Seguridad híbrida

DOI: 10.29236/sistemas.n167a1

Jeimy J. Cano M.

Andrés R. Almanza J.

Un ejercicio convergente de retos, contextos y saberes a nivel empresarial y nacional

Las inestabilidades globales y el contexto de "policrisis" y "permacrisis" que atraviesa el mundo actual establece con mayor claridad un escenario frágil, ansioso, No-Lineal e incomprensible (FANI), características que claramente superan cualquier estrategia de gestión de riesgos disponible a la fecha; por tanto, es necesario explorar nuevas fronteras y propuestas para avanzar en una seguridad híbrida, ajustada a los tiempos actuales, esto es, convergente, sistémica e interconectada.

El ejercicio de seguridad híbrida implica necesariamente una seguridad convergente, esto es, de acuerdo con Beck et al. (2019), "*un funcionamiento armónico de las funciones de seguridad/gestión de riesgos para abordar la seguridad de forma holística y cerrar las brechas y vulnerabilidades que existen en los espacios entre funciones para proporcionar una defensa empresarial integrada*". En este contexto, de acuerdo con los autores una organización con seguridad convergente, ha hecho confluir al menos dos o las tres funciones siguientes: seguridad física, ciberseguridad y continuidad de negocio. Una organización "no convergente" no ha combinado ninguna de las tres funciones.

En este proceso, se advierten aspectos positivos y retos claves que las organizaciones deben atender de cara a esta nueva realidad. Dentro de los aspectos positivos están: (Beck et al., 2019)

- Mejor alineación de la estrategia de seguridad/gestión de riesgos con los objetivos corporativos.
- Avances en la integración tecnológica/centros de operaciones de seguridad (físicos y cibernéticos).
- Mayor eficacia en las operaciones de seguridad y/o continuidad del negocio.
- Ahorros de costos.

De igual forma se plantean desafíos propios de una convergencia que implica mayor colaboración, cooperación, coordinación, comunicación y confianza entre equipos de trabajo para formular y desarrollar una perspectiva holística de la seguridad empresarial lo que se traduce en: (Beck et al., 2019)

- Resultados no negativos, es decir no se puede determinar con exactitud los logros del ejercicio.
- Confusión sobre funciones y responsabilidades.
- Confusión sobre las líneas de reporte/ comunicación.
- Conflictos, otros problemas de personal entre el personal convergente.
- *Baja formación interdisciplinar para reconocer el nuevo escenario de defensa integral*.

(La anotación en *cursivas* no hace parte del texto original)

Así las cosas, ya no es suficiente mantenerse informado y consciente de las volatilidades económicas y geopolíticas globales para avanzar en una propuesta de defensa integral de la organización y, por tanto, es necesario repensar los fundamentos de la seguridad tradicional (protección, prevención, cumplimiento y monitoreo) y traducirlos a uno de defensa que implica disuadir, demorar, confundir y anticipar, o mejor aún, integrar los dos alrededor del diseño y planeación de escenarios que permitan concretar y situar la inteligencia y lecciones aprendidas de las organizaciones.

En este sentido, el concepto de diseño base de amenazas (en inglés *Design Base Threats* - DBT), a pesar de haber sido fundado en 1970 alrededor de los retos de defensa de instalaciones nucleares en USA, resulta de interés comoquiera que permite: "una descripción general de los motivos, intenciones y capacidades de los adversarios potenciales contra los que se diseñan y evalúan los sistemas de protección", lo que se traduce en establecer la capacidad máxima de defensa disponible para una amenaza o grupo de amenazas, basada en información de inteligencia creíble (IAEA, 2009).

Un DBT no pretende ser una declaración sobre las amenazas reales e imperantes, sino un ejercicio de estimación y análisis situacional que permite abordar realidades inmersas dentro de los patrones de amenazas disponibles en la actualidad, sabiendo que pueden existir eventos encubiertos, donde los adversarios siempre están buscando nuevos métodos y tácticas para superar las medidas de seguridad, y que el adversario "individual" sigue siendo en gran medida impredecible (ISC, 2010).

En este contexto, la seguridad híbrida implica concretar un marco de pronóstico y prospectiva que le permita a las organizaciones, por un lado, aprovechar la información disponible desde una perspectiva base de identificación de patrones y tendencias de la realidad actual y, por otro, ejercicios de prospectiva en la producción de una variedad de futuros posibles para cuestionar la mentalidad de los responsables de la toma de decisiones (Poli, 2019). De esta forma, los líderes pueden ver a través de la complejidad del entorno e identificar, categorizar e interpretar sistemáticamente los riesgos. Esto les permite mirar más allá de los factores de riesgo conocidos y explorar intencionadamente riesgos aún por conocer, abrazando así la incertidumbre en lugar de mitigarla o evitarla (Sheth & Sinfield, 2023).

Es por esto que esta edición de la revista *Sistemas*, de la Asociación Colombiana de Ingenieros de Sistemas −ACIS−, apunta a revisar, explorar y analizar los retos y oportunidades de la seguridad híbrida, con el fin de traer al escenario actual diferentes posturas sobre el tema, como insumo para plantear alternativas y opciones en un entorno FANI. Con ese propósito fueron convocados profesionales especialistas, quienes desde su experiencia proponen reflexiones para seguirle la pista al desarrollo de las tendencias y prácticas vigentes en esta temática, capitalizando lecciones aprendidas, repensando las dinámicas de los negocios y retos actuales, así mismo explorar el futuro que se avizora en el horizonte.

El profesional en ciencias militares, seguridad y defensa Daniel Jiménez, columnista invitado, establece desde su práctica como presidente

del capítulo de ASIS Colombia, un marco base para reflexionar sobre el reto de concebir la seguridad de forma más holística e inclusiva en cuanto al alcance corporativo, donde cada una de sus aristas deben ser incluidas como son la seguridad de la información, la seguridad informática, el cumplimiento, las investigaciones, el manejo de crisis y emergencias, la seguridad ocupacional, la seguridad física y muchas otras que pueden convertirse en parte esencial dentro de los diferentes negocios, para establecer un diálogo convergente que permita alcanzar sus objetivos y/o prevenir las pérdidas.

En la entrevista el profesional en criminalística, Coronel (RA) Fredy Bautista García y actual director de Protección y Seguridad del Banco de la República, nos comparte sus reflexiones sobre los retos propios de una seguridad convergente, su visión sobre la evolución de esta temática en el mercado colombiano, así como aspectos relacionados con el cibercrimen y las amenazas a la ciberseguridad para las organizaciones modernas y sus activos digitales.

Con el ingeniero Andrés Almanza Junco presentamos el análisis de los resultados de una investigación internacional relacionada con las capacidades de los CISOs en Iberoamérica. Los resultados revelan, entre otros aspectos, que los participantes de la muestra perciben a los CISOs de una manera distinta impulsados por la realidad de sus países; que las capacidades relacionadas con aprender y accionar son las más visibles para sus clientes y que, en general, la brecha en el desarrollo centrada en sus capacidades estratégicas demanda una postura más flexible frente al incierto para poder anticipar y defender la promesa de valor de las empresas.

El foro de esta revista fue un espacio para compartir visiones desde diferentes ángulos sobre la seguridad híbrida. Los profesionales Hamilton Moya, especialista en ciberseguridad; Wilson Prieto, consultor en ciberseguridad, Héctor Calderazzi, consultor independiente en desarrollo de políticas, normas y procedimientos, Andrés Almanza Junco, consultor internacional independiente (y coeditor de este número) y Arturo García, Gerente de Seguridad en Tecnologías de la Información en el Banco Central de México, desarrollaron un diálogo abierto y nutrido para contrastar y complementar sus posturas alrededor de los retos que implica una seguridad híbrida para las organizaciones modernas. Ellos advierten sobre la necesidad de establecer un lenguaje común para comunicar y movilizar la distinción de seguridad, lo que implica salir de esa zona cómoda de los estándares y de la estrategia del miedo, la incertidumbre y las dudas para encontrarse con el negocio, y terminar (o minimizar) los desencuentros permanentes de la seguridad y el mo-

delo de generación de valor de la empresa.

Así mismo, nuestros lectores dispondrán de dos artículos para reflexionar sobre la seguridad híbrida y la ciberresiliencia en dos visiones conceptuales y prácticas que analizan las nuevas apuestas de las organizaciones y la necesidad de mantenerse operando a pesar de la materialización de eventos adversos.

En un primer documento el profesor Jeimy J. Cano M., director esta revista, se ocupa de plantear un modelo de seguridad asimétrica, híbrida e interconectada, que habilite una mirada más holística de la realidad y desde allí explorar el reto de seguridad y control de forma convergente y multidominio, como una respuesta natural a un entorno en el cual abundan los inciertos y escasean las certezas, y en donde las policrisis son el nuevo anormal que deben atender y superar las organizaciones y Estados para concretar su viabilidad en el largo plazo.

El segundo artículo, desarrollado por el doctor Arturo García Hernández, tiene por objetivo describir las similitudes y diferencias entre la ciberseguridad y la ciberresiliencia, disciplinas dedicadas a la protección del ciberespacio, resaltando sus características fundamentales, con la finalidad de conformar y desarrollar una estrategia de defensa integral y más efectiva ante los escenarios actuales que aplique tanto a las organizaciones como a los Estados.

En resumen, se trata de un panorama renovado y provocador de nuevas transformaciones, retos y propuestas alrededor de la seguridad híbrida, que tensionan las certezas de los saberes y prácticas existentes en las perspectivas e imaginarios de la seguridad integral actual. Su contenido invita a todos los profesionales en las diferentes áreas del conocimiento a explorar las nuevas realidades de un mundo digital y tecnológicamente modificado, sin perjuicio de los nuevos desafíos políticos, económicos, sociales, tecnológicos, legales y ecológicos, en donde las permacrisis, las policrisis, el aumento de las tensiones cibernéticas internacionales y las inestabilidades geopolíticas locales y globales (Colomina et al., 2022), revelan nuevas incertidumbres y potencian el desarrollo de capacidades de negocio inexistentes, de cara a los riesgos que aún no aparecen en sus mapas estratégicos.

Referencias

Beck, D., Gips, M., & MacFarland Pierce, B. (2019). *The state of security convergence in the United States, Europe, and India*. Alexandria, VA: ASIS International.

Colomina et al. (2022). El mundo en 2023: diez temas que marcarán la agenda internacional. *CIDOB Notes Internationals*. No. 238. https://bit.ly/3YHt7uK

International Atomic Energy Agency - IAEA (2009). Development, use and maintenance of the design basis threat. Implementing guide. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1386_web.pdf

Interagency Security Committe – ISC (2010). The Design-Basis Threat (U). *Department of Homeland Security*. https://info.publicintelligence.net/DHS-DesignBasisThreat.pdf

Poli, R. (2019). Introducing anticipation. En Poli, R. (Ed.) (2019). *Handbook of anticipation. Theoretical and applied aspects of the use of future in decisión making*. Cham, Switzerland: Springer Nature Switzerland AG. 3-16

Sheth, A. & Sinfield, J. (2023). Risk Intelligence and the Resilient Company. *Sloan Managemen Review*. *64*(4). https://sloanreview.mit.edu/article/risk-intelligence-and-the-resilient-company/

Jeimy J. Cano M., Ph.D, CFE, CICA*. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

Andrés R. Almanza J., M.Sc., CISM*. Chief Growth Officer en CISOS.CLUB, Investigador en Ciberseguridad SegInfo y Liderazgo. | Executive Certificate in Cybersecurity Leadership & Strategy by FIU University | Certificado como ISO 27001 Lead Implementer and 27005 Lead Manager from PECB | CISM, ITILv3, LPI| Certificado como Coach Profesional Internacional, Master in Leadership and Organizational Development with Coaching, Executive Master's in Leadership Skills Developed in Harvard, & Coach Profesional avalado por International Coach Federation| Profesional en Ingeniería de Sistemas | especialista en seguridad en redes y máster en seguridad de la información. Docente del programa de maestría de la Universidad Externado de Colombia y de la Universidad de las Américas en Ecuador. Creador de la Comunidad CISOS.CLUB, CISOS-COL y CISOS-LATAM (Linkedin) y Miembro del comité editorial de la revista sistemas de ACIS.*