La “falsa sensación de seguridad”

DOI: 10.29236/sistemas.n159a6

El reto de incomodar las certezas de los estándares y tratar de “domesticar” los inciertos.

Resumen
Las prácticas actuales de seguridad/ciberseguridad de las organizaciones modernas han estado fundadas en la aplicación de estándares y buenas prácticas que les han permitido alcanzar importantes niveles de aseguramiento y control en sus procesos e iniciativas de negocio. Sin perjuicio de lo anterior, con un entorno de cambio permanente, de inestabilidades e inciertos políticos, económicos, sociales, tecnológicos y legales que alteran la dinámica de los mercados y las tendencias internacionales, es necesario actualizarlas para habilitar a la empresa para navegar en escenarios de volatilidad e incertidumbre y mantenerla fuera de la zona cómoda y engañosa de la “falsa sensación de seguridad”. En este sentido, este artículo propone algunas estrategias y alternativas para retar las prácticas actuales y habilitar espacios de reflexión desde la resiliencia y la antifragilidad como fundamentos claves para la función de seguridad/ciberseguridad en las organizaciones del siglo XXI.

Palabras clave
Ciberseguridad, estándares, resiliencia, antifragilidad, inseguridad de la información

Introducción

Con el avance acelerado de la puesta en operación de tecnologías emergentes y disruptivas las organizaciones crean escenarios de nuevas experiencias para sus clientes, y al mismo tiempo motivan nuevas zonas grises de seguridad y control que pueden terminar aprovechadas por vulnerabilidades conocidas modificadas y otras emergentes, fruto de la convergencia tecnológica vigente. Esta realidad de conectividad exponencial, revela con mayor claridad el acoplamiento y la interacción que se tienen entre los objetos físicos y las implementaciones lógicas, temáticas que terminan definiendo la dinámica de operación y su confiabilidad (Perrow, 1999).

En este escenario las organizaciones deben comprender que la inevitabilidad de la falla se convierte en el nuevo normal que deben atender y enfrentar comoquiera que una mayor conexión entre los objetos físicos y las implementaciones lógicas, tendrá necesariamente puntos opacos de control, los cuales podrán ser capitalizados por los adversarios ahora o en el futuro. Así las cosas, la mecánica actual de seguridad y control que se funda en riesgos conocidos y métricas específicas, deberán actualizarse para dar cuenta con esta nueva realidad aumentada de "cosas" digitalmente conectadas (Cano, 2021).

Movilizar los esfuerzos corporativos en esta vía descubre algunas tensiones que generan diferencias y lecturas distintas entre los cuerpos de gobierno, los ejecutivos de riesgos y los directivos de seguridad/ciberseguridad, que van desde posturas que acentúan la necesidad de certezas y la productividad de la empresa, hasta las implicaciones claves de eventos adversos y sus impactos para el negocio y sus grupos de interés. En consecuencia, se advierten desencuentros entre la cultura de la productividad y la cultura del aprendizaje, así como asimetrías en la confianza entre las herramientas y las prácticas de seguridad y control.

Lo anterior crea una zona de inestabilidad estratégica que tiene el riesgo inherente de crear en una "falsa sensación de seguridad", la cual termina privilegiando la necesidad de certezas y productividad, para lo cual las inversiones en herramientas tecnológicas terminan siendo la respuesta a los retos de la inevitabilidad de la falla. Por tanto, cuando esto ocurre, la organización se debilita en su postura resiliente frente a los eventos inesperados, reaccionando a estas situaciones de formas no coordinadas, lo que no permite un mayor margen de maniobra por parte de los atacantes que buscan desestabilizar la empresa y sus negocios (Mckinsey-IIF, 2020).

En este sentido, este artículo busca explorar algunos elementos claves de la "falsa sensación de seguridad" con el fin de establecer puntos relevantes que muestren su manifestación e impactos, así como plantear un marco general de apoyo para movilizar a las organizaciones fuera de esa zona "cómoda y engañosa" donde muchas de ellas pueden estar sin percatarse de ello y así, plantear estrategias de resiliencia y antifragilidad que aumenten la capacidad de respuesta y anticipación de las empresas frente a la inevitabilidad de la falla y los adversarios digitales emergentes.

Cultura de productividad y cultura de aprendizaje. Dos mundos convergentes

En el mundo empresarial la necesidad de producir resultados es la norma base para desarrollar cualquier actividad de negocios. En la medida que se puedan superar con celeridad y confianza los retos que la organización requiere para alcanzar sus objetivos estratégicos, podrá avanzar explorando nuevas formas y estrategias que la habiliten para consolidar su posición estratégica en un segmento de mercado.

En esta línea, los ejecutivos de las empresas privilegiarán toda actividad que produzca resultados de forma eficiente y efectiva, manteniendo a la corporación en cumplimiento de las exigencias regulatorias, las indicaciones propias de la auditoría y los mandatos éticos y legales con los que cuente ella cuente. De esta forma, los planes de desarrollo de la organización tomarán forma desde la estructura general del modelo de negocio y las expectativas de los clientes.

Esta forma de operar responde por lo general al modelo de Planear, Hacer, Verificar y Actuar (PHVA) (Ver figura 1), el cual permite asegurar un resultado de forma repetible todo el tiempo. Cuando en la ejecución alguna situación no sale como estaba previsto, se activa el procedimiento de análisis causa-raíz, con el fin de entender, evaluar y cerrar aquello que no corresponde a lo esperado.

Este modelo permite automatizar la producción de los bienes y servicios con la calidad esperada y respondiendo a los estándares de operación que la empresa tiene.

Sin perjuicio de lo anterior, en un escenario cada vez más volátil e incierto, las condiciones cambian y se hace necesario analizar y explorar nuevas oportunidades que se presentan para concretar opciones antes inexistentes. En consecuencia, el modelo PHVA diseñado para entornos ciertos, comienza a ceder terreno para darle paso a una postura renovada que busca conectar los momentos inciertos con ventanas de aprendizaje que habiliten a la organización para repensar sus propios procesos y formas de hacer las cosas (Denyer, 2017).

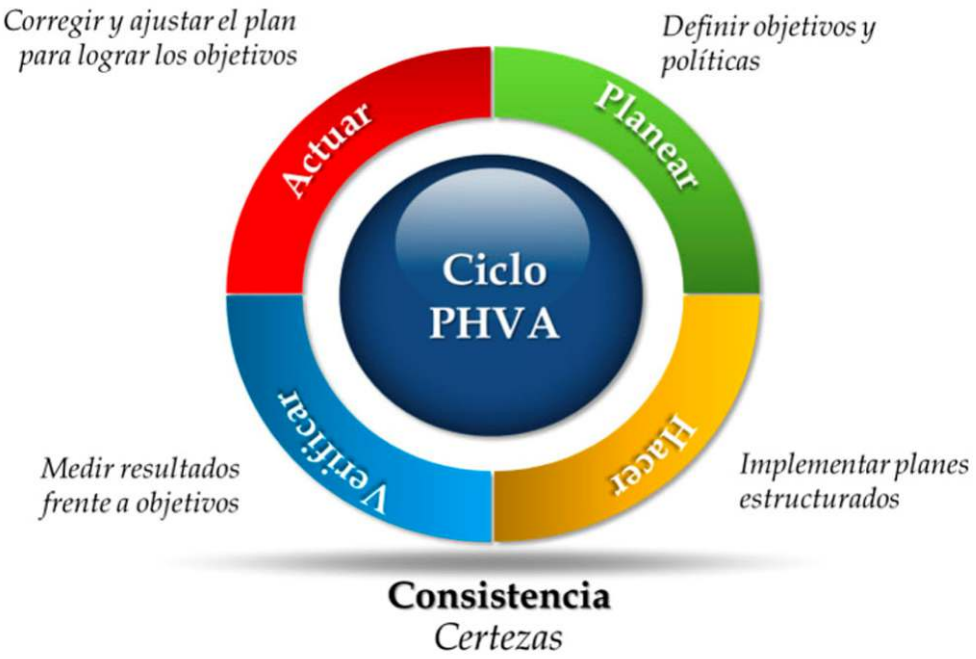

Figura 1. Ciclo PHVA (Elaboración propia con ideas de Denyer, 2017)

Considerando lo anterior se introduce el modelo A2RM (ver figura 2), que se traduce en Arriesgar, Anticipar, Responder y Monitorizar, en el cual se pasa de un PHVA que busca "hacer mejor lo que sabemos hacer", al reto de "hacer mejores cosas". Esta nueva apuesta conceptual busca motivar a la organización a navegar en el incierto, no de cualquier manera, sino declarando su apetito al riesgo (tomar riesgos para crear disrupciones y oportunidades), proponiendo futuros alternos (para anticipar escenarios), interpretando y analizando las tendencias actuales (para responder de forma ágil al presente), y finalmente monitorizando los cambios del entorno (para aprender y ajustarse rápidamente a ellos).

Cuando una empresa adopta el A2RM, se embarca en el reto de construir una cultura de aprendizaje, donde la norma es que se sabe que no se sabe, se duda de las prácticas existentes y se mantiene una curiosidad permanente acerca de nuevas rutinas y propuestas que se pueden intentar. En este contexto, se busca crear una zona psicológicamente segura, donde la idea no es relajar los estándares vigentes, o mantener a las personas en una zona cómoda, o acceder a todas las solicitudes y ser complacientes, sino más bien establecer

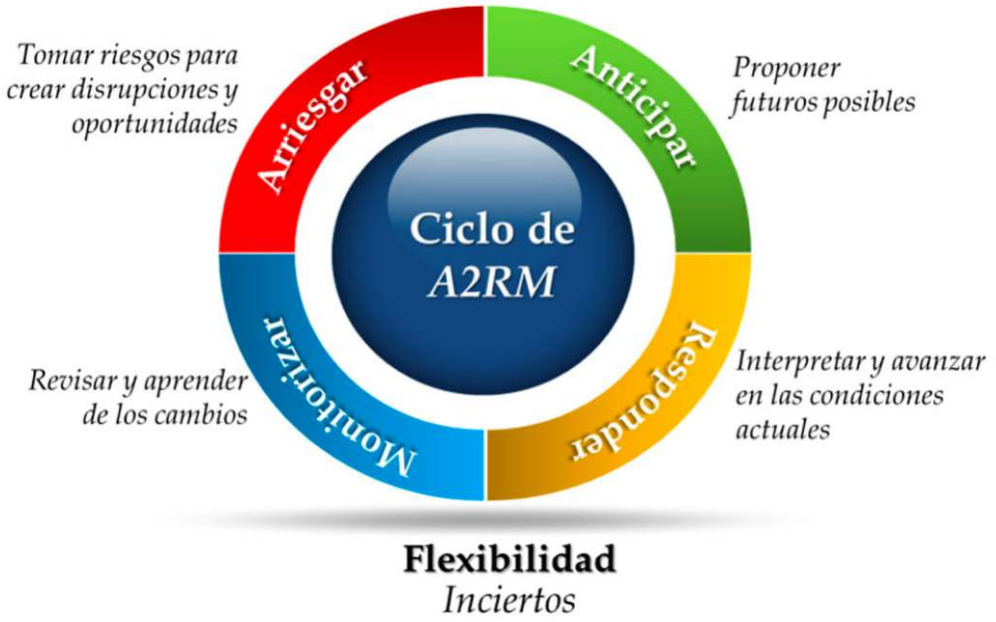

Figura 2. Ciclo A2RM (Elaboración propia con ideas de Denyer, 2017)

un clima de respeto, confianza y apertura donde se pueden poner sobre la mesa las preocupaciones, sugerencias y propuestas sin temor a represalias o juzgamientos (Edmondson, 2018).

Cuando se acentúa la cultura de la productividad o rendimiento, esto es, el énfasis en los resultados medibles, el entorno psicológicamente seguro se deteriora, dado que se advierte la cultura del castigo del "error", lo que necesariamente hace retroceder a las personas para no exponer sus propias capacidades y proteger sus carreras. En la cultura de la productividad se motiva el surgimiento de los expertos los cuales por lo general tienen todas las respuestas, particularmente en aquellas áreas donde no se tiene la competencia particular (Grant, 2021).

Cuando se privilegia una cultura de aprendizaje, los errores se convierten en oportunidades para ver puntos ciegos, comprender el entorno donde ocurren y cómo ocurren, tomando distancia del hecho en sí mismo (De la Torre, 2004). En este entorno de confianza, las personas tienden a revelar aquello que los llevó a esa situación y ubican nuevos puntos del contexto donde es posible ver otros elementos para entender la situación inesperada que se ha verificado. Por tanto, cuando es posible crear equipos

que se enfrentan al reto de “no saber” y tienen dispuesto un escenario psicológicamente seguro para abordarlo, no hay otro resultado de oportunidades para encontrar “feed-forward”, es decir, acciones proactivas, propositivas y centrada en las fortalezas y así, entender que es aquello que se debe dejar de hacer, que es eso que distingue al equipo y qué cosas no se han hecho antes y que es clave desarrollar ahora.

Ciberseguridad: Prácticas y herramientas ¿Cuánto creemos en unas y otras?

Cuando se encuentran las dos culturas la de productividad y la de aprendizaje, es posible encontrar una zona de movimiento que habilite la puesta en marcha de propuestas que terminen aumentando la capacidad de anticipación de la organización. En este sentido, la ciberseguridad debe ubicar esos espacios creados por estas dos culturas con el fin de fundar su nicho de negocio concreto, que permita capitalizar sus iniciativas en favor de la empresa, sus iniciativas innovadoras y sus grupos de interés.

No obstante lo anterior, mantiene un desafío permanente para establecer su marco de referencia y revisión en el contexto ejecutivo de la empresa, toda vez que muchas veces queda atrapada entre las dos culturas, lo que le impide desarrollar prácticas o apuestas resilientes de forma adecuada, dada las exigencias permanentes de resultados concretos, sobremanera por el nivel de inversión que la organización ha hecho particularmente en herramientas tecnológicas.

Así las cosas, el ejecutivo de seguridad/ciberseguridad se encuentra en la encrucijada de saber cuánto confiar en las herramientas tecnológicas que tiene desplegadas y en las prácticas y estándares actualmente utilizados en el desarrollo de la gestión y el gobierno de la seguridad/ciberseguridad. Este sentimiento mantiene en una tensión permanente a este directivo, comoquiera que sabe que en cualquier momento una brecha de seguridad puede ocurrir y traer como consecuencia una inestabilidad para la organización, lo que necesariamente significa que todos los ojos serán puestos en él.

Encontrar el lugar común que permita un postura resiliente para la organización frente a evento inesperados o adversarios emergentes, implica reconocer cuánto se cree en las herramientas (sabiendo que todas tienen vulnerabilidades conocidas y ocultas) y cuánto en las prácticas y estándares vigentes (sabiendo que todas ellas tienen limitaciones) (Abraham, Sims & Gregorio, 2020). Para lograrlo, es necesario que el director de seguridad/ciberseguridad habilite una cultura de aprendizaje fundada en el defender y anticipar, mientras mantiene y valida los riesgos conocidos a través del proteger y asegurar.

Defender y anticipar implica reconocer que siempre el atacante en algún momento tendrá éxito y por lo tanto la organización debe estar preparada, para "ver" cuando esa situación se esté manifestando, para tratar de demorar al adversario y tomar tiempo para la respuesta que se requiere en ese instante (Pillay, 2019).

Esto es, crear una confianza imperfecta que permite una zona de simulaciones y aprendizajes, que rápidamente se incorporan a las prácticas vigentes, y permiten actualizar las amenazas latentes y emergentes de la organización.

Lo anterior exige una postura vigilante que se traduce en algunas preguntas que el equipo de seguridad/ciberseguridad debe hacerse de manera permanente: (Day & Schoemaker, 2019)

Al interior:

- ¿Cómo podemos **mejorar** y **aumentar** la identificación de nuevos patrones de amenazas?
- ¿Qué **más podemos hacer** con nuestras capacidades actuales?
- ¿En **qué somos buenos** actualmente?
- ¿Qué **nuevas capacidades** necesitamos?

Al exterior:

- ¿Cómo han venido **evolucionando** las técnicas y tácticas de los adversarios?
- ¿Qué **adversarios** están anticipando y usando estás nuevas técnicas y tácticas?
- ¿Qué **nuevos ataques** pueden afectar a la organización?
- ¿Cómo nos podemos **anticipar y defender** de los nuevos ataques?

Cuando el equipo de ciberseguridad/seguridad se mantiene en este nivel de reflexión permanente, es capaz de superar la "falsa sensación de seguridad". Esto es, confiar en la capacidad para crear y alcanzar un entorno de operación confiable en el futuro y, al mismo tiempo, enfrentar el reto de la inevitabilidad de la falla y mantener la humildad para cuestionar si se tienen las herramientas y prácticas adecuadas en el presente. Esta duda razonable es lo que habilita una comprensión de las vulnerabilidades, no por su aprovechamiento, sino por la lectura y comprensión de su contexto.

Resiliencia y antifragilidad. Dos conceptos para superar la "falsa sensación de seguridad"

Cuando en el ejercicio de comprensión de una falla de control se concentra la atención en el hecho como tal, olvidando el contexto donde ocurrió, lo más fácil es buscar un culpable, una persona que termina siendo la responsable de un evento (Reason, 2000). Lo que en la lectura tradicional de la seguridad se denomina el eslabón más débil de la cadena, la acción "errada" de un humano al enfrentarse a

una situación conocida o desconocida.

Si en lugar de fijar la mirada en el evento y sus impactos, se toma distancia y se visualiza el contexto en el cual ocurrieron los eventos, las situaciones circundantes, las relaciones visibles e invisibles que se manifestaron, es posible comprender mejor por qué el evento sucedió, y cómo podemos hacer más resistente el sistema en una siguiente ocasión. Esto implica desarrollar umbrales de operación, tolerancia y capacidad de riesgo que buscan aumentar la resiliencia del sistema que se modela o analiza (Woods, Dekker, Cook, Johannesen & Sarter, 2010).

De acuerdo con documentos recientes del NIST existen algunas definiciones de resiliencia que se mencionan a continuación:

- D1 - La capacidad de un sistema de información para continuar: (i) operando en condiciones adversas o de estrés, incluso si se encuentra en un estado degradado o debilitado, manteniendo las capacidades operativas esenciales; y (ii) recuperarse a una postura operativa efectiva en un marco de tiempo consistente con las necesidades de la misión (NIST SP 800-39).
- D2 - La capacidad de un sistema de información para continuar operando mientras es atacado, incluso si se encuentra en un estado degradado o debilitado, y recuperar rápidamente sus capacidades operativas para las funciones esenciales después de un ataque exitoso (NIST SP 800-30 Rev. 1).
- D3 - La capacidad de adaptarse y recuperarse rápidamente de cualquier cambio conocido o desconocido en el entorno a través de la aplicación holística de la gestión de riesgos, la contingencia y la planificación de la continuidad (NIST SP 800-34 Rev. 1).

Estas tres definiciones hablan de palabras claves que se deben tener en cuenta al hablar de atender eventos adversos, ataques o cambios conocidos o desconocidos: (Clédel, Cuppens, Cuppens & Dagnas, 2020)

- *Capacidad* – Desarrollo de patrones de aprendizaje frente a eventos inciertos.
- *Adaptación* – Ajuste de prácticas y actualización de saberes previos frente a eventos inesperados.
- *Recuperación* – Volver a poner al servicio un sistema o proceso luego de haberse materializado una situación o condición no prevista.

Son estas tres palabras las que se requieren comprender en profundidad para mantener una postura atenta, vigilante y de aprendizaje permanente con el fin de preparar a la organización para atender situaciones de tensión que pueda sugerir cualquier agente externo o interno. En la medida que se cuente con

una postura de falla segura, que es aquella que se dispara cuando los umbrales previstos de operación se superan, los sistemas de información, podrán mantener niveles funcionamiento que les permita aumentar su capacidad para atender condiciones no estándar, adaptarse rápidamente mientras se opera con los mínimos y sobretodo, aprender lo ocurrido para recuperarse de forma eficiente y en condiciones mejoradas (Australian Government, 2011).

Lo que inicialmente se conocía de la realidad de los riesgos empresariales, se desdibuja rápidamente hoy, dejando de lado las certezas, para darle paso a la incertidumbre, como el nuevo insumo de las estrategias corporativas, donde se introduce la "idea peligrosa" de la "antifragilidad" (Taleb, 2013) como ese proceso de entender y alimentarse de la aleatoriedad, el azar, los errores y las fallas como forma de fortalecer una posición en el entorno de negocios y sobrevivir aún las amenazas se materialicen en el ejercicio y aplicación de su modelo de generación de valor.

La antifragilidad consiste entonces en navegar en los eventos inesperados, con el fin de "domesticar" la incertidumbre, lo que se traduce en: "reducir los riesgos perjudiciales y mantener el beneficio de las posibles ganancias" (Idem, pág. 214), un ejercicio retador de aprendizaje permanente, que invita a las organizaciones y los responsables de seguridad/ciberseguridad a elaborar un modelo de seguridad y control, basado en el reconocimiento del incierto como base, esto es en el azar, los errores, la imprevisibilidad, los comportamientos no lineales y manejar los impactos de la combinación de éstos, para alimentar la curiosidad, la capacidad de aprendizaje y resistencia del modelo, que claramente será contrario a lo que espera un ejecutivo de alto nivel de una empresa.

En este sentido la condición antifrágil que debe asumir la función de seguridad/ciberseguridad en las organizaciones modernas, es aquella que incorpora la inevitabilidad de la falla como parte natural de las prácticas de defensa y anticipación, que promueve la generación de escenarios de riesgo como parte se preparación y gestión, y que se prepara para superar las situaciones críticas e inesperadas incorporando la resiliencia como parte fundamental de su acción y operación (Weick & Sutcliffe, 2007).

Cuando convergen la postura antifrágil y las capacidades resilientes, el ejecutivo de seguridad/ciberseguridad no tendrá que decidir en qué confiar (prácticas o herramientas), sino que mantiene una dinámica de reto permanente sobre ambas cosas, que le permite desarrollar una competencia que lo mantiene fuera de la zona cómoda, sin experimentar superávit de futuro ni déficit de presente, sino navegando en medio de aguas profundas ab-

sorbiendo nuevas ideas, actualizando las vigentes y sobremanera experimentando para sorprender al adversario en su mismo terreno (Bodeau, Graubart, Heinbockel & Laderman, 2015).

Marco general para superar la "falsa sensación de seguridad". Algunas reflexiones

Con el fin de mantener a las organizaciones fuera de la zona cómoda de la "falsa sensación de seguridad", es necesario actualizar la mentalidad vigente de los estándares y las certezas, que es propia de la cultura de la productividad, por una que se sienta cómoda con la vulnerabilidad, con la ambigüedad y aceptar que "no sabe", y lo más importante abierta a los errores, que es propia de la cultura de aprendizaje.

Para ello, es necesario introducir el modelo A2RM: Arriesgar, Anticipar, Responder y Monitorizar, como base del nuevo modelo de gestión y desarrollo de la organización, y particularmente del área de seguridad/ciberseguridad. Lo anterior implica desarrollar una mentalidad de aprendizaje ágil que busca aumentar la colaboración, mejorar y habilitar ciclos de aprendizaje, focalizarse en la entrega de valor y la habilidad para adaptarse al cambio.

Esta mentalidad tiene como base cuatro elementos claves: (McGowan & Shipley, 2020)

- *Agencia* – Capacidad de actuar de forma independiente y hacer elecciones por sí mismo. Donde el aprendizaje es una responsabilidad propia de cada individuo.
- *Agilidad* – Es la habilidad para aprender y desaprender. Es el ejercicio de tomar nueva información, crear nuevo conocimiento y lanzarse a cambiar aquello que requiere actualizarse.
- *Adaptabilidad* – Capacidad para navegar en situaciones ambiguas y asumir los retos aun cuando no toda la información es clara o conocida. Esto es, desaprender lo conocido, diseñar una nueva propuesta, conectar los nuevos puntos y cambiar la lectura actual.
- *Atención* – Entender las acciones conscientes que cada persona hace, que definen su identidad para darle sentido a sus aportes en un contexto individual y empresarial.

En segundo lugar, comprender que la viabilidad de la práctica de seguridad/ciberseguridad "no es solamente mitigar los riesgos, ni evitarlos (si eso es viable), sino avanzar en la comprensión del entorno, profundizar en la construcción de confianza, concretar la identificación de las incertidumbres claves que afecten el negocio y desarrollar la capacidad de respuesta frente a un incidente" (Cano, 2020). En este sentido, se hace necesario conectar tres ciclos de operación que vinculan tanto la cultura de productividad como la de aprendizaje: el ciclo de regulación (productividad y aseguramiento de lo conocido), el ciclo

de adaptación (prospectiva y tendencias identificadas) y el ciclo de memoria y aprendizaje (sinergia que se genera al interior de la dinámica empresarial que habilita un aprendizaje colaborativo, para construir y conectar puntos aparentemente sueltos en el engranaje empresarial) (Cano, 2020).

En tercer lugar, entender que la ciberseguridad/seguridad es un "deporte colectivo" y de "contacto", por lo tanto se hace necesario mantener una cultura de aprendizaje que todo el tiempo rete y confronte las buenas prácticas, configure un entorno psicológicamente seguro para preguntar, tensionar y desafiar el statu quo de la dinámica de la ciberseguridad/seguridad, y defina zonas y lugares para desarrollar experimentos inteligentes, que permitan concretar cada vez más errores brillantes, que son aquellos que en los que se invierte poco y se obtiene mucho beneficio (Hepfer & Powell, 2020).

Estas tres condiciones básicas a nivel de gestión, a nivel individual y a nivel funcional, se convierten en la base para movilizar los esfuerzos del área de seguridad/ciberseguridad fuera de la zona cómoda de la "falsa sensación de seguridad", lo que implica una transformación de la dinámica de un concepto inicialmente estático y conocido, por uno que evoluciona, que es cambiante y se reinventa conforme los retos del entorno le plantean nuevas propuestas.

Reflexiones finales

Estudios recientes indican que mientras la tecnología crece exponencialmente la productividad de los negocios lo hace de forma lineal, lo que genera una brecha de adaptación, que de alguna forma define el potencial que tienen las empresas para lograr y cambiar la forma de hacer las cosas, lo que se traduce en nuevas oportunidades de negocio (McGowan & Shipley, 2020).

De igual forma ocurre con la seguridad/ciberseguridad, mientras crece y avanza rápidamente la capacidad de los adversarios para sorprender a las organizaciones con diferentes apuestas y estrategias novedosas, la respuesta de las áreas de seguridad y control se hace de forma más lenta y con dificultades para atender a los retos inciertos que los atacantes plantean (Pillay, 2019). Esto define una brecha de adaptación y aprendizaje, que tienen éstas áreas como una oportunidad para repensar lo que conocen y expandir sus reflexiones más allá de los estándares y buenas prácticas.

En este sentido, superar la "falsa sensación de seguridad" crea la crisis necesaria en los modelos de seguridad y control vigentes, que permite incomodar los saberes previos y romper la vitrina de los logros alcanzados, para entender la ciberseguridad/seguridad como un proceso inacabado que no termina con las métricas de efectividad de los

controles para los riesgos conocidos, sino que es parte de la ruta del nuevo territorio que se crea y actualiza con una mayor conectividad, acoplamiento e interacción de objetos conectados fruto del incremento de la densidad digital.

Este nuevo referente digital hace evidente que la seguridad/ciberseguridad sea un ejercicio de confianza imperfecta, donde tanto los clientes, como los objetos conectados y los servicios implementados, podrán tener puntos ciegos de seguridad y control, que tarde o temprano serán aprovechados por los adversarios.

En consecuencia, se hace necesario establecer las bases de una relación resiliente entre los diferentes participantes, para diseñar un entorno de operación basado de umbrales, tolerancias y capacidades que permitan actuar de forma coordinada cuando las cosas no salen como estaban planeadas (Fiskel, 2015).

Así las cosas, tanto la cultura de productividad como la de aprendizaje tendrán que converger para habilitar los nuevos espacios de cooperación, colaboración y coordinación para absorber la complejidad y la incertidumbre que puede generar la materialización de una brecha de seguridad/ciberseguridad, comoquiera que sus impactos van más allá del evento mismo, y revelan la característica sistémica del riesgo cibernético: se conoce dónde inicia la acción pero no dónde termina o cómo se propagan sus efectos.

Superar la "falsa sensación de seguridad" deberá ser el mantra permanente de los ejecutivos de seguridad/ciberseguridad, así como la motivación para mantener una conversación estratégica con los consejos de administración o junta directivas en términos de la resiliencia del negocio y la manera de asumir la antifragilidad como fundamento de unas relaciones simétricas, transparentes y reciprocidad con los diferentes grupos de interés, para así, capitalizar una postura vigilante que desequilibre e interrogue los planes de los atacantes en sus mismos fundamentos: incertidumbre, volatilidad y ambigüedad.

Referencias

Abraham, C., Sims, R. & Gregorio, T. (2020). Develop Your Cyber Resilience Plan. Sloan Management Review. https://sloanreview.mit.edu/article/develop-your-cyber-resilience-plan/

Australian Government (2011). Organisational resilience. Position paper for critical infrastructure. De: https://www.organisationalresilience.gov.au/Documents/organisational-resilience-position-paper-for-critical-infrastructure-australian-case-studies.pdf

Bodeau, D., Graubart, R., Heinbockel, W. & Laderman, E. (2015). Cyber

Resiliency Engineering Aid –The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques. MITRE Corporation. De: https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf

Cano, J. (2020). Repensando la práctica de la seguridad y la ciberseguridad en las organizaciones. Una revisión sistémico-cibernética. Global Strategy. Global Strategy Report 58. https://global-strategy.org/repensando-la-practica-de-la-seguridad-y-la-ciberseguridad-en-las-organizaciones-una-revision-sistemico-cibernetica/

Cano, J. (2021). Ciberseguridad empresarial. Reflexiones y retos para los ejecutivos del siglo XXI. Bogotá, Colombia: Lemoine Editores.

Clédel T., Cuppens N., Cuppens, F. & Dagnas R. (2020). Resilience properties and metrics: how far have we gone? Journal of Surveillance, Security and Safety. 1. 119-139. http://dx.doi.org/10.20517/jsss.2020.08

Day, G & Schoemaker, P. (2019). See soon, act faster. How vigilant leader thrive in an era of digital turbulence. Cambridge, MA. USA: MIT Press

De la Torre, S. (2004). Aprender de los errores. El tratamiento didáctico de los errores como estrategia de innovación. Buenos Aires, Argentina: Editorial Magisterio del Río de la Plata.

Denyer, D. (2017). Organizational resilience. A summary of academic evidence, business insights and new thinking. BSI-Crandfield University. De: https://www.cranfield.ac.uk/som/case-studies/organizational-resilience-a-summary-of-academic-evidence-business-insights-and-new-thinking

Edmondson, A. (2018). The fearles organization. Creating psychological safety in the workplace for learning, innovation, and growth. Hoboken, New Jersey. USA: John Wiley & Sons

Fiskel, J. (2015). Resilient by design. Creating Businesses That Adapt and Flourish in a Changing World. Washington, D.C., USA: Island Press

Grant, A. (2021). Think again. The power of knowing what you don't know. New York, USA: Viking.

Hepfer, M. & Powell, T. (2020). Make Cybersecurity a Strategic Asset. Sloan Management Review. 62(1). 40-45.

McGowan, H. & Shipley, C. (2020). The adaptation advantage. Hoboken, NJ. USA: John Wiley & Son

Mckinsey-IIF (2020). Cyber Resilience Survey. Cybersecurity posture of the financial services industry. https://www.iif.com/Portals/0/Files/content/cyber_resilience_survey_3.20.2020_print.pdf

Perrow, C. (1999). Normal accidents. Living with High-Risk Technologies. Princeton, NJ. USA: Princeton University Press.

Pillay, R. (2019). Learn penetration testing. Understand the art of penetration testing and develop your white hat hacker skills. Birmingham, UK:Packt Publishing Ltd

Reason, J. (2000). Human error: models and management. BMJ. 320-768 doi:10.1136/bmj.320.7237.768

Taleb, N. (2013). Antifrágil. Las cosas que se benefician del desorden. Barcelona, España: Paidos

Weick, K. & Sutcliffe, K. (2007). Managing the Unexpected. Resilient Performance in an Age of Uncertainty. Second Edition. San Francisco, CA. USA: Jossey-Bass

Woods, D., Dekker, S., Cook, R., Johannesen, L. & Sarter, N. (2010). Behind human error. Second Edition. Farnham, Surrey. England: Ashgate Publishing Limited

***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–.*