Ciberresiliencia organizacional

DOI: 10.29236/sistemas.n159a2

Afrontando la incertidumbre para sobrevivir y prosperar en un mundo digital. Solamente las organizaciones ciberresilientes tendrán la capacidad de sobrevivir ante los frecuentes ciberataques y frente al próximo gran evento disruptivo que enfrente la humanidad.

Mario Ureña Cuate

La pandemia por COVID-19 ha representado retos de gran impacto durante 2020 y 2021 para la sociedad y las organizaciones a nivel mundial, permitiendo renovar la importancia de la resiliencia organizacional a nivel individual y colectivo. La necesidad de implementar acciones y soluciones de continuidad del negocio, transformación y adaptación en respuesta a la emergencia sanitaria ha probado la capacidad de las empresas para sobrevivir y prosperar en un contexto global que presenta grandes cambios y retos.

La resiliencia organizacional es definida por BSI (*British Standards Institution*) en el estándar BS 650-00 como "la habilidad de una organización para anticipar, prepararse, responder y adaptarse al cambio incremental y las disrupciones repentinas con el fin de sobrevivir y prosperar" (BSI, 2014).

En este sentido, desde el punto de vista del ciberespacio como ese ambiente complejo que resulta de la interacción de personas, aplicaciones y servicios en internet a través de dispositivos tecnológicos y redes de comunicación que los conectan, hemos sido testigos de dos cambios profundos. Por una parte, la aceleración de la transformación digital en las organizaciones y, por otra, el incremento en los ciberriesgos que enfrentan.

La transformación digital se ha convertido en una estrategia primordial para mejorar las capacidades de resiliencia de las organizaciones al habilitar la posibilidad de adaptación en su forma de operar y el entendimiento de su rol y valor en la sociedad actual (Siebel, 2019).

Esta transformación digital va más allá del concepto común asociado a la digitalización, el cual es un elemento muy importante para lograr esta transformación; sin embargo, requiere de un cambio mucho más profundo que contempla: (Rogers, 2016)

- El entendimiento de los **clientes** como una red dinámica que exige una comunicación bidireccional y que representa la influencia principal sobre las decisiones de la organización

- Una búsqueda de **valor** hacia los clientes que permita descubrir dinámicamente las nuevas propuestas de valor encaminadas a una evolución antes de estar obligados al cambio.

- El reconocimiento de la **innovación** que acepte los fracasos como una fuente de aprendizaje y que permita el entendimiento y la resolución de los problemas correctos a través de la experimentación constante e inclusiva.

- La eliminación de los silos de **datos** con el objetivo de convertirlos en información valiosa para la toma de decisiones

- El entendimiento de la **competencia** como la implementación de redes externas que permitan la cooperación en áreas clave con socios que intercambian valor.

Este incremento en el uso del ciberespacio para habilitar nuevas formas de interacción en la sociedad conlleva riesgos que se han intensificado sustancialmente durante este tiempo de pandemia, debido al incremento sostenido en el uso de la tecnología y las consecuencias sociales asociadas al desempleo, impactos económicos y cambios culturales, que en ocasiones demuestran una degradación de los principios éticos y morales de grupos y personas a nivel internacional.

En consecuencia, los ciberriesgos han tenido una escalada preocupante con datos que confirman el estado de urgencia que debe ser

atendido. De acuerdo con datos del FBI (*Federal Bureau of Investigation*) se reporta un incremento del 300% en ciberataques a partir del inicio de la pandemia por COVID-19. Así mismo, la compañía de tecnología Verizon indica que, en 2020, el 86% de los ciberataques fueron motivados por aspectos financieros y el 10% por espionaje (Walter, 2021).

Un dato preocupante es el que presenta la asociación internacional en seguridad de sistemas de información ISSA (*Information Systems Security Association International*), la cual reporta que el 70% de los profesionales en ciberseguridad considera que su organización ha sido impactada debido a la falta de una calificación adecuada del personal de ciberseguridad para el desempeño de sus funciones (Oltsik, 2020).

Por lo que tomando en consideración el contexto en el que vivimos, respecto a la búsqueda de resiliencia mediante el uso de la tecnología y el incremento en ciberriesgos, es necesario asegurar una capacidad de ciberresiliencia demostrada para anticipar, resistir, recuperar y adaptarse ante eventos disruptivos que pongan en riesgo la actividad de las organizaciones en el ciberespacio, tomando en consideración las siguientes características:

- Una organización ciberresiliente asume que el adversario comprometerá o vulnerará sus sistemas en cualquier momento y que dicho adversario mantendrá una presencia en el sistema.

- Enfoca sus esfuerzos de ciberresiliencia en la misión y funciones del negocio, no sólo en aspectos técnicos.

- Se enfoca en los efectos de las amenazas persistentes avanzadas (APTs).

Para lograrlo, las organizaciones deben implementar las soluciones estratégicas, tácticas, operativas y técnicas orientadas a **prevenir o evitar** la ejecución exitosa de un ataque o la materialización de condiciones adversas; **preparar** un conjunto de cursos de acción en caso de que estos eventos se materialicen; asegurar la **continuidad** de la misión y funciones principales del negocio durante la adversidad; **limitar los daños** en la medida de lo posible, privilegiando siempre la vida humana por sobre todas las cosas; **reconstruir** la misión o funcionalidad de negocio tanto como sea posible después de la adversidad; **entender** el estado de los recursos involucrados; **transformar** la misión, funciones y/o procesos con la finalidad de atender los cambios en el ambiente y **rediseñar** arquitecturas para manejar esta y las futuras adversidades.

Finalmente, desde el punto de vista técnico, la atención de los riesgos ha requerido la creación y adopción de nuevas técnicas para mejorar

las prácticas de seguridad de la información y ciberseguridad, de manera de lograr una mayor capacidad de ciberresiliencia.

Algunas de las opciones técnicas que permiten mejorar esta capacidad de ciberresiliencia incluyen, pero no se limitan a la implementación de mecanismos de **monitoreo analítico** de las operaciones a través de sistemas de detección y respuesta que aprovechan los recursos de inteligencia artificial; **respuesta adaptativa** en la infraestructura tecnológica y procesos de operación; **protección coordinada** entre grupos y sectores de industria; mejora de la comunicación para asegurar la **concientización contextual** que involucra conocer el estatus de la situación conforme se va desarrollando entre las partes interesadas; **uso del engaño** como una forma de protección; **diversidad** en la infraestructura tecnológica para evitar que una sola vulnerabilidad pueda existir en todo el sistema de forma simultánea; **posicionamiento dinámico** que dificulte a un posible atacante la identificación de objetivos de ataque y la predicción de la operación; además de reducir la **persistencia** de información buscando que esta se encuentre disponible sólo cuando se requiere y se asegure su resguardo, ocultamiento y/o destrucción una vez aprovechada con fines legítimos (Verizon, 2021).

En conclusión, la ciberresiliencia debe formar parte de la agenda ejecutiva de las organizaciones y su atención requiere implementar modelos de trabajo que consideren, tanto los aspectos estratégicos como los elementos técnicos que sean soportados por una adecuada gestión de ciberriesgos, de acuerdo con el contexto interno y externo propio de cada empresa y en consideración de su rol en la sociedad. Solamente las organizaciones ciberresilientes tendrán la capacidad de sobrevivir y prosperar día con día ante los frecuentes ciberataques y frente al próximo gran evento disruptivo que enfrente la humanidad.

Referencias

Siebel, T. (2019). *Digital Transformation Survive and Thrive in an Era of Mass Extinction*. USA: RosettaBooks.

Roger, D. (2016). *The Digital Transformation Playbook: Rethink Your Business for the Digital Age*. USA: Columbia Business School Publishing.

BSI. (2014). Guidance on organizational resilience. UK: BSI. https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2014/november/Organizational-resilience-standard-published/

Verizon. (2021). Data Breach Investigations Report. USA: Verizon. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

Oltsik, J. (2020). The impact of the COVID-19 Pandemic on Cybersecurity. USA: ESG & ISSA. https://www.issa.org/the-impact-of-the-covid-19-pandemic-on-cybersecurity/

Walter, J. (2021). COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes. https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/

Mario Ureña Cuate. *CISSP, CISA, CISM, CGEIT, CDPSE. Es presidente de la firma de consultoría "Secure Information Technologies", y reconocido especialista en Gestión de Riesgos, Continuidad del Negocio, Seguridad de la Información, Resiliencia Organizacional y Auditoría. Con BSI (British Standards Institution) es instructor certificado y vocero para normas relacionadas con gestión integral de riesgos, continuidad del negocio, resiliencia organizacional y ciberseguridad. Ha participado como miembro de los comités CISA QAT (Quality Assurance Team) y EAC (External Advocacy Committee) de ISACA internacional, participó como miembro del comité de la conferencia internacional de ISACA y de la conferencia latinoamericana de seguridad y administración del riesgo, redactor de preguntas para las certificaciones CISA y CISM y colaborador en el desarrollo del material de estudio para la certificación CISM. Conferencista recurrente en eventos de Gestión de Riesgos, Seguridad de la Información, Auditoría de TI, Gobierno de TI y Resiliencia Organizacional. Participó como jurado para el Premio Nacional de Innovación y Buenas Prácticas en la Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).*