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.

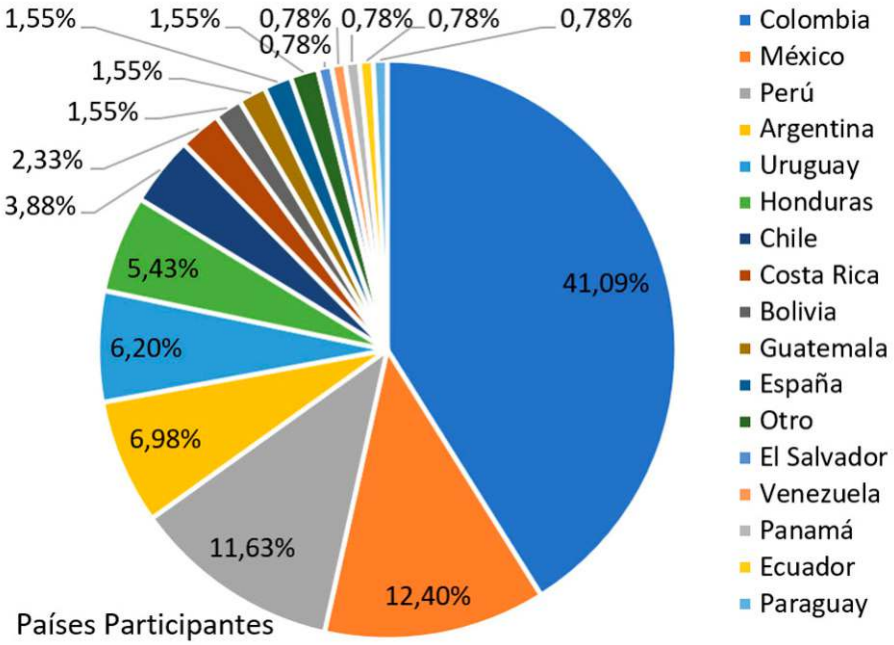

Figura 1. Países participantes

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:

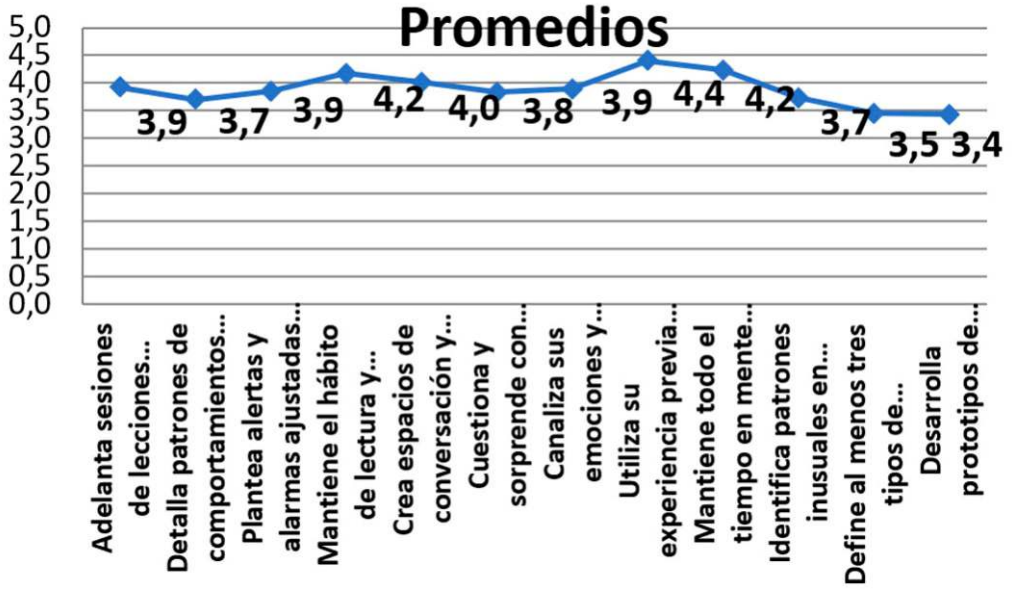

Figura 2 - Valores de los promedios de las 12 preguntas

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

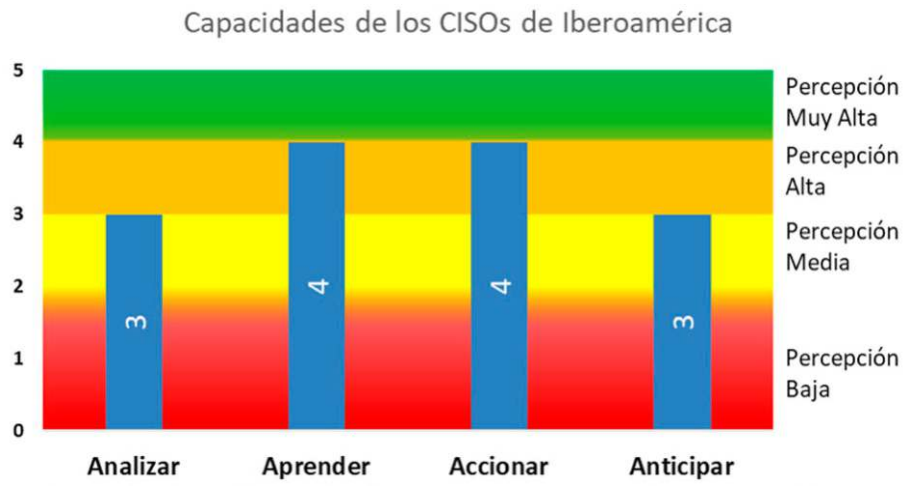

Figura 3. Distribución de respuestas por las capacidades

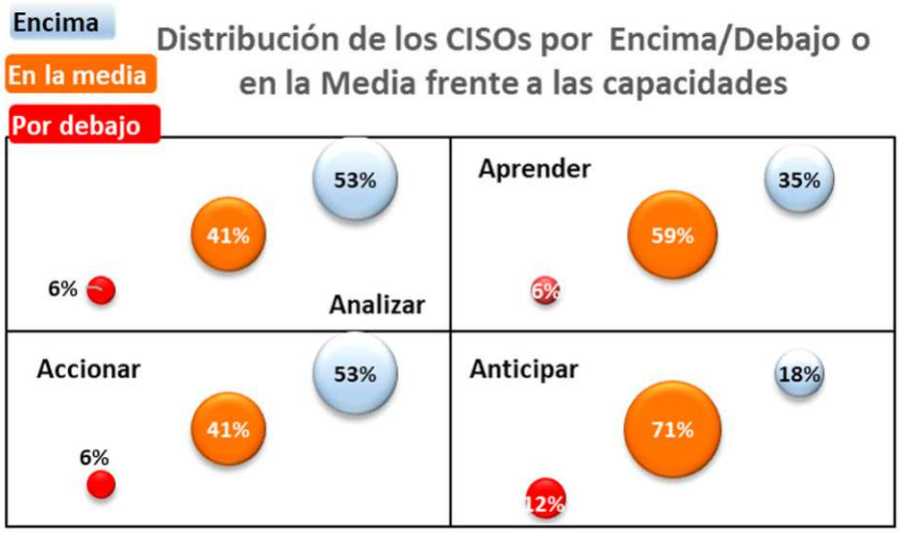

Figura 4. Análisis de cada factor por encima, igual o debajo de la media

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

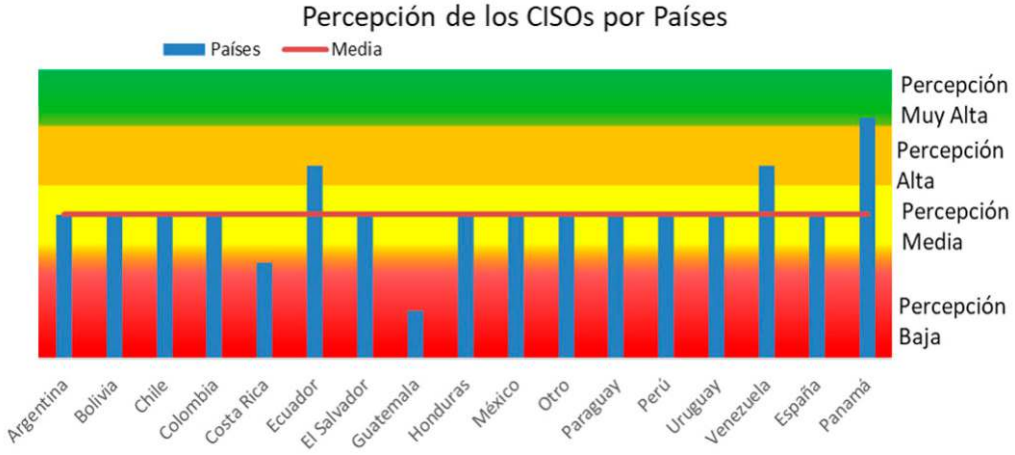

Figura 5. Percepción del CISO por país de la región

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.*