No. 167 Abril - Junio 2023 DOI: 10.29236/sistemas ISSN 0120-5919

SISTEMAS

Seguridad híbrida
Un paradigma emergente

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

JORNADA INTERNACIONAL DE SEGURIDAD INFORMÁTICA

La seguridad híbrida, como el nuevo desafío de la seguridad en un escenario interconectado.

MODALIDAD VIRTUAL

JULIO 25/28

ACIS
ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

Más información en:
www.ACIS.org.co
o escríbenos a:
301 5530540
Suscripciones@acis.org.co
Cursos@acis.org.co

En esta edición

Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2015-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Abril - Junio 2023
Calle 93 No.13 - 32 Of. 102
Teléfonos 616 1407 - 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

DE GERENTE DE PROYECTOS A

GERENTE ÉLITE DE PROYECTOS

Altamente Efectivo y con Proyección Internacional

Descubre cómo liberar tiempo para lo que amas, cómo posicionarte internacionalmente como gerente de proyectos de élite y tener los resultados que muy pocos logran obtener, gracias a tu mentalidad y resultados, en menos de 30 días.

Dirigido por

Mauricio F. Morales R. PMP, MCP, M3.0 - CEO Projectical SAS

ÚNETE AL ENTRENAMIENTO GRATUITO

WWW.PROJECTMANAGEMENTELITE.COM

Junio 19 al 22 2023 - 7:30 pm Colombia

Regístrate

Project Management Elite

PROJECTICAL

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.*

Algo básico de la seguridad híbrida

DOI: 10.29236/sistemas.n167a2

Daniel Jiménez, MBA, CPP®, PSP®, CHSS, ESRM, WVP&IP

Hablar de seguridad es un criterio muy amplio a nivel organizacional, pero también es algo especifico, que ayuda a las corporaciones a protegerse de diversas amenazas que conduzcan a múltiples tipos de pérdidas. Hoy el concepto debe ser visto de manera mucho más holística e inclusiva en cuanto al alcance corporativo; cada una de las aristas relacionada con la seguridad deben ser incluidas como parte de las responsabilidades del encargado de esta área en las compañías; seguridad de la información, seguridad informática, cumplimiento, investigaciones, manejo de crisis y emergencias, seguridad ocupacional, seguridad física y muchas otras que pueden convertirse en parte esencial dentro de los diferentes negocios, tendrían que integrarse a manera de factor diferencial de este hombre o mujer que no

solo tenga conocimientos de seguridad física.

Podría cuestionarse entonces, ¿por qué el gerente de seguridad tiene responsabilidades de protección de la información? Y el fondo de la respuesta radica en que su principal responsabilidad es evitar y ejercer control de las pérdidas, pero que en última instancia no lo hará de forma aislada o a manera de silo dentro de la facilidad sino que, con el concurso de un oficial de protección de la información, para que junto a este, logre alcanzar su objetivo de evitar y/ o prevenir las pérdidas, para ver de manera visible la adecuada gestión de los riesgos en las diferentes áreas, como las mencionadas en la parte superior de este escrito.

Además de esto, es significativo entender que la protección de activos dentro de las diferentes estructuras organizacionales se logrará de manera exclusiva con la integración de ***las personas; los procedimientos y el uso de la tecnología*** adecuada, todo esto basado en un excelente diseño que atienda las necesidades de las empresas y para que su efectividad se pueda apreciar en todo su esplendor, se necesita disponer de varios elementos en perspectiva, así:

El primero de ellos, un enfoque sistémico de gestión de riesgos, que deje apreciar aspectos como las diferentes condiciones internas y externas, y su integración para definir los contextos en los que trabajará la organización. Además de ello, la extensión de esas autopistas en las cuales se estará moviendo la evaluación de esos riesgos, y que se complementará con la definición de los criterios.

Entender y conocer cómo la valoración de riesgos define e identifica, analiza y evalúa los diferentes riesgos, para que de esa manera la misma organización logre comprender ¿qué se va a proteger? y ¿de qué se va a proteger?; y como complemento de esto dentro de ese enfoque sistémico, definir las opciones de tratamiento de riesgo.

Pero como lectores estaremos pensando, se está hablando de manera académica de lo que es parte del proceso de la gestión del riesgo y es totalmente cierto, porque no se debe perder como lo mencioné anteriormente, la perspectiva y, si pensamos en dejar de lado la aplicación de este sencillo procedimiento, pues difícilmente vamos a tener resultados alineados con un enfoque sistémico y metodológico.

Obviarlo nos lleva a entender el porqué nuestro mercado aparece infestado de una cantidad de personas que se auto endilgan la etiqueta de especialistas, simplemente porque han realizado un curso de formación como auditor en diferentes estándares, normas y otras iniciativas, sin tener en cuenta las responsabilidades que conlleva

el mismo título de especialista, además de que no es cuestión de autodeterminación, sino de reconocimiento por parte de un tercero con autoridad para definir la ***"especialidad de una persona"***, que es quien reconoce ante la comunidad la pericia y experiencia junto con el uso del conocimiento, en una ciencia o disciplina, que se pueden convertir en sendas vulnerabilidades dentro de la organización por su misma condición.

Como segundo aspecto, el manejo técnico de la disciplina que se logra, además de experiencia, con una educación, capacitación, entrenamiento y desarrollo a diferentes niveles, de pregrados y postgrados.

Ahora, desde lo relacionado con el ser humano y su conocimiento, el segundo gran aspecto que nos ocupa para hablar de la seguridad hibrida tiene que ver con los procedimientos, los que deben estar articulados con el mismo objeto del negocio, y enfocados al cumplimiento de las políticas que desarrollen o pretenden alcanzar la misionalidad dentro de ese planeamiento estratégico trazado por la empresa para la vigencia que determine.

El verdadero sentir de estos procedimientos radica directamente en la capacitación y disponibilidad de estos para que se puedan materializar, mucho más, cuando hablamos de asuntos relacionados con la protección de activos de la información y las medidas de protección sobre estos. Algo que nos dejó la pandemia generada por el COVID 19, fue la enseñanza asociada con las contramedidas que, desde el área responsable de controlar el flujo y la seguridad de la información, se iniciaron y que perdurarán en el tiempo; mucho más hoy como parte esencial para evitar las pérdidas dentro de múltiples compañías que transan sus operaciones haciendo uso de diferentes infraestructuras de TI y redes externas.

Tal como lo mencioné anteriormente, un correcto diseño teniendo en cuenta el Diseño Base de Amenazas o Amenaza Base del Diseño (DBT por sus siglas en inglés) permitirá que la infraestructura de protección o su planeamiento sea modular y adaptable a las diferentes amenazas que migren con el tiempo manteniendo un esquema siempre operativo y funcional, para proteger no solo los activos tangibles e intangibles sino que también a la misma facilidad, por lo que este se convierte en un factor decisivo para esta tercera parte, que tiene que ver con la seguridad hibrida y que es el uso de la tecnología.

Sabiendo y conociendo, nuestras vulnerabilidades, amenazas, habiendo identificado los riesgos y las opciones de tratamiento de los riesgos, lo que nos resta es transpolarlas con las diferentes contramedidas, para lo cual es imperioso que se sepa y conozca más allá de lo básico; muchos de los responsa-

bles de la protección de activos de una empresa recomendarán “se requiere una cámara en esta esquina, un molinete y lector biométrico en la entrada, un radio de tales características, un vigilante armado”, pero cuando se trata de justificar el porqué de estas recomendaciones, sus argumentos se diluyen como humo, dejando en evidencia su subjetividad ante el conocimiento de los conceptos ya señalados; por lo mismo, es necesario que las recomendaciones de uso de tecnología estén orientadas en principio a atacar o mitigar los riesgos identificados desde el punto de vista de protección de la organización, para que en función de ello, se logre entender la seguridad como una herramienta eficaz, eficiente y efectiva bajo un enfoque no solo sistémico y metodológico, sino con un resultado costo efectivo para todas las partes interesadas.

Para concluir, es necesario mencionar que la necesidad de las estructuras corporativas está orientada al cumplimiento de sus objetivos, independientemente de cuál sea su objeto social; y para ello, dentro de la protección de activos se requiere hacer uso de elementos y herramientas que dejen ver la manera costo efectiva de gestionar los riesgos de seguridad a diferentes niveles (estratégicos, tácticos/misionales y operativos), además que la seguridad es uno de los instrumentos que se pueden emplear a nivel organizacional para esa gestión de los riesgos en todos los grados.

***Daniel Jiménez**. MBA, CPP®, PSP®, CHSS, ESRM, WVP&IP*

Claves en el marco de la seguridad híbrida

DOI: 10.29236/sistemas.n167a3

Un pensamiento creativo, inquieto, basado sobre todo en la innovación y la prospectiva es fundamental en el marco de la seguridad híbrida, indica el Cr.(RA) Fredy Bautista García.

Sara Gallardo M.

La amplia experiencia de Fredy Bautista García, actual director del Departamento de Protección y Seguridad del Banco de la República, lo ha llevado por diferentes espacios en los que ha dejado una huella muy importante.

Es Coronel de la Reserva Activa de la Policía Nacional; ha sido presidente en dos oportunidades del Grupo de Trabajo de Cibercrimen en INTERPOL para las Américas; primer Jefe del Centro Cibernético de la Policía Nacional y gestor de Ciberseguridad en el sector público en Colombia. Así mismo, ha participado en iniciativas para la promulgación de los lineamientos de política pública en ciberseguridad y

ciberdefensa, seguridad digital y confianza digital.

Más allá de la seguridad y la ciberseguridad, disfruta de textos históricos, de ahí que su género literario favorito sea la novela histórica y policíaca. “Entiendo que el mundo cambió en solo tres años. Hemos vivido una pandemia, un conflicto bélico que amenaza con extenderse; una guerra híbrida basada en el ciberespionaje y la lucha por la hegemonía ideológica y económica de grandes potencias que trascienden a Latinoamérica y fomentan el rápido cambio del mundo como lo percibíamos. Sin embargo, reconozco que la resiliencia es tal vez la mayor cualidad del ser humano y su rápida adaptación debe ayudar a que las futuras generaciones dispongan de más recursos y de mejores líderes”, fue muy enfático en señalar antes de responder las inquietudes planteadas por la revista.

Revista Sistemas: *¿En su práctica actual qué se entiende como una amenaza híbrida? ¿Qué características tiene?*

Fredy Bautista García: En el contexto actual una amenaza híbrida se entiende como un conjunto de factores que pueden constituir una posible causa de materialización de un riesgo para nuestra organización y sus activos, valiéndose de situaciones no convencionales o poco comunes. Por ejemplo: una campaña de descrédito o desinformación en redes sociales que propicie o impulse un ataque en contra de la infraestructura física o un ciberataque enfocado a explotar una vulnerabilidad en sistemas de seguridad y detección electrónica, que faciliten el actuar de criminales en entornos físicos incrementando el riesgo de intrusión.

RS: *¿Piensa usted que el paradigma de la prevención se ha venido agotando? ¿Se deben habilitar nuevas propuestas para la seguridad?*

FBG: La prevención debe evolucionar hacia unos escenarios de seguridad basados en prospectiva estratégica que faciliten el diseño y aplicación de acciones para anticipar el riesgo en el futuro.

Hoy en día las amenazas tradicionales como el terrorismo o las acciones del crimen organizado aprovechan la realidad social en la región, para impulsar acciones malintencionadas en contra de infraestructuras críticas; para generar el caos y facilitar una intrusión violenta a una sede de especial interés en una organización (incluso un servicio esencial) o para que los esfuerzos de seguridad se distraigan y se concentren en situaciones específicas que permitan aprovechar vulnerabilidades desatendidas.

La posibilidad de anticipar estos escenarios de riesgo y amenaza, conlleva a identificar todas las oportunidades para la prevención, dando lugar a que se integren importantes desarrollos tecnológicos con las tareas de monitoreo y vigilancia física, de manera que las organizaciones trasciendan su perímetro para entender cómo esta realidad económica, política y social de nuestros países puede afectar o comprometer la seguridad en la organización.

RS: *¿Qué es lo más retador en el tratamiento de una amenaza híbrida?*

FBG: Sin duda alguna, el principal reto es incorporar este tipo de amenazas en el espectro de la gestión de los riesgos en la organización. Podrían ser considerados como inverosímiles los planteamientos de un analista de seguridad que advierta una potencial amenaza híbrida mediante el empleo de inteligencia artificial. Por ejemplo, alrededor de un DeepFake utilizado para suplantar a un funcionario o a un contratista y vulnerar el perímetro

de seguridad de un área restringida, la probabilidad de ocurrencia puede ser valorada en forma no acertada para que no sean implementados los controles necesarios.

RS: *¿Cómo define en su práctica actual lo que podría ser una seguridad híbrida?*

FBG: Una visión de la seguridad de manera íntegra. Es decir, que articule las capacidades desarrolladas en la seguridad física con las facilidades tecnológicas de detección y alertamiento. Sin duda, el perímetro se asegura con barreras que impidan los ingresos no autorizados; identificar cómo evoluciona el crimen en el entorno actual, el amplio uso de la tecnología y las vulnerabilidades inherentes, permite proteger procesos esenciales en la cadena logística que provee insumos y recursos a una planta de producción o asegura el traslado de productos hacia las áreas dispuestas para su distribución. Anticipar un bloqueo de vías, por ejemplo, contempla integridad en la trazabilidad en el proceso de traslado de bienes y valores, lo cual exige que la organización prevea nuevas herramientas para fortalecer la seguridad y la defensa.

RS: *¿Cuáles nuevos saberes y conocimientos son necesarios para avanzar en una seguridad híbrida?*

FBG: Considero que lo más importante es tener un pensamiento creativo, inquieto y basado sobre todo en la innovación y la prospectiva. Debemos adaptar la seguridad hacia tecnologías inteligentes que aprovechen por ejemplo la analítica de datos y los comportamientos para identificar potenciales riesgos.

Históricamente, la seguridad se concebía como un inamovible; hoy en día la inteligencia anticipativa, facilita entender cómo un evento futuro puede afectar la seguridad en la organización y se debe entonces adaptar los esquemas de seguridad y la tecnología aplicada para su mejor aprovechamiento. Es importante igualmente avanzar en la integración de tecnologías para la detección con las capacidades de monitoreo a través de operadores tecnológicos altamente capacitados.

RS: *¿Cuáles retos ve a futuro para las empresas en el contexto las amenazas y la seguridad híbridas?*

FBG: Indudablemente, la infoxicación basada en Fake News y la desinformación pueden generar escenarios de amenazas híbridas muy complejos, como los presentados en 2020 y 2021, en el denominado “Estallido Social”, en el cual muchas sedes financieras y estatales fueron vandalizadas e interrumpidos los servicios, particularmente en las ciudades de Cali y Bucaramanga, por citar solo algunas de las poblaciones más afectadas.

Igualmente, la operación logística y el abastecimiento de materias pri-

mas puede afectar los suministros necesarios para una adecuada gestión operativa en una organización, y ello conlleva a anticipar diferentes alternativas de rutas y medios de transporte que deben ser asegurados para mantener los estándares requeridos en la seguridad operacional.

La suplantación de identidad, con alcance virtual y físico pueden ser facilitadores de robos de activos informáticos o sabotaje y afectación a centros de datos o infraestructuras digitales. Sumados también a la robotización y uso creciente de inteligencia artificial en procesos críticos que pueden ser objeto de ciberataques o errores de configuración comprometiendo la seguridad en la organización.

Finalmente, el Malware “as a Service” seguirá creciendo y el crimen organizado podrá acceder a desarrollos de programas maliciosos enfocados en vulnerar la seguridad especialmente los sistemas electrónicos de monitoreo como los CCTV (Circuitos Cerrados de Televisión) o centros de datos de las organizaciones.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro “Lo que cuesta el abuso del poder”. Ha sido corresponsal de la revista Infochannel de México; de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador y corresponsal de la revista IN de Lanchile e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res) y editora de Alfaomega Colombiana S.A.; en la actualidad es asesora y editora en escritura y producción de libros. Es editora de esta revista.*

REDUC@TE 2023

Col - Mex

¿Qué es Reduc@te?

es un evento experiencial que aborda las últimas tendencias para enriquecer el uso de las tecnologías digitales y su convergencia en la educación.

9-14 Octubre

ACIS
ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

mprove

moodle Partner
CERTIFIED SERVICES PROVIDER

Más información en:
www.ACIS.org.co
o escríbenos a:
301 5530540
Suscripciones@acis.org.co
Cursos@acis.org.co

Capacidades de los CISOs en Iberoamérica

Este estudio independiente realizado en una muestra de profesionales en Iberoamérica busca identificar las capacidades y habilidades estratégicas que requieren los ejecutivos de seguridad de la información.

DOI: 10.29236/sistemas.n167a4

Resumen

Estudiar el rol del CISO (*Chief Information Security Officer*), es una necesidad en medio de una acelerada expansión de la densidad digital, el mayor apetito de riesgo de las empresas y las presiones de los equipos ejecutivos. Por tanto, el CISO no solo deber contar con capacidades técnicas especializadas, sino con un conjunto de habilidades y capacidades estratégicas para habilitar, desde su función, negocios más sostenibles y ágiles en el ecosistema digital en el que opera una compañía. 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.

Palabras claves

Ciberseguridad, Seguridad, Iberoamérica, Capacidades, CISO

Introducción

El ejecutivo y la función de seguridad de la información en las organizaciones son dos temáticas claves que se han venido revisando en la literatura internacional con el fin de establecer la manera como se articulan sus actividades y retos alrededor de los modelos de generación de valor de las empresas. En este sentido, es necesario que dicha función y sus directivos encuentren nuevos puntos en común con los otros miembros del equipo gerencial de las empresas, con el fin de motivar nuevas iniciativas de transformación de sus negocios y asegurar la promesa de valor para con sus clientes (Proctor, 2022; Darkreading, 2022).

Si bien en la actualidad se identifican una serie de factores de estrés que vienen afectando a los ejecutivos de seguridad de la información como son: el aumento de los riesgos del trabajo remoto, la transformación digital y sus impactos en la postura de seguridad de la organización y la amenaza creciente del ransomware (extorsión con datos) (Deepinstinct, 2022), los directivos de seguridad y sus equipos han venido avanzando en iniciativas que aumentan su capacidad proactiva y de monitorización de tal manera que, en un esfuerzo conjunto con sus socios estratégicos, y apalancados en el fortalecimiento de una cultura de seguridad se hacen más resistentes y resilientes frente a la inevitabilidad de la falla (Heidrick & Struggles, 2022).

Estudiar por tanto la función de seguridad de la información como factor articulador de los retos contemporáneos de las empresas, ahora con una mayor superficie de ataque disponible, mayor interconexión y una demanda creciente de nuevas experiencias por parte de sus clientes, resulta de interés no sólo para los profesionales de seguridad de la información, sino para los equipos ejecutivos de las organizaciones como una forma de dimensionar, entender e incorporar las capacidades humanas, procedimentales y directivas requeridas que permitan alinear el apetito de riesgo de las empresas frente a sus estrategias y ecosistemas digitales claves que le dan vida a sus iniciativas (Ozkaya, 2021; Onibere et al., 2017).

En este sentido, se adelantó un ejercicio de investigación entre la comunidad de seguridad/ciberseguridad en Iberoamérica con el fin de validar las capacidades del CISO (*Chief Information Security Officer*) en cuatro elementos concretos: analizar, aprender, accionar y anticipar, los cuales se articulan en un modelo de diagnóstico que se aplicó entre los meses de julio a septiembre de 2022. Los resultados sugieren importantes retos que

se deben atender en la región de cara a los retos e inestabilidades que se advierten en los próximos meses y años. Para ello, este trabajo se estructura considerando inicialmente unos antecedentes sobre los perfiles de los profesionales de seguridad/ciberseguridad y los cuatro elementos de valoración en que se enmarca el modelo usado, luego se presenta el detalle de la metodología utilizada, seguidamente los resultados que se obtuvieron y el análisis de los mismos, para terminar con algunas conclusiones que se traducen en un llamado a la acción para concretar la transformación necesaria de los oficiales de seguridad/ciberseguridad de Iberoamérica.

Antecedentes

La función de seguridad, así como los roles, responsabilidades, tareas y en términos generales el perfil del profesional de seguridad evoluciona y son importantes en el desarrollo de las capacidades claves de las organizaciones y naciones (ISACA, 2022; Fortinet, 2022). Conocer los retos de la función de la seguridad, y cómo el rol del profesional se transforma, es relevante para atender las dinámicas de cambio y disrupción que representa una transformación digital en el que las organizaciones actualmente se desenvuelven (Proofpoint, 2022).

Al hacer una revisión de literatura en repositorios académicos como Google Scholar, y buscar por “Oficial de Seguridad Informática” aparecen 75 resultados, solo 2 de ellos tienen alguna relación. El primero de ellos habla de los conocimientos deseables de un profesional de seguridad informática (Rodríguez, 2012), y el segundo relacionado con la implementación del cargo de oficial de seguridad informática en la empresa (Carvajal, 2015). Al buscar por “capacidades” y “Oficial de Seguridad de la Información” aparecen 339 resultados, de los cuales 5 documentos al momento de la revisión se conectan con el filtro de búsqueda, sin embargo, solo un documento tiene alguna relación con las palabras buscadas. En dicho documento no se especifica las capacidades del profesional de seguridad, sino la capacidad del programa de seguridad cibernética.

Adicionalmente, estudios internacionales como los de Marlin Hawk (2020), Shayo et al. (2019), Monzelo & Nunes (2019), Maynard et al. (2018), Whitten (2016) y Karanja & Rosso (2017) hacen una compilación de literatura académica y científica que revisa el rol del CISO en las empresas, las estructuras más importantes y las funciones generales que los profesionales de ciberseguridad han venido desempeñando. Nuevamente el tema de capacidades del oficial de seguridad no aparece como elemento fundamental para el estudio de este perfil en las organizaciones.

Estos resultados motivan el desarrollo de este investigación para

construir algunos elementos alrededor de las capacidades del CISO, entendiendo esta palabra como el desarrollo patrones de aprendizaje propios de este perfil que le permitan motivar y concretar acciones proactivas y prospectivas frente a un entorno que evoluciona cada vez más rápido, frente a un adversario que avanza y mejora sus estrategias y técnicas, con una mayor superficie de ataque, y una junta directiva que demanda orientación, apoyo y respuesta frente al apetito de riesgo de la empresa (WEF, 2022).

Metodología

Este estudio exploratorio es de corte cuantitativo basado en una escala de Likert busca medir una percepción de los participantes de Iberoamérica con respecto al CISO y comprender aquellos elementos relevantes a las capacidades de los profesionales de seguridad de la información (CISOs) de la región. Para ello se toma una muestra probabilística con un error de muestreo de 8.06% para un nivel de confianza del 95%. Por tanto, bajo esta perspectiva se busca entender cuáles son las capacidades de los CISOs y el desarrollo de las mismas en el marco de esta investigación como parte del ejercicio de su función en las empresas. En particular, se toman las respuestas de un formulario creado y distribuido al público de profesionales de seguridad de la información en cuatro elementos a saber: analizar, aprender, accionar y anticipar.

Instrumento de investigación

Comprender las capacidades de un CISO más que saber sobre sus habilidades técnicas es reconocer a la persona y sus capacidades para aprender y desaprender de un entorno inestable y volátil donde debe dar respuestas y aplicar estrategias para dar cuenta con el incierto y así poder comunicar los resultados del ejercicio de la gestión y gobierno del riesgo cibernético. En consecuencia, se plantean cuatro elementos clave que hablan del ese oficial de seguridad de la información con perfil estratégico que se detallan a continuación:

- Analizar
- Adelanta sesiones de lecciones aprendidas para reconocer y reformular lo que sabe.
- Detalla patrones de comportamientos (conocidos e inusuales) con los datos disponibles.
- Plantea alertas y alarmas ajustadas con la calibración de los controles definidos.

- Aprender
- Mantiene el hábito de lectura y revisión de informes y reportes académicos y de industria.
- Crea espacios de conversación y construcción colectiva con su equipo, con sus pares (dentro y fuera de la su industria) y con sus clientes.
- Cuestiona y sorprende con frecuencia su saber previo.

- Accionar
- Canaliza sus emociones y gestiona las presiones externas.

- Utiliza su experiencia previa y la información disponible para decidir.
- Mantiene todo el tiempo en mente el objetivo superior que persigue.

• Anticipar
- Identifica patrones inusuales en medio de las tendencias y señales débiles observadas en el entorno.
- Define al menos tres tipos de escenarios: de continuidad, de cambio incremental o de cambio abrupto.
- Desarrolla prototipos de eventos para los diferentes tipos de escenarios.

Estos cuatro elementos se detallan en una encuesta de 12 preguntas asociadas con una escala de Likert (5-totalmente de acuerdo, 4-de acuerdo, 3-ni en acuerdo ni en desacuerdo, 2-en desacuerdo, 1-totalmente en desacuerdo), con las cuales se busca entender cuáles son las capacidades más reconocidas en los CISOs y aquellas donde pueden existir oportunidades para apalancar el desarrollo de su perfil estratégico en las organizaciones actuales.

Luego de tabular el promedio de respuestas de cada uno de los participantes del estudio, se procede con la interpretación por bloques que se hará de la siguiente manera:

• 1 y 2 – Percepción baja – CISO reactivo y orientado a atender contingencias por materialización del riesgo cibernético.

• 3 – Percepción media – Bajo nivel de compromiso por parte del CISO en su actuación estratégica.

• 4 – Percepción alta – Existe un compromiso concreto del CISO que genera una postura proactiva y estratégica en sus actuaciones.

• 5 – Percepción muy alta – Hay un reconocimiento estratégico del CISO parte de la junta directiva, que hace que sus actuaciones sean sostenibles en el tiempo.

Población encuestada

Esta encuesta fue distribuida a través de correo electrónico, redes sociales y grupos de mensajería instantánea a una comunidad de más de 1000 profesionales de seguridad digital, a través de un formulario en la Web configurado a través de la plataforma *Google forms*. La población seleccionada responde a la comunidad de seguridad de la información que se tiene en la región de Iberoamérica, de los cuales, en promedio participan 129 profesionales a nivel regional.

Limitaciones del estudio

Este estudio realizado sobre las capacidades de los ejecutivos de seguridad de la información (CISOs), busca explorar y establecer aquellas mayormente reconocidas para

estos profesionales en el ejercicio de su perfil profesional, así como aquellas donde existe potencial de desarrollo. Los resultados son analizados en el contexto de la muestra tomada en la región de Iberoamérica con una perspectiva general, la cual revela elementos particulares y propios para los participantes de este ejercicio.

Resultados

Los resultados que se presentan a continuación corresponden a la tabulación de los promedios de las respuestas efectuadas por los participantes para cada pregunta según lo establecido en la escala de Likert previamente mencionada y detallada.

Los países participantes en esta encuesta se han extendido a toda la región de Iberoamérica (Figura 1).

Los países con mayor participación Colombia 41,09%, México 12,40%, Perú 11,63%, Argentina 6,98% y Uruguay 6,20%.

Luego de tabular los promedios de las respuestas (por bloques) de los participantes para cada uno de los elementos del modelo planteado se tiene como resultado la tabla 1.

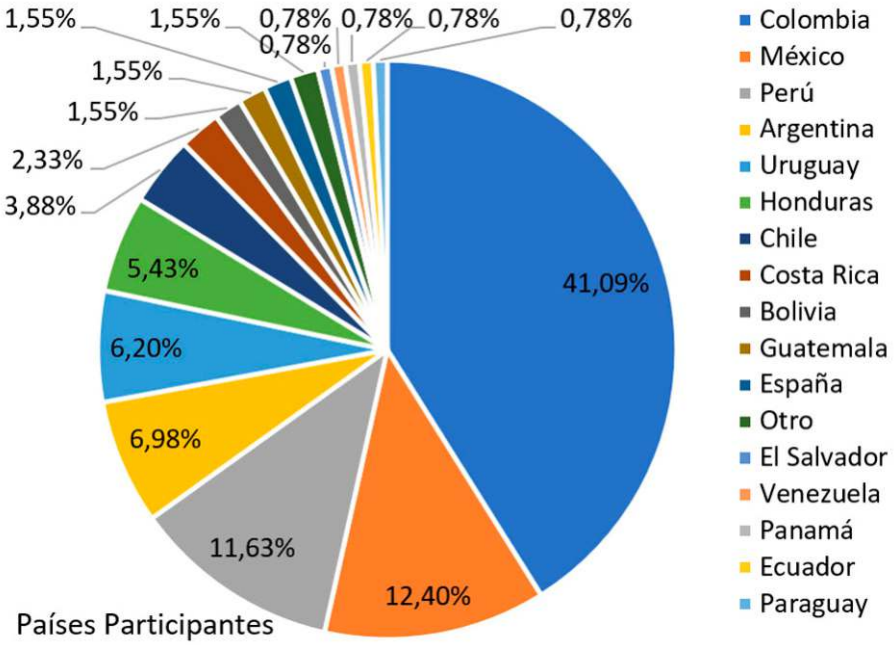


Figura 1. Países participantes

Capacidad	Valor
Analizar	3,8
Aprender	4,0
Accionar	4,2
Anticipar	3,5

Tabla 1. Distribución de respuestas por las capacidades

En una escala promedio se encuentra que la capacidad de *analizar* obtiene un promedio de 3,8, la capacidad *aprender* obtiene un promedio de 4,0, la capacidad de *accionar* un promedio de 4,2 y la capacidad de *anticipar* de 3,5. Al usar una escala de Likert, se redondean sus resultados a unidades enteras y completas (Matas, 2018).

Este redondeo, se hace hacia el menor valor, teniendo claro que cualquier sistema en general tiende al lugar donde se hace el menor esfuerzo. Por tanto, los valores quedan definidos de la siguiente manera:

- Analizar – 3,0
- Aprender – 4,0
- Accionar – 4.0
- Anticipar – 3,0

Al revisar cada una de las preguntas y sus respuestas en sus valores promedios (Figura 2) se encuentra:

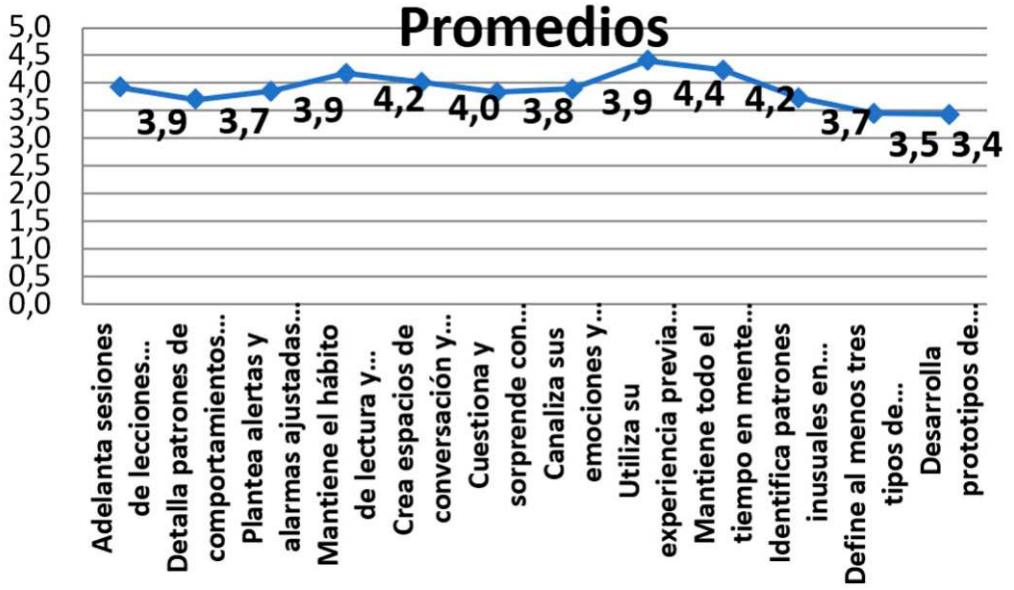


Figura 2 - Valores de los promedios de las 12 preguntas

Análisis de Resultados

Al revisar los elementos claves de un perfil del CISO ajustados en su escala de Likert encontramos.

La gráfica 3 muestra que la capacidad estratégica de los CISOs en relación con analizar y anticipar se encuentra en una percepción media; por el otro lado las capacidades de Aprender y Accionar están en una percepción Alta, esto para el promedio general de todos los participantes del estudio.

Esta percepción particularmente alta se ve motivada por características concretas reconocidas en los CISOs como son:

» Mantiene el hábito de lectura y revisión de informes y reportes académicos y de industria.
» Utiliza su experiencia previa y la información disponible para decidir.
» Mantiene todo el tiempo en mente el objetivo superior que persigue.

Que hablan del perfil general que dichos profesionales manifiestan en su práctica y, por tanto, sugiere una orientación básica en la formación de dicho cargo en la región.

Sin embargo, al hacer un análisis un poco más exhaustivo y estudiar cada factor de manera individual, tratando de agrupar aquellos que se encuentran por encima y por debajo de la media, podemos observar:

La figura 4 muestra que, en la capacidad de analizar el 53% se percibe

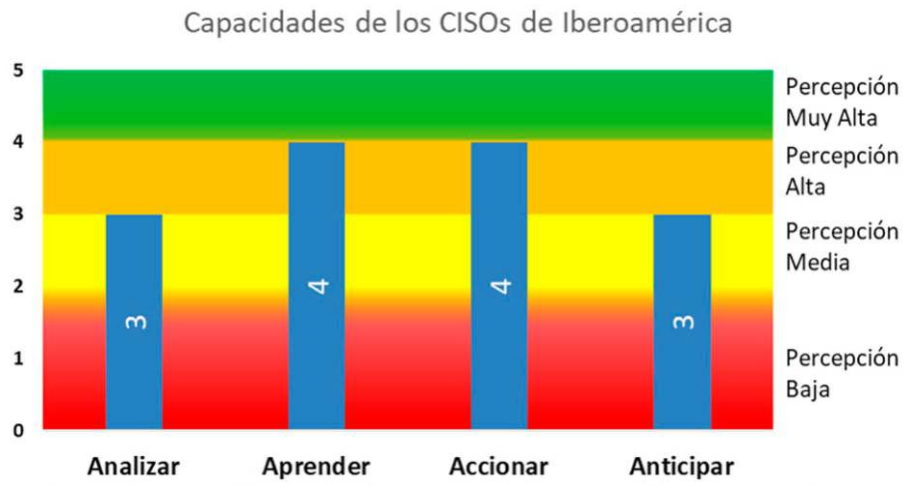


Figura 3. Distribución de respuestas por las capacidades

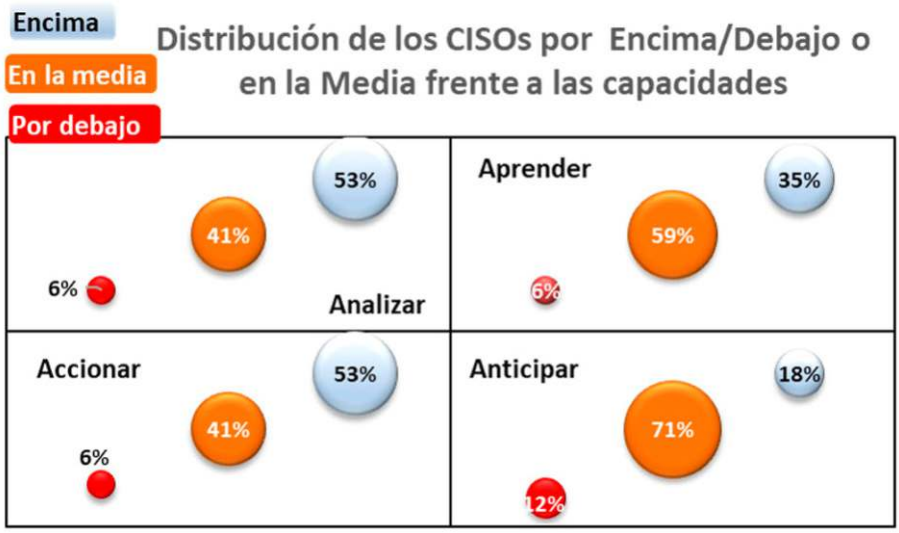


Figura 4. Análisis de cada factor por encima, igual o debajo de la media

que está entre Alta y muy Alta, el 41% se encuentra en una percepción media, mientras que solo el 6% de todos los participantes lo perciben de manera baja o muy baja.

Para el caso de la capacidad aprender, lo que se puede ver es que el 35% de los participantes perciben que el CISO tiene una capacidad alta o muy alta para aprender, el 59% percibe que está en la media de este factor, mientras que solo el 6% considera que está por debajo de la capacidad.

En el caso de accionar, el 53% de los participantes lo perciben por encima de la media, es decir se percibe entre alto y muy alto, el 41% lo percibe en un nivel medio, y el 6% lo percibe bajo y muy bajo.

Para el caso de anticipar, solo el 18% considera que está por encima del nivel medio, que está relacionado con alto y muy alto, mientras que el 12% se considera que están por debajo del mismo nivel relacionándose a bajo y muy bajo, mientras que el 71% de los participantes considera que está en el nivel medio de este factor.

Estos resultados muestran los retos concretos en dos de las capacidades para los CISOs particularmente en el analizar y el anticipar, que se reflejan en comportamientos concretos que se deben desarrollar y ajustar como:

» Detalla patrones de comportamientos (conocidos e inusuales) con los datos disponibles.
» Define al menos tres tipos de escenarios: de continuidad, de

cambio incremental o de cambio abrupto.
» Desarrolla prototipos de eventos para los diferentes tipos de escenarios.

Que implica un plan de ajuste y promoción de nuevas herramientas y prácticas que le permitan mantener una postura más vigilante y proactiva que mejore no solo su capacidad de respuesta, sino la oportunidad para concretar acciones viables y estratégicas ajustadas con los cambios de entorno y alineadas con la evolución del negocio y su apetito de riesgo.

La región de Iberoamérica es muy diversa, se mantienen con distintas percepciones que pueden estar sujetas a los avances que cada país a nivel nacional ha realizado basado en sus políticas públicas, esfuerzos de múltiples partes y demás actores que influyen en los ecosistemas de las naciones (OEA-BID, 2020). En este aspecto de manera general se pueden ver de la siguiente manera en la figura 5.

Países como Panamá, Ecuador y Venezuela se perciben sus CISOs por encima de un nivel medio en general, Panamá se percibe como un nivel muy Alto, Venezuela y Ecuador se perciben como nivel alto países como Costa Rica y Guatemala, se percibe por debajo de un nivel medio, de hecho, Guatemala se ve como un país donde sus CISOs se perciben en un nivel muy bajo, mientras que Costa Rica solo se percibe como un nivel bajo.

Un tres (3) en promedio para todos los países participantes confirma un bajo nivel de compromiso por

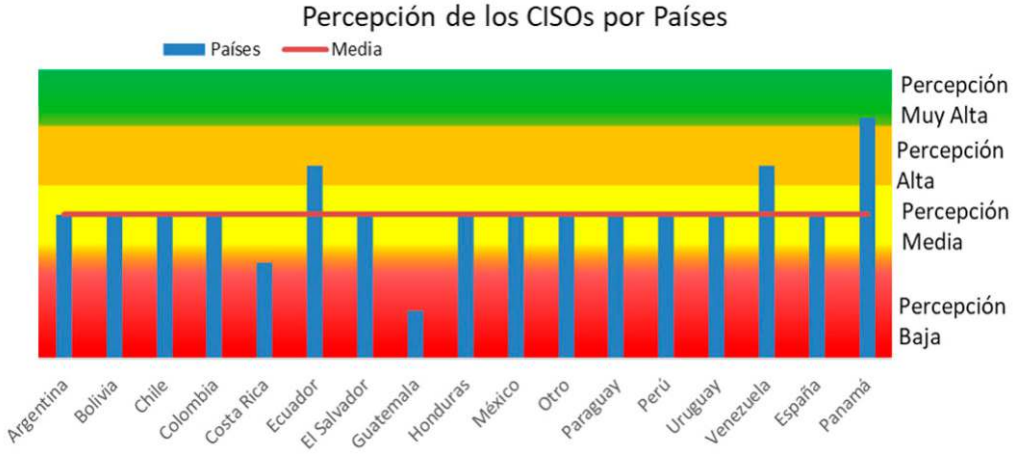


Figura 5. Percepción del CISO por país de la región

parte del CISO en su actuación estratégica, lo que implica que este cargo permanece generalmente operando en el nivel táctico y operativo, perdiendo espacio en las discusiones claves de la organización para acompañarla en nuevas y retadores iniciativas digitales, que demanda una lectura de la seguridad como habilitador de la confianza digital y por tanto de la transformación digital de la empresas.

Conclusiones

El CISO es uno de los cargos en las organizaciones que mayores presiones tienen en este momento, comoquiera que el avance acelerado de nuevas amenazas abre nuevos escenarios de ataques que las compañías deben advertir y asegurar. En este sentido, el oficial de seguridad de la información debe asumir una rápida transformación tanto en su práctica como en su cargo con el fin de habilitar espacios y reflexiones estratégicas que permitan ubicar sus propuestas y retos en el marco de la estrategia corporativa y los desafíos de las iniciativas digitales de las empresas (PwC, 2022).

Para ello, es necesario que desarrolle capacidades claves que permitan mejorar su desempeño y habilitar sus capacidades para pensar y actuar de forma estratégica (Fitzgerald, 2019; Bonney et al., 2022). En el desarrollo de esta investigación, basada en la muestra probabilística establecida, la evaluación general del CISO se ubica en el nivel tres (3), que se traduce en un bajo nivel de compromiso en su actuación estratégica, lo que implica una revisión de las prácticas actuales de estos ejecutivos, que por lo general se sitúan en el concepto de "gestión y medición", lo que conlleva a una mirada permanente a los eventos que ya ocurrieron, quedando atrapados en la vista del pasado, perdiendo capacidad de acción en el presente, y poca reflexión sobre los retos emergentes.

La transformación del CISO implica no sólo reconocer los riesgos actuales y las tendencias emergentes, con el fin de priorizar los riesgos más críticos, sino habilitar su capacidad de defensa y anticipación para movilizar a la organización en un escenario más resiliente, que le permita responder a eventos inesperados y abiertamente desconocidos, con el fin mantener la operación y asegurar las expectativas de los clientes (Deloitte, 2021). Lo anterior implica desarrollar una mentalidad en perspectiva sistémica dentro del marco de una revisión holística del entorno y los retos empresariales, además de promover una lectura de las amenazas actuales y futuras de la compañía. Así mismo, invita a considerar las diferentes tensiones locales o internacionales de cara a la disrupción en el negocio.

El resultado de este estudio iberoamericano y otros semejantes realizados a nivel nacional (Cano & Almanza, 2021) abren un espectro de

análisis tanto para las organizaciones como para la academia con el fin de enfilar los esfuerzos de formación y desarrollo del oficial de seguridad de la información, que le permita observar la percepción de sus propias prácticas y sus resultados, para renovar y ajustar sus capacidades, y desde allí concretar una ruta específica que cierre las brechas identificadas en los cuatro elementos del modelo utilizado: analizar, aprender, acciones y anticipar.

Si bien los hallazgos de esta investigación son válidos para los encuestados de la muestra y no pueden generalizarse, resaltan capacidades relativas al aprender y accionar del CISO. Por tanto, es necesario que el oficial de seguridad de la información se motive a reconocer la incertidumbre como parte de su ejercicio profesional para desde allí no sólo identifique patrones de comportamientos conocidos e inusuales, sino que igualmente desarrolle prototipos de eventos para los diferentes tipos de escenarios que aún no son conocidos.

Referencias

Bonney, B., Hayslip, G. & Stamper, M. (2022). *CISO Desk Reference Guide Executive Premier*, San Diego, CA: CISO DRG Publishing.

Cano, J. & Almanza, A. (2021). Reflexiones y retos para la academia en la formación de profesionales de seguridad/ciberseguridad en Colombia: 2010 - 2020. *ISLA 2021 Procee-dings*. 7. https://aisel.aisnet.org/isla2021/7

Carvajal, L. F. (2015). Implementación del cargo de Security Officer en la seguridad de Instalaciones de las FFMM de Colombia. [Trabajo de grado. Universidad Militar Nueva Granada]. http://hdl.handle.net/10654/14350.

DarkReading (2022). The state of CISO influence 2021. The maturing CISO role. https://www.coalfire.com/documents/reports/the-state-of-ciso-influence

Deepinstinct. (2022). Voice of SecOps 2022. https://info.deepinstinct.com/voice-of-secops-v3-2022

Deloitte. (2021). Building The Resilient Organization. https://www2.deloitte.com/content/dam/insights/articles/US114083_Global-resilience-and-disruption/2021-Resilience-Report.pdf

Fitzgerald, T. (2019). *CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers*. Broken Sound, NW: CRC Press

Fortinet (2022). 2022 Cybersecurity Skills Gap. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

Heidrick & Struggles. (2022). Global Chief Information Security Officer (CISO) Survey. https://www.heidrick.com/en/insights/compensation-trends/2022-global-chief-information-security-officer-ciso-survey

ISACA (2022). State of Cybersecurity 2022. Global Update on Workforce

Efforts, Resources and Cyberoperations. https://www.isaca.org/go/state-of-cybersecurity-2022

Karanja, E. & Rosso, M. (2017). The Chief Information Security Officer: An Exploratory Study. *Journal of International Technology, and Information Management*, 26(2), https://scholarworks.lib.csusb.edu/jitim/vol26/iss2/2

Marlin Hawk (2020). Global Snapshot: The CISO in 2020. https://www.marlinhawk.com/docs/Marlin-Hawk-Global-CISO-Research-Report.pdf

Matas, A. (2018). Diseño del formato de escalas tipo Likert: un estado de la cuestión. *Revista electrónica de investigación educative*, 20(1), 38-47. https://redie.uabc.mx/redie/article/view/1347

Maynard, S. B., Onibere, M. & Ahmad, A. (2018). Defining the Strategic Role of the Chief Information Security Officer. *Pacific Asia Journal of the Association for Information Systems*, 10(3), 61-86. Doi: 10.17705/1PAIS.10303

Monzelo. P. & Nunes. S. (2019). The Role of the Chief Information Security Officer (CISO) in Organizations. *19.ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI' 2019)*. https://www.researchgate.net/profile/Sergio-Nunes-2/publication/338833079_The_Role_of_the_Chief_Information_Security_Officer_CISO_in_Organizations/links/5e2eab2f299bf1e929d933b6/The-Role-of-the-Chief-Information-Security-Officer-CISO-in-Organizations.pdf

OEA-BID (2020). Ciberseguridad: Riesgos, Avances y el Camino a seguir en América Latina y Caribe. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Onibere, M., Ahmad, A. & Maynard, S. (2017). The Chief Information Security Officer and the Five Dimensions of a Strategist. *PACIS 2017 Proceedings*. 77. http://aisel.aisnet.org/pacis2017/77

Ozkaya, E. (2021). *Cybersecurity Leadership Demystified*. Birminghan, UK.: Packt Publishing Ltd.

Proctor, P. (2022). Make Cybersecurity a Priority Business Investment. *Gartner Webinars*. https://www.gartner.com/en/webinars/4014106/make-cybersecurity-a-priority-business-investment-in-your-apac-organisation

Proofpoint (2022). 2022 Voice of the CISO REPORT. Global Insights Into CISO Challenges, Expectations and Priorities. https://www.proofpoint.com/sites/default/files/white-papers/pfpt-us-wp-voice-of-the-CISO-report.pdf

PwC (2022). 2022 Global Risk Survey Embracing risk in the face of disruption. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/assets/pwc-global-risk-survey-report-2022-main.pdf

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, 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 Comunnidad CISOS.CLUB, CISOS-COL y CISOS-LATAM (Linkedin) y Miembro del comité editorial de la revista sistemas de ACIS.*

Seguridad híbrida

DOI: 10.29236/sistemas.n167a5

Un paradigma emergente

En este número 167 de la revista el tema para analizar en el marco de la sección Cara y Sello es la "seguridad híbrida, un paradigma emergente", encuentro al que fueron invitados varios especialistas.

"Es un privilegio contar con su presencia en esta reunión realizada en cada número de la revista para analizar los asuntos más relevantes del tema central, en este caso, sobre "seguridad híbrida, un paradigma emergente", señaló Jeimy J. Cano Martínez, director de la revista, acompañado en su bienvenida a los invitados por Andrés Almanza coeditor técnico en esta edición: Hamilton Moya, especialista en ciberseguridad; Wilson Prieto, consultor en ciberseguridad, Héctor Calderazzi, consultor independiente en desarrollo de políticas, normas y procedimientos y Arturo García, doctor en Defensa y Seguridad Nacional por la Universidad Naval de México, Gerente de Seguridad en Tecnologías de la Información en el Banco Central de México.

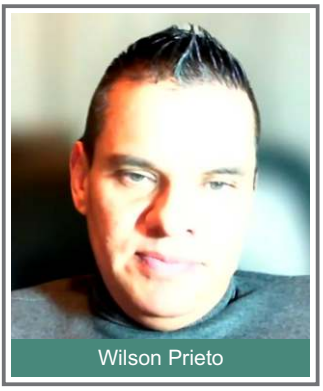
Después de la introducción los invitados procedieron a manifestar sus opiniones sobre las diferentes inquietudes planteadas.

Jeimy J. Cano M.
En un entorno cada vez más inestable, incierto, turbulento y ambiguo el concepto de seguridad debe evolucionar. En este sentido, ¿es necesario pensar ahora en una seguridad convergente? ¿Multidominio?

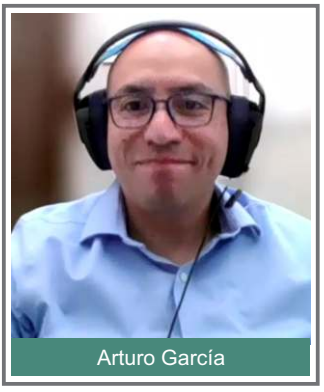
Arturo García
El término de seguridad nos refiere al concepto de paz. En ese sentido, sabemos que existen diferentes acepciones de paz. Las más comunes son la de "paz positiva", que refiere a la presencia de tranquilidad y armonía; y la "paz negativa" que implica la ausencia de conflictos. En mi opinión, lo que vivimos hoy en día en el ciberespacio es una "paz tolerada" que expresa la presencia continua de conflictos un punto tolerable pero que aún genera la sensación de tranquilidad.

De esta manera, existe realmente una evolución del concepto: estamos evolucionando hacia una paz que ya no es una ausencia de algo que nos ocasiona temor, pero tampoco estamos viviendo libres de preocupaciones. Yo creo que estamos tolerando esos conflictos, los cuales están escalando a diferentes dominios. Aquí es donde identifico claramente la connotación de


Hamilton Moya


Wilson Prieto


Héctor Calderazzi


Arturo García

"híbrido", que es lo que estamos revisando en este panel: se percibe tanto la parte de intangible, como el ciberespacio, como la parte tangible o física. Ambos dominios están convergiendo y ve claramente la tolerancia a esa inseguridad, un escenario gris de paz. Posiblemente estamos soportando más de lo que tal vez no deberíamos. Tenemos una gran tarea: repensar hacia donde queremos llegar.

Wilson Prieto

Entendiendo un poco la pregunta, pienso que la seguridad convergente o multidominio es un enfoque de seguridad que busca proteger múltiples dominios o sistemas informáticos utilizando una única solución de seguridad que proporcione la protección necesaria para minimizar el riesgo ante un posible ataque cibernético. Igualmente, este concepto se ha discutido durante los últimos años y puede verse como una estrategia enfocada a la protección de datos que unifique y coordine los esfuerzos del equipo de seguridad tanto en las entidades privadas como públicas creando un entorno seguro en diferentes contextos de la organización.

Por otra parte, la seguridad convergente puede aprovechar tecnologías emergentes que ayuden a prevenir posibles ciberataques y permite a las organizaciones enfrentar los desafíos de seguridad de manera más efectiva.

Hamilton Moya

Con respecto a la pregunta, desde mi punto de vista no es evolucionar hacia, porque los conceptos de una seguridad convergente y de seguridad multidominio ya se venían trabajando, por tal razón, creo que lo que se debe hacer es implementarla y arraigarla en las organizaciones, ya que muchos hablamos de que la seguridad debe ser aplicada en múltiples ámbitos de la organización, en los diferentes procesos, en las diferentes tecnologías que se utilizan, pero a veces se queda ahí, en aspectos aislados y no lo centralizamos, y esto, algunas veces, hace que se nos complique mucho más la tarea de asegurar o de disminuir ese factor de inseguridad que presentan nuestros activos. Como dije, para mí no es tanto evolucionar sino arraigar esos dos conceptos que ya se venían trabajando desde un tiempo hacia acá.

Héctor Calderazzi

Hay que tener una visión holística. Cuando me preguntan sobre seguridad convergente puedo afirmar que siempre he pensado con un enfoque integral de la seguridad de la información. Lo ideal es la convergencia, de tener el panorama del todo. Pero qué pasa, el costo de las herramientas para lograr esta convergencia y a veces aspectos estratégicos que no están bien definidos atentan contra dicha concentración. En este sentido me he encontrado con casos en los que, por ejemplo, adquirieron un "Qradar", con importantísimas inversiones en la herramienta y quedó "esperando en los cajones" un año o más, porque el personal no tenía la formación y no sabían cómo adecuar su implementación. Después me encontré con otro caso de migración de seguridad On-Premise a On-Cloud, en los que los responsables de sistemas decían "¿cuál es el sentido que nosotros controlemos a un proveedor On-Cloud de primer nivel internacional que lógicamente cumple con los estándares?". Es decir, tenemos una mezcla de situaciones estratégicas y culturales y observo que es más fácil una integración a nivel de lo que es el proceso de gestión de incidentes, antes que la integración de todo el ambiente. Coincido en comenzar por ahí, creo que lo dijo Wilson, integrar los conceptos más críticos, definirlos y establecerlos en forma uniforme a nivel de toda la organización. A su vez, varias organizaciones no tienen definiciones claras de todos los niveles de usuarios y sus permisos, no existen estándares de identificaciones de los usuarios, se utilizan usuarios genéricos y de servicio sin justificación, etc. Incluso no existen definiciones claras sobre control de cambios, muchas veces se implementa una metodología ágil y no se sabe dónde incluir el control de cambios. Dicho todo esto, estoy en un punto anterior todavía, me preocupa la estrategia integral de seguridad y después no tendría problemas que lo vayan implementando en forma multidominio, pero con un control centralizado.

Andrés Almanza

Quienes tenemos el privilegio de trabajar en el tema de seguridad llegamos a un momento en el que decimos la seguridad es de cobertura organizacional. Se trata de un pensamiento multidisciplinar para entender las múltiples vistas, las di-

mensiones de lo que empieza a suceder en la organización al hablar de protección y la generación de confianza de la información en sus diferentes formas.

Jeimy J. Cano M.

Las amenazas físicas se han transformado y evolucionado en diferentes contextos. En consecuencia, ¿cómo reconocer ahora estas amenazas en un entorno cada vez más incierto e inestable? ¿Cómo ayudar a las organizaciones en este nuevo ejercicio?

Héctor Calderazzi

Me parece que, respecto a metodologías y herramientas no hay una que sea la panacea. De hecho, si contamos con mucha información que puede servirnos como lecciones aprendidas y debemos ser autocríticos para repasar nuestro accionar hacia adelante. Pero, yendo a la pregunta concreta ¿cómo puedo reconocer las amenazas en un entorno cada vez más incierto? La respuesta sería por ejemplo mediante la realización de este tipo de reuniones, de la categoría de análisis de riesgo experto. En este momento no estamos leyendo ninguna matriz ni lista de amenazas específica, pero contamos con conocimientos de los riesgos en general, proponemos un escenario de riesgo, manteniendo los modelos a un costado que consultaremos en casos específicos. Proponemos el tema, abrimos el debate mediante lluvia de ideas, con una imaginación desde los zapatos del atacante, pensamos en el supuesto apetito que tiene el atacante, qué ven de interesante en nuestras organizaciones y en dónde estamos más débiles, en toda esa red que tenemos entre elementos lógicos, físicos (procesos, personas y tecnología). Por ejemplo, en una gran empresa de energía, hay una combinación entre lo que es la seguridad operacional y la seguridad lógica, que a veces no interactúa entre esos ambientes, no se comunican y esa desintegración juega en contra, cosas que sabe una parte de la organización y las desaprovecha la otra. Les cuento sobre esta organización que conocí, donde necesitaban tener una continuidad operativa durante los 365 días del año, con altos niveles de servicio y contaban con sensores automáticos (PLC – SCADA) que al llegar a utilizar un 80% a 90% de la capacidad instalada disparaban alertas. El punto es que todo ese control ope-

rativo no estaba integrado con la gestión de usuarios que llevaba seguridad lógica y tenía trabas para lograrlo. Creo que son aspectos propios de la naturaleza del negocio; en este caso el área operativa invirtió en tecnología avanzada y "desconoció" al área de TI, y por añadidura de pensamiento al área de Seguridad de la Información.

Finalmente, la incertidumbre de escenarios de riesgos que tenemos hoy en día surge sobre cuál es nuestro imaginario hacia adelante.

Hamilton Moya

Lo sintetizo en una expresión: vigilancia tecnológica. Considero que debemos estar haciendo vigilancia tecnológica permanente, pero, no únicamente de la tecnología que surge, esos cambios tecnológicos que nos ayudan a controlar, sino también en esos cambios tecnológicos que nos pueden llegar a generar más amenazas y que, por ende, nos pueden generar riesgos dentro de la organización. Por lo tanto, para mí es importante que quienes estamos gestionando la seguridad de la información, tengamos una actitud proactiva realizando actividades, como por ejemplo: análisis de riesgo, planificación, inteligencia de amenazas, estableciendo planes estratégicos, no haciendo trabajo individual sino colaborativo con el resto de las áreas de la organización, para evitar falta de comunicación y que los planes estratégicos vayan en una sola línea y cobijen al resto de la organización en procura de una seguridad multidominio.

Wilson Prieto

Es indudable que las amenazas físicas han experimentado una evolución y sofisticación considerable en los últimos años, lo cual ha generado un entorno de seguridad más incierto e inestable. En vista de ello, resulta crucial que las organizaciones adopten un enfoque holístico y proactivo en materia de seguridad física para poder identificar y hacer frente a estas amenazas en este nuevo contexto.

En consecuencia, resulta imperativo que las entidades dispongan de un plan de seguridad física sólido, el cual debe ser evaluado y actualizado de manera regular. Esto permitirá identificar posibles debilidades y vulnerabilidades que puedan comprometer la integridad de la entidad, y tomar las medidas necesa-

rias en línea con el plan de continuidad del negocio.

Otro aspecto de vital importancia radica en la inversión en tecnologías y herramientas de seguridad física avanzadas, que posibiliten la detección y monitorización de amenazas, así como el control de accesos no autorizados. Además, es esencial implementar medidas adicionales especialmente en un contexto en el que el trabajo remoto ha experimentado un incremento considerable, generando una brecha de seguridad en las organizaciones.

Por último, resulta fundamental proporcionar capacitación a los empleados en materia de seguridad física, dotándolos de conocimientos sobre técnicas de prevención y protección de datos para evitar el robo de información confidencial. Igualmente, fomentar la colaboración y cooperación con las autoridades locales y otras partes interesadas para mantenerse al tanto de las posibles amenazas cibernéticas y poder informar de manera eficaz cualquier incidente de ciberseguridad y seguridad física que pudiera surgir.

Arturo García

A pesar de que las amenazas y sus efectos están convergiendo, veo una constante en muchas organizaciones de todo tipo, públicas y privadas, en mantener una separación en las funciones de protección. Por ejemplo, en algunas corporaciones la seguridad muchas veces se focaliza en su vertiente física separada de las tecnologías de información, y viceversa, siendo que los efectos negativos implican afectaciones en ambos dominios, lo cual genera un problema mayor. Cuando ocurre un incidente, como en infraestructuras críticas del Estado, no importa si el origen es físico o del ciberespacio. Cuando el impacto escala se afecta en diferentes sentidos a la población, en diferentes campos: económico, político, diplomático, etc. Este escalamiento en las afectaciones no se está analizando como debía ser, siendo una causa intrínseca del escalamiento.

Me parece que es una parte de madurez en las empresas, en las organizaciones, en donde se debería dar un paso más fuerte, hacer una real integración de funciones. Como decía el doctor Cano: cuando tenemos un ambiente ciberfísico necesitamos gente que no solo deber saber de tecnología, también debe estar preparada en diferentes aristas y trabajar en equipo. Hay que tomar en cuenta el ambiente multidisciplinario de las consecuencias. Hoy debemos ver esas nuevas amenazas desde diferentes perspectivas y de manera integrada. En un mundo VICA esa es la única forma en afrontarlas de forma exitosa.

Jeimy J. Cano M.

El reto de la seguridad se ha transformado con el paso de los años.

En este sentido, la literatura advierte que el modelo de prevención se viene agotando. Así las cosas, si el reto es ir más allá de la prevención, ¿qué se debe actualizar, incorporar o deconstruir en las prácticas actuales para responder a la incertidumbre y la inevitabilidad de la falla propia de una sociedad cada vez más digital y tecnológicamente modificada?

Wilson Prieto

En la actualidad, el enfoque de prevención tradicional ha demostrado ser insuficiente ante el creciente número de ciberataques en un entorno digital y tecnológicamente cambiante. En este sentido, es crucial adoptar un enfoque integral de seguridad que incluya la detección temprana y una respuesta rápida frente a las amenazas cibernéticas. Esto implica la incorporación de tecnologías avanzadas de detección, análisis de amenazas y procesos ágiles y eficaces para gestionar los incidentes.

Es fundamental especializar a los profesionales en el tema de las amenazas cibernéticas y contar con expertos en caso de ataques, además de utilizar tecnologías y procesos especializados para la detección.

Debemos promover una cultura de ciberseguridad en toda la organización, no solo en el aspecto técnico, sino en todos los niveles, para que todos sepan cómo actuar en caso de un ataque cibernético.

La gestión de riesgos también desempeña un papel crucial y debe ser proactiva, basada en datos y estadísticas, para identificar posibles amenazas y evaluar su impacto potencial en la organización. El monitoreo continuo, respaldado por tecnologías y capas de seguridad especializadas, es esencial para identificar amenazas reales y garantizar la ciberseguridad de la compañía.

La integración de tecnologías avanzadas, como la inteligencia artificial y el aprendizaje automático, resulta imprescindible en la detección automática de amenazas. Asimismo, es importante contar con un plan de respuesta y recuperación efectivo que permita a la organización recuperarse y restaurar sus operaciones en caso de un ciberataque.

En resumen, es necesario abandonar el enfoque de prevención tradicional y adoptar un enfoque integral de seguridad cibernética que combine tecnología avanzada, capacitación especializada, gestión de riesgos proactiva y un sólido plan de respuesta y recuperación.

Hamilton Moya

Considero que prevenir no es la única forma de atacar la inseguridad a la que nos vemos enfrentados, pero entonces, que deberíamos hacer, pues adelantarnos a esta situación, entonces, si ya no puedo tener un modelo preventivo, tendría que tratar de pasarme a un mo-

delo predictivo, tratar de establecer a nivel de predicción que me puede llegar a pasar, a que riesgos puedo verme abocado pensando en esa tecnología tan prolifera que hay y tan avanzada y que sale constantemente, entonces, debemos ser predictivos y tratar de deconstruir ciertas ideas que tenemos. Un ejemplo muy pequeño, en cuantas empresas pequeñas, medianas, grandes, que invierten en seguridad o que ya tienen modelos de seguridad implementados, no hemos escuchado la expresión: "eso fue un problema de seguridad, se tiene que encargar el equipo de seguridad, el ciso, los analistas de seguridad". Debemos tratar de romper esa estructura mental de que la seguridad es solamente de un equipo, debemos interiorizar que la seguridad somos todos, volvernos convergentes, involucrar a todos los actores de la organización y decirles, ustedes hacen parte importante de esa protección, de esa seguridad de nuestra organización.

Adicionalmente, como parte de esa deconstrucción, es aplicar técnicas de resiliencia, participación activa de la alta dirección, esto último, es un concepto que hay que deconstruir, yo he visto y creo que muchos de quienes nos dedicamos a la seguridad, nos hemos encontrado en organizaciones donde la participación activa de la alta dirección es acá tienen el capital, acá tienen el presupuesto para algunas estrategias que se vienen trabajando y ya, y se considera que esta es la participación activa a través de la alta dirección, pero no, se deben involucrar en los procesos, impulsar y hacer esa divulgación de esa seguridad y decirle a todas las partes interesadas de la organización "hagámonos partícipes, somos uno solo protegiendo todos nuestros activos".

Arturo García

La pregunta me parece en extremo retadora: ¿cómo proceder ante la inevitabilidad? Esto es totalmente real; de hecho, esto es algo que he estado revisando en incidentes pasados de gran magnitud. A pesar de que existen países con fuertes estrategias de seguridad, mayor poder físico, legislación madura y múltiples organizaciones, te das cuenta que no necesariamente las hace invulnerables a brechas de ciberseguridad. Como dicen por ahí: "solamente existen dos tipos de empresas: las que ya hackearon y

las que van a hackear". Se podría añadir incluso unas terceras: las que no saben que las están hackeando. En ese sentido creo que hace mucho la labor de concientización sobre ese fenómeno.

También me parece que falta incorporar una figura diferente en las organizaciones que se conocería como "Chief Disruptive Officer", esto es, una figura de disrupción. Alguien que identifique escenarios cuando algo sale mal, que elabore escenarios donde algo no funciona como debería, y así pensar en cómo se podrían solucionar. Para muchos autores, esta es una gran diferencia entre la administración del riesgo, algo que piensas que puede ocurrir, y la ciberresiliencia, cómo adaptarse cuando algo que ni pensabas que podría ocurrir, sucede.

Recuperando las ideas del doctor Cano, debemos pensar en qué es lo que pasa después de un ciberincidente a más largo plazo, no inmediatamente, reflexionar sobre lo que ocurrió y cómo debes transformarte. Se debe tomar el tiempo necesario para meditar sobre las lecciones aprendidas, puede haber mucho conocimiento, mucha experiencia, mucha sabiduría, saber qué es lo que pudiste haber hecho diferente o que es lo que hay que transformar, conjugar el punto de vista académico y la experiencia práctica.

Actualmente no alcanzo a identificar con claridad qué es lo que cambiaron las organizaciones después de ser víctimas de un incidente de alto impacto, qué proceso cambió, qué personas o figuras se cambiaron para atender un nuevo escenario, qué fue lo nuevo que hicieron. Hoy en día, esto no se expresa y sería un excelente punto para mejorar.

Héctor Calderazzi

Pensar hoy en prevención es ser más resilientes. Esto significa contar con más información para poder actuar lo antes posible ni bien se detecta el incidente, toda vez que en varios escenarios no podemos prevenir su ocurrencia (generalmente porque no disponemos de las capacidades para hacerlo). Ser más resilientes es ajustar o tener la puntería de la detección lo más temprana posible, los pasos que hay que hacer para salir adelante y la recuperación si tuviera que recuperar la información en caso de un desastre. Ser resiliente es hacer una gestión del incidente de la forma más temprana posible y es parte de un análisis de riesgos preventivo, en donde ante la incapacidad de prevenir el incidente, se analiza qué se ejecutará o cómo se trabajará cuando el incidente ocurra. En otras palabras, es como ser lo más ágil para recuperarse lo más rápido posible, limpiar los falsos positivos, ajustar todas las situaciones y a su vez, definir que más se va a hacer ante el incierto o la ocurrencia de un incidente sobre el cual no tenemos experiencia, ni información de referencia.

En resiliencia podemos hacer un paralelismo con la prevención sobre lavado de activos, en donde se establece la política "conozca a su cliente". Aquí, se debe conocer cuál es la operatoria normal del cliente, pero este un día hace un depósito muy grande, entre otros controles, debemos averiguar sobre el origen genuino de esos fondos. Este análisis de comportamiento es trasladable al ambiente de Seguridad de la Información. Conocer si un usuario ingresa todos los días a nuestro sitio, en qué horarios y que acciones realiza. Este concepto que también se incluye dentro de la metodología "confianza cero". Asignar los mínimos privilegios necesarios, aplicar trazabilidad por todas las transacciones críticas que se realizan y análisis de comportamiento. A su vez, los análisis de comportamiento van a ligar a lo mejor con situaciones de "lecciones aprendidas" que ya conocemos, pero otras situaciones pueden ser nuevas, y algunas pueden ser operativas. En este sentido puedo agregar otro caso experimentado, relacionado con el sistema de información de prevención de lavado de activos (PLD). Cuando un cliente tomaba un préstamo por encima de los $50.000 se generaba un registro automático para PLD, pero el sistema fallaba y no controlaba el acumulado de varias operaciones que sumaban los $50.000 en su conjunto. Entonces el funcionario que conocía esa vulnerabilidad, y con mala intención confeccionó varios movimientos de cuyos valores individuales eran inferiores a $50.000, pero en su conjunto superaban ese parámetro. Esto determinó el análisis de la vulnerabilidad, el comportamiento de la persona, de las transacciones realizadas y permitió utilizar esa información para comprobar el adecuado funcionamiento de otras personas, procesos y tecnología, cruzando dicha información por vectores según diferentes criterios de análisis de comportamiento y proyección.

Jeimy J. Cano M.

Basados en sus respuestas se destacan algunas reflexiones. Prevención, no detección temprana; respuesta rápida y especializar personas. Así mismo, movilizar esfuerzos hacia los pronósticos basados en datos y en registros.

Hamilton Moya

Muchos de los CISO´S y de los encargados de la seguridad confundimos cumplimiento con aplicación de controles de seguridad, entonces asumimos que si cumplimos las normas, como la 27.001, cumplimos una lista de controles, ya estamos seguros, pero, esa implementación de controles solo la cumplimos para presentar una auditoría, mostramos en papel, si no tenemos algo implementado le damos manejo para poder responder lo que quiere oír el auditor, solo para pasar la auditoria, y al final, pasamos una auditoria, logramos la certificación, eso es lo importante, y ese tipo de cosas nos da una falsa sensación de seguridad.

Considero que todos debemos estar preparados para las fallas inevitables y para enfrentarlas, debemos ser proactivos, cambiar el esquema, pasar de un feedback a un feedforward, no llegar a mirar solo lo malo que sucedió, sino, mirar también que debo corregir para mejorar eso que hizo que se presentara una falla.

Resumiendo, aunque es importante contar con esas herramientas que nos dan confianza y nos dan tranquilidad, nos hace falta ir un poco más allá, ser proactivos, mejorar la cultura de ciberseguridad, nos falta mejorar muchos aspectos a nivel organizacional.

Jeimy J. Cano M.

¿Las buenas prácticas de seguridad y control vigentes en las organizaciones son suficientes para lograr concretar la confianza y tranquilidad que requieren las organizaciones en un escenario como el actual? Explique su respuesta.

Arturo García

Esta pregunta me fascinó pues la regulación es un problema complejo con soluciones inexactas y de difícil comprobación objetiva. Por ejemplo, ¿qué tanto es tantito?, ¿estás sobre regulando o subregulando? Existe literatura que indica que la sobrerregulación puede ocasionar exactamente el efecto contrario de querer fomentar la protección de la organización. Muchos CISOs están preocupados por el cumplimiento porque va a llegar una autoridad y los sancionará, o porque va a llegar una auditoria y les asignará observaciones, o porque no cumplieron un compromiso contractual que podría causar sanciones. Entonces tratan de cumplir lo mejor posible para obtener una palomita.

Lamentablemente, el fenómeno de "cansancio por cumplimiento" puede dejar sin atender algunos otros elementos básicos, muy necesarios para la protección informática. Coincido con lo que dice de la Ley de ciber-Pareto: el 80% de los ataques son generados por el 20% de las cosas que no hicieron bien, esto es, no se actualizó una aplicación o no se bloqueó un puerto de acceso.

A lo mejor esto sucede por causa de una sobre regulación y de la preocupación o estrés extremo que causa el cumplimiento. Por otro lado, también es un riesgo la subregulación; esto es, dejar de regular algún aspecto por el que podría generarse una brecha de seguridad. Eso también es observable. La sana medianía es muy complicada y es uno de los grandes retos a la hora de hacer políticas correctas, eficientes y efectivas. Ese punto aún no tiene una respuesta concreta y eso sería tal vez tema para otro panel.

Wilson Prieto

Es fundamental tener en cuenta que las buenas prácticas de seguridad y los marcos de referencia constituyen una base sólida en el

ámbito de la seguridad cibernética. Las organizaciones tienen a su disposición estándares y una abundante información que resulta valiosa. No obstante, es importante reconocer que los actores de amenaza actuales se encuentran en constante evolución y sofisticación, lo cual implica que estas prácticas pueden resultar insuficientes para responder de manera adecuada ante una amenaza o ciberataque.

En este sentido, es importante que las organizaciones adopten un enfoque proactivo y no reactivo en cuanto a la seguridad para que puedan responder rápidamente ante un incidente cibernético. Esto significa que deben implementar medidas de seguridad y control no solo para prevenir las amenazas conocidas, sino también para detectar y responder a las amenazas desconocidas y emergentes. Un plan de respuesta a incidentes robusto es de suma importancia y como mencionó Andrés, llevar a cabo simulacros o ejercicios de equipo rojo de forma regular resulta crucial para evaluar la capacidad de resiliencia de una organización frente a un posible ataque cibernético.

Es necesario que las organizaciones adopten un enfoque más proactivo y holístico de la seguridad, abordando todos los aspectos del ciclo de vida de la seguridad, que incluye la detección, respuesta y recuperación. Es fundamental identificar y evaluar tanto los riesgos actuales como los que puedan surgir a corto y largo plazo. Esto implica implementar sistemas de monitoreo continuo, adoptar tecnologías avanzadas de seguridad como la inteligencia artificial y el aprendizaje automático, y establecer planes de respuesta y recuperación en caso de emergencias. Además, el monitoreo continuo y la gestión de identidad son aspectos de vital importancia para prevenir accesos no autorizados en la empresa.

La realización de pruebas de penetración y simulaciones de amenazas, junto con la colaboración y comunicación con otras organizaciones, son medidas altamente efectivas para fortalecer las mejores prácticas de seguridad cibernética. Estas acciones contribuyen significativamente a mejorar las defensas y garantizar la protección de los sistemas y datos frente a posibles ataques.

Héctor Calderazzi

En este punto, lo primero que me pregunto es ¿qué requieren las organizaciones? Porqué lo tienen que bajar desde el directorio, involucrar al directorio. El dueño de la seguridad de la información de la empresa no es el CISO. De vuelta digamos que es un tema primario, el directorio es el que determina los lineamientos y aprueba las pérdidas anuales esperadas (ALE) que está dispuesto asumir por incidentes de Seguridad de la Información. Hay organizaciones que son más riesgosas, de por sí, que están acostumbradas a que juegan con

inversiones que son más volátiles y hay otras que son más conservadoras. Tienen distintas culturas de riesgos y eso mismo se baja hacia toda la organización. Existen directores que no quieren escuchar sobre temas de seguridad, cuando en realidad para darle más confianza y tranquilidad a las empresas, ellos primero tendrían que bajar como lineamiento y decir, por ejemplo, nosotros queremos en tema de seguridad compararnos con tal nivel del mercado, entonces el profesional vuelve con una propuesta, para que después no se generen falsas expectativas. Es fundamental determinar esos valores que tienen que venir desde la dirección, que justamente están relacionados con temas de la cultura de las organizaciones y que se necesitan para darle todo el apoyo a las estructuras, porque siempre se necesitarán inversiones en personas, procesos y tecnología, y este apoyo es todo lo que el directorio podrá dar en materia de seguridad de la información para seguir adelante.

Por otra parte, me ha pasado en otra organización donde el responsable de seguridad me pidió ayuda para implementar la norma ISO 27001. Comencé a interactuar con su colaborador quién me dijo que le gustaba el modelo “Cis Controls”, seguí con otros colaboradores y se veían muy apegados al modelo Mitre. Llevó un tiempo lograr un acuerdo sobre la metodología a adoptar. Entonces para dar la tranquilidad ¿qué se debe hacer? Involucrar a la dirección en la aprobación de la metodología. El hecho de preparar la metodología y simplificar su explicación para su aprobación logrará el acuerdo en las definiciones básicas de las buenas prácticas de seguridad y desde allí en más se podrá crecer permanentemente en los nuevos escenarios, que se necesitan para ofrecer mayor confianza y tener tranquilidad.

Asimismo, siguiendo con la buena práctica, en el hipotético caso que se defina apetito cero de riesgo para seguridad, nuestra propuesta sería detallar todas las inversiones que tendrían que hacerse en capacidades para lograr ese objetivo, que de hecho serían onerosas. Aunque la decisión será facultad de la dirección.

En otras palabras, tendremos que presupuestar fondos para procesos, personas y tecnología, y la dirección posiblemente nos diga “Uds. están locos”. Esto nos hace menos perfectos, es una negociación permanente.

Entonces, ¿qué hace el responsable de seguridad de la información?, mira si el presupuesto preparado hace a la empresa estar más expuestos, si podremos tener una brecha de seguridad o no; es decir este es el trabajo del CISO, alertar a la dirección, pero ellos son los que fijan la estrategia general de la organización y deciden cuál modelo adoptar, según la relación costo/beneficio.

Jeimy J. Cano M.
Interesantes aportes, particularmente la palabra "cumplimiento", que cuando se pronuncia en dos tiempos a veces se vuelve real: cumplo y después miento, en particular, frente a los estándares. De otra parte, está el tema de las pérdidas esperadas, un concepto que en seguridad nosotros debemos tener en mente, pues en algún momento nos sorprenderá la inevitabilidad de la falla. Lo anterior nos remite al apetito de riesgo para concretar una nueva conversación entre el CISO (*Chief Information Security Officer*) y el equipo ejecutivo. Aquí le doy paso a Andrés con la frase que generalmente usa donde la ciberseguridad ocurre en la conversación.

Andrés Almanza.

Así es. La frase completa es "la ciberseguridad no sucede en la implementación, sucede en la conversación". Yo creo que la pregunta si es pregunta, es decir, están listas las prácticas de hoy para el momento y coyuntura actual, mi respuesta es no. Eso no quiere decir que estas prácticas no sean buenas y su aplicación no genere beneficios importantes. De otra parte, hay una palabra clave que es confianza y si vamos a hablar de confianza, esto es un ejercicio de conversaciones, no de implementaciones. Por esto insisto en que la conversación de un CISO resulta de una habilidad esencial, y más en esta pregunta, en donde yo necesito establecer un vínculo de confianza. El reto es prepararse y anticiparse, más que prevenir, y creería que otra práctica muy de la pregunta es desarrollar adaptabilidad en el momento. La adaptación como dice un libro que me gusta "*The handbook of Anticipation*"[1], se da en los momentos desconocidos, y la anticipación dice el autor, se da para los momentos conocidos; por tanto, tenemos que trabajar una nueva práctica mucho más desarrollada en conversar y una muy buena en adaptarnos.

Jeimy J. Cano M.
¿Qué deben hacer en forma diferente los ejecutivos de seguridad (en sus diferentes especialidades) para acompañar a las organizaciones en su creciente apetito de

[1] Poli, R. (Ed.) (2019). *Handbook of anticipation. Theoretical and Applied Aspects of the Use of Future in Decision Making*. Cham, Switzerland: Springer Nature Switzerland AG

riesgo cibernético, una mayor demanda de negocios y oportunidades digitales?

Wilson Prieto

Considero que los ejecutivos de seguridad deben adoptar un enfoque proactivo y estratégico en su gestión de seguridad. Es fundamental que posean un sólido conocimiento del negocio para poder identificar los riesgos reales asociados a la organización. Esto implica participar en la planificación estratégica, implementar un enfoque de gestión de riesgos, colaborar y comunicarse efectivamente con otros líderes, invertir en capital humano especializado y tecnología, priorizar las medidas de seguridad en función del impacto potencial de negocio y promover una cultura de seguridad en toda la organización.

Es de vital importancia adoptar una postura proactiva en cuanto a seguridad se refiere. Esto implica comprender y anticiparse a las tendencias y amenazas emergentes. Los altos ejecutivos deben estar plenamente preparados para responder de manera ágil ante cualquier incidente que se presente, colaborando estrechamente con sus equipos de seguridad y otros ejecutivos involucrados. Asimismo, es fundamental evaluar el impacto económico, profesional y tecnológico que podría tener un ataque en la organización.

Además, es crucial comunicar la importancia de la seguridad de manera efectiva. Los altos ejecutivos deben tener un profundo entendimiento de la seguridad y ser capaces de transmitir este conocimiento desde la alta gerencia. También deben respaldar a los líderes internos para que promuevan las mejores prácticas de seguridad a través de su comunicación. La presencia de ejecutivos comprometidos con la seguridad desde la alta gerencia desempeña un papel fundamental en la educación de las personas en este ámbito.

En resumen, los ejecutivos de seguridad deben ser aliados de las organizaciones, comprendiendo tanto el negocio como la estrategia, alineando la seguridad con los objetivos empresariales, adoptando un enfoque basado en el riesgo y mostrándose proactivos en materia de seguridad. Además, es fundamental que puedan comunicar de manera efectiva la importancia de la seguridad y brindar apoyo a los líderes internos para promover la educación en las mejores prácticas. En mi opinión, eso sería lo que consideraría como la respuesta adecuada a la pregunta planteada.

Arturo García

Las preguntas que nos hacen son muy buenas pues son cuestionamientos que te hacen reflexionar. Por ejemplo, no sé si hay que hacer algo totalmente diferente, sino tal vez se requiere que lo ya se conoce se ejecute mejor, de forma efectiva, medible, auditable, concreta y objetiva. Por ejemplo, pensemos en al-

go básico que se hace en todo el mundo: la labor de concientización. Esas campañas y esfuerzos habría que fortalecerlas y mejorarlas. Me explico ¿qué tal si incorporamos profesionales de mercadología? Sí, de esos profesionales que saben vender productos comerciales; tal vez requerimos psicólogos que conocen la mente humana y cómo reaccionan ante elementos nuevos, sorpresivos o incluso del día a día. Hace poco estuve en unas sesiones de neurociencias aplicadas a la ciberseguridad, en donde revisaban por qué las personas hacen lo que hacen, ¿por qué caen en ligas de ransomware o de phishing? O en momentos de crisis ¿cómo reaccionan? Es muy probable que la solución es ver las situaciones con un enfoque más amplio que solo centrarse en el enfoque tecnológico. Desconozco el número de empresas que estén haciendo esto, pero definitivamente me parece la manera correcta de hacer algo que ya conocemos, pero de manera más efectiva.

Héctor Calderazzi
El tema de la comunicación, el involucramiento de toda la organización es fundamental y es necesario profundizar en este aspecto. Siempre digo que el profesional de seguridad en la información tiene que ser más estratega que un técnico. Ahora fíjense justamente cuando observamos y analizamos desde un lado, el ranking de riesgo de la organización, “no pega ni con cola” con un plan estratégico de seguridad. Y esto me paso más de una vez, yo espero que un plan estratégico en seguridad de la información esté relacionado de alguna forma con un orden de un ranking de riesgo de seguridad en información de la organización.

Y cómo son dos estamentos diferentes, por ejemplo, si a su vez cada uno trabaja con su criterio y falta la integración conceptual, los resultados no serán estratégicos o no conducirán a mitigar los principales riesgos de seguridad.

El tiempo del ejecutivo de trabajo de un ejecutivo de seguridad tiene que ser 50% con su gente, liderando el equipo, viendo que pasa, en lo que temas están procesos internos (personas, procesos y tecnologías afectadas) y el otro 50% haciendo “lobby sano” con toda la organización, trabajando con sus pares, con los gerentes de mandos medios y la comunicación con la dirección, además de tener en cuenta que cuando tiene reuniones con el comité directivo, tiene entre uno y cinco minutos para explicar la situación, y que después perderá la atención.

Jeimy J. Cano M.
Es decir Héctor, como dicen ustedes “nos dan pelota” solo cuando algo pasa.

Héctor Calderazzi
Desde la definición temprana de los riesgos de seguridad de la información, me surge la siguiente expe-

riencia para compartir. El gerente de seguridad en información de una empresa estaba molesto con el área de desarrollo. Decía que no le hacían caso en el desarrollo de los controles de seguridad en la información. Entonces mi pregunta fue ¿qué les pediste? Y decía simplemente que desarrollen controles. Y mi pregunta siguiente fue: ¿qué controles le pediste? Y la charla quedó allí, sin una respuesta concreta. Mi sugerencia fue, debería comenzar pidiendo tres controles y después su medición. Por ejemplo, controles básicos de restricción de acceso, control de cambios y limitaciones para la alteración de datos. Luego se ponen de acuerdo en desarrollar esos controles, en evaluar posibles dificultades, en consensuar su implementación y comienzan a hablar todo el mismo idioma.

Esta comunicación fundamental a veces no es bien manejada por personal de seguridad, que generalmente son muy fuertes en formación técnica, pero tienen más dificultades de manejo de relaciones humanas.

Creo que la persuasión sobre la necesidad de los controles es fundamental. Nosotros teníamos un gobernante, en los años ochenta, que decía “con la democracia se come, se vive, se respira…” y esta persona iba a todos lados con el mismo discurso. En este sentido podríamos decir, por ejemplo, que con la seguridad se come, se vive, se respira y a todos los lugares vamos con este léxico, y por supuesto obramos en consecuencia.

Hamilton Moya

Primero, más que cambiar considero que debe ser reforzar. Por ejemplo, dijimos dejar de ser tan reactivos y volvernos más proactivos, no es volvernos, porque ya somos proactivos, solo que nos falta un poco más, debemos reforzar y mejorar esta proactividad en todos los que tenemos un rol de seguridad y todas las partes interesadas de la organización.

Segundo, mejorar la comunicación entre las diferentes áreas de la organización, quienes cumplimos un rol de seguridad en la organización no somos un mundito aparte. Hablamos de que la seguridad es logística, pero casi siempre trabajamos solos, en ese orden de ideas, considero que debemos involucrar a todas las partes de la organización, a todos los directivos e incorporarlos en un plan de trabajo conjunto.

Tercero, tenemos que volvernos vendedores de la seguridad al interior de nuestras organizaciones, vender correctamente la seguridad, lograr ese patrocinio de los directivos o de la alta gerencia. Considero que debemos mejorar esta parte, mostrando como la seguridad se alinea con las estrategias y los objetivos de la organización, porque si no lo hacemos, sencillamente no nos ven, nos prestan atención únicamente cuando pasa

algo, y esto, porque no vendemos correctamente, porque nos falta ese marketing.

Jeimy J. Cano M.
Al revisar todas las intervenciones encuentro un hilo conductor que es el tema del lenguaje, construir un lenguaje común. Una manera distinta de comunicar, que nos lean. Connotaciones que hablan de un nuevo lenguaje que conecte y movilice 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 encontrarnos con el negocio, y terminar (o minimizar) los desencuentros permanentes de la seguridad y el modelo de generación de valor de la empresa. Por tanto, el CISO tiene que ser un estratega, esto es, alguien con una agenda que mueve, conecta y moviliza, desde un discurso concreto y seductor, para ubicar una distinción en el imaginario de las personas.

Jeimy J. Cano M.
Surtidas todas las preguntas lo que quisiera ahora para ir cerrando nuestro panel es que cada uno de ustedes haga una reflexión final a la luz de lo que hemos conversado.

Arturo García
Como cierre me parece que el escenario que estamos viviendo requiere de una visión interdisciplinaria, en donde tenemos efectos claramente ciber físicos, por lo que así hay que prepararnos y responder ante lo inevitable. Hay que pensar fuera de la caja, pensar las cosas que no nos han pasado, pero que nos pueden pasar. Reflexionar qué más se necesita, qué recursos nos hacen falta. Atender el binomio de escasez e inevitabilidad: escasez de recursos, tiempo, dinero, esfuerzo. Le pueden preguntar a cualquier profesional en cualquier parte del mundo sobre los recursos y siempre le va a faltar gente, dinero y tiempo. Estamos a tiempo de reflexionar e instrumentar acciones fuera de la caja.

Hamilton Moya
Mi reflexión es que debemos crecer como proceso a la par que va creciendo la tecnología, también debemos crecer a nivel profesional y tratar de entender todos esos nuevos conceptos, como lo planteaban hace un rato, no solamente es la parte técnica, no solamente es la parte tecnológica, sino la parte humana, la parte de liderazgo la que nos puede hacer mejorar las situaciones o las circunstancias de seguridad a las que nos enfrentamos dentro de una organización, en resumidas cuentas, el crecimiento continuo, la visión constante de los diferentes cambios y la adaptación a esos cambios que vienen surgiendo.

Héctor Calderazzi
Mejorar el sentido de la comunicación con todas las líneas, con la dirección, con los mandos medios y con las líneas inferiores, con los procedimientos que ya se conocen, que se trabajan.

Wilson Prieto
En resumen, la alta gerencia tiene la responsabilidad de liderar el negocio y debe adoptar un enfoque proactivo y estratégico para respaldar a la organización en cuanto a riesgo cibernético, así como aprovechar las oportunidades digitales mediante la implementación de tecnología emergente para mitigar el riesgo cibernético. Esto implica la contratación de personal especializado, promover una cultura de seguridad, diseñar nuevos procesos y procedimientos que sean ágiles y adaptables. Un aspecto destacado, mencionado por algunos colegas, es la formación de un equipo interdisciplinario con el fin de identificar posibles amenazas desconocidas para la organización. El compromiso tanto de la alta gerencia como de todos los líderes y miembros de la organización contribuye significativamente a la ciberseguridad de la entidad.

Seguridad A.H.I (Asimétrica, Híbrida e Interconectada)

DOI: 10.29236/sistemas.n167a6

El reto de una seguridad convergente y multidominio.

Resumen
La dinámica del mundo actual establece retos y exigencias para las organizaciones y sus planes estratégicos, así como para los Estados. Desde una perspectiva disciplinar, la comprensión de este escenario no permite reconocer y abordar la creciente y desbordada complejidad que implica desarrollar nuevas apuestas de negocios e iniciativas estatales para motivar transformaciones y crear experiencias novedosas.

En este sentido, es necesario transformar el paradigma de seguridad lineal y conocido, propio de los estándares y buenas prácticas vigente, por uno de seguridad asimétrica, híbrida e interconectada, detallado en este artículo, en la búsqueda de una mirada más holística de la realidad, para desde allí explorar el reto de seguridad y control de forma convergente y multidominio, como una respuesta natural a un entorno en donde 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 habilitar su viabilidad en el largo plazo.

Palabras claves
Asimétrico, Híbrido, Interconectado, Convergencia, Multidominio

Introducción

El mundo asiste a un cambio estructural y dinámico en la medida que múltiples dominios (políticos, económicos, sociales, tecnológicos, legales y ambientales) interactúan entre sí, reforzándose mutuamente unos a otros en ciclos de causa-efecto no lineales, creando escenarios inéditos y desconocidos que las organizaciones y las naciones deben comenzar a identificar, comoquiera que no hacerlo los expone a condiciones y resultados que posiblemente no podrán manejar o tratar de cara a la defensa de los intereses estratégicos y de sus grupos de interés (WEF, 2023).

Este nuevo escenario de "policrisis" resultado de una interrelación de momentos, contextos y situaciones que se materializan a nivel internacional, motivan inestabilidad, incierto y algunas veces caos, que llevan a las empresas y países a movilizar diferentes alternativas que les permita navegar con el menor impacto sobre los riesgos emergentes que se generan y las expectativas propias de sus clientes y ciudadanos (Colomina et al., 2022). En línea con lo anterior, saben que no podrán asegurar ningún resultado en sí mismo, por la fragilidad inherente de las relaciones internacionales y la cadena de suministro, las vulnerabilidades tecnológicas, sociales y cognitivas que revisten la sociedad actual y los mercados globales, obligando a un cambio de postura en su relación con su entorno y las prácticas de negocios.

Así las cosas, las organizaciones y las naciones deberán motivar acciones que preparen a sus colectivos para concretar condiciones de resiliencia empresarial y nacional respectivamente, sabiendo que el "nuevo anormal" es la nueva base de las capacidades que se requieren para enfrentar las debilidades de los gobiernos, las tensiones geopolíticas, la mayor superficie de ataque, la especialización e innovación de los adversarios, los estallidos sociales y la crisis climática (Renn, 2018). Esta nueva realidad, rompe con los paradigmas actuales de la gestión de riesgos que por lo general tratan de ubicar certezas desde perspectivas disciplinares para desde allí movilizar acciones que estimulen iniciativas en las organizaciones o Estados.

En este sentido, se requiere una revisión y desarrollo de nuevas propuestas para el análisis, comprensión y anticipación de los riesgos a nivel corporativo y nacional sabiendo que es necesario estar vigilantes para actuar y continuar operando aun cuando se materialice la inevitabilidad de la falla (visible o invisible). Esto es, reconocer un escenario interconectado con efectos cascada, donde la volatilidad multidominio crece de manera paralela

con efectos inesperados, y se erosionan cada vez más las capacidades resilientes de personas, empresas y Estados por cuenta de riesgos profundamente conectados con resultados no esperados y efectos de borde que exceden los mejores pronósticos de los analistas (Sheffi, 2020).

En consecuencia, este artículo introduce un modelo de seguridad asimétrica, híbrida e interconectada (Modelo A.H.I) que busca situar tanto a empresas como naciones en un ejercicio de comprensión y tratamiento de riesgos en un contexto multidominio. Lo anterior, implica la interdependencia y el acoplamiento de los diferentes actores, los flujos asimétricos de mercancías, tecnologías, personas, dinero e imaginarios sociales, para habilitar un diálogo interdisciplinar que tenga como insumos las inestabilidades y los inciertos con el fin de acelerar el aprendizaje/desaprendizaje colectivo, y así abrir nuevas fronteras para responder a la interconexión global y la necesidad de una seguridad convergente y multidominio.

Fundamentos conceptuales: Contexto asimétrico, híbrido e interconectado

Para concretar el reto de una seguridad A.H.I (Asimétrica, Híbrida, Interconectada) es necesario entrar en profundidad de estos tres conceptos con el fin de entender cómo se crea este nuevo escenario emergente y disruptivo para los especialistas en gestión de riesgos, en su tarea de proveer una postura razonable, balanceada y costo efectivo para las empresas en el contexto de sus estrategias de negocio, y las exigencias de confianza digital de los ciudadanos en los Estados.

En primer lugar, es necesario indicar que tanto organizaciones como gobiernos saben que no podrán asegurar ni riesgo cero, ni seguridad cien por cien en el logro de sus propósitos, por tanto deberán definir su **apetito de riesgo** (*riesgo con el cual se siente cómodo y sabe que tiene los mecanismos para responder frente a su materialización y de aquellos residuales*), su **nivel de tolerancia** (*nivel de desviación permitido del apetito de riesgo definido*, que genera las alertas claves) y su **capacidad** (*el máximo nivel de riesgo que puede soportar*) para establecer los márgenes de operación y estrategias de acción que le permitan balancear su operación y mantener la integridad de sus planes y retos empresariales y nacionales (IIA, s.f.).

Las definiciones anteriores son necesarias y constituyen el primer insumo de los fundamentos de una seguridad A.H.I, pues en un contexto donde abundan las incertidumbres y escasean las certezas, se debe tener claridad el margen de acción y movilidad cuando las cosas no salen como estaban previstas, o cuando las sorpresas (previsibles o inesperadas) aparecen en

medio de la dinámica de las organizaciones y las naciones.

La *asimetría* como primer elemento del contexto que hace referencia a un desbalance natural que existe en la dinámica de las sociedades, donde la información, las tecnologías, las personas, el dinero y los imaginarios sociales mantienen posiciones inestables que por cuenta de las relaciones entre los diferentes agentes de la sociedad que tratan de movilizar con sus labores algunos de estos elementos siguiendo intereses particulares y generales, de tal forma que los resultados de sus acciones favorecen alguna lectura particular del entorno, desde donde las organizaciones y las naciones deberán concretar un equilibrio dinámico que les permita situarse en posiciones privilegiadas y estratégicas para el logro de su agenda específica.

Por otro lado, el concepto de *híbrido*, generalmente utilizado y entendido en el contexto militar como un cambio de dominio de combate, es una distinción mucho más elaborada y desafiante. Lo híbrido, siguiendo las definiciones de la Real Academia de la Lengua, supone un objeto o cosa diferente que es producto de elementos de distinta naturaleza. Esto es, un resultado novedoso y distinto a las fuentes que lo crearon, es la manifestación de un proceso de transformación y trasmutación que da vida a un evento completamente inédito, que genera mayor inestabilidad e incertidumbre y, por tanto, es necesario volver a reconocer, entender, analizar y descubrir para situarlo en el escenario donde hasta el momento no es conocido.

Finalmente lo *interconectado*, se refiere al uso de tecnologías de información y comunicaciones, que habilita, potencia y refuerza los dos elementos anteriores, creando realidades complemente distintas con flujos de información conocidos e inesperados, realidades aumentadas e inmersivas, y dinámicas abiertas y globales (productos/servicios) que implica reconocer en la densidad digital, la manera como los objetos físicos se transforman en “artefactos digitales” que ahora cuentan con capacidades inteligentes que informan, controlan y asisten la dinámica de los humanos en medio de un escenario como el ciberespacio.

Lo digital, implica la experiencia de estar conectados (aprovechando las oportunidades de una mayor densidad digital) y al mismo tiempo expuestos (proclives a engaños, fallas y vulnerabilidades de los ecosistemas digitales) sabiendo que al final la diferencia estará en el comportamiento de los seres humanos frente al fenómeno tecnológico.

La relación entre estos tres elementos establece un sistema complejo, socio-técnico y multidimensional que los modelos tradicionales de riesgo no logran manejar. En este sentido, una seguridad A.H.I

busca sensibilizar a todos los participantes y actores del escenario para analizar contradicciones, rarezas e incompatibilidades (Charan, 2015), y aprender no solo a tolerar la ambigüedad, sino a celebrarla, esto es, crear una perspectiva de relaciones posibles y no establecidas, en una zona psicológicamente segura para construir desde la sabiduría del error y los inciertos.

Evolución de la seguridad en un escenario convergente y multidominio

La seguridad en general se ha configurado como una percepción humana que busca establecer un estado de certeza concreto que le permita a una persona, actuar y movilizarse con un marco de consecuencias conocidos y validados para avanzar en sus propios objetivos. Si se parte del principio que no existen negocios o ganancias sin asumir riesgos (apetito de riesgo) es natural que tanto las organizaciones como las naciones asuman riesgos calculados para concretar sus objetivos estratégicos (O'Hare, 2022).

En este ejercicio continuado que se hace a nivel Estado como empresarial, se han generado diferentes posturas que persiguen todo el tiempo disminuir los inciertos, pues resultan incómodos y poco confiables para el logro de sus propósitos. Esta situación ha llevado a que muchos de los modelos de seguridad y control, así como las metodologías de gestión de riesgos tradicionales, se ocupen todo el tiempo de buscar formas de encontrar certezas y en este proceso, las encuentran en los eventos que ya han ocurrido. Esto es, basan sus indicadores en resultados de eventos pasados, tratando de extrapolar el conocimiento adquirido para sugerir una propuesta de acción en el futuro (Hopkin, 2010).

En este proceso las organizaciones buscan *gestionar y medir* la capacidad de la empresa o Estado para tratar los riesgos y establecer mecanismos de prevención y control que le permitan saber qué tanto debe avanzar o detenerse frente a una situación fuera de lo previsto, y desde allí concretar la mejor posición posible con el máximo de beneficio. Desafortunadamente los estándares y buenas prácticas disponibles sólo se refieren a aquellos riesgos conocidos, donde aplican sus "recetas" particulares para encontrar las certezas que necesita la organización, particularmente los equipos ejecutivos en la toma de decisiones donde lo que está en juego no sólo son los activos empresariales (o nacionales), sino su promesa de valor para con sus diferentes grupos de interés.

Una organización o nación que ha superado el ejercicio de gestión y medición, por lo general situado en el pasado, se moviliza al presente donde se exige el *sensar y responder*, un ejercicio de reconocimiento y análisis de datos e información en tiempo real, para saber qué, cómo y

dónde ocurre, y desde allí, responder para atender la situación, y no esperar a los efectos adversos que se puedan concretar, y si algo inesperado ocurre, es viable tener información para aprender tan rápido como sea posible para actuar y no dejar margen a los efectos colaterales que terminen impactando la dinámica de la entidad (Benjamins, 2022).

Sensar y responder es una evolución natural en un ejercicio de seguridad convergente donde diferentes vistas se conjugan para darle sentido a la nueva realidad enriquecida que transforma un incierto particular situado en un dominio, en una lectura enriquecida y aumentada del contexto que permite observar patrones de actividad por fuera de los marcos generales y formales establecidos para habilitar reflexiones y posturas proactivas que dan cuenta de las inestabilidades no para controlarlas, sino para comprenderlas y encontrar oportunidades que permitan situar la agenda estratégica de la organización, bien sea empresa o Estado.

La conexión entre el pasado y el presente implica una transición de un paradigma mecanicista y repetible, a uno marcado por el uso de los datos y la identificación de patrones en tiempo real, que retan el conocimiento hasta el momento adquirido por la organización. En este contexto, pensar ahora en el futuro (que no es posible predecir o conocer) se hace más retador el ejercicio de gestión de riesgos y de seguridad, comoquiera que mirar y caminar hacia adelante sin saber el comportamiento o situación que se puede presentar, implica navegar y asumir el incierto como la materia prima de la estrategia de seguridad y control. Esto es, pensar y advertir diferentes futuros, para establecer estrategias y acciones que lleven a la materialización de aquel que ofrezca las mejores condiciones y los menores impactos para la organización o Estado (Medina, 2023).

Defender y *anticipar* se configuran como los nuevos verbos de acción que se conectan con una seguridad convergente y multidominio pues demanda que los participantes exploren y se muevan en la zona de los riesgos emergentes, donde la dinámica de los inciertos es la norma y la resiliencia organizacional el objetivo fundamental. En este escenario los analistas de seguridad y control deben abandonar las certezas, cuestionar sus saberes previos y abrirse a las posibilidades más que a las probabilidades, con el fin de encontrar nuevos lugares comunes de riesgos sistémicos que puedan involucrar a su organización en efectos dominó que terminen comprometiendo su viabilidad en el mediano y largo plazo.

En este ejercicio de defender y anticipar, tanto las organizaciones como los Estados deberán mantener estrategias asociadas con disuadir, demorar, confundir y engañar para ganar espacios de acción y tiempo

de análisis, con el fin de contar con una tribuna de observación privilegiada, y desde allí, con la capacidad analítica de datos disponible, no sólo descubrir los patrones actuales, sino las tendencias consolidadas que permitan situar a la organización y los Estados en diferente futuros posibles donde pueden iniciar desde el hoy a construir las capacidades requeridas y los protocolos necesarios para actuar y avanzar cuando las señales del entorno muestren algunas características de ese futuro posible (Day & Schoemaker, 2019).

Al observar la transformación de la seguridad en un escenario convergente y multidominio, es clave entender que los conceptos vigentes de seguridad y control se quedan cortos y ubicados en una perspectiva que fragmenta la realidad dada su alta especialidad, análisis particular y disciplinar. Por tanto, habilitar una seguridad A.H.I implica combinar de forma simultánea el análisis y la síntesis de los diferentes dominios, observando en particular sus relaciones para revelar tanto los patrones como las tendencias con el fin de traducir el ejercicio de comprensión de esta dinámica en distinciones novedosas y prospectivas que le permitan a los involucrados no sólo tomar las decisiones del caso, sino aprender rápidamente de los acontecimientos y escenarios inéditos que ocurren o van a ocurrir en el mediano y largo plazo, así como sus posibles impactos.

Modelo de seguridad asimétrica, híbrida e interconectada

Desarrollar un modelo de seguridad que reconozca la dinámica y convergencia de diferentes dominios de operación, así como la capacidad de aprendizaje y resiliencia, implica no sólo navegar en el tiempo presente, sino influenciar igualmente el futuro. En este sentido, la propuesta que se presenta a continuación demanda una formación interdisciplinar, desinstalación intelectual, mentalidad de principiante y conciencia de la temporalidad de las cosas (Spitz, R., 2022), como base para movilizar esfuerzos, decisiones, acciones y retos que transformen los inciertos y ambigüedades en oportunidades y patrones de comportamiento que transformando el presente exploren nuevas ideas que reten el futuro.

El modelo propuesto cuenta con seis (6) pasos básicos, los cuales hacen parte de la definición de una seguridad A.H.I:
Es una percepción de confianza, confiabilidad e integridad multidominio basada en la capacidad de percibir, adaptar, disuadir, demorar, amortiguar y avanzar en medio de la incertidumbre, la inestabilidad y el caos que un evento adverso puede producir en el modelo de seguridad y control de una organización o nación.

1 Dominios: Social, Tecnológico, Económico, Político, Ambiental y Legal

El primer paso es *percibir*. Esto es, la observación de tendencias, definición y seguimiento de las incertidumbres críticas, y definición de escenarios para evaluar. El resultado de la percepción establece la vista panorámica de la situación, así como las diferentes alternativas de acción que se pueden concretar frente a diferentes escenarios posibles y probables.

El segundo momento es *adaptar*. La adaptación implica antifragilidad, configuración y reconfiguración de defensas en función de tendencias y analítica de comportamientos. Es un espacio para capitalizar el incierto sobre la dinámica actual de los eventos que tienen potencial de afectación para la organización. El resultado es una postura de objetivo móvil que deteriora la inteligencia del adversario (Cho et al., 2019).

El tercer paso es *disuadir*. La disuasión como la desmotivación del adversario o la pérdida de interés por parte del atacante para concretar su acción contraria en un objetivo específico, a través de la incorporación de tecnologías de engaño y de blanco móvil siguiendo los resultados del *adaptar* (Jasper, 2017).

El cuarto elemento es *demorar*. Demorar al agente agresor es diseñar espacios o zonas de distracción y contención de sus ataques en los diferentes dominios de operación creando confusión en sus acciones, que lleven a la variación de su plan y estrategia de desestabilización previamente definida. El resultado mayor distracción del agresor y aumento de su exposición y visibilización por parte de los controles organizacionales.

El quinto paso es *amortiguar*. La amortiguación es un ejercicio de capacidad de aguante y soporte de un evento adverso, esto es una declaración de umbrales de operación, apetito, tolerancia y capacidad de riesgo frente a un ataque exitoso. Este ejercicio de resistencia exige de todos los participantes un nivel de coordinación y comunicación definido, practicado y fluido que permite una actuación organizacional conjunta frente a la inevitabilidad de la falla (Fiksel, 2015).

Finalmente, y no menos importante, el paso seis que es *avanzar*. Esto significa capacidad de aprendizaje ágil, cuestionamiento del saber previo y reconocimiento del error como parte del proceso y no como resultado. Lo anterior implica, aprovechar las nuevas estrategias y tecnologías de defensa y anticipación para proteger la promesa de valor de la empresa o nación, y así habilitar la percepción de confianza, confiabilidad e integridad multidominio objetivo, que no es otra cosa que encontrar el balance real y concreto del apetito de riesgo y las apuestas por la implementación de experiencias innovadoras que transformen y superen las expectativas de los diferentes grupos de interés (Saydjari, 2018).

Si bien la propuesta conceptual se alinea con las necesidades actuales de seguridad y control tanto de negocios como de naciones, requiere un cambio de mentalidad y desacoplamiento de los modelos de riesgos tradicionales, para repensar la seguridad ahora desde los inciertos, no como una manera de evitar daños o impactos negativos, sino como la oportunidad de crear nuevas opciones y transformaciones que cambien el statu quo de las empresas y movilicen alternativas que acompañen y den sentido a los inciertos y eventos inesperados.

Reflexiones finales

Con un mundo cada vez más inestable, donde escasean las certezas y abundan los inciertos, los modelos de seguridad y control entran en crisis existencial, pues la base de su operación (las certezas) se deteriora y no permite mayor capacidad de acción y/o asesoría. En este sentido, se hace necesario superar el paradigma de la prevención basado en un conjunto de actividades sugeridas y probadas para disminuir el nivel de exposición, para transformarlo en una postura vigilante de defensa y anticipación que si bien, no garantiza un resultado específico, si habilita una acción coordinada y resiliente que permite actuar y sobrevivir aún en los escenarios más adversos e inesperados (Hepfer & Powell, 2020).

Las condiciones actuales de los escenarios asimétricos, híbridos e interconectados expanden y superan las capacidades actuales de las organizaciones y naciones por cuenta de una explosión de complejidad que escapa a los mejores análisis y pronósticos de los analistas. En este sentido, los Estados y las compañías se deben preparar para mantener sus operaciones y acompañar a sus grupos de interés en medio de un creciente ambiente hostil donde las tensiones en los diferentes dominios de acción: político, económico, social, tecnológico, ecológico y legal, se refuerzan entre sí, creando un entorno donde cualquier evento puede ocurrir y la capacidad de respuesta y resiliencia deberá ser la marca e impronta natural de la organización para ajustar su plan de navegación para alcanzar sus objetivos estratégicos (Medina, 2023).

El modelo A.H.I establece una propuesta conceptual que más allá de entender y visualizar los cambios del entorno, introduce una forma de incorporar los inciertos, la complejidad y los cambios como parte fundamental del reconocimiento de la gestión y gobierno del riesgo, ahora con perspectiva sistémica, con apertura frente la inevitabilidad de la falla y foco en la resiliencia organizacional. Esta apuesta conceptual busca mover a las organizaciones y los Estados fuera de la zona cómoda de las certezas y buenas prácticas, para avanzar y alcanzar sus objetivos en medio de la inestabilidad y los eventos inesperados propios del entorno actual.

Así las cosas, en mundo cada vez más desconocido, volátil, interconectado, complejo y exponencial, se hace necesario mantener una postura relevante y vigilante para lo cual es importante entender la seguridad y el control como una distinción multidominio donde todo el tiempo pueda dar respuesta a preguntas como: (Spitz, 2022)

- ¿Cuándo y cómo identifica los cambios?
- ¿Cada cuánto y cómo define su apetito de riesgo?
- ¿Cuándo y cómo aprende de aquello que no salió como estaba planeado?
- ¿Cuándo y cómo toma decisiones audaces?
- ¿Cómo reconcilia el corto y el largo plazo?
- ¿Cuándo y cómo identifica tendencias y patrones relevantes?
- ¿Cuándo y cómo reta sus propios saberes previos?

En resumen, cuando la seguridad no se concibe desde una perspectiva disciplinar particular, ni se asocia con la protección frente a daños, ni se ajusta con las inversiones que se hacen para lograr mayor tranquilidad (Proctor, 2023), se advierte una transformación de la distinción seguridad hacia un concepto de confiabilidad y balance dinámico, que responde, aprende y se adapta frente a las inestabilidades del entorno como una respuesta natural que entiende la disrupción y los inciertos como el fundamento de la toma de decisiones y del apetito de riesgo de las organizaciones en un contexto más asimétrico, híbrido e interconectado.

Referencias

Benjamins, R. (2022). *A data-driven company. 21 claves para crear valor a través de los datos y la inteligencia artificial*. España: LID Editorial

Charan, R. (2015). *The attacker's advantage. Turning uncertainty into breakthrough opportunities*. New York, USA: Perseus Books Groups

Cho, J., Sharma, D., Alavizadeh, H., Yoon, S., Ben-Asher, N., Moore, T., Kim, D. S., Lim, H. & Nelson, F. (2019) Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. *IEEE Communications Surveys & Tutorials*. 1-39. Doi 10.1109/COMST.2019.2963791

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

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

Fiksel, J. (2015). *Resilient by Design. Creating Businesses That Adapt and Flourish in a Changing World*. Washington, DC. USA: Island Press.

Hepfer, M. & Powell, T. (2020). Make Cybersecurity a Strategic Asset. *Sloan Management Review*. 62(1). 40-45. https://sloanreview.mit.edu/article/make-cybersecurity-a-strategic-asset/

Hopkin, P. (2010). *Fundamentals of Risk Management. Understanding, evaluating and implementing effective risk management*. London, UK. Kogan

Page Limited - The Institute of Risk Management.

IIA (s.f.) Definición e implantación de apetito al riesgo. *Fábrica de Pensamiento*. Instituto de Auditores Internos de España. De: https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-original.original.pdf

Jasper, S. (2017). *Strategic cyber deterrence. The active cyber defense option*. Lanham, Maryland. USA: Rowman & Littlefield.

Medina, J. (2023). *Prospectiva para un mundo interdependiente*. Bogotá, Colombia: Editorial Aurora – Academia Colombiana de Ciencias Económicas.

O'Hare, D. (2022). *Introduction to Safety Science. People, Organisations, and Systems*. Boca Raton, Fl. USA: CRC Press.

Proctor, P. (2023). Cybersecurity Spending Does Not Equal Protection. *Gartner Blog*. https://blogs.gartner.com/paul-proctor/2023/02/12/cybersecurity-spending-does-not-equal-protection/

Renn, O. (2018). *Risk Governance. Coping with Uncertainty in a Complex World*. London, UK.: Earthscan.

Saydjari, O. (2018). *Engineering trustworthy systems: get cybersecurity design right the first time*. New York, USA.: McGraw Hill.

Sheffi, Y. (2020). *The new (ab)normal. Reshaping business and supply chain strategy beyond Covid-19*. Cambridge, MA. USA: MIT CTL Media

Spitz, R. (2022). *The definitive guide to thriving on disruption. Essential frameworks for disruption and uncertainty*. Vol II. USA: Disruptive Future Institute LLC.

WEF (2023). The Global Risks Report 2023. 18th Edition. *Insight Report*. https://www.weforum.org/reports/global-risks-report-2023/digest

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, 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–.*

NOS RENOVAMOS

LA ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

Queremos expandirnos. Es por esto, que hemos decidido ampliar nuestro nombre, para poder tener mayor alcance a todas las personas e instituciones que van de la mano con la tecnología.

Más información en:
www.ACIS.org.co
o escríbenos a:
301 5530540
Suscripciones@acis.org.co
Cursos@acis.org.co

La ciberresiliencia ante la inevitabilidad de los ciberataques

DOI: 10.29236/sistemas.n167a7

Resumen
La protección del ciberespacio demanda la participación de procesos durante todas las etapas del desarrollo de un incidente: antes (preparación y prevención), durante (contención y reacción inmediata) y después (continuidad de negocio y adaptabilidad). Lamentablemente la inevitabilidad es una constante, por más mecanismos preventivos: la probabilidad de ser víctima de un ciberataque resulta casi una certeza. La ciberseguridad y la ciberresiliencia son disciplinas dedicadas a la protección del ciberespacio, conceptos que muchas veces se usan como sinónimos, pero que realmente presentan diferencias importantes, sobre todo en su alcance y especialización. Un entendimiento erróneo de estos conceptos puede derivar en una protección parcial y a largo plazo, deficiente. El presente artículo tiene por objetivo describir las similitudes y diferencias de cada una de estas disciplinas, resaltando sus características fundamentales, con la finalidad de que podamos conformar una estrategia de defensa integral y más efectiva ante los escenarios actuales.

Palabras clave
Ciberseguridad, ciberresiliencia, ciberespacio, estándares, marcos de trabajo

Introducción

La historia reciente ha dejado claro que la inevitabilidad es una constante: actualmente ninguna nación ni organización está exenta de sufrir un ciberataque. Lamentablemente, aún con numerosos esfuerzos preventivos que se vierten en regulaciones, estrategias y mejores prácticas para fortalecer la ciberseguridad, siempre existe la posibilidad de ser atacado con éxito. Aunado a esto, se encuentra el factor de la escasez, los recursos humanos y materiales para prevenir y reaccionar en forma inmediata, ante un incidente de esta magnitud siempre son limitados. Adicionalmente, en la actualidad las organizaciones cuentan con centenas de controles de seguridad a los que se debe dar cumplimiento, conforme a las regulaciones y estándares, los cuales se han mostrado insuficientes y no han mitigado de manera eficaz los ciberataques. Como se ha observado, la exigencia puntual e inflexible en su cumplimiento puede conllevar el efecto contrario: en lugar de disminuir el número de ciberataques exitosos, se han incrementado. La causa raíz no es nada sencilla, sino compleja y multidisciplinaria.

Las estadísticas a nivel nacional y mundial muestran un crecimiento sostenido de los ataques informáticos dirigidos hacia diferentes países, originados por adversarios en el ciberespacio, particularmente hacia infraestructuras de redes informáticas y de telecomunicaciones a través de las cuales las personas se comunican e interactúan como lo hacen en el mundo físico, y que son indispensables para la operación de los procesos de los Estados (Mandiant, 2021).

Los ataques de alto impacto originados en el ciberespacio son cada vez más frecuentes, más especializados, más complejos, más silenciosos, más coordinados y, desafortunadamente, inevitables, los cuales incluso están siendo dirigidos a infraestructuras críticas de los países, con amplios efectos multiplicadores que, si bien tienen origen en espacios virtuales, están afectando al mundo físico y viceversa.

Además, la especialización de los ciberataques es cada vez mayor, generando incluso organizaciones de tipo Estado-Nación dedicadas exclusivamente a causar daños por diferentes vías. Ante esta nueva forma de afectación se pueden generar mayores conflictos asimétricos, en los que países de menor poder tradicional pueden causar graves daños a naciones con un mayor poder.

Así pues, ninguna organización está exenta de ser atacada exitosamente en el ciberespacio, por más

medidas preventivas que se procuren. Incluso países con amplios recursos y medidas de ciberseguridad son víctimas de ataques. Por ello, resulta esencial que se sigan suministrando bienes y servicios a pesar de haber sido objeto de un ciberataque. Eso es materia de la ciberresiliencia, el cual es un fenómeno complejo, que requiere la aplicación de capacidades multidisciplinarias, lo cual también lo convierte en ocasiones, hasta en un problema subjetivo, que requiere una profunda interpretación a partir de diversos puntos de vista.

Concepto general de resiliencia

El Diccionario de la Lengua Española (2020) señala que la palabra **resiliencia** proviene del latín ***resilire*** que significa **volver atrás, volver de un salto, resaltar o rebotar**. Dicho concepto ha sido utilizado en diferentes disciplinas como, por ejemplo, en el uso de materiales, ecología, planeación urbana, por mencionar algunas.

Originalmente, en el entorno de los materiales la resiliencia se refería principalmente a la propiedad de absorber la fuerza exterior que se aplicaba a dicho material y que permitía recuperar su forma después de haber sido doblado o comprimido (Dupont, 2019). Mismo término que después se aplicó con más difusión en las disciplinas de psicología y ecología.

En psicología se emplea para referirse de forma general a la capacidad de una persona para superar circunstancias traumáticas como la muerte de un ser querido, un accidente, etc. Si bien este concepto es ampliamente aceptado hoy en día, aún no se determinan con claridad las circunstancias o actividades que logran regenerar nuevamente a la persona que sufrió un evento traumático (Bork, Henkel, Stirna, & Zdravkovic, 2014).

El uso de este concepto con relación a la atención de desastres en las naciones, ya sea por causas de la naturaleza o humanas, no es nuevo y se puede rastrear su uso desde hace varias décadas. De hecho, la Organización de las Naciones Unidas en 2005 fomentó el concepto de la resiliencia en las naciones para afrontar desastres y reducir los riesgos relacionados (NAP, 2012). Desde entonces, el concepto de resiliencia ha sido utilizado para referenciar a procesos para afrontar eventos adversos en distintas áreas como las tecnológicas, políticas o sociales.

En el espacio físico, las Academias Nacionales en EUA analizaron este concepto desde el punto de vista de desastres a nivel nacional (huracanes, inundaciones, terremotos, actos de terrorismo, enfermedades, etc.) en el cual se enfatizó sobre la importancia de la resiliencia y en que los incidentes se gestionaran desde diferentes áreas, desde los ámbitos local, estatal y federal, así como integrando esfuerzos de la sociedad civil, instituciones priva-

das y gubernamentales (NAP, 2012). En dicho documento se definió resiliencia como "la habilidad para preparar/planear, absorber, recuperar y, sobre todo, **adaptarse** exitosamente a futuros o actuales eventos adversos" (pág. 16).

En ese sentido, esa definición complementa las concepciones que comúnmente se utilizan, las cuales generalmente se centran en las primeras etapas defensivas y reactivas, minimizando las fases de absorción y de adaptación. De la misma forma, resalta la importancia de priorizar la inversión en los elementos de resiliencia con el fin de tomar mejores decisiones para incrementarla, disminuyendo el impacto no inmediato de estos tipos de eventos (NAP, 2012).

En dicho texto se enfatizó en que los desastres no dejarán de suceder y señaló algunas de las causas para ello como, por ejemplo: el crecimiento de la población, migrantes hacia zonas costeras, limitaciones en infraestructura pública, cambio climático, etc.

Los puntos anteriores ponen de manifiesto las siguientes ideas:

1. El evento adverso ocurre en la vida de una persona[1], esto es, **la resiliencia no es preventiva**, no evita un incidente. Se habla de resiliencia como parte de la superación de ese suceso.
2. La esencia de la resiliencia radica en **sobreponerse** ante tal incidente, el cual afectará de forma distinta a cada persona o grupo de ellas. Existen reflexiones que incluso indican que el ente afectado saldrá fortalecido al sobreponerse de dicho evento.
3. La ocurrencia de eventos desafortunados [pe. desastres] **no es opcional**.

Finalmente, Boris Cyrulnik (2014), considerado como padre del concepto en psicología, en su libro "¿Por qué la Resiliencia?" indica que "…lo más difícil de descubrir son las condiciones que permiten iniciar un nuevo desarrollo después del trauma". Lo que pone de manifiesto que es de gran importancia conocer cuáles son los elementos que incrementan la resiliencia *después* del fenómeno traumático.

Resiliencia en el ciberespacio

Las observaciones realizadas anteriormente son importantes, toda vez que los conceptos y definiciones utilizados comúnmente para denotar la resiliencia en el ciberespacio (o **ciberresiliencia**), difieren en la orientación de procesos clave. Por ejemplo, la muerte de un ser querido no se podrá evitar mediante la resiliencia, ni tampoco este evento impactará de la misma forma a cada persona.

En el mundo del ciberespacio, lo anterior lleva a observar que la ci-

[1] Aunque en este documento se indica una "persona", se puede hablar de familias, grupos o comunidades con características similares.

berresiliencia no es en principio para evitar ciberataques; en caso de que ocurran, será para determinar el grado en que afectarán a las organizaciones y deberán adaptarse ante las **nuevas** condiciones. Es de gran importancia que muchos estudios de ciberresiliencia parecen tener un enfoque preventivo y de reacción inmediata; no obstante, existen otros documentos en los que se resalta la resiliencia como la capacidad para evolucionar, **adaptarse** y alcanzar un nuevo equilibrio. En el primero podría ser una resiliencia total [no pasó nada]; en el segundo, hubo un evento y se derivan **secuelas**, pero se debe seguir adelante. Para el autor de este artículo, esa última es la noción que se debe tener de ciber-resiliencia.

Resulta de suma importancia señalar que un ciberataque, por su naturaleza, no puede ser impedido o mitigado por completo. Como lo indica Dupont: "el paradigma de protección y prevención resulta insuficiente, y la ciberresiliencia tiene que estar entre las estrategias de administración de riesgo… generando una estrategia complementaria" (Dupont, 2019, pág. 1). Esta misma idea la manifiesta Linkov (2013) y agrega que, hay que tener cuidado de no mezclar los términos del análisis de riesgo con ciberresiliencia: el primero requiere de una cuantificación que mide la probabilidad de que un evento conocido ocurra; mientras que el segundo, corresponde al ámbito de eventos inimaginables y por tanto no cuantificables, que ocurren por sorpresa.

Esa última característica resulta de suma importancia, toda vez que la sorpresa implicará un nivel de **improvisación** en la gestión del incidente (Dupont, 2019). No hay nada escrito y, por ende, posiblemente los protocolos de actuación en ese momento sean limitados o en el peor caso inservibles, pues se estará reaccionando a un evento que ni siquiera ha sido planeado. La improvisación es un punto que normalmente es concebido como una parte negativa de la planeación en general [se hacen planes para no improvisar], pero aplicada a la planeación de la resiliencia resulta ser de gran valor. Como lo indica Dupont (2019), al hacer el símil con la música de Jazz (pág. 7): "La resiliencia requiere del arte de combinar espontaneidad e intuición, con disciplina y experiencia".

Una definición propia basada en las que contemplan todas las fases de un ciberincidente podría ser: **ciberresiliencia es la capacidad de anticiparse, soportar y recuperarse, parcial o totalmente, ante un ciber-ataque con el fin de proveer continuamente bienes y servicios hasta adaptarse bajo condiciones diferentes al estado inicial alcanzando un nuevo equilibrio.**

La definición anterior deja en claro que no se está hablando del concepto de **continuidad de negocio**,

el cual precisamente busca regresar a un estado inicial casi idéntico, previo al incidente y por lo general en un tiempo limitado. De ahí que existan muchas métricas al respecto como RTO [*Recovery Time Objective*] para especificar el tiempo que una organización necesita para recuperarse después de sufrir un incidente, RPO [*Recovery Point Objective*] para determinar el tiempo máximo que una organización está dispuesta a perder información o el RTA [*Recovery Time Actual*] que es el tiempo en el que se activa el plan de recuperación de desastres. En este aspecto, la **continuidad de negocio** [BCP por sus siglas en inglés] y el "plan de recuperación ante desastres" [DRP por sus siglas en inglés] representan un concepto diferente a la ciberresiliencia, la cual contempla una fase de adaptación al final que regresará a la organización a un estado diferente al incidente previo, esto es, bajo un nuevo escenario [o equilibrio].

Diferencia entre ciberseguridad y ciberresiliencia

En este punto resulta de suma importancia revisar dos términos relacionados con la protección del ciberespacio: ciberseguridad y ciberresiliencia. Las definiciones simples de estos conceptos pueden apoyar en la identificación de la diferencia fundamental: mientras la ciberseguridad se enfoca a la protección general del ciberespacio [pre y reacción inmediata], la ciberresiliencia se enfoca en dicha protección, pero en un nivel adaptativo [post y mediano-lago plazo]. Este último nivel es la parte diferenciadora entre ambos conceptos.

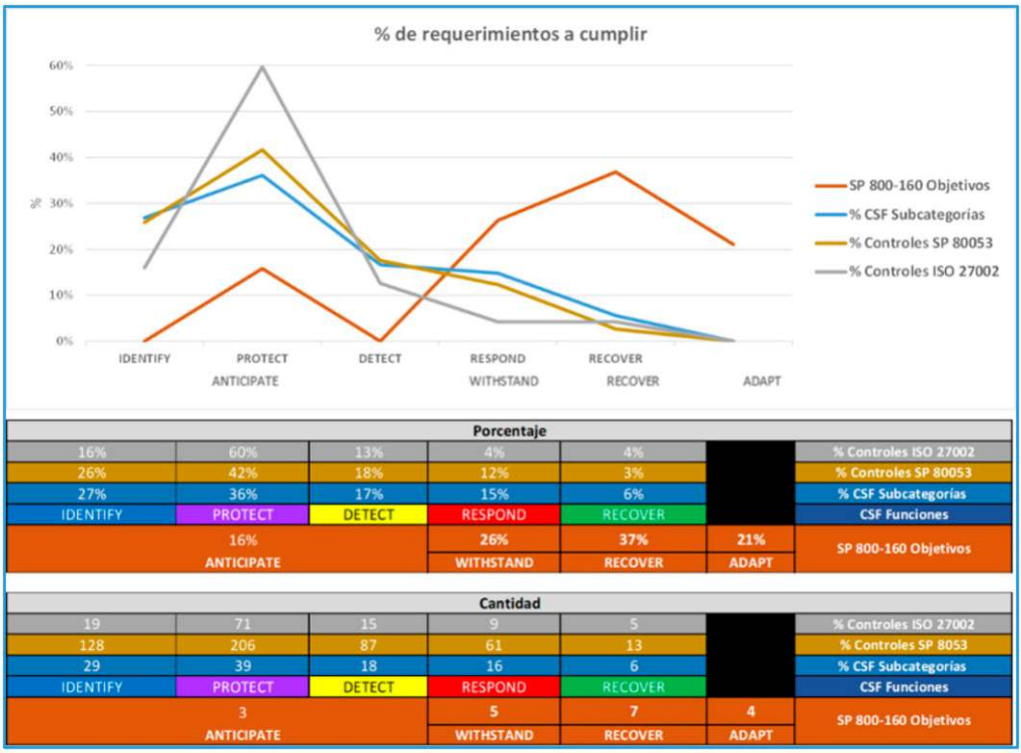
Como parte de este artículo se revisaron algunos estándares que demuestran exactamente este comportamiento:

Figura 1
Fases que cubren los estándares

La gráfica 1 fue elaborada con base en 4 estándares de amplio uso en organizaciones de países en todo el mundo:

- ISO 27002 [*International Organization for Standarization*]
- NIST 800-53 [*National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations*]
- NIST CSF [*National Institute of Standards and Technology, CyberSecurity Framework*]
- NIST SP 800-160 [*National Institute of Standards and Technology, Developing Cyber Resilient Systems*]

Los primeros tres estándares están enfocados en la ciberseguridad, mientras que el último NIST SP 800-160 es el único que se especializa en ciberresiliencia. Como se aprecia en la gráfica anterior, esos primeros tres estándares tienen un porcentaje amplio de cobertura de las primeras 3 fases **sin cubrir la fase de adaptación**. Si bien el NIST SP 800-160 tiene controles



Porcentaje						
16%	60%	13%	4%	4%		% Controles ISO 27002
26%	42%	18%	12%	3%		% Controles SP 80053
27%	36%	17%	15%	6%		% CSF Subcategorías
IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER		CSF Funciones
16% ANTICIPATE			26% WITHSTAND	37% RECOVER	21% ADAPT	SP 800-160 Objetivos

Cantidad						
19	71	15	9	5		% Controles ISO 27002
128	206	87	61	13		% Controles SP 8053
29	39	18	16	6		% CSF Subcategorías
IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER		CSF Funciones
3 ANTICIPATE			5 WITHSTAND	7 RECOVER	4 ADAPT	SP 800-160 Objetivos

Figura 1
Fuente: Elaboración propia basada en (Ureña Cuate, 2021)

para la ciberseguridad, es el único que tiene objetivos de protección que contemplan fase de adaptación.

Resulta oportuno señalar que la figura anterior **no** desea expresar que los marcos de trabajo o estándares enfocados a ciberseguridad sean menores o deficientes en cuanto a la protección ante amenazas del ciberespacio, sino que los enfoques difieren en su alcance y finalmente resultan complementarios.

Para finalizar, Cano (2020) indicó con claridad que, no solo es cuestión de seguir prácticas comunes de continuidad de negocio y recuperación para enfrentar un ciberataque de alto nivel, diseñado de forma particular para irrumpir en una organización vital. Si bien eso es esencial en todo programa de seguridad, se deben incorporar estrategias de resiliencia de forma complementaria.

Interrelaciones en ciberresiliencia

La ciberresiliencia es un componente organizacional, un elemento que coadyuva al correcto funcionamiento de las organizaciones. Además, resulta importante seña-

lar que este componente está interrelacionado con otras áreas que tienen un propósito complementario como se muestra en la figura:

Figura 2
Relaciones de la ciberresiliencia

La gráfica 2 permite identificar la interrelación entre varias disciplinas que se relacionan para alcanzar una resiliencia organizacional sin importar que un riesgo provenga del mundo físico o del lógico, y este gráfico envolvería a las demás áreas. Asimismo, se puede observar lo siguiente:

- La continuidad del negocio está más enfocada en la disponibilidad de los procesos y abarca un mayor número de actividades organizacionales [no solamente los que tienen contacto directo con el ciberespacio].
- La gestión de riesgos también atiende diferentes amenazas hasta que se concrete un incidente, entonces un riesgo deja de serlo para convertirse en incidente.
- La ciberseguridad está acotada al espacio virtual del ciberespacio, y como se vio, su alcance es menor que la ciberresiliencia, aunque comparten estrategias y controles en las primeras etapas.

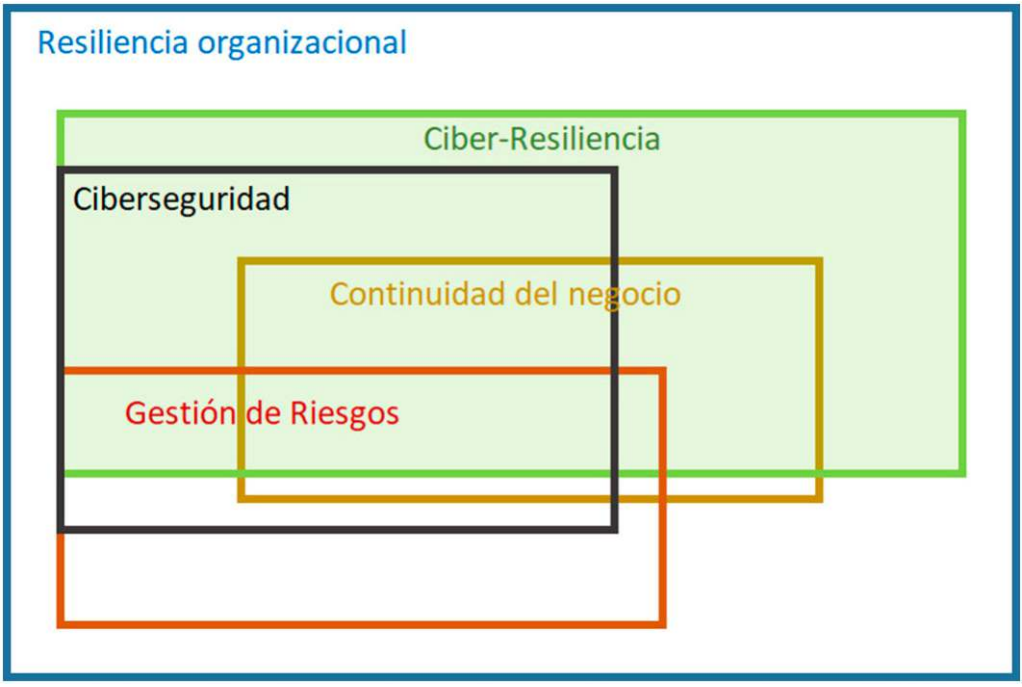


Figura 2
Elaboración Propia basada en (Vargas Pedroza, 2019)

Conclusiones

La ciberresiliencia es un término que requiere de un análisis profundo para identificar con más claridad sus componentes y relaciones. A través de este artículo se resaltó que la fase **adaptativa** es la que hace la principal diferencia con otros conceptos relacionados en el ciberespacio, y que generalmente se confunden ocasionando una aplicación incompleta del término. Dada la magnitud de algunos ciberataques, es posible que las actividades de adaptación no sean por completo claras o no hayan sido publicadas todavía: ¿en qué se han modificado los procesos involucrados?, ¿qué es ahora diferente de lo que se hacía?, ¿cuánto cambio?, ¿cuánto mejorará la protección integral del ciberespacio? En fin, son preguntas que aún están en investigación por lo que tenemos mucha tarea por hacer en este entorno virtual.

Referencias

Bork, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2014). Cyber Resilience- fundamentals for a definition. Suecia.

Cano, J. (2020). ¿Por qué los ciberataques son inevitables?: Prácticas y capacidades claves de la ciberseguridad empresarial. En V. Gauthier-Umaña, R. Méndez-Romero, & D. Suárez, *Voces diversas y disruptivas en tiempos de Revolución 4.0* (págs. 223-248). Bogotá: Universidad del Rosario. doi:10.2307/j.ctv123x566.14

Cyrulnik, B., & Anaut, M. (2014). *¿Por qué la resiliencia?* (A. Diez, Trad.) Barcelona, España: Gedisa.

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, 1-17. doi:10.1093/cybsec/tyz013

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Covertino, M., Allen, J. H., . . . Seager, T. P. (2013). Measurable Resilience for Actionable Policy. (A. Publications, Ed.) *Environmental Science & Technology*, 108-110.

Mandiant. (2021). *M-Trends.* Obtenido de https://www.mandiant.com/resources/m-trends-2021

NAP. (2012). *Disaster Resilience. A National Imperative.* Washington DC, USA: The National Academies Press.

Real Academia Española. (2020). *Real Academia Española*. Obtenido de https://www.rae.es/

Ureña Cuate, M. (1 de Octubre de 2021). Curso de Ciber-resiliencia organizacional. CDMX, México.

Vargas Pedroza, G. (Marzo de 2019). El estado del arte para enfrentar los ciberataques y el cibercrimen organizado. *Gerencia. Noticias, Análisis e Información*. Obtenido de http://www.emb.cl/gerencia/articulo.mvc?xid=4647&ni=ciber-resilencia-el-estado-del-arte-para-enfrentar-los-ciberataques-y-el-cibercrimen-organizado

Arturo García Hernández
Estudioso de la ciberseguridad con más de 25 años de experiencia. Obtuvo el grado de Doctor en Defensa y Seguridad Nacional con mención honorífica en la Universidad Naval de México, especializándose en la ciberresiliencia de las infraestructuras críticas. Cuenta con varias certificaciones profesionales de reconocimiento internacional como DSE, CISM y CISSP. Labora en Banco Central de México como Gerente de Seguridad en Tecnologías de la Información.

CONECTA CON NOSOTROS

@Comunidadacis

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

WWW.ACIS.ORG.CO