trata de hacer transformaciones profundas que movilicen la cultura de seguridad, salud y cuidado ambiental a otro nivel de conciencia, hemos no solo de concienciar sino avanzar en esa nueva cultura de seguridad global, integral e integrada, pública y privada.