Repensando la efectividad de los controles en la era digital

En medio de una turbulencia geopolítica, de intereses y confrontaciones nacionales e internacionales, las organizaciones deben establecer movilizar sus esfuerzos para mantener la dinámica de su negocio y detallar una carta de navegación que defina algunos puntos de interés para avanzar en medio de las inestabilidades y así establecer una postura estratégica de mediano y largo plazo[1]. En este sentido, la práctica de aseguramiento de controles, se advierte como uno de los elementos claves para continuar sus operaciones y mantener la dinámica organizacional frente a eventos adversos conocidos y latentes que se puedan presentar.

La práctica general de aseguramiento de los controles establece su efectividad en la medida que se encuentren bien definidos, respondan al riesgo que quieren mitigar y se ejecuten en tiempo y forma de acuerdo a lo que se requiere, esto es con oportunidad. Esta efectividad tradicional, habitualmente validada por ejercicios de medición sobre los elementos previamente mencionados, generan resultados que son insumos para establecer el nivel confianza que se tiene en el cierre de brechas de riesgo que se han identificado en las diferentes esferas de las organización, con particular énfasis en los temas operativos y transaccionales[2].

En un escenario como el actual, donde se identifica una mayor densidad digital, esto es, un incremento de conectividad y flujos de información de los objetos físicos, así como una relación interdependiente de acoplamiento e interacción entre estos, se revelan nuevas amenazas y retos emergentes que posiblemente están más allá de los riesgos conocidos de tecnología de información (TI). Esta realidad digitalmente modificada, manifiesta la aparición de un riesgo emergente, sistémico y disruptivo como lo es el riesgo cibernético, que no corresponde con las prácticas y controles de TI, y por tanto, requiere un enfoque y tratamiento complementario y renovado[3, 4].

Por tanto, comprender la efectividad de los controles en un ambiente hiperconectado y "cosas conectadas", exige ajustar la aproximación natural y tradicional basada en los estándares y medidas de seguridad conocidas, con conceptos nacidos en el área industrial como son confiabilidad, calibración y mantenimiento, los cuales hablan de una tarea de adaptación y actualización periódica que reconoce los cambios, las nuevas tendencias y la transformación del escenario de las operaciones de las organizaciones[5]. Lo anterior, supone un cambio de perspectiva frente a la seguridad y el control, pasar de una visión estática, definida y conocida, a una visión dinámica, cambiante y muchas veces desconocida.

Con esta postura enriquecida de la efectividad de los controles, estos pasan de ser objetos o elementos de una única definición y monitoreo periódico,

JEIMY J. CANO M. | PH.D., ED.D., CFE, CICA

Tiene más de 25 años de experiencia como ejecutivo, académico y profesional en seguridad de la información, ciberseguridad, informática forense, crimen digital y auditoría de TI. En 2016, fue nombrado Educador de Ciberseguridad del Año para América Latina, y en 2022, fue nombrado Personalidad de Resiliencia para América Latina. Ha publicado más de 200 artículos en diversas revistas y ha presentado ponencias en eventos del sector a nivel internacional.

al reconocimiento de éstos como sensores que adicionalmente a las definiciones básicas que se requieren, basadas en el entorno de negocios y sus relaciones, se hace necesario validar su confiabilidad, su calibración y asegurar su mantenimiento periódico, con el fin de ajustar sus mediciones a las nuevas condiciones del entorno, que posiblemente no sean equivalentes a las circunstancias de tiempo, modo y lugar en el que se hizo por primera vez su definición.

Por lo tanto, es importante comprender la evolución de la noción de control, sus fundamentos conceptuales y la transformación que viene afrontando la medición de su efectividad por cuenta de la acelerada dinámica digital, que si bien abre nuevas posibilidades y experiencias distintas para los clientes, igualmente genera tensiones y amenazas que pueden terminar comprometiendo la promesa de valor de la compañía.

Fundamentos del concepto de control

Entender el concepto de control implica reconocer que en la naturaleza existen diferentes formas a través de la cual se mantiene un equilibrio dinámico, esto es, un balance situado y contextual que responde a las inestabilidades que se presentan, con el fin de encontrar un lugar común de operación que encuadra y conecta con los otros componentes del ecosistema analizado. En este contexto, sin importar el tipo de control específico existen cuatro elementos comunes y fundamentales en todos los sistemas de control, que se detallarán a continuación[6]:

1. Las características medibles y controlables, de las cuales se conocen los estándares que las orientan
2. El sensor como dispositivo que habilita la medición de la característica
3. El comparador quien efectúa la discriminación entre los datos entregados por el sensor y los estándares conocidos para las características establecidas
4. El ejecutor que es el medio para efectuar los cambios en el sistema, con el fin de ajustar las características pertinentes

Por tanto, establecer la distinción de un estado "controlado" o "fuera de control" dependerá directamente de la evaluación de los resultados por parte el ejecutor. Esto es, es el ejecutor quien toma las decisiones, evalúa las alternativas de acción basado en las desviaciones o diferencias entregadas por el comparador y valora los beneficios de llevar nuevamente al sistema a un estado de "control" frente a las acciones correctivas que se deban implementar.

Las conclusiones sobre el estado final "controlado o no controlado" estarán basadas en algunas consideraciones a tener en cuenta:

- El detalle que se tenga de las características a evaluar y sus estándares, los cuales deberán ser conocidos y validados previamente con el fin de mantener el sistema lo más cercano posible a esta especificaciones
- La calibración periódica del sensor que permita identificar variaciones frente al estándar determinado
- La confiabilidad del comparador para establecer la discriminación de los datos recogidos por el sensor y los estándares conocidos
- La visión y el contexto del ejecutor para adelantar la interpretación de los resultados y proceder con la toma de decisiones

Así las cosas, la distinción de control está orientada a regular, disminuir y evitar cualquier condición adversa que pueda atentar contra la especificación inicial del sistema y los estándares que lo gobiernan. En este sentido, el control busca disminuir el incierto que se pueda generar en la operación del sistema, lo que implica necesariamente ignorar o reportar cualquier condición que no esté dentro de las especificaciones que tiene el comparador, y de esta manera, informar al ejecutor para que tome las acciones del caso[7].

Para lograr el estado de control deseado en el sistema, el concepto clave que se implementa es la retroalimentación, como el proceso que tomando el resultado de la ejecución del sistema y luego de su evaluación, es capaz de incorporar nuevos datos para ajustar su comportamiento. En la medida que la retroalimentación sea eficiente (oportuna) y con datos confiables, la ejecución del proceso tomará los rumbos deseados y se buscará que se desarrolle dentro de los parámetros previamente definidos y conocidos[8].

El concepto de control desde la cibernética: regulación y adaptación

La cibernética es la ciencia de la comunicación y el control en los seres vivos y artificiales[9]. El uso de los

fundamentos de la cibernética y de los conceptos de variedad requerida, junto con los aportes del funcionamiento del sistema nervioso humano permitió a Stafford Beer desarrollar el concepto de cibernética organizacional como la ciencia de la organización efectiva[10].

Beer propone el modelo de sistema viable como base para el desarrollo de la cibernética organizacional, que establece dos ciclos fundamentales para lograr la viabilidad de las organizaciones: el ciclo de regulación y el ciclo de adaptación. Mientras que el ciclo de regulación se asocia a la dinámica natural y general de las organizaciones que busca asegurar su funcionamiento con base en las buenas prácticas y la coordinación de actividades, el ciclo de adaptación busca desafiar la dinámica existente explorando el entorno e identificando las tendencias emergentes[11].

La variedad, que se define como el conjunto de estados identificables que un sistema puede tomar. Así las cosas, un sistema que exhiba muchas interrelaciones y acoplamientos entre sus componentes no sólo podrá tener múltiples estados identificables, sino momentos no identificables que lo lleven a estados que estén por fuera de las especificaciones inicialmente establecidas, los cuales podrán ser catalogados como positivos o no, de acuerdo con las expectativas, propósitos y lecturas de aquellos que lo ha diseñado y sus relaciones con el contexto[12].

Según los clásicos cibernéticos existen al menos tres formas que un sistema puede usar para establecer sus necesidades de variedad:

- puede *amplificar* su propia variedad,
- *mantener* una variedad equivalente a la del sistema controlado, o
- *reducir* la variedad del sistema controlado más que reducir la propia[13].

En este sentido, la distinción de control va más allá de la lectura reduccionista de la operación para lograr cumplir un estándar. Lo anterior implica que los sistemas son viables (permanecen en el tiempo) en la medida que pueden mantenerse por sí mismos independientemente del medio. Esto es, tienen la capacidad para responder no sólo a las inestabilidades conocidas, sino manifestarse y avanzar en medio de situaciones fortuitas, inesperadas o desconocidas, lo que exige la disposición del sistema para adaptarse a los entornos cambiantes. Para lograrlo, deben mantener un balance de amplificación y atenuación de la variedad que reconoce la dinámica propia de la organización y sus umbrales de operación, así como los retos que propone el entorno que son relevantes para permanecer en el largo plazo[14].

Luego la distinción de control desde la lectura de la cibernética, no solo asegura el funcionamiento del sistema dentro de los estándares definidos (ciclo de regulación), sino que establece mecanismos para aumentar la variedad del sistema, explorando e identificando condiciones novedosas e inciertas del entorno (ciclo de adaptación), que son relevantes para la su supervivencia, lo que implica una actualización de los referentes iniciales y por tanto, de las características básicas a controlar, las cuales deben llevar a los ajustes necesarios tanto en el sensor, el comparador, así como en los criterios de ejecutor, donde finalmente se hace realidad el estado del control[15].

Es importante anotar que cualquier variedad residual que no sea asimilada por las respuestas del entorno, debe ser asumida por el sistema, pues de no hacerlo corre el riesgo de crear puntos de inestabilidad y comprometer su supervivencia en el mediano y largo plazo, por cuenta de la inevitabilidad de la falla.

La efectividad del control. Más allá de los estándares y buenas prácticas

La perspectiva de la definición y operación de los controles en el contexto organizacional ha venido evolucionando por cuenta de un entorno cada vez más FANI, acrónimo introducido en 2021 por el Instituto para el Futuro que traduce fragilidad (asociada con la vulnerabilidad), ansiedad (creada por la incertidumbre), no linealidad (derivada de la complejidad) e incomprensibilidad (fruto de la ambigüedad)[16]. En este contexto, los controles tradicionales entran en crisis dada su marcada visión estática basada en prácticas y estándares que responden situaciones conocidas, así como una operación fundada en reducción de inciertos para asegurar una adecuada toma de decisiones.

Comprender la efectividad de los controles en un escenario como el actual, no sólo es asegurar que se cumplen ciertas condiciones que se detallan en los marcos conocidos, sino mantener actualizado el sensor inherente al control de acuerdo con las

variaciones e inestabilidades que pueda identificar en su entorno. Así las cosas, la efectividad del control en un mundo más FANI, implica:

- Comprender la dinámica propia de la organización y sus propósitos.
- Entender la dinámica del entorno.
- Contribuir a la disminución del riesgo que cubre.
- Calibrar los sensores de acuerdo con el uso y ajustes propios de la dinámica de la organización y su entorno.
- Identificar los cambios relevantes del entorno.

La **figura 1** ilustra la efectividad del control en un escenario cambiante.

Se parte de la dinámica de la organización donde se establecen los modelos base y las características que se quieren comparar y medir. Este ejercicio inicial define la confiabilidad del modelo que se quiere implementar, lo implica cuestionar si el estándar base definido se ajusta a la dinámica y retos de la organización. Luego, se despliegan los mecanismos de control en los lugares y plataformas establecidas en la empresa, como pueden ser los sistemas de información, sistemas de control industrial, o cualquier estrategia automatizada que se tenga. En este punto, la pregunta que se hace es si éstos se activan correctamente, es decir son consistentes con la condiciones establecidas y reportan las alertas previstas cuando un evento ocurre por fuera de los estándares definidos.

Surtidas estas dos primeras fases, viene la dinámica propia de la operación y funcionamiento del control donde es necesario entrar a detallar el comportamiento tanto de las personas como de los objetos sobre los cuales se han definido los mecanismos de control, para preguntar sobre su uso (funciona como es debido), que ajustes se deben hacer basado en su funcionamiento y que otras tendencias se pueden ver al integrarse con otras plataformas. Esta fase, debe generar la información suficiente para calibrar el control y actualizar los modelos base previamente definidos en su diseño.

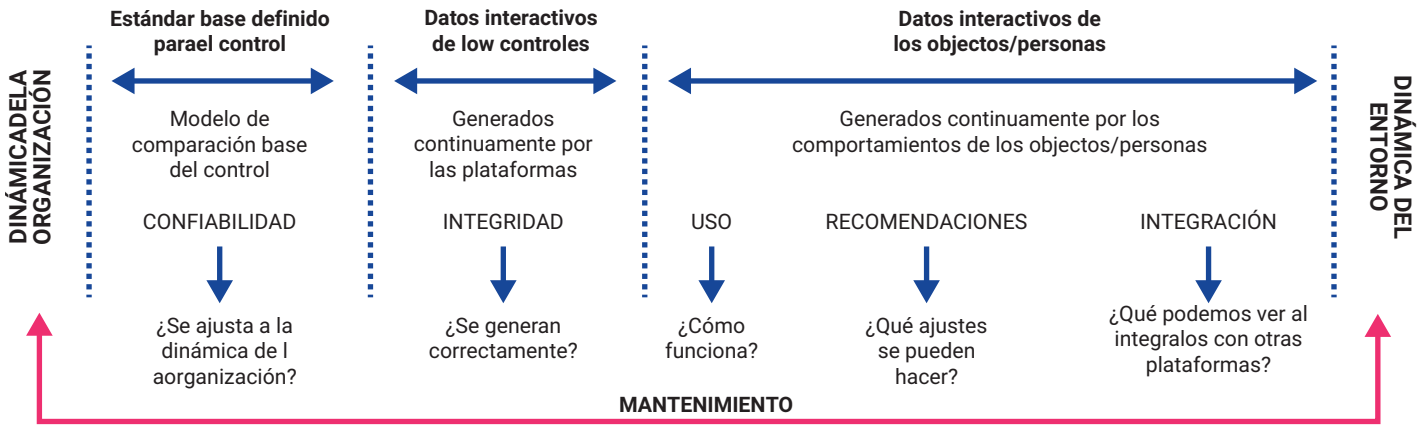
Finalmente, se hace necesario leer, analizar y explorar las nuevas tendencias y señales débiles que se advierten en la dinámica del entorno, con el fin de efectuar un mantenimiento y actualización de la dinámica organizacional, el cual demanda amplificar la variedad para asegurar la viabilidad de la empresa en el mediano y largo plazo[17].

La inevitabilidad de los fallos de control de la ciberseguridad

Los controles que en la actualidad se definen en el escenario de la seguridad de la información y la ciberseguridad, muchos de ellos responden a una perspectiva de atenuación de la variedad, que buscan encontrar certezas y tratar de eliminar los inciertos, como fundamento de su efectividad. En esta línea, se generan reportes ejecutivos donde se informan sobre la identificación y contención de riesgos conocidos como una forma de indicar que la medidas implementadas responden a la dinámica del entorno de la empresa, lo cual puede llevar a una falsa sensación de seguridad por excesiva confianza en los estándares y las herramientas tecnológicas[18].

FIGURA 1

Comprensión de la efectividad del control en contextos dinámicos (Elaboración propia)



Los controles desde la perspectiva de la seguridad/ciberseguridad lo que buscan es demorar, disuadir o confundir al posible adversario. Son mecanismos, que deben todo el tiempo validar y reconocer patrones emergentes en el entorno basado no sólo en el comportamiento de la infraestructura y las personas, sino en las condiciones de tiempo, modo, lugar y contexto en el cual ocurren los eventos. Lo anterior, supone una calibración permanente del modelo base, el cual debe aprender y correlacionar de forma permanente eventos para establecer señales débiles, que pueden terminar en alertas tempranas[19].

Así las cosas, el concepto de control en seguridad/ciberseguridad exige un balance permanente entre atenuación de la variedad (reportes y alertas conocidas) con una amplificación basada en patrones de eventos novedosos, situaciones inesperadas y sorpresas, los cuales deben articularse en el diseño de escenarios retadores y emergentes que permitan actualizar la dinámica de protección definida por la organización. En consecuencia, las posibles vulnerabilidades vigentes detectadas y no detectadas se convierten en insumos básicos para crear una cultura de aprendizaje y flexibilidad requerida frente a la inevitabilidad de la falla.

Cuando se materializa un riesgo cibernético o se genera una brecha de seguridad, lo que supone la "falla" de un control, se advierte en el marco de los estándares tradicionales un control inefectivo. Esto es, un resultado que termina con una afectación no deseada por la empresa que tiene implicaciones mayores o menores dependiendo de la sensibilidad del proceso y su información. Comprender la efectividad de esta manera, es volver al modelo operacional básico y mecanicista del control, donde el error es un resultado y no parte del proceso[20].

Nada más natural en el escenario que se vive en la actualidad que se materialice una brecha de seguridad o una falla por cuenta bien de una vulnerabilidad, por un comportamiento o por evento inesperado y no previsto fruto de la dinámica digital. Por tanto, la efectividad del control no debe estar ligada a la reducción del incierto, sino a la capacidad de poder mantener alertas y acciones concretas sobre los riesgos conocidos, y desarrollar escenarios y pronósticos de patrones y señales de riesgos latentes y emergentes, con el fin de mantener una postura vigilante para la organización, que cuestiona y valida todo el tiempo lo que tiene, fortaleciendo su práctica y su músculo resiliente desde las simulaciones y los prototipos[21].

La efectividad de los controles en la práctica de seguridad y la ciberseguridad se deberá medir desde la capacidad de aprendizaje que estos pueden desarrollar de cara al reto del entorno de inestabilidad donde opera la organización, no como un referente técnico aislado de la dinámica del negocio, sino como una lectura interdisciplinar que acompaña los procesos de la empresa para descubrir y advertir eventos inesperados y adversos (que revelan puntos ciegos en el modelo de seguridad y control vigentes), para desarrollar posturas vigilantes, ágiles y flexibles que se ajustan a los umbrales de operación de la compañía, aún cuando se ha materializado una amenaza[22].

Conclusiones

El mundo actual atraviesa una tormenta de cambios y tensiones que crean una zona de inestabilidad permanente que reta los más elaborados y sofisticados sistemas de control y gestión de las organizaciones. En este sentido, comprender y evaluar la efectividad de los controles establece un desafío de incertidumbre y complejidad, que exige desarrollar capacidades de aprendizaje/desaprendizaje que implican reducir la variedad de los riesgos conocidos y amplificar aquellos patrones de los riesgos latentes y emergentes, con el fin de tomar acciones y posturas flexibles y ágiles acordes con los umbrales de operación de las organizaciones[23].

La vista del control como solo una lectura de reducción de inciertos basada en buenas prácticas aumenta las zonas de opacidades en los modelos de seguridad y control, comoquiera que todo aquello que no sea reconocido por los estándares definidos puede ser ignorado, generando una falsa sensación de seguridad que puede ser aprovechada por los adversarios y eventos inesperados, dada la característica natural de la materialización del riesgo cibernético como lo es sus efectos en cascada: se conoce donde inicia pero no donde pueden terminar[24].

Ahora bien entender el control desde la perspectiva cibernética, como un balance entre amplificación y reducción de la variedad expande las fronteras de las definiciones de los controles para habilitarlos como elementos con dinámica propia y ajustes permanentes que buscan adaptarse para dar

cuenta con la variedad relevante para organización y su permanencia en el largo plazo[25]. De esta manera, la efectividad del control busca encontrar nuevos puntos de estabilidad en la dinámica de la organización y el entorno de tal forma que se identifiquen puntos de equilibrio dinámico que cambian a lo largo del tiempo, y preparan a la organización para responder y movilizarse en medio de tensiones e inestabilidades que se presenten.

Con estos análisis de fondo, los controles de seguridad y ciberseguridad deberán seguir la comprensión propuesta de la efectividad del control en contextos dinámicos que exige reconocer y validar la confiabilidad e integridad de las plataformas que materializan dichos controles, así mismo generar la calibración necesaria basado en el uso, ajustes e integración con otros sistemas, y finalmente configurar una estrategia de mantenimiento que consultando la dinámica del entorno pueda aprender/desprender rápidamente, para ajustar (en la medida de los posible en tiempo real) los estándares y modelos base sobre el cual genera sus alertas tempranas y patrones emergentes.

Por consiguiente, entender la efectividad de los controles implica una distinción de doble vía:

1. Cambiar la vista mecanicista en la cual fueron diseñados inicialmente y habilitar los medios y estrategias para crear ventanas de aprendizaje que establezcan umbrales de operación que se ajusten según la evolución del entorno y sus retos.
2. Aprender/desaprender rápidamente de las inestabilidades y desafíos del ambiente de operación de la empresa, para cambiar los modelos y lecturas estándares disponibles con el fin de desarrollar respuestas ágiles y flexibles a pesar de posibles evento adversos.

En resumen, aceptar la vulnerabilidad inherente y propia de la dinámica de la infraestructura, los procesos, las personas y las normas, como fuente natural de aprendizaje para reconocer en el control, no un mecanismo que revela fallas y comportamientos adversos, sino como una oportunidad de calibrar permanentemente un sensor para avanzar en la construcción de una postura vigilante y resiliente que es capaz de responder y advertir sobre realidades latentes y eventos que aún no son visibles.

Notas finales

1 Sheffi, Y.; *The New (Ab)Normal: Reshaping Business and Supply Chain Strategy Beyond COVID-19*, Massachusetts Institute of Technology (MIT) Center for Transportation and Logistics, Cambridge, Massachusetts, USA, October 2020, *https://sheffi.mit.edu/book/new-abnormal*

2 Mejía, R.; *Administración de riesgos*. Un enfoque empresarial, Universidad EAFIT, Medellín, Colombia, 1 May 2020

3 Sieber, S.; J. Zamora; "The Cybersecurity Challenge in a High Digital Density World," *The European Business Review*, 18 November 2018, *https://www.europeanbusinessreview.com/the-cybersecurity-challenge-in-a-high-digital-density-world/*

4 Subramanian, M.; "The Four Tiers of Digital Transformation," *Harvard Business Review*, 21 September 2021, *https://hbr.org/2021/09/the-4-tiers-of-digital-transformation*

5 Avizienis, A.; J.-C. Laprie; B. Randell; C. Landwehr; "Basic Concepts and Taxonomy of Dependable and Secure Computing," *Institute of Electrical and Electronics Engineers (IEEE) Transactions on Dependable and Secure Computing*, vol. 1, iss. 1, 4 October 2004, p. 11–332

6 Kast, F.; J. Rosenzweig; *Organization and Management: A Systems and Contingency Approach, 3rd Edition*, McGraw-Hill College, USA, 1 January 1979

7 Reason, J.; *Managing the Risks of Organizational Accidents*, Routledge, UK, 20 January 2016

8 Beer, S.; *Decision and Control*, John Wiley and Sons, UK, 1994

9 Beer, S.; *Cybernetics and Management*, John Wiley and Sons, UK, 1964

10 *Ibid*.

11 Beer, S.; *Diagnosing the System for Organizations*, John Wiley and Sons, UK, 1995

12 Espejo, R.; R. Harden; *The Viable System Model: Interpretations and Applications of Stafford Beer's VSM*, John Wiley and Sons, UK, 1989

13 *Op cit* Beer 1995

14 *Op cit* Espejo and Harden 1989

15 Espejo, R.; "Giving Requisite Variety to Strategic and Implementation Processes: Theory and Practice," Proceedings of the JAIST Conference, Ishikawa, Japan, September 2000, *https://www.researchgate.net/publication/228772758_Giving_Requisite_Variety_to_Strategic_and_Implementation_Processes_Theory_and_Practice*

16 Cascio, J.; "Facing the Age of Chaos," *Medium*, 29 April 2020, *https://medium.com/@cascio/facing-the-age-of-chaos-b00687b1f51d*
17 Schrader, R.; M. McConnell; "Security and Strategy in the Age of Discontinuity: A Management Framework for the Post-9/11 World," *Strategy+Business*, 9 January 2022, *https://www.strategy-business.com/article/11439*
18 Cano, J.; La 'falsa sensación de seguridad'. El reto de incomodar las certezas de los estándares y tratar de 'domesticar" 'os inciertos. *Revista SISTEMAS. (SYSTEMS Journal)*, Asociación Colombiana de Ingenieros de Sistemas. (Colombian Association of Systems Engineering), vol. 159, p. 82–95, 2021, *https://doi.org/10.29236/sistemas.n159a6*
19 Day, G.; P. Schoemaker; *See Soon, Act Faster: How Vigilant Leaders Thrive in an Era of Digital Turbulence*, The MIT Press, USA, 1 October 2019
20 Schoemaker, P.; *Brilliant Mistakes: Finding Success on the Far Side of Failure*, Wharton Digital Press, USA, 2011
21 *Op cit* Day and Schoemaker 2011
22 *Op cit* Cano 2021
23 Espejo, R.; W. Shuhmann; M. Schwaninger; U. Bilello; *Organizational Transformation and Learning: A Cybernetic Approach to Management*, John Wiley and Sons, UK, 1996
24 Martin, P.; *The Rules of Security: Staying Safe in a Risky World*, Oxford University Press, UK, 2019
25 *Op cit* Espejo and Harden 1989