Fraude informático: una realidad emergente en un mundo digitalmente modificado

Jeimy J. Cano M., Ph.D, Ed.D(c), CFE

Introducción

Los temas de seguridad y control se han convertido en un tema prioritario para las organizaciones [1]. Las diversas formas de controvertir las medidas de protección, por parte de terceros no autorizados o de personal interno de las empresas, establecen verdaderos retos de monitoreo y seguimiento que los encargados de la seguridad o del control de fraude deben afrontar para poder determinar que algo está fuera de un patrón normal [2].

Las conductas engañosas mediadas por estrategias digitales o informáticas, revelan una faceta distinta del fraude, aumentando su capacidad de influencia, sus impactos y, sobre todo, aprovechando ahora la movilidad y las nuevas propuestas de servicios, pueden ser usados por terceros para crear escenarios creíbles y motivadores de actuaciones en las personas, para conducirlas a un artificio [9].

El fraude con componente digital o tecnológico es ahora la evolución natural de las conductas falaces, que

encuentran en el fenómeno técnico un aliado de su actuar, como quiera que el anonimato, la inestabilidad de los rastros y los vacíos jurídicos fundan una dinámica base para desarrollar actividades que permitan lograr defraudar a un tercero, generar una ganancia y desaparecer sin advertir presencia [4].

El fraude como conducta abiertamente contraria al contexto social y que afecta claramente la confianza en las instituciones, es una realidad sistémica que no se encuentra en la tecnología, los procesos o las personas, sino que es una combinación de ellas, tendiente a afectar la buena fe y por ende crear una zona de zozobra para el afectado, con el fin de lograr un beneficio ilegítimo como fruto de sus acciones engañosas y contrarias al orden establecido.

Detectar y procesar conductas de fraude digital o informático, implica comprender la dinámica de la inevitabilidad de la falla, por lo menos en cuatro dominios: las personas y sus comportamientos; los procesos y sus riesgos; la tecnología y sus fallas; además de los cuerpos normativos y sus vacíos, habida cuenta que es allí, en la convergencia de estos cuatro elementos donde se configura la posibilidad de una falacia que lleva consigo la semilla de un delito mayor [7].

Este documento hace una breve introducción a la temática del fraude informático, como una primera mirada sistémica de la problemática, entendiendo que aún existen muchos aspectos por resolver e investigaciones que desarrollar, con el fin de dar cuenta de una realidad que aparentemente sabemos dónde se encuentra, pero no necesariamente conocemos de donde surge.

Fraude: algunas definiciones básicas

El fraude es una condición de engaño, situación que revela una ilusión creada y planeada con determinación para motivar un comportamiento particular en una persona. Este ejercicio crea una ventana de vulnerabilidad -no percibida por la víctima-, donde el defraudador aprovecha su “halo de confianza” para envolver a la persona y materializar su objetivo principal: obtener un beneficio personal o para un tercero.

Cualquiera que sea la técnica de engaño utilizada, es la tecnología la que potencia sus efectos y aumenta su impacto, como quiera que la superficie de acción de la misma, está determinada por artefactos técnicos de uso masivo, que generan suficiente confianza en los suscriptores para que una campaña bien diseñada, basada en gustos y expectativas de las personas tenga éxito [8].

Basta un clic para comprometer la información de un individuo; para generar un vacío de seguridad de la información y para concretar un robo de identidad o materializar un ciberataque de grandes proporciones. Detrás de él, debieron existir meses de revisión y estudio de gustos y rutinas de las personas; inteligencia de fuentes abiertas sobre sus aficiones y preferencias, perfiles de navegación, inclinaciones sociales, académicas o políticas, para definir los vectores de ataque y afectar a la persona objetivo.

Defraudador digital: habilidades sociales, técnicas y de exploración

Los defraudadores digitales son personas hábiles con la tecnología, las relaciones sociales y las estrategias de búsqueda en internet. Estas habilidades llevadas con propósitos contrarios desarrollan contextos enriquecidos y creíbles, crean escenarios fértiles para que individuos desprevenidos caigan en las trampas que los llevan a perder activos de información claves, los cuales pueden ser usados por los delincuentes para cometer otros ilícitos con sus credenciales.

El defraudador digital, no es necesariamente un experto en tecnología, no tiene edad ni condición social ni género específico, pero lo que sí lo identifica es su capacidad para ver la realidad conectada de la persona o personas objetivo, con lo cual determinan su patrón de acción y en forma escalonada acumulan y relacionan información, para fundamentar su estrategia de engaño, elaborada y concreta.

La dinámica de las redes sociales y los constantes bombardeos de la publicidad en línea, crean una vitrina privilegiada para los delincuentes en internet, toda vez que se camuflan detrás de una de estas estrategias legítimas de los comerciantes, para establecer un perfil de invisibilidad capaz de engañar hasta el cibernauta más especializado. En este sentido, contar con el apoyo de la tecnología de información y su capacidad de correlación es clave para aumentar la expectativa de detección y acción sobre actividades ilícitas que comprometan la esfera personal, social, económica y política de las personas. La mentalidad causal de los analistas de fraude, contrasta con la mentalidad relacional de los defraudadores. Mientras unos buscan perfiles de actuación que respondan a patrones de actividad sospechosos, detectados con anterioridad, los delincuentes usan la dinámica de la realidad para crear versiones ligeramente modificadas, que los hagan pasar desapercibidos frente a las tendencias. En tal sentido, el defraudador estará tratando de evaluar la realidad y definir la cotidianidad, como factor clave de éxito para lograr su objetivo con un bajo nivel de detección.

Conexión consciente. Aprender de la dinámica del fraude

Si sabemos que no podemos anticipar muchas de las estrategias de los delincuentes para superar o sabotear los mecanismos de control dispuestos, es necesario desarrollar habilidades complementarias orientadas a aprender y conectar la realidad del fraude, para detectar la frecuencia de su intencionalidad y comenzar a seguirle el rastro más de cerca.

En este sentido, el analista del fraude informático debe ser lo suficientemente abierto para desaprender y quebrar sus modelos mentales, de manera de entrar en una conexión consciente con la realidad del fraude, que lo lleve a experimentar nuevas propuestas y a ampliar su visión estratégica de detección, usando realidades alternativas antes inexploradas.

En este sentido, parafraseando las prácticas de conexión consciente de un *Chief Information Security Officer* –CISO-, Oficial de Seguridad de la Información [3], en la lectura del analista o ejecutivo de control y

prevención del fraude, se proponen las siguientes acciones:

- **Dejar de luchar, aprender y anticipar**. El fraude no es una lucha contra el engaño; se trata de encontrar formas diferentes de mejorar las prácticas de prevención, detección, monitorización y control. Mientras más lucha se ejerza contra el oponente, menor capacidad de acción habrá para estudiarlo y superarlo (o anticiparlo). Siempre es posible dar un paso adelante del fraude, si el afectado es capaz de conectarse con él. Es decir, aprender y desaprender de su dinámica.

- **Escuchar la voz interior**. No importa lo hábil que el usuario se haya vuelto para identificar y afrontar retos en la detección, prevención y monitorización del fraude, pues siempre habrá momentos de incertidumbre y confusión. Meditar en los mensajes de voz interiores y en los diferentes análisis y reflexiones frente a la situación difícil, es una alternativa. Así mismo, detenerse en el silencio de la conexión con el fraude, para superar los límites mentales autoimpuestos y poder actuar en consecuencia.

- **Retar los límites**. Buscar dentro de sí aquellos paradigmas que parecen haber funcionado y ponerlos en práctica frente a la realidad existente. No es necesario hacer grandes cambios de estándares y prácticas, sino tomar aquellos que son claves, cuyas transformaciones pueden leer mejor las expectativas de los clientes y aumentar la confianza de estos frente a la detección, prevención y monitorización del fraude.

- **Permanecer centrado, en equilibrio**. Estar centrado es estar conectado con la propia fuente de equilibrio. En la detección, prevención, monitorización y control del fraude es necesario estar en constante exploración y conocimiento, conscientes de la ambigüedad permanente y en movimiento con el engaño. El responsable antifraude está centrado, cuando su atención está en el fluido del presente y su energía concentrada en la dinámica del cambio. No se dispersa; por el contrario, identifica la incertidumbre estructural presente en la realidad.

- **Superar las creencias personales**. Entre más fuertes sean las creencias, más estrecho será el punto de vista [5]. El ejecutivo antifraude que quiera tener éxito deberá ser flexible, conjugar los distintos puntos de vista y combinarlos con la perspectiva de riesgos. En la medida en que es posible reconocer otras miradas sobre la misma realidad de la amenaza identificada, es posible superar y confrontar los límites que imponen los propios paradigmas.

- **Capturar información de todas las fuentes posibles.** Cuando se advierten situaciones donde se configuran dilemas, es preciso consultar diferentes puntos de vista, aceptando lo que todos tienen que ofrecer. La lectura del riesgo es relativa al contexto y cada persona lo puede leer según la propia experiencia. En este sentido, es necesario configurar una vista agregada de opiniones para revelar aquellos intereses inmersos, para poder tomar una decisión conforme a lo que requiere el momento y la situación, sin dejarse invadir o

seducir por una postura en particular.

- **Aprender a tener intenciones claras**. En la detección y prevención del fraude, una intención clara, significa tener un propósito. Una afirmación que contempla la dinámica de la organización y los objetivos de negocio, para hacer congruente la práctica antifraude con las necesidades y retos de la empresa. Un ejercicio que permanece alerta a las señales del entorno, para tener conciencia de cada paso en la dirección que confirma dicho propósito.

Reflexiones finales

La dinámica del fraude informático o hiperconectado en el contexto de un mundo digitalmente modificado, comporta un proyecto de transformación social y cultural contrario a la sociedad, que busca desestabilizar y tensionar el orden existente, no de forma preferente y directa, sino con acciones discretas y poco visibles, de tal forma que los miembros de esta comunidad con intencionalidad criminal, independientemente de su condición personal, económica, política, religiosa, social, aportan capacidades distintivas que capitalizan de forma integrada, cuando se concretan los engaños para una empresa, persona o grupo de interés.

En este entendido, los defraudadores digitales comparten información y analizan datos de forma colectiva, para detectar las tendencias más sobresalientes, habida cuenta de que ellas servirán de puente y apoyo necesario para coordinar actividades o intentos de nuevas formas de trampas. De esta forma, estas comunidades crean un proceso de cambio de percepción, con una secuencia asimétrica de intenciones aparentemente llenas de "luz", las cuales terminan en resultados que enriquecen sus bolsillos, dejando al vaivén de las otras variables del entorno, las marcas cognitivas, afectivas, personales y sociales en sus víctimas.

Frente a esta realidad es necesario un diálogo transdisciplinar orientado a una reflexión desde la persona, los procesos, la tecnología y las regulaciones, para facilitar la construcción de fundamentos conceptuales de forma holística [6], adaptados a la realidad de un mundo digital y conectado, con el fin de crear una red de conocimientos complementarios que valore las contradicciones impuestas por la realidad del fraude y haga de ellos, una capacidad clave que considere las estrategias disponibles a la fecha para su prevención, monitorización, detección y control en las organizaciones modernas.

Referencias

[1] Bughin, J., Lund, S. y Manyika, J. (2016) Five priorities for competing in an era of digital globalization. *Mckinsey Quarterly*. Mayo. Recuperado de: http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/five-priorities-for-competing-in-an-era-of-digital-globalization.

[2] Álvarez, M. (2016) Insider Attacks May Be Closer Than They Appear. Recuperado de: https://securityintelligence.com/insider-attacks-may-be-closer-than-they-appear/.

[3] Cano, J. (2015) Conexión consciente. Siete prácticas para habilitar una visión

trascendente en seguridad de la información. Recuperado de: https://www.linkedin.com/pulse/conexi%C3%B3n-consciente-siete-pr%C3%A1cticas-para-habilitar-en-jeimy.

[4] Cano, J. (2016) Cinco premisas de la delincuencia digital en un mundo digitalmente modificado. Recuperado de: https://www.linkedin.com/pulse/cinco-premisas-de-la-delincuencia-digital-en-un-mundo-jeimy.

[5] Chopra, D. (2014) *El alma del liderazgo. Descubre tu potencial de grandeza*. Bogotá, Colombia: Punto de Lectura.

[6] De Geus, A. (2011) *La empresa viviente. Hábitos para sobrevivir en un ambiente de negocios turbulento*. Buenos Aires, Argentina: Gránica.

[7] Kessem, L. (2016) 2016 Cybercrime Reloaded: Our Predictions for the Year Ahead. Recuperado de: https://securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead/.

[8] Vax, S. (2016) Mobile Malware on Smartphones and Tablets: The Inconvenient Truth. Recuperado de: https://securityintelligence.com/mobile-malware-on-smartphones-and-tablets-the-inconvenient-truth/.

[9] Verizon (2016) 2016 Data breach investigations report. Recuperado de: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

Jeimy J. Cano M., Ph.D, Ed.D(c), CFE. *Ingeniero y Magíster en Sistemas y Computación por la Universidad de los Andes. Ph.D in Business Administration por Newport University; Especialista en Derecho Disciplinario por la Universidad Externado de Colombia y candidato a Doctor en Educación en la Universidad Santo Tomás. Cuenta con un certificado ejecutivo en gerencia y liderazgo del MIT Sloan School of Management, MA, USA. Profesional certificado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners y Cobit5 Foundation Certificate de ISACA. Director de la revista "Sistemas", de la Asociación Colombiana de Ingenieros de Sistemas –ACIS-.*