FEATURE

Analista y Adversario

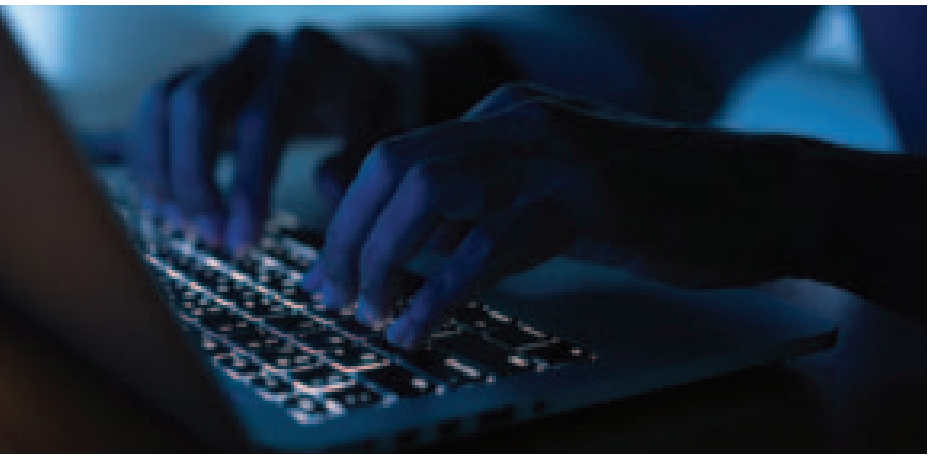
Deconstruyendo el "imaginario" de los profesionales de seguridad y ciberseguridad.

Cada año los reportes de nuevas amenazas y brechas de seguridad informan sobre la mayor sofisticación de los atacantes, sus diferentes formas de tensionar las medidas de protección y de engañar los mecanismos de control disponibles[1, 2]. Esto supone una evolución de un adversario que permanentemente busca formas de sorprenderse a -sí mismo y encontrar maneras inéditas de crear inestabilidad en los contextos corporativos, militares y nacionales.

La mente del atacante es un objeto de estudio en seguridad y ciberseguridad, como quiera que tratar de comprender su forma de pensar, revisar, actuar y desarrollar sus actividades, generalmente está mediada por condiciones contrarias y adversas, que pocos encuentran atractiva para estudiar y recrear, toda vez que pueden cruzarse límites éticos que los especialistas de seguridad y ciberseguridad saben que deben mantener en el ejercicio de sus actividades profesionales[3].

En este contexto, el atacante se convierte en un fenómeno cercano y lejano al mismo tiempo, creando una zona de contradicción que no permite avanzar fuera de los linderos que se han establecido para la práctica de los profesionales en seguridad y ciberseguridad. Intentar estudiar las propuestas de los adversarios, deberá ser una parte natural de la práctica de los especialistas de seguridad y control, como quiera que los alcances de sus actividades terminan creando inestabilidad y lecciones aprendidas tanto para las empresas como para los encargados de la seguridad.

Mientras los denominados analistas, es decir, aquellos que están en el lado claro de la fuerza, asistidos de la formalidad y ajustados a las regulaciones vigentes, mantienen un lenguaje basado en amenazas, controles e impactos, los que se han dejado tentar por su lado oscuro, se mueven entre sus intenciones, sus capacidades y vulnerabilidades posibles, como fundamento de sus actuaciones. Este aparente contraste, revela en sí mismo la dinámica que se presenta cuando se requiere alcanzar una mayor confiabilidad y confianza imperfecta[4, 5] en un mundo cada vez más hiperconectado y digitalmente modificado.



En consecuencia, se desarrolla este documento que busca comprender y analizar los imaginarios vigentes de los profesionales en seguridad y ciberseguridad, con el fin de desconectar las bases conceptuales que han permanecido en el desarrollo de su formación y práctica, para incorporar nuevas opciones y consideraciones alternativas, que permitan reconstruir sus saberes y experiencias previas, de tal forma, que sus reflexiones, no sólo protejan y aseguren los activos digitales estratégicos de las empresas, sino que abran nuevos debates sobre la manera como se defiende y anticipa en un mundo asimétrico e incierto como el actual.

Jeimy J. Cano M., Ph.D, Ed.D, CFE, CICA
Es un profesor distinguido de la Facultad de Derecho de la Universidad de los Andes, Colombia. Cuenta con más de 22 años de experiencia como ejecutivo, académico y profesional en seguridad de la información, ciberseguridad, computación forense, delincuencia digital, infraestructuras críticas y auditoría de TI.

La formación de los analistas de seguridad y ciberseguridad. Un imaginario vigente.

Afirman los profesores Echeverría y Martínez que "uno de los más imperiosos retos a los que se

enfrenta la educación superior es responder a la necesidad ineludible de actualizar y mejorar las competencias de cada vez mayor número de personas y además a lo largo y ancho de sus vidas"[6] como quiera que los cambios constantes y las respuestas parciales a los desafíos del mundo, los deben convertir en estudiantes para toda la vida.

Lo anterior plantea la crisis del modelo tradicional de la ciencia y la educación, donde existe un profesor que posee el conocimiento y una serie de estudiantes que son depositarios de sus enseñanzas. De igual forma, estos educandos, de manera homogénea, deberán adquirir nuevos aprendizajes, de tal forma que se repitan las indicaciones de sus mentores, para lograr las mejores calificaciones y reconocimientos por parte de sus docentes, y por lo tanto, de la institución universitaria donde se cursan los estudios.

Este modelo educación recrea un modelo mecanicista, donde es posible pronosticar el comportamiento del sistema y sus participantes, creando un marco de trabajo y de aprendizaje que, trata a todos sus educandos como seres idénticos, desconociendo con frecuencia los saberes previos e individualidades de sus estudiantes, y ajustando sus visiones del mundo a los estándares vigentes a la fecha, para resolver problemas o retos que posiblemente ya cuentan con respuestas conocidas por parte de sus docentes.

La formación en seguridad y ciberseguridad ha sido influida por este tipo de entrenamiento y conceptualización de la educación, creando marcos de trabajo y formas de aprender, casi incuestionables, los cuales han hecho carrera en la manera como los especialistas de seguridad y control toman sus decisiones. La aversión al riesgo, la necesidad de control de sus acciones y el temor por la inevitabilidad de la falla, configuran la forma como muchos de los encargados de la protección de la información terminan actuando, frente a una realidad completamente distinta que demanda una mirada diferente para dar cuenta con los nuevos riesgos y amenazas emergentes.

En este sentido, los marcos de trabajo vigentes tanto en seguridad como en ciberseguridad, buscan generar certezas y sensación de control para todos aquellos que los aplican, entendiendo que como buena práctica, son capaces de influenciar la realidad y anticipar las posibles acciones de los adversarios.

Estas prácticas estándares que se han configurado e instalado en el imaginario de los profesionales de seguridad y ciberseguridad, no deben convertirse en dogmas o verdades incuestionables, sino en referentes útiles para revisar y analizar frente a situaciones conocidas, las cuales se presentan aún en la dinámica de las organizaciones.

> "EL ADVERSARIO DIGITAL CONFIGURA UNA INTELIGENCIA QUE SE SIENTE CÓMODA CON LA INCERTIDUMBRE Y LA INESTABILIDAD, QUE NO TIENE TEMOR DE EQUIVOCARSE Y ENCUENTRA EN CADA RESULTADO, UNA OPORTUNIDAD PARA CAPITALIZAR Y ACTUALIZAR SU SABER."

Así las cosas, los encargados de seguridad y control, deben romper el paradigma de los controles conocidos, para dejarse cuestionar e interrogar por el contexto volátil, incierto, complejo y ambiguo, con el fin de desinstalarse de las respuestas y acciones programadas y validadas en sus marcos de trabajo, para encontrar propuestas alternativas que no sólo reaccionen a los eventos inesperados, sino que permitan defender y anticipar los movimientos del adversario, conectando los puntos desconectados de su entorno y crear una visión enriquecida de sus recomendaciones y actuaciones. Recuerde que: "El éxito de un analista es el nuevo reto para un adversario", esto es, un incremento de la creatividad del atacante para tensionar las nuevas apuestas de la seguridad y control.

El adversario digital. La capacidad para sorprender.

Mientras los especialistas en seguridad y ciberseguridad buscan implementar, asegurar y proteger los activos que tiene a su cargo, para custodiar la promesa de valor de la empresa, su contraparte, los adversarios constantemente mantienen sus mentes ocupadas experimentando, sorprendiendo y comprometiendo, es decir, quebrando o engañando los estándares y protecciones conocidas, creando la incertidumbre natural que este tipo de acciones genera.

El adversario digital configura una inteligencia que se siente cómoda con la incertidumbre y la inestabilidad, que no tiene temor de equivocarse y encuentra en cada resultado, una oportunidad para capitalizar y actualizar su saber. El adversario digital acelera sus procesos de aprendizaje/desaprendizaje creando entornos de prueba y experimentación permanente, donde insiste y recrea contextos que, para muchos pueden ser no controlados, con el fin de alcanzar una nueva frontera de conocimientos que hasta el momento la práctica y la ciencia no han logrado.

Nótese que esta forma de pensar y actuar, insiste en el desarrollo de una capacidad, en una estrategia constante por desconectar las verdades conocidas, exponerlas en escenarios no probados, para encontrar nuevas oportunidades y condiciones desconocidas, que le permitan concretar apuestas inéditas que sorprendan las posturas más avanzadas de protección digital, de tal manera que entender lo que ha sucedido, le tome a su contraparte recorrer un camino, que él ya previamente ha transitado y demarcado.

El atacante entiende la seguridad no como un objetivo que se quiere lograr, sino como un camino inacabado donde existen respuestas preliminares, y las vulnerabilidades, establecen metas volantes, que dan cuenta con las exigencias de aseguramiento necesarias para crear una confianza imperfecta. El adversario es luego, una mente inquieta que no ha sido formada en la mentalidad y marco de la educación tradicional, sino que responde a la adrenalina que supone romper con el paradigma de protección vigente y establecer a la inevitabilidad de la falla como el nuevo normal en la formación de los especialistas en seguridad y control.

Comprender la mente del adversario, es abrir espacios para la formación de profesionales de seguridad y control que entiendan la inestabilidad del escenario actual, las posibilidades que se abren en un mundo hiperconectado y sobretodo, una racionalidad sistémica, que no se basa en una relación causal y en una explicación de la realidad que asume inmutable y con leyes conocidas, sino en una relacional y emergente que es capaz de ver en medio de las rarezas, inconsistencias y contradicciones[7], creando un escenario entre realidad e imaginación, donde el incierto se transforma en una oportunidad para crear incentivos y motivaciones, que quiebren el status quo y revelen aquello que no era posible ver previamente. Recuerde que: “El éxito de un adversario, es la lección aprendida de un analista”, es decir, nuevas motivaciones para que el analista explore y desafíe su propio conocimiento previo.

Analista y adversario. Dos visiones encontradas.

Si bien la sección anterior no pretende hacer una apología del adversario y sus acciones contrarias a la ley, si busca fijar la atención sobre la versatilidad de una manera de pensar y cómo es posible encontrar propuestas alternas para enriquecer la formación de los profesionales de seguridad y ciberseguridad, como quiera que no es sostenible una práctica estática de controles (y sus respectivas verificaciones), como fuente de confianza imperfecta para las organizaciones del siglo XXI.

Mientras el analista interpreta una melodía con su partitura de amenaza, control e impacto, lenguaje reconocido y aceptado por las organizaciones, el adversario interpreta desde su intencionalidad, sus capacidades y vulnerabilidades, con efectos que son conocidos tanto por empresas y analistas (**figura 1**). Esta aparente contradicción crea un escenario donde es posible encontrar la armonía de los contrarios, de tal forma que se incrementen los niveles de desaprendizaje de los especialista de seguridad y ciberseguridad, basados en la generación de tensiones naturales que los adversarios crean sobre sus modelos de protección.

Lo anterior demanda considerar un marco pedagógico que habilite la “armonía de los contrarios”, las prácticas del analista y las acciones del adversario. Esto es, que sensible al contexto de los encargados de la seguridad y la ciberseguridad, se establezca una zona psicológicamente segura[8]donde las decisiones que se toman frente a condiciones inciertas permitan que éstos “estudien la situación, definan los problemas, lleguen a sus propias conclusiones sobre las acciones a emprender, contrasten ideas, las defiendan y las reelaboren con nuevas aportaciones”[9].

De forma concreta, se habilita esta nueva pedagogía considerando al menos cuatro momentos particulares como fundamento de la transformación del marco de aprendizaje y desprendizaje en la formación de los profesionales de seguridad y control (**figura 1**).

El primer paso es crear una **suspensión** o quiebre de la realidad conocida, esto es, rasgar el velo de la inercia de lo conocido hasta el momento. En este ejercicio se permite indagar y cuestionar los supuestos que soportan su práctica vigente, para revelar aspectos desconocidos de la situación identificada, posiblemente no resuelta por los estándares conocidos, y sus interacciones con el contexto. Esto abre la posibilidad para pensar fuera de los márgenes establecidos.

Luego, se habilita una **conexión** con la experiencia previa, con el conocimiento anterior adquirido de situaciones, donde el error concebido como proceso, habilita oportunidades para instalar aprendizajes y habilidades que se convierten en prácticas probadas que dan cuenta de situaciones conocidas y superadas, y de igual forma, establece la base de sus actuaciones en contextos semejantes. Se tensiona los saberes previos frente a la condición de incertidumbre.

Un tercer paso, abre la puerta para concretar la **transformación**, la construcción de una base de conocimiento y entendimiento, de aproximaciones novedosas que están articuladas desde lo incierto. Esto es, desconectar los elementos conocidos de las prácticas, incluir las amenazas y riesgos desconocidos hasta el momento, así como distinciones de condiciones inéditas identificadas, para luego conectar y desarrollar una propuesta emergente que responda a las anomalías, contradicciones y rarezas del escenario analizado.

Finalmente y no menos importante, la **incorporación**, como una fase donde se funda y apropia una nueva estructura de conocimiento previo, basado en las nuevas interpretaciones que, considerando la asimetrías del contexto, transforman la persona no solamente frente a la inevitabilidad de la falla, sino de cara a su ejercicio práctico y real de custodio de la promesa del valor de la empresa, donde se hace evidente su responsabilidad de protección aun en situaciones inciertas.

Lograr fundar una educación en seguridad de la información y ciberseguridad con estas características, implica romper la tradición mecanicista de la formación que se tiene a la fecha, producir escozor y malestar al interior de las prácticas vigentes de protección de la información y sobre manera, quebrar los lentes actuales del entendimiento de la seguridad de la información y la ciberseguridad, donde los estándares exigen que el proceso de gestión sea repetible, para poder establecer una medida del nivel de "protección" disponible y requerido en la organización y, complementarlos con otros que privilegien la capacidad para percibir y evaluar las consecuencias de las actuaciones de las personas y los adversarios frente al tratamiento de la información ahora y en el largo plazo[10].

Reflexiones finales

A medida que se incrementan los riesgos y amenazas emergentes, y de igual forma las exigencias legales y de cumplimiento[11], la formación mecanicista de los analistas de

Figura 1—Analista y adversario. Dos visiones encontradas (Elaboración propia)

	Actores		
	Analista	**Adversario**	
Vista mecánica: Lineal	Amenaza	Intención	Vista relacional: Circular
	Control (Práctica)	Capacidad	
	Impacto	Vulnerabilidad	
Postura: Implementar, asegurar y proteger	<-- VISIONES ENCONTRADAS-->		Postura: Experimentar, sorprender y comprometer

seguridad de la información y ciberseguridad revela sus limitaciones inherentes, respecto de un entorno altamente dinámico e incierto, para dar respuesta a las inquietudes y demandas de las organizaciones embebidas en un escenario digital.

Esta realidad hace evidente que, la forma como se entiende la seguridad y el control en la actualidad, requiere complementar su enfoque de protección y aseguramiento, con uno de defensa y anticipación. Lo anterior, supone cuestionar los marcos educativos que a la fecha se tienen para entrenar formalmente a los profesionales en seguridad y ciberseguridad, los cuales por lo general privilegian las buenas prácticas que brindan certezas y tranquilidad para recomendar y actuar.

Defender y anticipar, implica reconocer, enfrentar y aprender (desaprender) de las situaciones de incertidumbre e inestabilidad que comporta la materialización de los riesgos emergentes, de tal forma que, incorporando las dinámicas de la mente del adversario, el analista de seguridad y control, pueda contrastar sus saberes previos, para desconectar los elementos ciertos de su base conceptual y darle cabida a la experimentación y sorpresa propio del lenguaje de los adversarios.

"Dejar de ver la orilla" de los estándares y buenas prácticas, implica que el encargado de seguridad y control se compromete reinventar sus conocimientos y experiencia, desde las capacidades y exigencias presentes, sabiendo que si bien no tiene todos los elementos para hacerlo, cuenta con la capacidad para aprender y desprender, y así visionar de forma activa lo que quiere lograr: construir una ventana de pronósticos, donde los incidentes son parte natural del paisaje donde habitan las organizaciones modernas.

Dice un investigador que :

> *El asombro es el descubrimiento de lo oculto que se esconde en lo evidente de la originalidad de lo común, de lo extraordinario que permanece escondido en lo cotidiano y lo ordinario, de lo que estando ahí siempre se percibe (como) por primera vez*[12].

En consecuencia, la experiencia del asombro, debe ser el nuevo normal de los encargados de la seguridad y la ciberseguridad, como quiera que es el punto de inicio donde se encuentra la esencia del aprendizaje, que como anota el mismo autor, es esa "explosión de luz que se produce en nosotros" cuando se revela una realidad oculta a nuestros ojos.

Finalmente, tanto analista como adversario comparten una base común de construcción de

Figura 2—Proceso de Aprendizaje y desaprendizaje

Adaptado de: Reyes, A. & Zarama, R. (1998). The process of emboying: a re-construction of the process of learning. *Cybernetics & Human Knowing*. 5(3). 19-33.)

conocimiento y desafíos, donde pensar de manera audaz, exige salir de la zona cómoda, de la vista disciplinar a la que los analistas están acostumbrados y darse la oportunidad de explorar puntos de vista distintos desde otras disciplinas o propuestas de pensamiento, y así desarrollar una serie de disciplinas (hábitos, actitudes, capacidades, significados) que Krupp y Schoemaker[13] establecen como claves para superar las cegueras cognitivas, actuar de forma anticipada y sobre manera movilizar los esfuerzos en aspectos estratégicamente relevantes para el ejercicio de mantenerse delante de la curva: anticipar, retar, interpretar, decidir, alinear y aprender.

Endnotes

1 Accenture, *The Post-Digital Era Is Upon Us. Are You Ready for What's Next?* Accenture Technology Vision 2019, *https://www.accenture.com/t20190201T224653Z__w__/us-en/_acnmedia/PDF-94/Accenture-TechVision-2019-Tech-Trends-Report.pdf*

2 EUropean Union Agency for Network and Infomrmation Security (ENISA), *Threat Landscape Report 2018: 15 Top Cyberthreats and Trends*, January 2019, *https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport*

3 Do, Q.; B. Martini; K. R. Choo; "The Role of the Adversary Model in Applied Security Research," *Computers & Security*, vol. 81, March 2019, p. 156-181, *https://eprint.iacr.org/2018/1189.pdf*

4 En un mundo hiperconectado todos los participantes van a tener una falla y necesitan hacer un acuerdo de acción cuando esto ocurra. La fiabilidad se basa en el impacto de las acciones adversas y en cómo gestionarlas.

5 Cano, J. (2017) Riesgo y seguridad. Un continuo de confianza imperfecta. En Dams, A., Pagola, H., Sánchez, L. y Ramio, J. (eds) (2017) *Actas IX Congreso Iberoamericano de Seguridad de la Información*. Universidad de Buenos Aires - Universidad Politécnica de Madrid. 34-39. Recuperado de: *https://www.researchgate.net/publication/321197873_Riesgo_y_seguridad_Un_continuo_de_confianza_imperfecta*

6 Echeverría, B. & Martínez, P. (2018). Revolución 4.0, competencias, educación y orientación. *Revista Digital de Investigación en Docencia Universitaria*, 12(2), 4-34. doi: *http://dx.doi.org/10.19083/ridu.2018.831*

7 Charan, R.; *The Attacker's Advantage: Turning Uncertainty Into Breakthrough Opportunities,* Public Affairs, USA, 2015

8 Edmondson, A.; *The Fearless Organization: Creating Psychological Safety in the Workplace for Learning, Innovation, and Growth,* John Wiley & Sons, USA, 2018

9 Acosta, S.; *Pedagogía por competencias. Aprender a pensar,* Editorial Trillas, Mexico, 2012

10 Cano, J.; "La educación en seguridad de la información. Reflexión pedagógicas desde el pensamiento de sistemas," *Memorias 3er Simposio Internacional en "Temas y problemas de Investigación en Educación: Complejidad y Escenarios para la Paz", 2016, http://soda.ustadistancia.edu.co/enlinea/congreso/congresoedu/2%20Pedagogia%20y%20dida%B4ctica/2%209%20LA%20EDUCACION%20EN%20SEGURIDAD%20DE%20LA%20INFORMACION.pdf*

11 IT Governance, "Managing Cyber Risk: Transform Your Security With Cyber Resilience", *https://www.itgovernance.co.uk/managng-cyber-risk*

12 García, A.; *Educar para el asombro. Sencillez, confianza, paciencia y profundidad,* Ediciones Mensajero, España, 2018

13 Krupp, S.; P. Schoemaker; *Winning the Long Game: How Strategic Leaders Shape the Future,* Public Affairs, USA, 2014