Ciberseguridad privada: la seguridad privada necesita digitalizarse

Mikel Rufián Albarrán
Director global de Ciberseguridad & Inteligencia de Bidaidea

La seguridad constituye el cimiento sobre el cual la sociedad puede desarrollarse y garantizar la prosperidad de sus ciudadanos. La relevancia de la seguridad privada como parte integrante de la seguridad pública es hoy un hecho innegable. Su labor (empresas, personal de seguridad privada, sistemas de seguridad…) contribuye con la ejecución de los servicios de seguridad privada a completar la seguridad pública, de la que forma parte, tal y como se reconoce el texto legal que la regula. Además, colabora con las Fuerzas y Cuerpos de Seguridad en garantizar el ejercicio de nuestros derechos y libertades.

Inversión en innovación

Hay que convertir la crisis en oportunidad para aprender a trabajar de forma diferente y, por supuesto, invertir en innovación; un nuevo contexto donde los elementos anteriores han quedado obsoletos y el valor de la información por sí sola no es ya un elemento diferencial de ventaja competitiva. Ahora es preciso tener conocimiento, adelantarse a los movimientos de países y empresas. Y una de las claves en este sentido es la inteligencia en materia de ciberseguridad; es decir, el conocimiento estructurado para la toma de decisiones.

Y es que el mundo actual no se entiende sin las tecnologías y el desarrollo del ciberespacio. Es el entorno donde se da una verdadera y real globalización. La creciente aceptación e introducción de las tecnologías digitales en la planificación y el armamento militares dan paso a la perspectiva de una ciberguerra en la cual, habida cuenta de la interdependencia global de las estructuras de red, podría, inevitable y profundamente, afectar a la economía y a activos esenciales de la sociedad. La utilización militar hostil de estas tecnologías podría, de hecho y de derecho, no estar claramente diferenciada de los ciberconflictos de carácter general y despertar serias dudas sobre su control y legitimidad.

Esta situación ha provocado también el aumento de amenazas, riesgos y vulnerabilidades sobre las aplicaciones del ciberespacio. Por tanto, este último se está convirtiendo en el objetivo de los grupos dedicados a la ciberdelincuencia, cibervándalos, ciberterrorismo, *hackitvistas*, actores internos (*insiders*) y Estados y grupos patrocinados por ellos.

Digitalización

La seguridad privada necesita digitalizarse para no quedarse atrás. De hecho, este sector ya se ha quedado atrás y precisa evolucionar hacia la necesaria transformación digital con "ciberseguridad privada", inversión, formación, actualización de la regulación y la incorporación de la Inteligencia Artificial, los datos, la robótica y el resto de las tecnologías emergentes OT/IoT.

> Es necesario fomentar una cultura de la ciberseguridad privada a nivel nacional

Recordemos que la ciberseguridad se esfuerza por asegurar el logro y el mantenimiento de las propiedades de seguridad de la organización y los activos del usuario contra los riesgos relevantes de seguridad en el entorno cibernético.

Pero a lo largo del tiempo, la seguridad privada ha representado un elemento indispensable para la sociedad. Sobre todo en el entorno empresarial, este elemento tiene mucho protagonismo, ya que permite resguardar el recurso material y humano que forma parte de cualquier compañía. Es por esta razón que dejar esta responsabilidad en manos de profesionales ha resultado fundamental.

La cantidad de información y los dispositivos que la soportan están aumentando constantemente en cada sector de la vida cotidiana. Es el Internet de las Cosas, lo que llamamos la inclusión de miles de millones de máquinas, comenzando con tabletas, teléfonos inteligentes, cajeros automáticos, instalaciones de seguridad, CCTV, sistemas de controles de acceso, etc.

En definitiva, la ciberseguridad es imprescindible para que progrese la transformación digital. De ahí la necesidad de una Ley de Ciberseguridad Privada donde el ciudadano tenga a disposición nacional un directorio profesional de empresas, tecnologías y profesionales de ciberseguridad debidamente homologados y preparados para ofrecer cualquier servicio con garantía en el país.

De este modo se contribuiría a reforzar los procesos de seguridad nacional y de contrainteligencia, cubriendo la seguridad integral y cibercapacidades propias. Es una necesidad a nivel nacional que las personas con niveles gerenciales o directivos, ya sean trabajadores en el área pública o en el sector privado, puedan contar con las herramientas y con las metodologías más de vanguardia para hacer frente a la realidad delictiva que hoy enfrentamos.

Colaboración

También cabe destacar que la colaboración público-privada no es privatización; mensaje que a veces no llega de la manera adecuada al conjunto de la ciudadanía. Hay que recalcar aún más que los servicios públicos lo siguen siendo, independientemente de cómo sea su forma de gestión. Lo importante es que la titularidad es y será pública, indistintamente de que la gestión u operación se realice de forma directa por las administraciones públicas o a través de empresas, ya sean públicas, mixtas o privadas.

Hoy las organizaciones necesitan seguridad integral. Pero también es cierto que sin una cultura de la seguridad integral basada en la técnica y en la ciencia será muy difícil avanzar.

Cultura

En este sentido, es clave la colaboración público-privada. Pero esto no es solo financiación; también compromiso social de las empresas con el conjunto de la ciudadanía en materia de (ciber)inteligencia. Son las compañías las que tienen los mayores avances en I+D+i y, por tanto, la colaboración entre ellas y las administraciones es la forma más rápida de hacer llegar las últimas innovaciones al sector público y al conjunto del país en materia de ciberseguridad e inteligencia.

Hay que transformar a la Administración para que sea ágil prestando servicio al ciudadano y atendiendo sus necesidades reales. Y también fomentar e incentivar de forma activa una cultura de la ciberseguridad privada a nivel nacional que permita implantar los procedimientos y herramientas necesarias para el correcto funcionamiento en conjunto con la seguridad privada.

No en vano, la seguridad privada no es un gasto, sino una inversión. Hacer un traje a la medida después de evaluar las necesidades de información de una organización es sinónimo de rentabilidad y optimización de los beneficios a corto, medio y largo plazo. Los escenarios actuales de amenazas, riesgos y oportunidades a los que se enfrenta una organización son complejos y difíciles de abordar desde una perspectiva tradicional de seguridad privada. Por lo tanto, se necesitan soluciones complejas, creativas y efectivas con ciberseguridad. Y los elementos que facilitan dichas soluciones son las personas, la inteligencia, la ciberseguridad y la colaboración público-privada. Un ciberespacio seguro es posiblemente el mayor desafío al que se enfrentan todas las organizaciones y países desde el punto de vista de la seguridad. Por consiguiente, los riesgos y amenazas que se ciernen en él requieren una respuesta oportuna, proporcionada, eficaz y coordinada que garantice la libre y segura utilización del mismo por el conjunto de la sociedad.