Resiliencia digital: más allá de la continuidad del negocio

DOI: 10.29236/sistemas.n159a1

En un contexto volátil, incierto, complejo y ambigüo (VICA) lo normal es enfrentar "eventos inesperados"; en este sentido, la resiliencia digital se configura como el nuevo referente para vivir atentos y vigilantes en procura de mantener las operaciones a pesar de la inevitabilidad de la falla y las acciones exitosas de agentes adversos.

Jeimy J. Cano M.

Las organizaciones hoy se enfrentan a una dinámica de cambios permanentes que demandan una mirada distinta al entorno y a las tendencias que allí se advierten. La incertidumbre como elemento natural para los ejecutivos de las empresas e insumo base de la innovación, establece dos puntos de análisis que exponen a las compañías a tomar acciones sobre un escenario que se transforma con las diferentes posturas que pueden aparecer desde cualquier mercado o sector (Day & Schoemaker, 2019).

En este contexto, la tecnología juega un papel fundamental como ha-

bilitador de posibilidades, servicios o productos que terminan capitalizando nuevas experiencias para los individuos y cambiando muchas veces la forma de hacer las cosas. Por tanto, los conceptos de digitalización (digitalizar) y transformación digital (ser digital) adquieren una relevancia estratégica para las empresas, habida cuenta que permite preparar los componentes de infraestructura requeridos para fundar una estrategia digital y, además, transforma el modelo de negocio y la cultura organizacional para crear apuestas novedosas que reten los saberes previos (Ross, Beath & Mocker, 2019).

Así las cosas, ya no es suficiente con reconocer y asegurar los activos de información claves que se generan en la organización por cuenta de las estrategias digitales, sus productos y servicios, sino que es necesario centrarse en la experiencia del cliente, en el reconocimiento y desarrollo de la confianza digital, para desde allí habilitar las opciones de seguridad y control, basadas en su apetito al riesgo, a de fin crear entornos con umbrales de operación y tolerancia que conecten las capacidades empresariales y los acuerdos claves cuando las cosas no salen como estaban previstas (Zongo, 2018).

Es por esto que la resiliencia digital, como una nueva capacidad organizacional, se consolida como el nuevo horizonte y reto corporativo, que exige a las empresas alcanzar por lo menos cinco objetivos claves: (Robinson, 2020)

- **Anticipar disrupciones**: detección temprana y patrones de ataques emergentes.
- **Resistir interrupciones**: establecer niveles de defensa para mantener la operación.
- **Recuperarse de los ataques**: ejecutar las estrategias control y restauración frente a los ataques.
- **Aprender de los riesgos**: incorporar la inteligencia y cacería de amenazas.
- **Adaptar y modificar las capacidades vigentes**: desarrollar simulaciones y prototipos frente a escenarios inciertos y emergentes.

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 resiliencia digital, con el fin de traer al escenario actual diferentes posturas y comprensiones sobre el tema, como insumo para plantear alternativas y opciones en un entorno VICA. 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, capitalizando lecciones aprendidas, repensando las dinámicas de los negocios y retos actuales, así como al futuro que se avizora en el horizonte.

El ingeniero Mario Ureña Cuate, columnista invitado, establece desde su práctica de consultoría un marco base para reflexionar sobre la ciberresiliencia, en el marco de la capacidad empresarial demostrada para anticipar, resistir, recuperar y adaptarse ante eventos disruptivos que pongan en riesgo la actividad de las organizaciones en el ciberespacio. En esa dirección presenta una serie de propuestas en el campo empresarial y técnico que orienta a los ejecutivos y profesionales de TI para asumir el reto de permanecer a pesar de los eventos adversos.

En la entrevista el ingeniero Andrés Mauricio Bolívar Arias nos comparte sus reflexiones acerca de la resiliencia digital, desde la perspectiva de los negocios y los retos empresariales, además de afirmar que la resiliencia es más que seguridad e implica agilidad y velocidad para cambiar y adaptarse a las nuevas condiciones de los mercados.

Por su parte, el ingeniero Andrés Almanza Junco presenta el análisis de los resultados de la versión número veintiuno de la encuesta nacional de seguridad de la información, realizada cada año por ACIS, estudio que revela las tendencias más representativas de las empresas colombianas en los temas de protección de la información y la evolución del líder digital de seguridad, así como sus respectivos contrastes con la realidad internacional. En esta ocasión, se presentan los aspectos más representativos de las tendencias y algunos contrastes frente a patrones identificados en los datos acumulados.

El foro de esta revista fue un espacio para compartir visiones desde diferentes ángulos sobre la resiliencia digital. Los ingenieros Víctor Vásquez Mejía, Édgar Fernando Avilés, Milena Realpe Díaz y Armando Carvajal Rodríguez desarrollaron un diálogo abierto y nutrido para contrastar y complementar sus posturas desde la práctica de consultoría, la visión de defensa y seguridad nacional, la dinámica del sector público y los estándares disponibles a la fecha. Ellos advierten sobre la necesidad de incorporar los nuevos retos que impone la resiliencia digital y cómo avanzar en una perspectiva interdisciplinaria que permita a los profesionales y ejecutivos de seguridad y control enfrentarse a un escenario cada vez más disruptivo, inestable e hiperconectado, ambiente que demanda una mayor anticipación y capacidad de aprendizaje.

Así mismo, nuestros lectores dispondrán de dos artículos para reflexionar sobre la ciberresiliencia como integración entre seguridad de la información y continuidad, y por otra parte, sobre el reto de superar la falsa sensación de seguridad. En un primer documento el ingeniero Norman Ramírez se ocupa de explorar y analizar cómo es el ejercicio de convergencia entre las prácticas de seguridad de la informa-

ción y los retos de la continuidad de negocio y contrastar algunos marcos de trabajo para avanzar en la configuración de una organización ciberresiliente.

El segundo artículo, escrito por este servidor, aborda una revisión y análisis del reto de la falsa sensación de seguridad, esa zona cómoda y engañosa en la que se materializan y concretan sesgos y puntos ciegos en los modelos de seguridad y control; en que la necesidad de certezas enfrenta la cultura de productividad con la de aprendizaje. Frente a esta realidad, el artículo plantea una propuesta de un modelo de gestión que pase del tradicional "Planear, Hacer, Verifica y Actuar", a otro que privilegie las inestabilidades basado en "Arriesgar, Anticipar, Responder y Monitorizar.

En resumen, se trata de un panorama renovado y provocador de nuevas prácticas y desafíos alrededor de la resiliencia digital, que tensiona las certezas de los saberes y prácticas existentes. Su contenido invita a todos los profesionales en las diferentes áreas 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, que los diferentes grupos de interés buscan para darle forma a las incertidumbres del entorno y desarrollar capacidades de negocio inexistentes, de cara a los riesgos que aún no aparecen en sus mapas estratégicos.

Referencias

Day, G. & Schoemaker, P. (2019). *See sooner act faster. How vigilant leaders thrive in a era of digital turbulence*. The MIT Press.

Robinson, C. (2020). Are We Cyber-Resilient? The Key Question Every Organization Must Answer. *IDC Market Spotlight*. Noviembre. https://www.bankinfosecurity.com/whitepapers/are-we-cyber-resilient-key-question-every-organization-must-answer-w-7136

Ross, J., Beath, C. & Mocker, M. (2019). *Designed for digital. How to architect your business for sustained sucess*. The MIT Press.

Zongo, P. (2018). *The five anchors of cyber resilience. Why some enterprises are hacked into banksruptcy while other easily bounce back*. Broadcast Books.

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–.*