Nº 75 marzo 2022

2022… Sector de las Seguridades. Nuevos Retos y Oportunidades

Vivimos momentos para la reinvención y el cambio. La pandemia del COVID-19 nos ha vuelto a recordar que navegamos en un “mundo líquido”, adaptativo, que se caracteriza por atributos como la flexibilidad, la versatilidad y la resiliencia.

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad

El polaco Zygmunt Bauman, premio Príncipe de Asturias 2010, fallecido en 2017, fue el autor del concepto complejo de modernidad líquida. El sociólogo acuñó el término de “mundo líquido” para definir el estado fluido y volátil de la actual sociedad, sin valores demasiado sólidos, donde la incertidumbre, por la vertiginosa rapidez de los cambios, ha debilitado los vínculos humanos.

Bauman luchó contra la superficialidad del momento, de tanta información y tan poco tiempo para profundizar y con tan poca base detrás. Su propio pensamiento sufrió la situación que tanto criticó y su “mundo líquido” se ha convertido en un concepto que cada uno interpreta a su manera.

En esta situación, y con la presión del COVID-19 hay muchas actividades, especialmente estratégicas y críticas, que se están sometiendo a procesos de cambio para seguir siendo viables y no generen riesgos para sus gestores.

Así podemos hablar de un nuevo concepto que, bajo el acrónimo LICA (Líquido, Incierto, Complejo, Ambiguo) evoluciona rápidamente.

En este sentido, cada actividad, cada servicio público o privado, requiere actualizarse con nuevos procedimientos y estrategias distintas. Desde el aeropuerto al hospital, desde los centros comerciales a las fábricas, todo deberá licuarse para sobrevivir en otras condiciones. Nos esperan más cambios radicales tras los que tendremos que aprender de nuevo a sobrevivir.

También las seguridades están sufriendo una nueva orientación y estrategia hacia el concepto de continuidad de negocio y funcionamiento.

Es fácil relacionar el término continuidad de negocio con el ámbito tecnológico o con las grandes organizaciones, pero este no es exclusivo de las grandes infraestructuras pues las incidencias y los desastres afectan igualmente a las pymes y a los autónomos.

Cualquier organización, con independencia de su tamaño o sector de actividad, debe estar preparada para prevenir, proteger y reaccionar ante incidencias de inseguridad que pueden afectar e impactar en su actividad.

Hay que diseñar un Plan de Continuidad de Negocio que comprenda planes de actuación en emergencia, planes financieros y de comunicación y planes de contingencia destinados a minimizar el impacto provocado por la materialización de determinados riesgos o amenazas sobre la información y los procesos de funcionamiento de una organización.

Infraestructuras Críticas. Planes y gestión de Seguridad Global

Vivimos un panorama globalizado de nuevas amenazas, mayores riesgos en las actividades sociales, industriales y comerciales que ratifican nuevas demandas y exigencias de la sociedad para la protección de sus actividades con plenas garantías para su seguridad y, muy especialmente, en el entorno de las Infraestructuras Críticas o de funcionamiento esencial.

Así, por estas múltiples amenazas y los nuevos retos y desafíos para la seguridad, en la Estrategia de Seguridad Nacional (ENS-2021), en "Objetivos generales y líneas de acción de la Seguridad Nacional", identifica cinco objetivos generales: "Avanzar en un modelo integral de gestión del riesgo y de crisis, promover una cultura de Seguridad Nacional, favorecer el buen uso de los espacios comunes globales, impulsar la dimensión de seguridad en el desarrollo tecnológico y fortalecer la proyección internacional de España".

Y como riesgos y amenazas transversales se encuentran los ciberataques donde nos cabe destacar cinco recomendaciones para proteger estas infraestructuras críticas, como son la: Creación de una estrategia de ciberseguridad en cada país y así formar un frente de defensa que permita intercambiar eficientemente información de alertas, vulnerabilidades y amenazas para actuar rápida y coordinadamente; Mejorar la capacidad de inteligencia al incluir la protección de la infraestructura crítica dentro de las responsabilidades del Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT); Continuar con la implementación del Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad; Continuar con la actualización del Catálogo de Infraestructuras Críticas; Realizar auditorías regulares que además de revisar el estado de la seguridad de la infraestructura, permitan conocer el nivel de implementación e implicación en la nueva cultura de seguridad.

En este sentido, cabe destacar la importancia de establecer nuevos planteamientos y herramientas para la Gestión Integral del Riesgo y las Seguridades. Debemos invertir en gestionar el riesgo para prevenirlo y garantizar, en todo lo posible, el poder superar las crisis o contingencias con mayor resiliencia.

Nuevos retos y oportunidades

Uno de los retos importantes, es el desarrollo de un nuevo concepto de Seguridad Global, con la convergencia de las seguridades, la transformación digital y la digitalización para la gestión operativa de la seguridad integral e integrada, pública y privada.

Igualmente, ante la gran variedad de riesgos inherentes a las Infraestructuras Críticas, su protección debe tener un enfoque basado en esta Seguridad Global, abordada como una gestión integral del riesgo, implementando un modelo holístico de seguridad incorporando la cultura proactiva de prevención y protección.

Igualmente, hemos de seguir avanzando hacia la integración operativa de la Seguridad Pública-Seguridad Privada (Cooperación, Colaboración).

Con todo ello, y como recomendación, debemos potenciar una nueva cultura de seguridad con una visión sobre la base de las amenazas complejas e incrementar los recursos de análisis y liberarlos de viejas patologías y rigideces desarrollando el esquema de la Gestión Integral del Riesgo y las Seguridades.

Acciones y reacciones

En cuanto a las nuevas acciones y reacciones cabe subrayar los avances establecidos hacia el planteamiento de seguridad integral e integrada, pública y privada, así como el inicio de la importante transformación en los Departamentos de Seguridad hacia un nuevo esquema o estructura neuronal con mayor implicación y compromiso de todos sus integrantes.

Todo ello con una nueva Dirección Ejecutiva Seguridad Global, en muchos casos basada en un liderazgo ejecutivo de mayor: Implicación permanente, Integración de las seguridades, Inteligencia corporativa, Innovación tecnológica, e Imaginación e Iniciativa muy proactiva.

Esto conlleva la revisión y nuevos planteamiento, principalmente dentro del Plan Nacional de Protección de Infraestructuras Críticas, que se establecen con el contenido de los siguientes planes y bajo un enfoque integral: Seguridad física-Seguridad lógica; Coordinación de las actividades de los agentes implicados en la protección de IC, en sector público y privado; Medidas y aplicación de normativas, buenas prácticas, planes generales de protección, planes específicos de sector e instalaciones, coordinación con FFCC de Seguridad; y Canalización de la Cooperación Internacional.

Todo ello, exigirá nuevos programas de Formación Especializada con planteamientos y adecuación a los nuevos retos, exigencias y tendencias ya explicitadas.

Nuevos medios y medidas de seguridad

Ante la implantación o evolución de nuevos medios tecnológicos y medidas organizativas y operativas de seguridad hemos de plantear la revisión y reinvención de nuevos indicadores o métricas que permitan realizar una evaluación sobre la eficiencia y eficacia del tratamiento y gestión del riesgo y las seguridades.

Dentro de los indicadores, podemos encontrarnos distintos en función de lo que pretendamos analizar. Veamos los más comunes y aquellos que tienen una mayor utilidad práctica como: Indicadores en clave de riesgo, que cuantifican el perfil de riesgo de la organización. Indicadores de control, que se encargan de medir la efectividad, tanto de diseño como de desempeño, de un control específico; Indicadores de resultado, que hacen referencia a los términos de conclusión de una tarea; Indicadores de desempeño, que aportan información sobre el rendimiento asociado a una tarea, proyecto o proceso, en función de los métodos empleados para su ejecución; Indicadores reactivos y activos, que hacen referencia a los hechos consumados o a la identificación de los esfuerzos que se realizan desde la organización evitar riesgos; Indicadores de eficacia, relacionados con la capacidad para la consecución de una actividad; Indicadores de eficiencia, determinados en función de la capacidad para ejecutar un trabajo en condiciones de economía, recursos y ajuste de tiempo.

Todo ello basado en los nuevos planteamientos de transformación digital y digitalización con nuevas herramientas de gestión operativa en Seguridad Pública y Seguridad Privada así como, mediante la implantación de nuevas soluciones en sistemas y servicios integrados.

En este sentido, en la reciente convocatoria del Salón Internacional de la Seguridad, SICUR 2022, se han puesto de manifiesto los últimos desarrollos tecnológicos e innovaciones del sector que, igualmente, se encuentra inmerso en momentos de cambio y transformación.

Nuevos objetivos, nuevos retos, y también nuevas respuestas que han venido siendo exigidas durante dos años de una pandemia y que ha pasado por una adaptación, con nuevos criterios y responsabilidad hacia una nueva realidad, donde la digitalización e innovación son los pilares fundamentales.

Un sector de las seguridades con nuevos proyectos y estrategias de sus integrantes ante esta nueva realidad con tecnologías evolucionadas y nuevas soluciones en seguridad adaptadas a un diferente escenario tecnológico y de globalización, donde surgen nuevas amenazas y riesgos, muchos de ellos, impredecibles.

La seguridad privada se ha reinventado, evolucionado y adaptado para garantizar la prevención y protección de personas y bienes con una seguridad integral e integrada.

Pero, ninguno de todos los nuevos planteamientos y soluciones para los nuevos retos y exigencias de seguridad serán posibles sin la revisión, adecuación y adaptación al cambio de la reglamentación de Seguridad Privada por otras exigencias a nivel de requisitos como: tipo de contratistas homologados, certificaciones en el ámbito de seguridad de la información ante las nuevas amenazas como el ciberataque o el cibercrimen y las nuevas medidas de seguridad y ciberseguridad que debieran implementarse.